OpenBMC Security Working Group

Meeting Notes and Agenda

Purpose: This has the agenda and meeting notes for the OpenBMC Security Working Group. These notes are in reverse chronological order with new material at the top and older material below. See the wiki for additional information about the group's activities.

This document is intended only as a record of the meeting, not as a discussion platform. Please move discussions which happen after each meeting to appropriate communication channels such as email, Gerrit review, or Discord.

See also: Action items in the wiki.

Meeting access information - meets 10:00am PDT (12:00 US Central) every other week See https://github.com/openbmc/openbmc/wiki/Security-working-group
Next agenda: Review security work in progress, review Security Assurance Workflow for updates. 1. **As of August 28, 2023 this meeting is discontinued - see below.** 2. **Please do not add agenda items. See below for where the discussion moved to.**

Meeting access is on Discord > OpenBMC > Voice channels > Security:

- First, join Discord via https://discord.gg/69Km47zH98
- Then join: Discord > OpenBMC > Voice channels > Security.
- Join: https://discord.com/channels/775381525260664832/1002376534377635860

Please note: As of Monday August 28, 2023, the regular meetings are discontinued. An email was sent with the explanation (copied here):

> OpenBMC community,
>
> I am discontinuing the OpenBMC Security Working Group meetings. About a year ago, these meetings moved to Discord voice and project's open security work moved to the Discord security channel. As intended, the content of the voice meeting has significantly

reduced as the discussion increased in the Discord security channel. Attendance and topics have fallen to zero. So it is time to discontinue having regular meetings. Thanks to everyone who helped move the project forward during this time!

As a direct consequence, the meeting agenda and minutes will no longer be appended:
https://docs.google.com/document/d/1b7x9BaxsfcukQDqbvZsU2ehMq4xoJRQvLxxsDUWmAOI
Instead of this wiki, please use the Discord OpenBMC security channel for this discussion.

To discuss OpenBMC security topics on Discord.
- first join Discord via https://discord.gg/69Km47zH98
- then go to the Discord OpenBMC server:
https://discord.com/channels/775381525260664832
- and browse to the #security channel - or any other appropriate channel.

Also feel free to email questions to the community.

If you need to talk to someone so you can move forward, please use the regular security channel to schedule a call on the Discord OpenBMC Security voice channel. (NOTE: This is a voice channel, different from the regular security channel.) See Discord > OpenBMC > Voice channels > Security ~
https://discord.com/channels/775381525260664832/1002376534377635860
^^ Typically used only for discussion about the voice channel itself.

Note the OpenBMC project's security wiki is here:
https://github.com/openbmc/openbmc/wiki/Security-working-group
I don't have any plans to change this wiki, and I wish for the security assurance work it outlines to continue.

To ***privately*** report a security vulnerability to the project (or think you want to ask about reporting such as vulnerability), please do not use public channels. Instead follow the process here:
https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md

Yours truly,
Joseph Reynolds

Meeting planned July 19

Meeting canceled July 5 - cancel due to US Holiday on July 4

Meeting held 2023-06-21
Attended: Daniil, Joseph, (Surya tried to join?)

Cancel next time - july 5 due to US Holiday on July 4

Topic 1: How to get 2FA / MFA for bmc users? Direction from Redfish, from OpenBMC? Google authenticator? Email? Need Redfish interfaces, implementation, and need infrastructure external to the bmc.
Focus on HTTPS:
Curl POST /redfish/v1/SessionService/Sessions/ – username and password
https://github.com/openbmc/docs/blob/master/REDFISH-cheatsheet.md
WebUI exclusively uses Redfish (+URI /login)

2 Security response team:
OpenBMC has started using GitHub security advisories like
https://github.com/openbmc/bmcweb/security/advisories/
Anyone can subscribe to yocto security emails (https://lists.yoctoproject.org/g/yocto-security) which tracks cves and their fixes, typically as a version bump

Meeting not held on 2023-06-07
Attended: Joseph
Although I did talk to myself, it was not about security topics.

Meeting held 2023-05-24:
Attended: Joseph Reynolds, Dhananjay Phadke (dsp), Daniil

TOPIC: JWT / OAuth2 discussion
Store the anti-replay token where: BMC flash? BMC RoT chip? How can an attacker modify this?
The primary pattern to use this function is:

1. The manufacturer/service organization creates a JWT security token.
2. The BMC admin uploads this JWT to their BMC.
3. The BMC validates the JWT (including signature, system serial number, expiration, anti-replay, etc.)

4. The BMC carries out the function encoded in the JWT. For example, it resets the BMC's local admin account password.

A use case: upload token, then boot insecure image for debug, next boot is secure boot
Anti-replay: Use the timestamp of the signing server as anti-replay. Follow JWT spec as in See Rfc 7519 section 4.1.7
TODO: Joseph to email next round of design discussion

Tangentially related: Work on https://gerrit.openbmc.org/c/openbmc/docs/+/33847 Provide an admin account

Meeting held for **2023-05-10:**
Attended: Joseph Reynolds, Dick Wilkins
No topics.

Meeting held 2023-04-26 with no topics
Attended: Joseph Reynolds, Dick Wilkins, dsp [Dhananjay], Daniil Engranov
There were no topics.

Meeting held 2023-04-12:
Attended: Joseph Reynolds, James Mihm, Dick Wilkins
1 (Joseph) There is a design point from the "service access" email thread: https://lore.kernel.org/openbmc/53fade52-2afc-f375-40b1-f6781bf5d117@linux.ibm.com/T/#m427774ad2aec4469efa3acdd9c7b8ee3c1493acc
In the next draft, I will clarify a requirement: before access is given, a BMC admin (via service access credentials) and a service agent (via a digitally signed service access token) must both present credentials to the BMC:

- BMC admin (via service access credentials, for example, valid BMCWeb SESSION credentials), and
- Service agent (via a digitally signed service access token, which only authorized service agents can digitally sign)

My question is: What is the right way to present these credentials to the BMC?
Background notes:

- Please note my presentation here is biased toward practices used by IBM Power servers, but the intention is to expand this design to handle all use cases.
- In the access model presented in the design sketch referenced above, the admin user has access to the BMC's network interface, and the service user does not necessarily have this access.
- A logged in BMC admin will have a session token (an X-Auth-Token per https://github.com/openbmc/docs/blob/master/REDFISH-cheatsheet.md, or a SESSION cookie and its XSRF token for Web users).

- The way the service user's authorization is presented to the BMC is in the form of the digitally-signed "service access token" (where the BMC can validate the signature). The service agent is the only person who can create this token, and the act of creating it and giving it to the BMC admin constitutes authorization.

What is the right way to present these credentials?
NOTE: If the "service access token" is an OAuth2 JWT [https://auth0.com/docs/secure/tokens/json-web-tokens] then the normal way to pass this token is in the HTTP request header ("Authorization: Bearer {the.jwt.token}").
Alternatives:

1. The admin logs into the BMC and gets an active session. Then uses that session to upload the "service access token" using a REST API, passing the JWT in the HTTP request body. Is this an acceptable way to upload JWT tokens?
2. The admin logs into the BMC and gets an active session. Then adds the "service access token" (OAuth2 JWT) to their HTTP request header ("Authorization: Bearer {the.jwt.token}"
3. Some other way? [Please note I am not a web or access control expert.]

DISCUSSION: Effectively none. Continue email discussion, then ask Redfish.

2 Are there any other use cases or access patterns for the "service access" design to consider before making a design?
DISCUSSION:
Some systems use "physical presence" such as pushing a button or flipping a switch (typically located inside the system's external case and hard to reach) to assert that a person has a privileged presence physically co-located with a server/BMC. When this physical presence is asserted, the BMC allows some privileged operation (such as service access). → It is desired to remove or limit the need for physical presence. The digitally signed "service access token" proposed by the "service access" design is intended to help.

Meeting held 2023-03-29:
Attended: Joseph Reynolds, dsp, Daniil Engranov, jejb, cacih

1 Joseph: Is there a common use case to get "service" access to the BMC? A "service user" means a person authorized by the system manufacturer or OEM who is trusted to access BMC internals as needed to diagnose or fix problems on the BMC; they are allowed to use interfaces which are not accessible to BMC admin user, for example REST APIs only allowed to "service" users, or to get root user access to the BMC command shell.

For context, assume the BMC admin user does not have access to the BMC command shell and can only access the BMC's REST APIs and similar external interfaces; that is, the BMC

admin has no access to BMC internals. Also, assume the BMC admin has access to the BMC's management network, and can share that access with a service user.

DISCUSSION (joseph and dsp):
Joseph discussed IBM's custom Access Control File (ACF) solution, and Dhananjay discussed Microsoft's Secure Unlock.

IBM ACF: Joseph reviewed the steps for an IBM service agent to get service access to a customer BMC. The steps are:

1. The customer calls for service and gives the system serial number to the service rep.
2. The service rep uses their access (access to the private key, which is stored behind their organization's firewall) to create a token (an ACF file). This ACF file contains a request to access to BMC, identifies a date range, and identifies the system serial number. It is digitally signed by a private key held by the service organization, and the BMC can validate the signature via a public key which is built into the BMC firmware.
3. The service rep gives the ACF file to the customer/admin. (The ACF file has no secrets other than the secure hash of the service account's password.)
4. The BMC admin uploads the ACF to the BMC. Doing so enables the service user password access.
5. The service user can now login to the BMC, using the password stored in the ACF.
6. If desired, the admin or service agent can delete the ACF, or allow it to expire.

WIP Design: https://gerrit.openbmc.org/c/openbmc/docs/+/45201 . The implementation is in IBM's public downstream (github.com/ibm-openbmc) version of bmcweb and phosphor-certificate-manager.
Note: the ACF is ASN.1-encoded (binary file) but is not an x.509 certificate.

Microsoft Secure Unlock: Dhananjay reviewed Secure Unlock. The approximate steps are:

1. Retrieve info from BMC's RoT.
2. This info goes to the service organization (behind the firewall), which uses it to create a token needed to access the BMC.
3. This access token is uploaded to BMC.

Touchpoint: a use case for this token is to disable secure boot

The common use case?
There is a common use case for REST APIs to:

- Initiate a request for service access to the BMC.
- Upload a service access token to the BMC.

With additional APIs desired for inspecting and deleting the access token.
[Although not discussed, I presume at most 1 access token at a time is allowed.]

A common use case:
In addition to the use case to get BMC root access…

Recover admin account access. Customers regularly call for service because they lost access to their admin account. Recovery means, for example: recreate the admin account or set it to a usable state, and set its password to a known value, reset its password lockout, etc.
It is desired to be able to create an access token which performs only this admin account recovery, and does not grant general access to BMC internals.

There are at least 2 shared use cases for the access token. That is, the access token can be create for one of these purposes:

1. Enable service user login.
2. Recover access to the BMC's admin account.

There are multiple other purposes; one mentioned is to disable secure boot.
In other words, the token encodes a specific action, such as listed above.
Each manufacturer would have a different set of purposes for the tokens, and we do not image these would be shared.

Anti-replay protection for these access tokens is assumed. For example, an access token used to get access to a BMC command shell could not be used twice: the second attempt to upload it should result in permission denied with reason: anti-replay protection. (In this example, login access is allowed multiple times until the ACF expires or is deleted.)

TODO for Joseph: We decided to start a design for this. Daniil asked: Create a new bitbake image feature to optionally build in the "service access" APIs. When present a system integrator would have to hook up an appropriate implementation ~ https://github.com/openbmc/openbmc/wiki/Configuration-guide.
When the service access APIs are built into the image, should there be an API to disable it?

Meeting held 2023-03-15:
Attended: Dick Wiklins, Joseph Reynolds, Daniil
1 Joseph introduced with no comment: Design to isolate host console access away from the admin role ~ https://gerrit.openbmc.org/c/openbmc/docs/+/60968

Meeting held 2023-03-01:
Attended: Joseph, James, Daniil, [Dick Wilkins], caci, Ruud
1 Actually create the new wiki: Threat Model Topics (and link to other wikis)

2 Intention for OpenBMC fw running on AST2600 to be FIPS 140-2 certifiable. (So a platform using such a BMC could become FIPS 140 certified.) See topic from previous meeting.
Note your FIPS 140 certification must show your architecture and configuration: silicon crypto capabilities, how entropy is gathered, which algorithms are supported and exposed (for example to TLS connections).

Note that complete platforms can be certified; nobody would ever certify just the BMC alone.

Meeting held on 2023-02-15:
Attended: ddaniil, Dick Wilkins, RuudHaring, skhoteswara, cacih, Daniil Engranov, James Mihm, Joseph Reynolds

1 What security guidelines do we have?
DISCUSSION:
For BMC firmware builders, installers, and BMC admins, see
https://github.com/openbmc/openbmc/wiki/Configuration-guide
Interest in adding topics for: Build > bmc secure boot and for attestation. ← Please edit these into the wiki, referencing project docs as needed.

We should have a threat model so the above-mentioned people know which security features to enable or configure.
Consensus was to create a new wiki: Threat Model Topics - TODO Joseph
Purpose: Collect existing thoughts about threats. Note this will not be complete, and does not follow any specific threat modeling process.
Use cases for this threat model? (1) Inform developers on needed security features, (2) guidance for integrators, installers, and admins (per the Configuration Guide), and (3) for security audits.

2 James mentioned work toward having th
e OpenBMC community project provide information needed for downstream users to certify their solution to the FIPS 140-2 (not yet -3) spec. To be clear, such users must necessarily refer back to their decision to use the OpenBMC community project, so this material should be in the OpenBMC community scope.
DISCUSSION:
We discussed an example of a FIPS 140 topic: an entropy collector needed to create cryptographically secure random numbers needed to create secure TLS connections.
Specifically, AST2600 entropy generator
https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=13789
, versus entropy collector -
https://atsec-information-security.blogspot.com/2019/10/stephan-mueller-publishes-sp800-90b.html

The consensus was to produce this as a new openbmc/security/docs document which would list each of the FIPS requirements and give info for each. For example, how openbmc satisfies that requirement. Let's create a gerrit review (marked WIP) for this.

Meeting held for 2023-02-01 (Feb 1):
Attended: ddaniil, Joseph Reynolds, skhoteswara, ssekar
1 How to report suspected BMCWeb vulnerabilities?
If you are not sure how to handle security vulnerabilities, please email the openbmc-security email list.
[https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md]
Introduce the items. Feel free to copy the bmcweb maintainers. We can help assess and route the items where they need to go.

Meeting held for 2023-01-18:
Attendees: Joseph Reynolds, krishnan, skhoteswara, Ruud Haring, dsp, cacih, ashroom (joined briefly and left)

1 abandoned code review for BMC secure boot
https://gerrit.openbmc.org/c/openbmc/docs/+/26169
This is implemented. Can we work to merge this doc?

2 implementation work continues on secure and measured boot, and on selinux. Gerrit designs are paused while implementation toward a working POC continues.

Meeting held for 2023-01-04 (Wednesday Jan 4, 2023):
Attended (Discord screen names): Attendance was low, possibly due to the recent holiday - Joseph Reynolds, Dick Wilkins, ddaniil, ssekar.

1 CVE-2022-40259
DISCUSSION:
Per Joseph, the OpenBMC BMCWeb team investigated CVE-2022-40259 and believes it does not apply to OpenBMC. Will remove this agenda item.

In general, is it fair to ask if a non-OpenBMC CVE applies to OpenBMC? Yes, this analysis is typically requested for high severity CVEs. For example, a security response team needs definitive information to be able to make a statement like “We investigated CVE xyz and it does not apply”.

In general, do security response teams (such as OpenBMC SRT) reach out to competing projects for help to perform confidential analysis? Yes, for example, UEFI reaches out to other SRTs as needed. It is helpful when analyzing a problem to first expand the scope of the problem, for example to ask if it affects other implementations.

We discussed alternate options for working with the OpenBMC SRT:

- Join the OpenBMC SRT. Note that membership is generally limited to active members who make fixes in the OpenBMC project.
- Attend security working group meetings (this meeting). But note that private discussions cannot be discussed in this public meeting, so information about vulnerabilities will be delayed compared to other communication methods.
- The OpenBMC SRT can reach out to other SRTs as needed.

How can OpenBMC SRT reach out to other SRTs? Use their confidential vulnerability reporting process (variously named Product Security Incident Response Team (PSIRT), SIRT, Security Team, etc).

Meeting held on 2022-12-21:
There was low attendance likely due to US holidays.
Attended (Discord screen names): Joseph Reynolds, dsp (Dhananjay), Jiangz

1 Security advisory backlog
Next steps: SRT work through the backlog, and have each repo maintainer setup their github repo's security tab. Need TSC involvement? We recommend the OpenBMC project use github security advisories.

2 CVE-2022-40259
Remaining questions.

Meeting held for 2022-12-07
Attended (Discord screen names): Joseph Reynolds, alda, ddaniil, Dick Wilkins, RuudHaring, skoteshwara, ssekar, YatukaSugawara, Chris Engel.

1 **(Discussion from email:) The BMC physical UART serial port provides access to uboot and then to a Linux login process.**
This email (representative email from email thread):
https://lore.kernel.org/openbmc/b3a14275-1c66-4d54-5a91-4ddf73d16992@linux.ibm.com/T/#t
This port is present on some BMC's like the AST2600's pins, but may not be hooked up through the BMC card. See a brief overview at
https://github.com/openbmc/docs/blob/master/architecture/interface-overview.md

This port allows anyone with physical access to get to the U-Boot console or BMC command shell. When the BMC is booting, this port is used as the U-Boot console, and then U-Boot transitions control to Linux which allow BMC command shell access.

The OpenBMC community uses this port for system development and testing scenarios, and possibly also for manufacturing and service scenarios. However, most use cases for the

OpenBMC community regards this port as an unintended interface for end-users and customers (contrast with Redfish, IPMI, etc.).

Is there a use case for protected physical access to this port? Note the customer has physical access, and the customer is responsible to protect against threat actors gaining access. That is outside the scope of the OpenBMC project. (This question was not completely answered.)

Uboot:
This access allows anyone (without any credentials) to access the uboot environment. This gives them details about the BMC's booting process, and is configured by default to allow a user to stop the booting process so they can control it. For example, they can use U-Boot's simple shell to configure U-Boot parameters, access BMC hardware registers, change the boot source, or perform netboot.

Note: U-boot's interaction capability can be configured (via BMC root command shell access) so it cannot be stopped or controlled by anyone. This limits debug scenarios.

Some protection from U-boot threats are:

- BMC secure boot can help detect and prevent booting an unintended image.
- Measured boot (TPM) can check if BMC hardware registers are as intended.

Linux login process:
When Linux starts, systemd starts up a login process (https://man7.org/linux/man-pages/man1/login.1.html) which can allow BMC users to get access to a BMC command shell. Note that OpenBMC has a common user management (https://github.com/openbmc/docs/blob/master/architecture/user-management.md#common-user-manager---d-bus-api-phosphor-user-manager) shared between Redfish, SSH, and the login process. So, for example, a ReadOnly user who has physical access to the port can try to get a login shell.

Code in the user manager (https://github.com/openbmc/phosphor-user-manager/blob/master/user_mgr.cpp) implements the "SSH" privilege group as a change to the user's login shell, setting it to /bin/sh to authorized users, or to /sbin/nologin for unauthorized users. This is the shell used by both SSH and the login process. To be clear, when a user's shell is set to /sbin/nologin, that user can login and authenticate okay, but they will be kicked out instead of getting a command shell.

I (Joseph reynolds) remember something (in BMCWeb) that tied the SSH privilege to the Administrator role, but I cannot find it now. :-(

When the root user gets BMC command shell access, they have enormous authority over the BMC. This is not an intended administrative interface, but may be needed for some use cases where no other interface has the needed function.

When non-root users get BMC command shell access, they have limited authority. They can read some BMC files, but don't have authority to do much else. This is not an intended interface.

Some protection against getting shell access:

- Restrict access to the BMC command shell, for example when bmc is in mfg mode (different from BMC "field mode").

Added to the https://github.com/openbmc/openbmc/wiki/Configuration-guide

- Protect access to the BMC UART serial port
- Disable U-Boot's interaction capability
- Ensure intended users do not have the "SSH" group privilege

Meeting held for 2022-11-23
Was US Thanksgiving holiday week.
Attended: (Discord screen names): alda, ddaniil, Joseph Reynolds, skoteshwara.

1 Measured boot update
Discussion in discord #security channel Nov 9. Patch pushed to others can view the source.
Next steps: Feel free to submit to gerrit review.

Meeting held for 2022-11-09
Attended (Discord screen names): alda, aruocco, cengel74, ddaniil, Dick Wilkins, James Mihm, Joseph Reynolds, Nan Zhou, RuudHaring, skoteshwara.

1 Use OAuth 2.0 - https://gerrit.openbmc.org/c/openbmc/docs/+/58313
Can you all hear eachother?
I can hear again! Some microphone setting.

2 Measured boot

Meeting held for 2022-10-26
But no notes were taken.

Meeting held 2022-10-12:

Attendees: alda, cengel74, Dick Wilkins, dsp, galmasi, Joseph Reynolds, Rob, russWilson, RuudHaring, skoteshwara, YutakaSugawara.
1 Ruud: Working gerrit reviews for SELinux and for measured boot.
Wanted: branch in public repo to show progress for measured boot.
Can we start code before the design is approved? Specifically, create a public fork?
Clarification: The team working on the "measured boot" proof-of-concept wants to share their code with other teams, and was looking for a way to do so. It was suggested to create a public fork for this purpose, something like https://github.com/SOMEUSER/openbmc. The overall direction remains to do the work in the community repositories.

2 Joseph mentioned interest in some code reviews with security focus:
https://gerrit.openbmc.org/c/openbmc/phosphor-certificate-manager/+/54947 Allow for expired certificate
https://gerrit.openbmc.org/c/openbmc/webui-vue/+/56719 Old password input in change password screen

3 New meeting time?
Anyone can hold a security workgroup meeting. It is fun and easy! The steps are:

1. Set a meeting time. Choose a date and time when others can meet.
2. Publish (email) the meeting time and its agenda.
3. Hold the meeting and keep notes about topics discussed.
4. Publish (email) the notes.

Meeting held 2022-09-28
Attendees: Joseph Reynolds, Dick Wilkins, krishnan, russWilson, ddaniil, RuudHaring, dsp, YutakaSugawara, edtanous, skoteshwara, radsquirrel.

1 Question about user management over interfaces: Redfish, IPMI, SSH. And related password management (change expired password with same password).
DISCUSSION:
https://github.com/openbmc/docs/blob/master/architecture/user-management.md
https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md
Please followup by re-asking in public forum: email, discord…
Please push changes for better project docs.

2 Measured boot.
DISCUSSION:
Port Facebook Measured boot to openbmc
Also need work from uboot community , and revisit openbmc's uboot fork (and update to newer version) -or- use uefi boot
Follow Up in gerrit review.

3 General issue: firmware image size limits. New features require more space. There is an ongoing need and effort to reduce image size by removing unused pieces. New features which consume image size must be configurable (out of image by default).
To help find how much space a change takes up, see
https://github.com/openbmc/openbmc-tools/tree/master/rootfs_size

4 (Joseph:) Can BMCWeb require additional authentication for sensitive operations (like changing a password)?
DISCUSSION:
See Redfish public discussion:
https://redfishforum.com/thread/540/additional-auth-sensitive-operations
See previous discussions in discord, email list. Example:
https://lore.kernel.org/openbmc/959CAFA1E282D14FB901BE9A7BF4E7724E51562F@shsmsx102.ccr.corp.intel.com/

Meeting held 2022-09-14
Attended (discord screen names): Joseph Reynolds, alda, cengel74, ddaniil, Dick Wilkins, dsp, galmasi, krishnan, russWilson, RuudHaring, skoteshwara, YutakaSugawara.

1 Discuss alternate meeting times (continued from previous meeting).
DISCUSSION in discord indicated to use the Discord #security channel for security-focused discussions. And feel free to set up a meeting on the Discord #security voice channel at any time. We will continue with the regular security working group meetings (once every other week).

2 SELinux design and implementation progress.
DISCUSSION:
Ruud. How to approve the design? https://gerrit.openbmc.org/c/openbmc/docs/+/53205 Ideas to ask the docs repo maintainers for feedback
https://github.com/openbmc/docs/blob/master/OWNERS
Yutaka Status: Working two areas:

- Creating bitbake recipes to enable SELinux on AST2600 EVB in non-enforcing mode.
- Working to get tests to pass before requesting to merge. The tests fail on the AST2600 EVB because the CPU is not present.

The interim plan is to get SELinux working on the Witherspoon reference platform (which should be possible to get all tests to pass). Then adapt the config to other models such as AST2600.

3 Measured Boot. Sandhya K.
Please review the design: https://gerrit.openbmc.org/c/openbmc/docs/+/57138
Still working on the design for the keylime agent which runs on the BMC.

Bonus topic: How does communication work? Where is code reviewed? Which channels?

For code changes: Note the Linux and U-boot pieces of OpenBMC use the email patch process. Nearly all other OpenBMC repos use the Gerrit review process.
https://gerrit.openbmc.org/dashboard/self
https://github.com/openbmc/docs/blob/master/CONTRIBUTING.md#submitting-changes

4 BMC Secure boot.
Please review the design. https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169

Meeting held 2022-08-31
Attendees (as Discord screen names): josephreynolds, galmasi, alda, ddaniil, dsp, fnichols3, jiangz, pgc, Rob, RussWilson, skotheshwara,YutakaSugawara.

0 We took about 15 minutes to try out the new Discord voice access and to escort folks from the old Webex meeting.

1 Continue Measured Boot discussion
DISCUSSION: Create two separate designs for:

- Enable measured boot.
- Enable Keylime Agent. Direction is for the keylime agent to open the BMC network port (using systemd, sort of like how SSH works). The intention is to engage with Redfish for how to configure the Keylime Agent: certificates, start/stop the application, etc.

2 Proposal for dynamic changes to Redfish authorization rules
https://gerrit.openbmc.org/c/openbmc/docs/+/56401
No discussion.

3 Proposal to change the meeting time so folks from other time zones can better participate.
We are also looking for alternate (non voice) ways to cover the material.
We looked at recording the call, but Discord does not have a record button.
We proposed alternating meeting times to cover time zones in California, US Central, Europe, India, China, and Australia. (So, pretty much the whole world.)
TODO: Joseph to create a poll, suggest alternate meeting times: 9am CDT & 5pm CDT or 8am Australia.

Meeting held 2022-08-17:
Attendees: Joseph Reynolds, Yutaka Sugawara, Ruud Haring, James Mihm, Dhananjay, Krishnan Sugavanam, Sandhya Koteshwara, Dick from Phoenix, Chris Engel, Paul Crumley, Mark McCawley, Angelo Ruocco, Daniil, Robert Senger.

0 Move the next meeting access to Discord? Discord > OpenBMC > Voice channels > Security
~ https://discord.com/channels/775381525260664832/1002376534377635860

Yes, agreed.
The next meeting planned for 2022-08-31 will be on discord.

1 Measured Boot.
DISCUSSION:
Single design or separate designs? Let's have separate designs:

1a. Enable measured boot: Kernel Device driver is available. Collect measurements into TPM.
See https://review.trustedfirmware.org/q/measured-boot

1b. Enable attestation: use the Keylime-Agent REST server on default BMC port 8890.
Design Question: Keylime vs Redfish vs other (VMWare is not OSS, Intel's design is proprietary).
Design Question: what gets measured by the TPM? Follow the TCG standard.
https://trustedcomputinggroup.org/resource/tcg-server-management-domain-firmware-profile-specification/
Design question: when and how to init the TPM? This is partly in scope to community project, but some parts will depend on hardware outside the scope of OpenBMC.
Root-of-trust Issue: Does BMC hardware (for example, the next ASPEED AST2x00 BMC hw) init the TPM and measure the Uboot image? ⇒ Or does Uboot init the TPM? Can ew use a FIP image?
Pre-req design: the measured boot design requires the signatures provided by secure boot.

2 CVE Response.
DISCUSSION:
Add guidance to
https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md
for submitting proof-of-concept exploits. How to ensure the exploit is not harmful to the recipient , and is not tagged by the email sanitizers? Encrypt? Or quoted with: > text Or add to the security advisory?
We are still working on:

- Github repo maintainers need to create security tabs so they can handle security advisories.
- Proposal to restructure repos
- Which CNA to use? The Openbmc CNA vs the github CNA?

3 FIPS compliance.
DISCUSSION:
Note that OpenBMC is not the kind of thing which can be FIPS compliant. The way it works is this: a system "built on OpenBMC" seeks FIPS compliance. As part of the compliance process, they need to ask questions about the portions of the system which OpenBMC provides, therefore the OpenBMC project needs to answer those questions.
FIPS reference: https://en.wikipedia.org/wiki/FIPS_140

The way I (Joseph) see the next steps are:

3a. What FIPS requirements apply to the BMC? Note that some FIPS requirements will not apply to the BMC and will apply only to the overall system. (OpenBMC does not need to address those requirements.) The work is to go through the FIPS standards, and list which requirements apply to the BMC, and if needed, how they apply. For example, the BMC is part of the management component of the system, and the FIPS requirements apply to the management subsystem.

3b. Given the requirements from the previous work item, what can the OpenBMC community say about them? For example, if OpenBMC documentation shows how a default build of OpenBMC would pick up some code or configuration to satisfy the requirement, that would go a long way to help the FIPS evaluator. More specifically for example, the BMC does provide role-based authentication to help satisfy the FIPS requirements.

3c. Create a new openbmc document to capture the answers above. This document use case is as a starting point for the information someone needs when they are working to FIPS-certify their system and try to roll down the FIPS requirements to their BMC. A secondary use of this document is to identify any gaps in BMC security function.

4 SELinux design. Request for re-review. https://gerrit.openbmc.org/c/openbmc/docs/+/53205
Advice on how to create interest in re-reviewing a design. Use Discord: Ping specific reviewers and ask specific questions about design issues, if it is solved; ask if the design can be approved.

Meeting held 2022-08-03
Attended: Joseph Reynolds, Russel Wilson, Yutaka Sugawara, Ruud Haring, James Mihm, Dhananjay, Krishnan Sugavanam, Sandhya Koteshwara, James Bottomley, Dick from Phoenix, Chris Engel, Gheorge Almas, Alda Ohmacht.

1 Continue discussing CVE response, SELinux, and Measured Boot
DISCUSSION: (We skipped over the first topic and went to the second topic.)

2 Recommend http header values per email dated 2022-07-22 with subject: BMCWeb support new HTTP headers Referrer-Policy and Feature-Policy renamed to Permissions-Policy.
DISCUSSION:
No discussion. The email archive is
https://lore.kernel.org/openbmc/CAH2-KxBuPhrv3bBu3ihr1AW6jpLXWvhr3pY0a4zqdFw0eFKkbw@mail.gmail.com/

3 Consider increasing the TLS DH session keysize from 1024 to 2048 bits per best practice (reference needed).

DISCUSSION:
BMCWeb references the OWASP guidelines.
Reference: NIST SP 800-131A recommends DH keysize 2048 bits. This is to protect against a supercomputer cracking the session key.
An alternative defense is to disallow the Diffie Hellman (DH) algorithm and use Elliptic Curve (ECDH).
Note that removing support for DH will break older browsers which don't support ECDH. Can we increase keysize? Yes, will take more of the limited BMC compute power.

Two of the places which use SSL: BMCWeb, dropbear SSH. To change these would need a configuration or code change to update the key size. Note the BMC creates other SSL connections which also may need similar configuration. See https://github.com/openbmc/docs/blob/master/architecture/interface-overview.md.

Tangentially-related topic: Use the AST2600 BMC's Hash and crypto engine (HACE) engine?
Kernel patch series for AST2600 crypto engine:
https://lore.kernel.org/linux-crypto/?q=s%3Ahace ; note just has HACE (AES/SHA), no ACRY yet. ASpeed is working on Kernel driver for the ACRY engine for RSA, etc.

New topic: Enhance OpenBMC to enable compliance with NIST FIPS compliance? IBM and Intel are interested in this. Add to applicable standards https://github.com/openbmc/openbmc/wiki/Security-working-group#applicable-standards. Next steps: Articulate what FIPS compliance means, and document how the FIPS requirements apply to OpenBMC. Perhaps a design or security doc?

4 Consider migrating this meeting to Discord > Voice channels > Security.
DISCUSSION:
Three responses were: Why? Seems okay. Don't like Discord.
Access question: Can a web client access the discord voice session?
Also, let's use the discord #security channel.
The direct link is https://discord.com/channels/775381525260664832/1002376534377635860

We went back to the first topic:
1 Continue discussing CVE response, SELinux, and Measured Boot
DISCUSSION: We only had time for the "CVE Response" subtopic.
Email: Change the OpenBMC project to use github security advisories:
https://lore.kernel.org/openbmc/f52f9a67-b515-8e4d-f904-6ef73346e599@linux.ibm.com/ with gerrit review here: https://gerrit.openbmc.org/c/openbmc/docs/+/55974

New sub-sub-topic: to help with static scanning tools (scanning either the firmware image file or scan the source code), there is a desire for all OpenBMC repos to have versioning numbers (versus using git commitID). This helps the static source code scan tools report version. Specifically, it helps a security-vulnerability-responder to map from a BMC firmware version

back to the list of source package+version used to create that version. This is related to the software bill of materials (SBOM) concept.

The request for repo maintainers is to periodically increment the package version (bitbake PV variable) (either within the recipe or the recipe filename) per best practices (need reference). Examples:

- Uboot has the package version as part of the recipe filename: https://github.com/openbmc/openbmc/tree/master/poky/meta/recipes-bsp/u-boot
- BMCWeb has no branches or tags (https://github.com/openbmc/bmcweb/tags) and specifies a generic package version (PV = "1.0+git${SRCPV}") within its recipe (https://github.com/openbmc/openbmc/blob/master/meta-phosphor/recipes-phosphor/interfaces/bmcweb_git.bb) which merely references the latest bmcweb commit.

James and the security response team to drive this. Is this a question for the Technical Oversight Forum (TOF)?

Next meeting, please cover the Measured boot topic.

Meeting held 2022-07-20

Attendees: Daniil Engranov, Russel Wilson, Yutaka Sugawara, Ruud Haring, James Mihm, Joseph Reynolds, Dhananjay, Jiang Zhang, Krishnan Sugavanam, Sandhya Koteshwara

1 CVE Response guidelines

The OpenBMC Security Response Team is meeting regularly to determine next steps for how to improve the vulnerability handling process. See background docs here: https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team.md

The direction is to move new problems into github advisories as quickly as possible.

For example, security vulnerabilities in OpenBMC documentation are reported in https://github.com/openbmc/docs/security/advisories, BMCWeb defects reported in https://github.com/openbmc/bmcweb/security/advisories, etc. Each repo has its own set of security advisories.

The team is working to understand how to give security responders access to private security advisories. Obviously, then we would have to work with each repository maintainer to set up its security tab.

2 SELinux updates.

We discussed ideas for the right way to structure the code. The consensus is there are three layers:

Layer 1. Use the existing **meta-selinux** bitbake layer. This layer has the poky/meta config changes to use selinux: adds the SELinux support, updates coreutils, and introduces policies.

Layer 2: Propose a new bitbake layer, **meta-phosphor-selinux**, to work on top of the meta-selinux layer, to adapt the OpenBMC phosphor applications to use SElinux. This

approach avoids changing the base repos, so they don't need to know or care about SELinux. This further customizes openbmc:

1. Override various recipes via *.bbappend to add selinux to recipes like busybox, pam, more updates to coreutils, etc.
2. Define minimal/trivial SELinux policies for OpenBMC applications

Layer 3: Add detailed SELinux policy files to the existing meta- layers for each target. For example, add SELinux policies to the OpenPOWER platform (the OpenBMC reference platform) **https://github.com/openbmc/meta-ibm/blob/master/conf/machine/witherspoon.conf**
This would do thing like:

1. Increase size of the readonly file system (which is per TARGET).
2. Introduce policy files for that target (test FEATURE to know if selinux is enabled).

This three layer approach puts the parts that can be shared into the new meta-phosphor-selinux layer, and leaves policy decisions to each TARGET machine.

To add SELinux to a machine or a build, the configuration work would be here:

1. Insert the meta-selinux layer
2. Insert the meta-phosphor-selinux layer
3. Enhance the layer for your target.

3 TPM/attestation updates.
Working on PoC for the following:

- Working to extend measurements to the TPM
- Working to integrate keylime for remote attestation.

Next steps are to create a design for the step above. For remote attestation: An agent on the BMC collects data. How can a network client get that data? WIP: Redfish schema for network clients to get access to read attestation. Is there a common solution? We want to avoid OEM APIs.

Redfish public discussion here: https://redfishforum.com/thread/685/support-bmc-attached-tpm

Meeting CANCELED for 2022-07-06 - per 2022-06-22 decision (US holiday)

Meeting held on 2022-06-22
Attendees: Daniil Engranov, Russel Wilson, Yutaka Sugawara, Ruud Haring, James Mihm, Joseph Reynolds

1 Agreed to cancel July 6 due to US holiday week

2 CVE management.
Intel's internal hack-a-thon 3 was held in May 2022. Working toward private disclosure to OpenBMC SRT.
Next steps: James will set up a private meeting with the OpenBMC security response team (SRT) to write some privately-disclosed vulnerabilities to the private issues database.

3 Measured boot
Measured boot writes firmware images to TPM
There is an effort to enable measured boot for ASPEED AST2600 platforms with a TPM attached to the BMC (distinct from host TPM).
Current work: Working toward measured boot for U-boot.
Pre-requisite work: Openbmc's ASPEED UBoot was forked and is about 1000 commits old and will need to be updated because it does not have new features needed.

Will need a design for this. Design to cover:

- Enable the mechanism to push measurements into the TPM. The design may have parts which are specific to AST2600.
- Describe which pieces get measured: SPL(?), U-boot image, kernel image, readonly file system.
- Enable network agents (like keylime server, possibly the host system) to get measurements from TPM. Note the measurements are digitally signed by the TPM to ensure their integrity.
- Intent to comply with OCP standards.
- [Addition: this was discussed in the meeting but not added until after the meeting]: How will clients access the TPM measurements? Is there a Redfish interface?

The design will omit policy questions: Use cases for the attestation data, keylime or other servers, policy questions about what to do when attestation fails.
Example policy when BMC goes bad (fails attest): BMC is isolated from its management network? From host control? External agent is notified, e.g., datacenter admin, who will then isolate the BMC and schedule it to be replaced.

Consider two underlying use cases: BMC management agent is (1) network-based or (2) host-based. The intent to enable use case 1. Use case 2 may be problematic when the policy is to isolate the BMC from its host, but nothing in the design is intended to block this use case.

4 Progress on SELinux
Still working on SELinux design (Ruud): implementation work continues to help the design.
Implementation progress (Yutaka): Enabled SELinux on AST2600 using Yocto Kirkstone version. BMC boots in selinux permissive mode and basic commands work. The initial readonly flash size increase is 20Mb, (was 16Mb, now is 16+20Mb = 36Mb total on flash). Will look into configuration changes to reduce the size.
Will need a later/updated version of busybox which has SELinux features enabled.

Starting to define policy for basic BMC workloads.

Meeting held 2022-06-08
Attended: Joseph Reynolds, Yutaka, Ruud Haring, Dick from Phoenix, Krishnan Sugavanam, Mark McCawley, Russel Wilson

The meeting went about 20 minutes over time (80 minutes total).

1 Progress on SELinux gerrit review https://gerrit.openbmc.org/c/openbmc/docs/+/53205
Note the design is intended for BMC which have a larger flash image size. For example the OpenBMC witherspoon reference platform has a 64Mb flash divided into 2 sides, with space for a 20Mb readonly filesystem, so it is too small. SELinux is intended for BMC with 256Mb SPI flash, where SELinux adds about 20Mb (initial guess).

Ruud is continuing to work on the design. Discovering what config changes are needed by enabling SElinux. For example, SELinux adds a `-Z` flag to many commands to show SELinux attributes. SELinux-enabled busybox (-Z flag) exists. Attempting to build from Yocto recipe. Attempting to follow meta-selinux docs. Debugging. Reach out with questions to the yocto community (perhaps via email list in https://wiki.yoctoproject.org/wiki/Security).

We did a deep dive on BMCWeb authority checking by following a Redfish API call:

- After a Redfish session is created, that session has a role and a set of privileges.
- When that session is used to invoke an HTTP operation, that operation's privileges are checked against the session's privileges.
- The Redfish spec described this in DSP0266 > Security details > Authorization. We peeked at this spec.
- We looked at the Redfish "delete user" API as implemented by BMCWeb. https://github.com/openbmc/bmcweb/blob/002d39b4a7a5ed7166e2acad84e0943c3def9492/redfish-core/lib/account_service.hpp#L1941 This defines:
    - the HTTP operation (DELETE /redfish/v1/AccountService/Accounts/<str> where <str> is a username).
    - along with the privileges required to perform that operation: namely redfish::privileges::deleteManagerAccount, which only Administrator users have.
    - The C++ code to implement the operation (which basically invoke the phosphor-user-manager API via D-Bus system bus with parameters
        - Bus: xyz.openbmc_project.User.Manager
        - Object path: (as C++ variable userPath)
        - Interface: xyz.openbmc_project.Object.Delete
        - Method: Delete
- We talked about, but did not look at BMCWeb's router function, which routes operations to their implementation (such as "delete user" above), and we talked about but did not look at the authority check it performs. That code is in the "handle" method, here:

https://github.com/openbmc/bmcweb/blob/002d39b4a7a5ed7166e2acad84e0943c3def9492/http/routing.hpp#L1236

- We looked at BMCWeb's implementation of the Redfish privilege registry. Specifically, the generated header file here https://github.com/openbmc/bmcweb/blob/master/redfish-core/include/registries/privilege_registry.hpp is a translation of the redfish spec's privilege registry. The BMCWeb contributors maintain this file (runs as needed and checked in to the repo), and the definitions are used within the operations handlers (such as "delete user").

A basic understanding is that OpenBMC's authority checking (which asks: "am I allowed to perform this operation?") is handled by BMCWeb, and there is no authority checking at the D-Bus layer. (Currently anyone who needs to use a D-Bus API must have root authority). This is a security problem we are trying to solve. (TODO: articulate why this is a problem.)
Two approaches were briefly discussed (not necessarily as complete solutions):

- BMCWeb drops to the logged-in user (switch user command (su) or the setuid kernel call).
- SELinux labeling model.

For example, if desired, we can use SELinux to ensure the "delete user" dbus api can only be used by bmcweb and that it cannot be used by any other service (like IPMI or by SSH/bash). Then we can ensure only the phosphor-user-manager service is allowed to modify the /etc/passwd & shadow files. Doing so will lock down who is allowed to perform BMC user management.

Revisit some initial use cases for selinux (examples):

1. Limit what files bmcweb process can reach. In my opinion (Joseph) this would be an easy initial use case for SELinux because BMCWeb only touches a small set of files,and has no reason to touch other files. Also phosphor-user-manager only touches a small set of files (including /etc/shadow), and has no reason to touch other files or to reach out to the network.
2. Control which D-Bus apis bmcweb is allowed to use. (All of them?)

Here is an attempt to state a security problem more clearly: How do we limit specific dbus calls to specific users or to specific processes? Alternatively: How do we push down the BMCWeb's authority model into the D-Bus APIs? And what additional security would this give us?

Meeting held 2022-05-25
Attended: Joseph Reynolds, Daniil, Dick, Mark McCawley, Paul Crumley, Robert Senger, Russel Wilson, Yutaka Sugawara, Dhananjay

1 We discussed progress toward following our CVE process. Documented workflow: Allocate CVEs from Mitre. Move existing vulns from email list to github issues. Publish CVEs.

Allocated CVE block. Use vulnogram tool.

Meeting held 2022-05-11
Attended: (did not record attendance)

1 Dhananjay - progress on writing CVEs?
DISCUSSION:
James has credentials (as a CNA) to write CVEs for the OpenBMC project. TODO: Dhananjay and Joseph need to get credentials, then the response team to start working vulnerabilities through the new workflow, and approve the workflow.

2 Review D-Bus threat analysis is work in progress
DISCUSSION:
What bmc resources do we need to protect?
Idea: Push the authority model bmcweb has into the D-Bus layer. That is, currently services like ipmi and bmcweb perform authority checks, and then use their root authority to invoke the D-Bus APIs. The idea is for BMCWeb to drop from root to the user who is requesting the operation, and use that user's authority to invoke the D-Bus API. The D-Bus layer should have to be enhanced to support this. (It currently requires root to perform most operations.)

Protect interfaces which implement sensitive functions, for example mctp/pldm/spdm. Or explain existing protection mechanisms. For example: a bmc non-root user should not have the ability to run arbitrary spdm commands. (The BMC should only ever use a subset of the commands.)

TODO Nirav Shah: Document BMC/host interfaces in a way similar to https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md as a way to get started with a model for what need to be protected.
For example: Both bmcweb and the network IPMI service both have user management functions, that is, they can create new admin users. They use the phosphor-user-manager D-Bus interface to do this, and user manager uses Linux functions (useradd and usermod commands, etc.) This model would help us systematically identify interfaces which need to be protected.

3 What is the current status of bmc secure boot?
DISCUSSION:
Progress to date: Uboot merged, secure booting the Linux kernel

The design is under review here: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169
Some discussion here:
https://lore.kernel.org/openbmc/20220131034147.106415-1-andrew@aj.id.au/

Some of the discussion related to system lifecycle (like how re-key the BMC, or how to temporarily disable secure boot). TODO: describe use cases for system lifecycle.
TODO: Follow up on design review.
Ref:
https://www.opencompute.org/blog/ocp-security-announces-version-10-specs-for-root-of-trust
Use case example: Example: Always enable first stage secure booting with no way to disable it: hardware checking uboot spl. How to use secure boot jumpers?

Meeting held 2022-04-27
Attendees: Joseph Reynolds, Ruud Haring, Dhananjay, Jiang Ziang, Daniil, Nirav Shah, Mark McCawley, Terry Duncan.

1 Followup to SELinux discussion from last time.
TODO Joseph: post the session recording and the presentation.
Note design in gerrit review https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/53205
We clarified the goal of the design is to make it easy for a system integrator to add SELinux to their BMC firmware image, and to set some basic SELinux policies which do not create "too many" denial event log entries when SELinux is switched to permissive mode. The usefulness of this design is to collect data for policies needed to switch SELinux to enforcing mode. It remains an open question what policies are generally useful to the OpenBMC community.

Dhananjay mentioned a SELinux policy analysis tool:
https://ossna2020.sched.com/event/ckpF/selint-an-selinux-policy-static-analysis-tool-daniel-burgener-microsoft
https://www.youtube.com/watch?v=Gx5bxwvzN_Y

2 Is there a tie-in between Penetration testing and SELinux?
Note: Pen testing is performed by individual platforms, and the testing effort is not shared: only vulnerabilities and fixes are shared. Help wanted at the community level.
The idea is that the same kind of analysis is needed for both Pen testing and to make SELinux policy. Can we share that analysis or develop it in the OpenBMC community?

3 Nirav Shah - Alternate idea: Use D-Bus session buses (vs the system bus).
Note that all OpenBMC applications use the D-Bus system bus, which only the root user is allowed to access.
Nirav presented an idea to change some applications to use a session bus (and away from the system bus). Doing so allows BMC applications to run as non-root and makes it easier for different applications to communicate via D-bus APIs.
We believe this work is relatively independent of SELinux policy configuration.

Meeting held for 2022-04-13:

Attended: Joseph Reynolds, Ruud Haring, Chris Engel, Dick (Phoenix), Dong Chen, Jesse Arroyo, Yakatawa Sugawara, Russel Wilson, Krishnan Sugvanam, Manojkiran Eda, McCawley, Robert Senger, Sandhya Keteshwara, Surya (Intel), James Mihm, Terry Duncan, (and unknown caller who joined as the meeting was ending).

1 Renewed interest in securing D-Bus interfaces and using SELinux. Ruud Haring and Yataka Sugawara and Russel Wilson from IBM Research presented a proposal.

A recording was made of the presentation and discussion. TODO: Post the recording.

DISCUSSION:
The proposal PDF will be shared with the OpenBMC community. Here is my summary of the main points: SELinux is preferred by IBM and some large customers to solve several related access control problems: limiting access of root processes, application trust, systemd, and D-Bus. See previous discussion 2020-05-13 below: SELinux email use cases and email https://lists.ozlabs.org/pipermail/openbmc/2020-April/021477.html

Next steps: Follow https://github.com/openbmc/docs/blob/master/CONTRIBUTING.md#planning-changes with email discussion, Discord (per https://github.com/openbmc/openbmc#contact) and creating a design for phase 1 (below).

TODO: Joseph to send email to begin the discussion about SELinux use cases which might be shared by multiple OpenBMC users.

IBM plans to work in the OpenBMC community project: stage 1 is an opt-in SELinux in permissive mode to collect data about which policies are needed. Later stages are to create SELinux policies for access control, and then to change configure SELinux to enforce them.

Does OpenBMC have existing SELinux policies? None are known, but see the Yocto/OE meta-selinux layer and associated docs.

We discussed some difficulties in using SELinux: Configuring the meta-selinux layer, configuring the Linux Kernel, and additional space requirements (about 20MB)

We discussed SELinux vs AppArmor. IBM has chosen SELinux because it is well known to IBM and customers, and has an active community. Note the planned SELinux support is opt-in, so another contributor can add AppArmor as needed.

The intended reference platform is an x86 system running with the AST2600 and 256Mb (or more) flash storage.

We discussed SELinux & D-Bus tie-ins. (OpenBMC D-Bus runs in system mode.) Note that D-Bus has built-in support for SELinux.

Meeting not held 2022-03-30: Not held

Meeting held for 2022-03-16:
Attended: Joseph, Ratan, James, Mark, Daniil, Dhananjay, Dick, Jiang

1 Please review the phosphor audit design
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/46023 and related code under https://github.com/openbmc/phosphor-logging directory phosphor-audit.
IBM is interested in working on this.

We also discussed encrypting data like logs, and storing keys in a vault / trust zone / TPM.
See also encrypted volume https://github.com/openbmc/estoraged

2 CNA work update
James is working on the OpenBMC vulnerability backlog. First transferring each one to our private github issues database together with its reserved CVE. James will share JSON-formatted CVEs with the security response team (SRT). Currently working to upload/submit CVEs to mitre. (Note these are not yet public.)
Helpful tools: formatted vulnerabilities using vulnogram. Use Redhat's Cvelib Python-based tool
TODO: Joseph and Dhananjay (as the OpenBMC CNAs): get credentials from mitre to allow you to create CVEs.

Meeting held 2022-03-02:
Attended: Joseph, Mark McCawley, Vernon, Mauery, Caci, Daniil Engranov, Jiang, Dick (Phoenix)
1 We briefly discussed the NoAccess role. It may have been conflated with the IPMI Callback or NoAccess privileges or with channel access. Newly created IPMI users currently default to NoAccess, and there is a patch to make new users have "User" (read only) privilege. Note that in OpenBMC's IPMI implementation, creating users requires multiple IPMI commands, for example: ipmitool user add, user set password, channel, etc.
https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-host-ipmid/+/50824

Meeting held 2022-02-16:
Attended: Joseph, Daniil, Dhananjay, Dick, James, Jiang

1 Discuss the concept and need for NoAccess users and how they would be different from disabled BMC user accounts? See discussion in https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/49295
DISCUSSION:
Does the project have any NoAccess (priv-noaccess) users?
Is noaccess needed to implement IPMI Callback users?
Note that we prefer to disable ipmi users, not change their role.
Can ipmitool be used to create a callback user? If so, what role does phosphor-user-manager use for that user?
Is the IPMI callback role deprecated? Can we remove it from OpenBMC?
Is callback needed to implement trusted system interfaces and sessionless interfaces IPMB?

2 Update on OpenBMC becoming a CNA.
James got CNA admin credentials, and is able to create test CVEs.
James is working on documentation for OpenBMC security responders who work to create CVEs . James is working to document the process for the OpenBMC CNA to work with Mitre's CVEs. (For example, how OpenBMC will reserve CVEs and ensure they are published in a timely manner.)
Next steps: (1) Document process steps in openbmc/docs. (2) Reserve CVEs for existing privately reported vulnerabilities.

3 Question: How does BMC respond to too many failed login attempts?
DISCUSSION:
DISCUSSION: It uses (the deprecated module) pam_tally2 (and should move to pam_faillock).
See https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-user-manager/+/39853 questions:
Background: https://github.com/openbmc/docs/blob/master/architecture/user-management.md
Note: The default is to not lock out users due to excessive password attempts.

Meeting held 2022-02-02:
Attended: Joseph, Jiag, Dick, Michael Richardson, Daniil, Surya, Dhananjay

Note that we started on topic 1 (RoT), and then covered topic 3 (CNA) before returning to topic 1. Topic 2 (NoAccess users) was not covered.

1 followup from previous meeting: OpenBMC's AST2600 RoT work is here https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/49789 with the underlying OE/bitbake recipe here:
https://github.com/openbmc/openbmc/blob/master/meta-aspeed/classes/socsec-sign.bbclass .
Note OTP refers to one-time programmable memory used to set the signing key, etc. Also I (Joseph Reynolds) believe the AST2600 specs are not public domain.
… and general OpenBMC Root of Trust (RoT) discussion

DISCUSSION:
Secure boot trust chain: the BMC hardware performs secure boot of the bootloader (e.g., U-Boot, then U-Boot verifies {kernel,devicetree,rootfs}, etc., up to starting the application.

Secure boot has three layers: 1 hardware validates uboot, 2 U-Boot validates the Readonly fs, 3 the operation system validates applications.
To validate before starting applications: DMverity, IMA

The OpenBMC project is working to support the first layer, specifically AST2600 secure booting U-Boot. The intention is then to support U-Boot securely booting the next layer (kernel, etc.)
Also there is interest in using DMverity and IMA, but no agreements.

Who programs the BMC's OTP memory? Different use cases: one of: BMC vendor, board manufacturer, or customer/installation.

How to validate the BMC hardware? Different use cases: RoT is the BMC -vs- an external component.

Does BMC download applications as part of its intended operation? Different use cases.
In the base use case, the BMC read only file system has all applications. Only developers (and advanced diagnostics) download code, presumably to test fixes or collect more diagnostic data.
Use cases include both validating the filesystem which has the code, and validating the app itself as it is loaded (exec'd) into a Linux process.

Does OpenBMC support Firmware encryption? symmetric/asymmetric. AST2600 supports AES encrypted bootloaders. But there is not currently support for this in OpenBMC.
Note that the latest U-Boot version supports encrypted firmware (for example, it decrypts the kernel).

Note added Feb 9, 2022 – Some of the information above was corrected and expanded in an email thread - see archive https://lore.kernel.org/openbmc/281326.1643993671@dooku/T/#t

2 Do we need to discuss the concept and need for NoAccess users and how they would be different from disabled BMC user accounts? See discussion in
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/49295
DISCUSSION - was not discussed because we were out of time.

3 CNA Organization Admin account and authorized users
DISCUSSION:
James is working with Mitre to get a "CNA organizational admin" account so OpenBMC can write CVEs in its role as a CNA.
Working the OpenBMC vulnerability backlog…intends to write CVEs.

We briefly discussed our direction to use Github security workflow to publish OpenBMC security bulletins on github.

Meeting held 2022-01-19:
Attended: Joseph, Dhananjay, James Mihm, Aviram from Kameleon, Dick Wilkins, Daniil, Jiang Zhang.

1 James mentioned two topics from last time: (a) integrate OpenBMC Security Response Team (SRT) docs into github, and (2) enhance the SRT process (as the OpenBMC CNA) to follow the correct process to write CVEs.
James renewed the call to push to writeup security issues in (private repo)
https://github.com/openbmc/security-response/issues
We are still working on this, with the limited amount of time we have.

2 Aviram from Kameleon briefly outlined interest in an OpenBMC Root of Trust (RoT).
The RoT controls access to the flash for both the BMC and host, following WIP standards from OCP:
https://www.opencompute.org/blog/ocp-security-announces-version-10-specs-for-root-of-trust

Meeting held 2022-01-05:
Attendance: Joseph R, James M, Dick W, Ratan G, Dhananjay P

1 We discussed some current topics:
1a email thread subject: meta-phosphor: enable `allow-root-login`
We discussed the prospect of moving away from root logins and creating a new “admin” userid and then how that admin user would get the root access they needed to run commands like busctl and systemctl. We discussed solutions including Restricted bash and sudo.
Note that all processes run as root, and work for “daemon privilege separation” needs help, see “https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/49100 and related code reviews.

1b gerrit review “Disallow no-access user login” (the NoAccess role)
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/49295 and
https://github.com/openbmc/bmcweb/issues/227
A NoAccess user can login but cannot logout. There seem to be two ways to fix this.

2 The OpenBMC security response team wants to use the github security tabs, and is looking for best practices. https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/50115
How can the OpenBMC SRT get authority to publish security advisories on github? What are the best practices? What repo should be used? openbmc/openbmc? openbmc/security-response? A new repo openbmc/security-advisories?

See
https://docs.github.com/en/organizations/managing-access-to-your-organizations-repositories/repository-roles-for-an-organization

3 The OpenBMC security response team is working to become a Mitre CNA (see minutes from 2021-12-22 meeting) so they can have better control over CVEs for the OpenBMC project. James to follow up questions with Mitre.
See CVSS scoring example doc https://www.first.org/cvss/v3.1/examples

Meeting held 2021-12-22:
Attendance: Joseph R, James M, Dhananjay P

This meeting had low attendance because of the holiday season.

1 CVE Numbering Authority (CNA) onboarding
Discussion
The CNA training session was held. We are working on the homework now (creating dummy CVEs). We found this tool easy to use: vulnogram.github.io
TODO: Document new procedures and guidance for the OpenBMC Security Response Team to follow when working as a CNA.
TODO: Create a test issue under https://github.com/openbmc/security-response/issues
And see if it leaks out into public communication channels, then start writing up old vulnerabilities.

Meeting held 2021-12-08:
Attendance: James, Joseph, Anton, Dhananjay, Ratan

1 OpenBMC CNA onboarding
DISCUSSION:
James started the process to onboard the OpenBMC project as a CNA. (See agenda item 2 from 2021-11-10.) Onboarding process is next week for James, Joseph, and Dhananjay.
Onboarding time commitment: unknown - watch videos
Here are the training links:

> please view the six on-boarding videos, available on the CNA On-Boarding Channel on YouTube--> Click here<https://www.youtube.com/playlist?list=PLWfD9RQVdJ6c4eMkdqbOKqF7zPCqXkgX3>

1. CVE Program Overview
2. Becoming a CNA
3. CNA Processes
4. Assigning CVE IDs
5. CVE Record (previously “CVE Entry”) Creation
6. CVE Record Submission Process to the MITRE Top-Level Root Only

* CVE Record (previously “CVE Entry”) GitHub Submissions

Softcopies of the presentations are available here (https://www.cve.org/ResourcesSupport/Resources#CVENumberingAuthorities)

2 Daemon privilege separation design doc for review (PoC change for ACLs)
DISCUSSION:
This is a multi-stage project, and having a design will make it easier to move forward.
Next steps:

- approve design doc (need reviewers),
- then write acl rules
- Then change process to an unique user
- List all services which need to participate - all D-bus service owners and clients
- Move to a role-based approach?

Idea: Complete the privilege separation work for a service to use as a model for other services. When this is done, repo maintainers will have an easier time to understand what changes are needed.
We briefly talked through an example set of rules for bmcweb and ipmid talking to phosphor-user-manager.

3 Move meeting earlier by 1 hour? Let’s renegotiate the meeting time.

4 Progress on BMC secure boot?
AST2600 hardware secure U-boot boot, then secure booting the Linux kernel. No additional pieces.
See the AST security guide. How is signing-key management done?
Dhananjay to follow up.

Meeting was CANCELLED for 2021-11-24 because of US Thanksgiving holiday
This would be a good time for someone in another time zone to run the meeting in their time zone.

Meeting held 2021-11-10:
Attended: Joseph, Bruce, Vernon, James, Caci, Jiang, Dick, Ratan, Dhananjay

1 Next meeting Nov 24 “Thanksgiving eve”
Votes: cancel, cancel, cancel. Agreed. Someone else schedule a meeting?

2 Should OpenBMC become a CVE Numbering Authority (CNA).
Ref: https://www.cve.org/ResourcesSupport/AllResources/CNARules
This would better integrate the CVE process with github.

OpenBMC looked into become a CNA years ago. See the old review:
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/15621
Is it worthwhile for openBMC to become a CNA? Yes, we have had multiple CVEs per year and believe this will continue. We have filled out the form (at cve.mitre.org) to create CVEs and have become familiar with writing CVE language.
We agreed to pursue becoming a CNA. No objections. James will follow up.

3 Make progress on these competing reviews:
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/48564
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/48633
Ensure we have a CI test for this. TODO: Joseph to contact George on email.

4 The OpenBMC security response team (SRT) is working toward improving the way it handles private security vulnerabilities before they are disclosed. (See notes from previous meetings.)
The repo https://github.com/openbmc/openbmc/security-response was created for this, the idea is to make this private to the SRT members and use https://github.com/openbmc/openbmc/security-response/issues to identify issues and track progress.
Open questions: What content should this repo have?
How to add content? Do we need files? Any private content? Web interfaces vs gerrit vs command line (git submissions?)
The README should have content like:

- the purpose of the repo (to track security vulnerability issues for the overall openbmc organization before public disclosure).
- the fact that the repo is private and access is controlled by the github @security-response team.
- Link to https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md
- Instructions to use github.com/openbmc/openbmc/security-response/issues for new issues

Nothing in the README needs to be private. The content which must remain private is in the issues.
Code reviews for fixes would use their own repo, and perhaps private gerrit review process, as stated in the obmc-security-response-team-guidelines.md.

The question for github is: What should a security response team (like https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team.md) use to track private security reports before public disclosure?

The overall structure might be like this:

- github.com/openbmc/openbmc/issues -- currently stores security advisories: search for “advisory”

- github.com/openbmc/openbmc/security/advisories -- proposed place for all advisories; this is what github wants us to use.
- github.com/openbmc/openbmc/security-response -- new PRIVATE repo for the SRT to track new security vulnerabilities toward closure

See https://docs.github.com/en/organizations/managing-access-to-your-organizations-repositories/repository-roles-for-an-organization

Next steps:
- Add github.com/openbmc/openbmc/security-response README -- see above for ideas
- Create first low-sev issue in https://github.com/openbmc/openbmc/security-response/issues and ensure it is not accidentally disclosed via a Discord bot, an email bot, or any other way.

Meeting held 2021-10-27
Attended: Joseph R, Bruce Mitchell, Vernon M, Jiang Zhang, Dhananjay Phadke, James Mihm

The meeting ran about 25 minutes overtime (1h 25m total).

1 FYA: Changing the os-release BUILD_ID back to its default value of DATETIME (recipe os-release.bb) - https://lore.kernel.org/openbmc/CAH2-KxB6P2HTE5iqJMx1Gwrrq_w2-gXCZ47ZXaO_x5kZ2RAzCg@mail.gmail.com/T/#m0065dab191fe8048ea02ab3c28b31362252f7622 (background reference: https://man7.org/linux/man-pages/man5/os-release.5.html).

a. Will the builder need to supply BUILD_ID to maintain a stable (aka deterministic, aka reproducible) build?
b. https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/48204
c. https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/48205

DISCUSSION:
This was resolved: the project defaults are not being changed.

2 (Joseph, followup): discuss progress toward (1) using github advisories, and (2) the Security Response Team's (SRT) using a private github issues database.
DISCUSSION:
This was discussed at two separate times during the meeting. The first discussion notes:
Must test, e.g., no leaks to discord.
The second discussion notes:
To clarify: the private database is needed by the OpenBMC security response team (SRT) to organize the security problems which were reported and are not yet made public. For background, see:
https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md

Access to the database would be given to the Openbmc SRT members, plus access to each issue is given to the problem reporter and the people working on that problem.
Please reply to the email thread “start using github security advisories” Oct 13-18. Example: https://lore.kernel.org/openbmc/cd2f6175-475f-0e5a-0b65-4f7a12959ab6@linux.vnet.ibm.com/
We resolved to create the issues database and test it with real but well-known vulnerabilities.
We also discussed how the project handles Linux kernel security issues, like how we fix CVEs:

- Joel Stanley is active in this area - https://github.com/openbmc/linux/
- Our security wiki (https://github.com/openbmc/openbmc/wiki/Security-working-group) describes how: Yocto security efforts flow directly into the OpenBMC project. For example, Yocto puts security fixes into its fix branches.

3 Continued discussion: IPMI password over DTLS
DISCUSSION:
Per Vernon, Opaque is not mature and Intel prefers SCRAM or sending cleartext username+password through the secure channel (similar to basic auth https://en.wikipedia.org/wiki/Basic_access_authentication).
Could use scram. Preferred because it can detect man in the middle attack via channel binding.
Looking for scram implementation.
Will add to https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/31548
Staging question: Do we need a protocol to support certificate auth, vs password auth via basicAuth or scram?
Would DTLS remove RMCP+’s 20 character password limit. Yes.

4 Questions about: Password strength (cleartext), lockout after failed password attempts
DISCUSSION:
See AccountLockoutDuration and AccountLockoutThreshold in the https://github.com/openbmc/openbmc/wiki/Configuration-guide
See MinPasswordLength property in https://github.com/openbmc/bmcweb/blob/master/redfish-core/lib/account_service.hpp
Which is brought into the BMC image via recipe: https://github.com/openbmc/openbmc/blob/master/poky/meta/recipes-extended/pam/libpam/pam.d/common-auth and is customized by OpenBMC here: https://github.com/openbmc/openbmc/blob/master/meta-phosphor/recipes-extended/pam/libpam/pam.d/common-auth with pam_tally2 docs here: https://man7.org/linux/man-pages/man8/pam_tally2.8.html for example, “even_deny_root”.
Do these policies apply to root users? It doesn’t look like it, per https://github.com/openbmc/openbmc/blob/2b59705148feb8ca6aafd9cf050229b069284515/meta-phosphor/recipes-extended/pam/libpam/pam.d/common-auth#L11
Ideally remove root user logins.
We discussed using Linux “capabilities” so we don’t need root (uid=0) processes.
Is this general topic (“https://github.com/openbmc/openbmc/issues/3383”) important enough to escalate to the Technical oversight forum (TOF)?

Meeting held for 2021-10-13:
Attended: Joseph Reynolds, Bruce Mitchell, Vernon Mauery, mbhavsar, Jiang Zhang, pravisash, James Mihm

1 CVE-2021-39296 is already publicly disclosed. OpenBMC is ready to disclose.
Here are the existing public disclosures:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39296
- https://www.ibm.com/support/pages/node/6495437

IBM PSIRT - https://www.ibm.com/trust/security-psirt
ASPEED Linux kernel patches are made regularly.
We discussed the desire to improve the OpenBMC Security Response Team's (SRT) coordinated disclosure. Specifically, OpenBMC disclosed first, then whatever products which are built on OpenBMC disclosure the same day and refers to the OpenBMC disclosure.

We agreed to publish advisories on https://github.com/openbmc/openbmc/security/advisories
TODO: Joseph to make this work, and look into creating a private issues database for the https://github.com/openbmc SRT team

2 Question about ipmi suite 3. This was removed: see notes 2020-04-29 below.
Existing ipmitool users can adapt in one of two ways: invoke ipmitool to use cipher suite 17 (`ipmitool -C 17 ...`) or use the latest ipmitool.
Was this change in the release notes? Yes, here:
https://github.com/openbmc/docs/blob/master/release/release-notes.md#security-audit-results-1
The link to the latest ipmitool source is here: https://github.com/ipmitool/ipmitool/ sha 7772254b62826b894ca629df8c597030a98f4f72 April 2018

3 We discussed "password over IPMI over DTLS" from before.
Email excerpt Oct 5, 2021 "SPAKE, DTLS and passwords + aPAKE and SCRAM":

> Weakness of SRP (Secure Remote Password):
> - Server spoofing, there is nothing that prevents a server from being spoofed.
> - Widely adopted with very little proof of being cryptographically secure and has been shown vulnerable to pre-computation attacks
> - No feasible way to check for password complexity in the protocol (true for most aPAKE - asymmetric Password Authenticated Key Exchange)
> - Some debate over if actually provides forward secrecy.
>
> Recommendation to look at at OPAQUE aPAKE:
> https://blog.cloudflare.com/opaque-oblivious-passwords/
>
> Suggestion to use SCRAM
> https://en.wikipedia.org/wiki/Salted_Challenge_Response_Authentication_Mechanism

The SRP Server spoofing weakness is fully compensated for by the IPMI protocol which prevents spoofing, so is not an issue. The other items apply. We'll continue to study this.

4 https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39756 BMCWeb "Fix authorization rules" was mentioned in passing

5. USB control was continued from the previous meeting
Use case: UPS power supply plugged into USB port, uses RS-232 protocol.
Threat: Physically present attacker plugs in a USB device which says it is a UPS which lost power and will drop immediately so the BMC can do an orderly shutdown. [Never mind that same attacker can just hit the power button.]
In this case, do we want to (1) ignore the signals from the UPS, or (2) read and log the signals but take no action.
In a hypothetical BMC systemd service to serve a UPS, if we wanted to disable it, would we (1) stop the service, or (2) reconfigure the service to continue to log signals but not take action.
Which approach is better?

BMC hardware SuperIO provides USB port capability. Are there any other use cases within the OpenBMC community for BMC USB ports? Is this an IBM-only use case?

Meeting held 2021-09-29
Attended: Joseph, Bruce, Milton, Dick, Vernon, James Mihm, Jiang Zhang, Sanjay, Daniil

1 Continue discussion: Password based auth for IPMI over DTLS
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/31548
Want to use password auth over DTLS.
DISCUSSION:
The planned IPMI over DLTS function will have certificate-based authuentication. For our use cases, we would like to add password-based authentication, and we want to do so as securely as possible, meaning what protocol we should use. In particular, we want to know if we should avoid sending a "cleartext" password (tunneled over DTLS) to the server.
However note the Redfish password authentication passes in the cleartext password to the Redfish/HTTP server (tunneled over HTTPS). Does not need the existing ipmi_pass file, or will at least store the password securely in it.
Contrast with Redfish password change and with Basic Auth.
Consider RAKP which does not require the password to be transmitted in cleartext.
Can we use consider SRP (dropped in OpenSSL 3.0 -- why?) or other implementations such as GnuTLS?
Want to know what protocol to use for password auth over DTLS. And then implement it correctly.
TODO: Call for experts to weigh on.

2 (Joseph) Who wants a function to enable/disable BMC USB ports?
https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-dbus-interfaces/+/47180
What does disable USB port mean? USB for BMC use. [Discussion excludes host USB ports, and any USB ports further from the BMC.]
DISCUSSION:
Threats: USB protocol attack, power-based attack, epoxy-based DoS attacks, use of functions built on top of USB function.
Can disable ports independently: Does Redfish want to model topology? Sets of USB ports, such as those with physical external connectors, and internal. ANSWER: Yes, see below.
Need to model topology (machine architecture, USB hubs, etc.) as part of understanding the issues? Or can we partition USB ports and call it either BMC or host?
Consider essential connections such as USB-based BMC keyboards, USB-based BMC/host connections, etc.
The design is interested specifically in used-by-BMC external-to-the-box USB ports.
Note that if USB ports are needed for BMC recovery (such as a USB key), then disabling the USB will remove that recovery option.
Note: The U-Boot is an independent OS which may have access to a “disabled” BMC.
Where to disable USB ports? In OpenBMC kernel? In Uboot kernel (does not have support for USB?)? Via pgood gpio?
What does the Redfish endpoint control? TODO: Joseph to investigate. DONE: After the meeting. Notes:

> Summary: Redfish models USB Controllers (as USBController), USB Port Collections (as PortCollection), and USB Ports (as Port). Implementations who want to implement powering off ports can use the USBController Resource_PowerState schema. Implementations who want to disable USB ports can use the USBController Resource_State schema or the Port Enabled property.
>
> DETAILS: A Redfish USBController: http://redfish.dmtf.org/schemas/v1/USBController.v1_0_0.yaml#/components/schemas/USBController_v1_0_0_USBController where properties include: Ports (PortCollection), Status (which can have a Resource_PowerState schema or a Resource_State schema (includes enabled/disabled))
> Ref: https://redfish.dmtf.org/schemas/PortCollection.yaml has property Members which somehow presumably can get to a https://redfish.dmtf.org/schemas/Port.yaml where Port_v1_5_0_Port has an “Enabled” property.

Do we need a custom OEM solution?
How do testers check if a USB port is disabled? Power? Signals?

Meeting held 2021-09-15
Attended: Joseph Reynolds, Milton Miller (attended second: IPMI over DTLS topic), James Mihm, Vernon Mauery, Daniil Engranov, Dhananjay MSFT, Dick [Phoenix], John Wedig, John Broadbent, Nancy Yuen

1 (gerrit review) Encrypted eMMC design - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/46573
DISCUSSION:
John reviewed the design: eMMC exposed as Dbus object.
We briefly discussed the need for a device-provided cryptographically secure erase function, because the block-by-block algorithms don't work in the presence of wear leveling.
How to provide encryption key/password. Use cases and risk models:

- Key is stored off of the BMC (by client, on eeprom, by host).
- Intent of encryption is to protect against someone physically removing the emmc.
- This design does not does not protect against an attacker who has BMC root access.

2 (email) Reminder that configuration matters. https://lore.kernel.org/openbmc/6593206c0bc90186f255c6ea86339576576f70dc.camel@codeconstruct.com.au/ Discusses AST2500 default register configuration (ESPICTRL[9] = 0) which allows the host to have full control over the GPIOs.
NO DISCUSSION.

3 (meeting process) Discuss the use of this document (https://docs.google.com/document/d/1b7x9BaxsfcukQDqbvZsU2ehMq4xoJRQvLxxsDUWmAOI) as a record, and not intended as a living conversation. Idea: Add a note to the top of this document to that effect.
DISCUSSION:
Agreement: This doc is only for minutes only, please move discussions elsewhere. Add note.
DONE.

4 (gerrit review) https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/46811 Change the dropbear SSH server "scp" protocol to use "sftp" internally (while still supporting scp connections).
DISCUSSION:
We discussed:

- Why do we need sftp?
- Sftp has a better user experience than scp. The client has better controls.
- We should explain how specific platforms or downstream configurations can disable sftp? Should it be disabled by default? Reference: https://github.com/openbmc/openbmc/wiki/Configuration-guide

Agreed: Eventually disable scp by default? Yes.
There was a general agreement with this proposal: Enable sftp now, have both scp and sftp enabled for one release (about a year), then disable scp by default. (The overlap is intended to give time for testers and operational procedures to convert to sftp or reconfigure.)
Discussion will continue in the gerrit review.

BONUS TOPIC:

Added after the meeting started, and went about 8 minutes over time.

5 IPMI over DTLS (gerrit review) - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/31548
DISCUSSION:
This is a continuation from last time.
A new question is: Should password authentication be supported?

- Use case: Large scale datacenters will use cert auth, but cert or 2FA requires infrastructure which small scale users may not have.
- Both cert-based 2FA auth require a synchronized clock:
    - The BMC TOD clock may reset to beginning of epoch 1970
    - 2FA and cert solution needs steady clock: battery backup or NTP

Is it okay to use the same cert for both host and for IPMI? If one service allows the private key to be disclosed or learned, that jeopardizes the other services which use that same key.
Disambiguation: User CA cert, host cert.
If we look ahead to process isolation (where each service has its own user), what solution will work?
Can we use trusted execution environments: (Op-tee, TPM, kernel support, ARM TrustZone), so we don't expose the key (as much) when establishing a session?
We also discussed if IPMI has a service identifier vs a system identifier. IPMI can get the server's GUID, same as from Redfish.
Discussion will continue in the gerrit review.

Meeting held on 2021-09-01
Attended: Joseph Reynolds, Milton Miller (attended first half: IPMI over DTLS topic), James Mihm, Ratan Gupta, Andrei Kartashev, Daniil Engranov, Dhananjay MSFT, Dick [Phoenix], Jiang Zhang

We discussed the second topic first (IPMI over DTLS).

1 Ratan Gupta wants to join the Security Response Team (SRT) for NVIDIA. See https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md#team-composition-and-email-maintenance . Considerations:

d. Current members are all from OpenBMC technical steering committee (TSC) companies.
e. What criteria for membership in this private group? See link.

DISCUSSION:
We discussed some criteria for SRT membership:

- Although individuals join the SRT, it is really organizations which join as represented by their SRT members. The SRT member candidate should be able to affirm that they participate in their company's SRT.

- The organization should have a “vested interest” in OpenBMC security response. Here are some examples to consider:
    - Organizations which use OpenBMC to produce products or services which are publicly available, and disclose security bugs to their users. For example, any org which produces systems which use OpenBMC and have a sufficiently mature SRT.
    - Downstream organizations, for example, who aggregate BMC-based systems into larger systems.
    - Security research orgs, open source SRTs, etc. which have a significant interest in BMCs.
- The default stance should be to deny membership in the SRT. This is to support the requirement to limit membership so as to not prematurely disclose security vulnerabilities.

History: The initial SRT membership was the TSC members plus their delegates.

In UEFI Forum, the founder companies formed the initial SRT, and then explicitly invited select organizations to join, such as OS orgs like RedHat and Debian. Call for more orgs who use OpenBMC who fit these criteria to join the SRT.

2 (gerrit review) https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/31548 IPMI over DTLS - questions about use of OpenSSL and sharing of private keys
DISCUSSION:
Structure: The IPMI server and the BMCWeb server belong to the same BMC. So should they share the same certificate? Or should they have different certificates because they are different services?
Opinion: Have separate certificates for each service. The BMC admin can install the same certificate for both, if they wish.
Items to add to the design:

- Describe certificate management.
- If DTLS and Redfish share a cert, what happens when the cert changes because of a Redfish API operation?
- Talk about how DTLS will configure or consume OpenSSL.

Call to action: please comment in the review.
Let’s invite Ed and Vernon next time if open questions remain from the gerrit review.

Meeting held on 2021-08-18
Attended: Joseph Reynolds, Bruce Mitchell, James Mihm, Jiang Zhang, Richard Wilkins, Surya Intel, Daniil Egranov Arm
Note: The date of this meeting was incorrectly stated in the email notice as September 18; the correct date is August 18.

1 Wholesale changes to bitbake recipes were made. See https://lore.kernel.org/openbmc/YQ1FD5q8KbhbXVBK@heinlein/T/#u My non-specific security concern (Joseph) is accidentally mis-configuring something with these changes.
DISCUSSION: None

2 Gerrit review - The BMCWeb session idle timeout changed to 30 minutes (was 60): https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/45658
DISCUSSION: None

3 Yocto is planning a security configuration guide. See https://bugzilla.yoctoproject.org/show_bug.cgi?id=14509
DISCUSSION: None
I saw the following after the meeting ended: see related email: https://lore.kernel.org/openbmc/4c6d60fc-f290-c92f-421f-4fcfd1a87d29@linux.ibm.com/T/#t

Bonus items:
4. What database? Bugzilla? github.com issues?
DISCUSSION:
James and Surya looked at github issues. Will test drive github. Need dashboard/query function. Worries about accidental disclosure.
Tianocore uses bugzilla per Richard. UEFI has a separate database (not bugzilla).
Use github private branches?
What development process for security code reviews (Github reviews vs gerrit)?
Next steps: James and Surya will come up with critical objections to using github issues.

5 How to add session timeouts to host console?
DISCUSSION:
See the diagram in the README under https://github.com/openbmc/obmc-console.
We thought obmc-console-client was the right place to implement the timeout mechanism.
I created https://github.com/openbmc/obmc-console/issues/18.

Meeting held on 2021-08-04
Attended: Joseph Reynolds, Bruce Mitchell, ashokm, James Mihm, Andrei Kartashev, Daniil Engranov, Dhananjay MSFT, Jiang Zhang, Surya, Mayank Intel.

1 (Joseph): IBM ACF design (2FA authentication for the special IBM service account) is in review - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/45201
DISCUSSION: Joseph gave a brief overview with Q&A.

2 (Joseph): Updated password hash algorithm from MD5 to SHA512 (while keeping the same cleartext password) https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/45214

DISCUSSION: Joseph gave a brief overview and mentioned the pre-requisite patch https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/45614. Please review!

3 (Joseph): Change the SSH server per-session idle timeout to an hour (was unlimited)? (Sent idea to upstream project yocto-security@yoctoproject.org.) Alternatively, update both SSH and BMCWeb to 30 minutes.

f. Guidelines:
    i. NIST SP800-63B requires a timeout of 30 minutes for "assurance level 2" (high confidence that the authentication is still valid), or 15 minutes for "assurance level 2" (very high confidence). https://pages.nist.gov/800-63-3/sp800-63b.html
    ii. OWASP suggests idle timeouts of 15-30 minutes. https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#session-expiration
g. Alternatively, use the bash shell's TMOUT variable?
h. See Yocto discussion (representative archived email): https://lists.yoctoproject.org/g/yocto-security/message/381

DISCUSSION:
There was general agreement that OpenBMC should set a default idle timeout:

- Must be able to configure each interface separately: SSH port 22 (BMC command shell), SSH port 2200 (host console).
- 30 minutes was suggested for the command shell.
- The BMC admin should be able to configure the timeout. Need to check if there is a Redfish API or property for this.
- The technology to have a timeout may be present in the SSH server, the underlying application (command shell, host console, etc.), or provided by an intervening program such as "screen".

Joseph to follow up via email.
Asked Redfish here: https://redfishforum.com/thread/518/api-set-ssh-managerconsole-timeouts
We also discussed the risks of allowing SSH at all.

4 Surya set up a bugzilla within Intel and will administer it. Demo'd the database.
Who has access?: The security response team (see Joseph as admin). Also the bug submitter and the bug fixer will have access to each of their bugs.

https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team.md
Side discussion: Can we add a security responder from Nvidia? Yes, first review See https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md#team-composition-and-email-maintenance
And then petition the TSC via email: https://github.com/openbmc/openbmc#technical-steering-committee.

5 How to escalate bugs reported to the security response team?

DISCUSSION: We briefly discussed this as the meeting time was past the end. It is hard to make people fix bugs. Ideas: keep sending reminder emails, and try to get someone to fix the bug.

Meeting held on 2021-07-21

0 What support for mTLS client cert management?
DISCUSSION: See the Redfish APIs referenced below. Redfish doesn't support mTLS, but BMCWeb does support mTLS. Is there a supported interface for the BMC admin to upload an mTLS client cert to the BMC?
References:

- https://github.com/openbmc/openbmc/wiki/Configuration-guide#bmcweb (mTLS)
- https://github.com/openbmc/openbmc/wiki/Configuration-guide#site-identity-certificate

1 See Google's "unified vulnerability schema for open source"
https://security.googleblog.com/2021/06/announcing-unified-vulnerability-schema.html?m=1
DISCUSSION:
This was included for awareness only, not to propose using this schema.
This seems similar to the forms needed to create CVEs such as here: https://cveform.mitre.org/
OpenBMC's current guidelines for collecting this kind of information are here:
https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md
Related discussion: Should OpenBMC consider becoming CNA? See previous effort here:
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/15621 ("Proposed answers to DWF CNA Registration Form")

2 Email: Update phosphor-defaults with stronger root password hash algorithm -
https://lore.kernel.org/openbmc/34f5b89a-3919-e214-a744-4277fba0bbbb@linux.ibm.com/T/#u
DISCUSSION:
The group agreed to change the project's default root password hash, while leaving the cleartext password the same. TODO: Joseph will propose the change via a gerrit review. DONE July 23
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/45214 -

3 What is the status of the OpenBMC BMC secure boot function? Who is working on it?
DISCUSSION:
ASpeed AST2600 BMC secure boot using AST2600 hardware without TPM and without any special hardware (other than pullup resistors). Interest in avoiding Cerberus.
See also Design https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169

Two ways to validate uboot: via AST2600 hardware, via Cerberus
Once uboot is running, use uboot to validate the FIT image, kernel, etc.

4 What is happening with the Intel Hack-a-thon 2?

DISCUSSION: Creating CVEs.

5 What is happening with getting a private database to track vulnerability submissions? This would be used by the OpenBMC security response team https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team.md to record security vulnerabilities which were reported to OpenBMC and not yet fixed or publicly disclosed. Only members of the OpenBMC security response team would have access (read/write access).
DISCUSSION:
Surya plans to set up bugzilla.
Contact Andrew Geissler in his role as OpenBMC community infrastructure if you need a server.

6 What is happening with deploying AppArmor?
DISCUSSION:
Nobody was tracking it closely enough to answer. Anton had been working on it. See reviews under https://gerrit.openbmc-project.xyz/q/owner:rnouse%2540google.com

Meeting **cancelled** for 2021-07-07
Not held

Meeting held for 2021-06-23
Attended:
Joseph Reynolds, Andrei Yadro, James Mihm, Bruce Mitchell, Chris Engel, Daniil Engranov, Dhananjay Phadke, Jiang Zhang.

1 How can the security response team track items reported to openbmc?
DISCUSSION:
Urgency? The security response team is not losing track of issues, but is having difficulty keeping focus on issues. Will create a spreadsheet of currently open issues and email it to the private email list.
We want a database to track issues (see ideas below).
The database needs to be secure. Meaning (a) a secure database which has an active security community, (b) hosted on a secure system, (c) handled by a trusted admin.
Options for secure database:

1. Redmine
2. Github based? Does github have a solution? TODO: Joseph to look at a private issues database.
3. Bugzilla? Note UEFI uses bugzilla with a “security attribute”

Idea: Set up a secure bug database on a server donated to OpenBMC. TODO: Joseph talk to AndrewG

TODO Joseph to ask for help from the Linux Foundation.

2 Gerrit review BMCWeb “Automate PrivilegeRegistry to code”
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/43939 .
DISCUSSION:
Item 1:
Yes, the consensus is: please separate the tools to (A) download the new privilegeRegistry JSON file, and (B) transform a Redfish PrivilegeRegistry into the privilege_registry.hpp header file. The tool (B) to transform a Redfish PrivilegeRegistry into the privilege_registry.hpp header file should run when the image is being built, that is, during bmcweb build-time.

Item 2: Joseph brought up the Redfish spec DSP0266 and described how the Redfish operation to privilege mapping worked, and described privilege overrides. The consensus was: the way BMCWeb currently handles property overrides and subordinate overrides seems okay. And: having separate follow-on commits to change which privileges are required seems like the right approach.

Meeting **held 2021-06-09**:

1 Updated the wiki “Purpose” section. Specifically
https://github.com/openbmc/openbmc/wiki/Security-working-group#purpose
No discussion.

2 Will resume recording meeting attendance
Discussion: good idea

3 Cancel the July 7 meeting? Interest in someone else running? And possibly scheduling for daytime in Australia/China/India?
Discussion: The US-based attendees agreed to cancel.
I (Joseph Reynolds) would be happy to have someone else run the meeting. There was interest in having the meeting sometime when people from Australia/China/India time zones could attend.

4 Interest in BMC command line via BMC web interface. See
https://github.com/openbmc/obmc-console/issues/17. IBM’s interest here:
https://github.com/ibm-openbmc/dev/issues/2243.
No discussion.

5 (gerrit review) BMCWeb change affects login/authentication function “Move Sessions to non Node structure” https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/43759
No discussion. Joseph plans to review.

6 (Discord discussion) Do we need a more general way to support Redfish PrivilegeRegistry SubordinateOverrides. Per discord discussion June 3, June 9:

i. Sunitha EthernetInterface SubordinateOverride questions
ii. Described in Redfish spec DSP0266 "Security details > Authorization > Redfish service operation-to-privilege mapping > Subordinate override"
iii. Apply to URI=/redfish/v1/Managers/bmc/EthernetInterfaces/ in https://github.com/ibm-openbmc/bmcweb/blob/master/redfish-core/lib/network_protocol.hpp and in https://github.com/ibm-openbmc/bmcweb/blob/master/redfish-core/lib/ethernet.hpp

DISCUSSION:
This was really two discussions (6a) Sunitha's issue with EthernetInterface privileges required, and (6b) a more general way to represent the Redfish operation-to-privilege mapping within BMCWeb.
6a:
Joseph will write email describing how BMCWeb's privileges required for URIs like /redfish/v1/Managers/bmc/EthernetInterfaces/ should be changed (from ConfigureComponents to ConfigureManager) because of the EthernetInterface SubordinateOverride. This change means BMC role=Operator users would no longer be able to configure the network.

UPDATE: I wrote issue https://github.com/openbmc/bmcweb/issues/209 for this in lieu of email.

6b:
We discussed the fact that BMCWeb hard codes the privilege registry.(For example, the code here:
https://github.com/ibm-openbmc/bmcweb/blob/900f9497737951412662711072l9ea019f2839cd/redfish-core/lib/account_service.hpp#L1333
hard-codes the privileges required to work with a ManagerAccountCollection under URI /redfish/v1/AccountService/Accounts/. For example, to POST (create) a new account requires the ConfigureUsers privilege. This corresponds to the entry in the Redfish PrivilegeRegistry in the OperationMap for the ManagerAccountCollection.

We had previously agreed on an approach to remove this hard-coded code and directly consume the PrivilegeRegistry provided by Redfish. See minutes below for 2020-12-09 and related community emails. However, that work has not yet been started.

Topics added after the meeting started
7 We need a bug tracker for the OpenBMC security response team, where only that team (and possibly the problem subimitter) can see work on the bug. This would be used by the security response team to keep track of bugs until they are resolved. (See item 11 below for continued discussion). Can we ask Kurt Taylor or the Linux Foundation or a member company for help here? [UPDATE: See item 11]

Security response team guidelines are here:
https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md

8 Can we populate the link https://github.com/openbmc/openbmc/security
DISCUSSION: Yes
See previous efforts here: agenda item 2 from the 2020-10-14 entry below
James will follow up

9 Surya was introduced.

10 Can we use a tag like [SecurityWorkGroup] in relevant email headers?
DISCUSSION: Yes, let's try it

11 The security response team has difficulty tracking reported security vulnerabilities to closure and writing CVEs in a timely manner. Can OpenBMC become a CVE numbering authority (CNA)? [CNAs can directly write CVEs without having to ask Mitre.]
DISCUSSION:
Having a confidential bug tracker would help.
Per Dick, the UEFI team uses bugzilla and has a restructured corner for the security response team: anyone can write a bug, but only they and the security response team members can see it. Also, the UEFI is a CNA with folks from more than one company contributing.

OpenBMC (Joseph) attempted to become a CNA; see agenda item 3 on 2019-2-6 and https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/15621 . At the time, OpenBMC had few CVEs and little interest in them. Now we have more interest and can try again.

UPDATE: Joseph sent email re the bug tracker

Meeting **held 2021-05-26**:
0 Bonus topic: We reviewed the reason for and structure of "Security schemes", and pointed to the work started here:
https://github.com/openbmc/openbmc/wiki/Security-working-group#security-assurance-workflow

1 Followup from the previous discussion (held on 2021-05-12) re notifying kernel developers.
DISCUSSION:
We think there are cultural differences between Linux and open source with respect to how we handle security items (but we didn't get into any details).
ARM kexec does not currently offer a way to validate kernel signatures.
1a. The discussion turned to additional technical discussion of kexec:
Kernel's modules expect BMC hardware to be in a particular state. Kernel kexec'ing might lead to undefined behavior for such modules. Worried about interactions with secure boot.

Scenario: kernel 1 boots, then the BMC gets compromised, then kernel 2 is kexec'd.
Kexec has two parts: load kernel, start kernel
Kexec does not significantly improve the boot time of BMC.

TF-A Vs. kexec: https://www.trustedfirmware.org/about/ -- does kexec fit TF-A?

kexec to new kernel version with enabled modules (worrying about modules in the rootfs, e.g. Nuvoton)
kexec Vs A/B partitions?

2 Per recent discussion in Discord > #test-automation, is there interest in reviewing supported TLS protocols?
DISCUSSION:
We are at TLSv1.2. Remove support for CBC?? Although CBC ciphers are considered weak and have been removed, the CBC HMACs were still allowed.
Don't allow client to negotiate protocols?
2a. The default HTTPS self-signed certificate duration is 10 years and should be much shorter. See previous discussion below **2020-02-19.** See also https://github.com/openbmc/openbmc/wiki/Configuration-guide#site-identity-certificate
Need OpenBMC to be usable by modern browsers.
Which happens first, BMC gets the current time-of-day -vs- generate self-signed cert?
We are not sure how to proceed.

3 user-manager: authentication & password management helper for netipmid and bmcweb for non-root environment to drop direct PAM use. Privilege separation and Master processes to handle users' sessions (mouse@).
DISCUSSION:
Idea: Forward all authentication & password change & account change requests to user-manager which would then need to be enhanced to check authority when a request is made. The user-manager would need root-like auth or capability to use PAM to change any user's password.
Does user-manager also need to be a session manager? Then we can remove session management from IPMI network and from BMCWeb , which would be modified to use user-manager.
Also consider how sessionless unauthenticated host-IPMI would work.

Meeting held on 2021-05-12:
1 Kexec (load and optionally execute new kernel). Security impacts? How does this work and play with secure boot and with IMA?
https://gerrit.openbmc-project.xyz/c/openbmc/meta-aspeed/+/37820
Use cases:

A. BMC booting- uboot uses kexec to load the production kernel.

B. handle kernel panic as a way to recover from a non functioning BMC. See agenda item 3 below.

Security impacts:

- Can be used to defeat secureboot.
- Can this function be disabled? Via kernel config. Default?
- Can restrict which images kexec can load?
- Recommend? Validate the kernel signature before kexec'ing it. But that doesn't stop an attacker who uses wget to get a malicious image which they pass to kexec.
- Why would an attacker want to use kexec? Opportunity to modify BMC code, load device drivers, create trojan horse(?) or back doors.
- How can we force kexec to perform the same signature validation as uboot? (each part and the whole: kernel, device tree, file system, …)

See discord > OpenBMC > kernel-and-uboot
https://discord.com/channels/775381525260664832/775694683589574659

2. Threat: `echo c >/proc/sysrq-trigger` causes kernel panic
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/42731
Requires root permission
Use case: help recover a malfunctioning BMC. See agenda item 3 below.
Security impacts:

- Terminates BMC processing (DoS)
- ...and dumping (kdump) takes a long time
- Can this function be disabled?

UPDATE: This was later narrowed to "p10bmc" systems via
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/42913

3 Here is a design which requires the features described above:
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/42948/5/designs/bmc-service-failure-debug-and-recovery.md
Security impacts:

- BMC dumps may contain sensitive data -- should encrypt?
- BMC dumps which happen during a kernel recovery process may take a while to complete, thereby extending denial-of-service.

Meeting held on 2021-04-28

1 Gerrit review : passwordless sudo access to members of the wheel group -
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/42429
ANSWER:
sudo - Use ACLs instead. File system size of sudo command.
Concern: using {sudo + overlay with executable code} interacts with secure boot
Different systems have different use cases. Please abandon this commit.

2 Intel HaT2021 results are being reviewed internally and are planned to be sent to the OpenBMC security response team.

3 How to model devices the BMC interacts with? Continuation of discussion from last time (2021-04-14)
ANSWER:
Various systems which use OpenBMC have very different architecture models. We are struggling with a common architecture model. Ideas:

1. Use the DC-SCM's DC-SCI as a reference (https://www.opencompute.org/documents/ocp-dc-scm-spec-rev-0-95-pdf). https://www.opencompute.org/documents/ocp-dc-scm-spec-rev-0-95-pdf DISCUSSION: This is a specification and not a common model. It has some good details, for example it shows the BMC interacts with the host processor module. Idea: Does the OCP DC-SCM have a threat model?
2. Reference several supported system architectures (per https://github.com/openbmc/openbmc#3-target-your-hardware), then abstract them. DISCUSSION: This approach would work, but is very time consuming, so it is not likely that anyone will do it.
3. Model the BMC's interaction with the host-processor module, specifically the host interface. DISCUSSION: This seems like a good place to start.

The direction is to enhance the existing BMC interfaces doc (https://github.com/openbmc/docs/blob/master/architecture/interface-overview.md#physical-interfaces) with the next level of detail. For example, with enough detail to show what host devices the BMC talks to (perhaps beginning with the host processor module) and relate those to functions OpenBMC provides. [Joseph asked after the meeting:] What OpenBMC source repos are we talking about?

Meeting held on 2021-04-14:
1 Continuing (or restarting) the "physical interface" discussion from 2021-03-17.
This is an edited summary of the discussion, not notes as the discussion happened.

Why focus on BMC interfaces? Shouldn't we focus on threats?

- Agreed we should focus on threats. But the threats come from the BMCs interfaces, so we need a clear model of the BMC interfaces first to help organize and talk about threats.
- Many organizations have tried threat modeling, and they all say to start with modeling the architecture of the thing you want to protect. For OpenBMC, that's the BMC.
- The high level security schemes used by OpenBMC contributors (see https://github.com/openbmc/openbmc/wiki/Security-working-group) all say the same thing:
    - Create a threat model
    - Describe the interfaces as the first part of the threat model

Should we focus on the BMC or focus on the overall system?

Spoiler alert: The focus is on the BMC itself.

This is a tricky issue. Discussion:
The BMC is a component in its host and the BMC operates various host components outside of itself. This makes it hard to understand the BMC's security boundary. Both the BMC and the overall host system need to be protected.

The trust model for using BMCs in computer servers (OpenBMC's initial model) is:

- The BMC does not trust its host system.
- The host system (for example, the host hypervisor) does not trust its BMC.
- Various host elements effectively trust everyone, that is, they take no steps to protect themselves. They may be operated by either BMC or host. (See examples below.)

Expect the host system to protect itself from the BMC. How it does so is outside the scope of the OpenBMC project. It is expected that host security experts will review the shared host-BMC access to host components and their complex interactions as carefully as the BMC security experts.

In summary, the BMC's threat model's focus is on protecting itself. When the BMC is integrated into a host system, the BMC's threat model is integrated into the host system's threat model.

Scope of the BMC architectural model:

The model needs to be sufficient to show **all** BMC interfaces. This includes host components outside the BMC which the BMC interacts with. A rule of thumb: if the OpenBMC project has code to interact with something, the BMC's architectural model should have a place for that something.

[Joseph: After the meeting:

Idea: Should the threat model architecture cover "exactly" the same elements as the BMC's Linux device tree? Does the device tree have all the elements the BMC interacts with?
Idea: Should we model elements across the DC-SCI interface from https://www.opencompute.org/documents/ocp-dc-scm-spec-rev-0-95-pdf

The model begins with physical architecture: the physical BMC device (as a card or board builtin), continues with its physical interfaces to its host, and physical host elements the BMC connects with (as outlined below). [This is intended to be descriptive and should not be interpreted to exclude virtual BMCs like QEMU].

Examples of items in scope:

- All inband and all host-BMC interfaces.
- All out of band interfaces.
- All management interfaces (such as IPMI and Redfish).
- All physical presence interfaces (like power buttons, physical USB ports, and intrusion detection switches).

The model then builds layer by layer. For example, each layer needed to describe:

- PLDM over MCTP over {LPC, PCIe, UART}
- Virtual media is USB over IP over {the BMC's network}
- The BMC's network block device (nbd)

Some of the individual items are merely used by OpenBMC and are not very interesting. (Example: i2c). The BMC's threat model will likely not say much about them, but they need to be present in the architectural description.

Each item ought to be described separately so a system integrator who mix&match protocols (example: MCTP over PCIe -vs- MCTP over LPC) can cleanly refer to the items they need.

Examples of physical elements shared between BMC & host:

- Physical USB ports (BMC-attached and host-attached)
- Physical network port (NC-SI)
- Access to host processors
- Access to cooling fans
- Watchdog timers(?)

Additional examples of complex BMC / host interactions:

- BMC handling host firmware. The BMC provides firmware to the host, and the host may validate its firmware before using it, such as via digital signatures.
- Virtual media aka USB over IP
- BMC control of host BIOS settings. For example, BMC can disable host USB ports.
- BMC access to host serial, typically host console

How to organize?

- Physical (hardware) organization of hardware component themselves
  - BMC's position inside its host (card or built in to the board)
  - Bmc-host interfaces
    - Buses for i2c, gpio, etc.
    - BMC dynamic configuration: multi-purpose pins or rate of speed
  - Physical presence:
    - Person, logic probe, servers drawer open indicator. Define where the BMC scope ends and host begins.
    - flash, usb, power button
- I think we agreed in principle to partition BMC interfaces like this:

- Host-facing interfaces
- System management interfaces
    - Network
    - Physical presence

Next steps:

- Agree on a basic architectural model, and abstractions for host elements.

Meeting **held on 2021-03-31**

1 Joseph: https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/41560 Add PerformService privilege. ← Abandoned (because it was too concrete)
Dropping the OemOpenBMCPerformService privilege and custom OemOpenBMCServiceAgent role in favor of a more general design.

2 Joseph: Design for User role configuration
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/41652
DISCUSSION:
Key requirement: Have a way for OpenBMC developers to be able to specify a delta set of changes, so when the underlying spec changes, those changes are picked up by everyone who has customized them. Need to consider use cases here. One scenario us:

1. BMCWeb provides the default privilege model.
2. Developer X customizes their privilege model with a set of deltas from the default.
3. Redfish updates to a new standard model, and it gets picked up by BMCWeb.
4. At this point, developer X should(?) get the new standard plus their customizations.

The current design will intersect with its counterpart “operation-to-privilege design” - in that they both specify privileges. We should sketch out that design before proceeding with this one.
Next piece is operation-to-privilege customization design because it affects this design.
Look for oem schemas under redfish/schemas - migrate to new?

3 Joseph: Interest in OpenBMC learning series talk “OpenBMC secure engineering”?
Nope.

4 Anton: Privilege separation
DISCUSSION:
Anton reviewed his doc. We discussed having the D-bus broker use ACLs.
To help solve the problem of co-requisite commits: Use a bump with nobranch=1
Key to get reviews: create something each maintainer can test.
Need to cover all D-Bus users with ACL before we can throw the secure switch (rough number of services to be changed for a based set of targets runnable under qemu).

Meeting held on 2021-03-17

Discussed first: Bonus topic from GUI WorkGroup : GUI security web page also shows insecure items. Could an attacker who has read access to the BMC use this page to exploit any additional weaknesses? Is that a vulnerability?
ANSWER: No. Yes, an attacker could use that page to learn about additional exploits. But I (Joseph) hope the attacker would be a little bit more sophisticated and read OpenBMC's threat model docs to learn about all the places they could try to get into an OpenBMC system. The proposed web page doesn't give them any more information than they could learn for themselves by using a scan tool with their current authority level. In that respect, in my opinion (Joseph again), having a web page show BMC insecure items does not represent a security risk. I believe it may help an absent-minded BMC admin.

Then we skipped over item 1 and discussed it last.

2 Discord discussion c. 2021-03-08: Should BMC users have a home directory? It is not needed for login. General consensus was that users should not be SSHing to BMC or storing data related to their account.
No comments.

3 Gerrit review adding meta-security layer for libseccomp
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/41373
No comments.

4 Gerrit review for updated Linux-PAM modules -
https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/41357
No comments.

1 Improve the OpenBMC interface overview > Physical interfaces documentation. The docs should be the right level of abstraction for threat modeling; something we can point to while we talk about items such as: BMC chips and BMC cards, placement of TPMs and TOD batteries, connection between BMC and PCIe cards such as video, and as a base to describe higher-level functions which are built on top of these interfaces. == Email sent Feb 17 archive:
https://lore.kernel.org/openbmc/6e0484bd-302a-8e2f-e299-727bb28bf087@linux.ibm.com/
Discussion:
...
Want to read a doc to understand all security considerations.
Review designs. To get started see https://github.com/openbmc/docs/blob/master/features.md and also https://github.com/openbmc/docs/tree/master/designs and please contribute.
…
I did not document all the discussion :-(

Meeting held for **2021-03-03**:

We started with agenda item 2.

Item 1
Agenda item 1 was skipped over, and we did not get back to it. It remains on the agenda for next time.

Item 2
Email questions about overlayfs, well known root password, SecureBoot vs IMA, etc. - **https://lore.kernel.org/openbmc/19011.1613860179@localhost/T/#t**
motivation: https://www.theregister.com/2021/03/03/hafnium_exchange_server_attack/
Created issue to track this: https://github.com/openbmc/openbmc/issues/3766

DISCUSSION:
Agreed intention is for overlays only for /etc (only selected subdirs), /var, /home. We should not have overlays over /bin /usr /sbin -- on /lib? On /opt? Is this different for different systems? Is there an overlay on '/'?

Agreed an intention to to disallow executables being loaded onto the BMC and run. But does the overlayfs offer a capability to disallow running code from the overlay? Is this better addressed by technology such as IMA?

There is likely interaction between this work and our initiative to use systemd to not run as root/ privilege isolation ~ https://github.com/openbmc/openbmc/issues/3383 ; will have to coordinate efforts. Perhaps privilege isolation should be done before this.

Scenarios:

- SSH is not an intended interface for end-users (like BMC admins). From this position, there is low risk of a user affecting which overlays are used.
- SSH may be an intended interface for manufacturing and service agents, depending on use case. That is, some installations will not allow SSH access and just take the BMC offline. Other installations will attempt to service the BMC in place, for which SSH access is generally needed.
- SSH is an intended interface for BMC developers who can SSH into the BMC shell and use sudo. They need that access to do their jobs. For example, they can create additional overlays, load and run additional code.

The overlays are mounted during the BMC booting process, possibly close to here: https://github.com/openbmc/meta-phosphor/blob/master/recipes-phosphor/initrdscripts/files/obmc-init.sh

How does the BMC protect itself by running only the code provided in its firmware image? That is, how does it prevent code from being added in an overlay or as a kernel module? For example, can we Enable kernel modules signature verification (CONFIG_MODULE_SIG). <= loading kernel modules is not enabled. The project might want this feature to reduce BMC

bootup wall clock time, but that is not even a design. Idea for CI test: test the kernel module loader is not present.

Agreed ideas for next steps:

1. What items in /etc can be legitimately changed by BMC operation?
    a. Make a list.
    b. Create patches to separate the configs
2. Help OpenBMC developers by documenting best practices for OpenBMC service config files (“separate static and dynamic configs”). Perhaps as a separate doc or as a topic in https://github.com/openbmc/docs/blob/master/anti-patterns.md

When overlays or mounts fail, is there an autocorrect feature? Example: BMC resets password back to default, but this could allow unintended access. Example: Network defaults to DHCP or non-VPN address, but this could expose the BMC to unintended network access (depending on use case).

Does systemd have an overlay feature? Or is there an alternative to overlayfs?

Separating static config into a read only file system makes the following attack harder: attacker gets bmc root access and then either (1) changes configs in the readwrite overlayfs, or (2) attempts to mount a readwrite overlayfs over the static config. When the BMC reboots, the attacker’s code has nowhere to regain control.

Item 3
Per https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39756 “Fix authorization rules” created https://github.com/openbmc/phosphor-user-manager/issues/9 to enhance phosphor-user-manager to use inotify to learn about /etc/shadow changes and send appropriate D-Bus PropertiesChanged signals.
DISCUSSION:
We agree with this approach (use inotify and send a signal).
The current direction for changing the password remains the same: Each service should use PAM directly. This can be revisited when we have privilege isolation. That is, perhaps we can enhance phosphor-user-manager with a new “change password” API when D-Bus sends the cleartext password only to phosphor-user-manager.

Item 4
Gerrit review https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169 Secure boot design.
No discussion.

Meeting held **2021-02-17**:
1 Gerrit review FYI: log failed authentication attempts
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39872

No discussion.
2 Gerrit review FYI: tie-in between Redfish sessions and IPMI sessions. Redfish will GET & DELETE IPMI sessions https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/37785
ANSWER: Why is this needed?
3 (Joseph) Discuss adding Web-based SSH to BMCWeb ~ https://github.com/ibm-openbmc/dev/issues/2243
ANSWER: Don't call this SSH because it is not. Do the webui part the same as the host console. Do the BMCWeb portion using a new D-Bus service (do not fork in bmcweb).
4 Interested in improving the documentation for the OpenBMC interface overview > Physical interfaces? (See related review https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/40424.)
ANSWER: Yes, worthwhile. Add to the agenda.
Is the ASCII art helpful or distracting?
Diagram for BMC cards and PCIe cards. Alternate Placement of TPMs, TOD battery.
Mention RunBMC cards.
5 Openssl released version 1.1.1j.
This led to a discussion of how much the OpenBMC project should be tracking and announcing CVEs -- Security Incident Response Team (SIRT) work. Currently members are tracking this privately. Is it even worthwhile, for example, to announce that CVE-2021-3326 affects OpenBMC and the fix is going to the latest kernel version? (No clear consensus was reached.)
Inhibitors to open source SIRT work includes: (A) some members are already doing this privately, and are not able to share due to confidentiality and repeating in open source is just extra work, (B) we are not all on the same release - that is: OpenBMC has not identified any Long Term Support (LTS) releases.
At present, there is no OpenBMC effort to show which CVEs are fixed. Left as exercise to interested downstream projects.

Meeting held **2021-02-03**:
1 Continue to discuss APIs to disable HTTPS
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39006
ANSWER:
Is there a use case to allow users to disable the interface they are currently using? For example, a Redfish user might disable IPMI and SSH, but why would they disable HTTPS?
Agreed: Redfish should not be allowed to disable HTTPS. IPMI should not be allowed to disable IPMI in a way that it could not be used to re-enable itself.
We also mentioned MCTP channels.

What {does|should} happen to login sessions {ipmi|https} when an interface is disabled? They get logged off. The ports get "cut" and the services get disabled.
We discussed a race condition such that HTTPS disables IPMI at the same time IPMI disabled HTTPS. Both might become disabled, resulting in no usable interfaces. The consensus was this problem is not worth solving at this time.

2 Review Linux-PAM changes https://gerrit.openbmc-project.xyz/c/openbmc/openbmc/+/40102 and https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-user-manager/+/39853
ANSWER: Joseph described the effort to replace deprecated and removed PAM modules. These modules were used by OpenBMC and their configuration arguments were modified by Redfish APIs (details are in the reviews).

3 Joseph summarized plans for IBM Enterprise system "service" login support.

1. Implement restricted roles and restricted privileges per Redfish spec DSP0266 1.12.0 aka 2020.4 https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.12.0.pdf
2. Story here: https://github.com/ibm-openbmc/dev/issues/1756
3. Need a special REST API to require variable privileges: https://github.com/ibm-openbmc/dev/issues/2875

ANSWER: Joseph introduced the Redfish spec changes (DSP0266 referenced above).
We talked about aspects of the Access Control File (ACF) design
The ACF design is similar to mutual TLS (mTLS) which is already implemented in OpenBMC.
Can we build on top of the mTLS design?
What are the similarities between IBM's & Intel's approach?

4 Need help for https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39756 ?
Need reviews.

5 (Discord > OpenBMC > #yocto 2021-02-02) Security concerns using a sstate cache.
ANSWER:
[Copied from Joseph's Discord post]: I think yocto security agrees that you should trust a shared sstate cache that someone else built only if you trust that other party. (Reference email: https://lists.yoctoproject.org/g/yocto-security/message/264). For someone to use the OpenBMC project-level sstate cache, they would have to trust whoever has write access to that cache (such as: the host system, the host system admin, and the CI build process -- in other words, the geissonator). With this outlook, it seems okay to me to have a shared sstate cache.
DISCUSSION: General agreement that this is okay, with the understanding that individual companies may decline to use this cache.

Bonus topic:
6 There is interest in using yocto reproducible builds

Meeting **held 2021-01-20**:
1 Call for OpenBMC 2.9.0 release.
ANSWER: Reviewed the security wiki item for this.

2 Dropped openssl support for deprecated algorithms, including TLS 1.0 and TLS 1.1. TODO: Add Link. I (Joseph) believe we already have dropped TLS below TLSv1.2, but let's take a look to see if we want any changes in this area.
ANSWER: dropped for HTTPS, not necessarily for SSH. Related discussion:
Move away from dropbear SSH to OpenSSH? Why? See the new issue https://github.com/openbmc/openbmc/issues/3756. The group had general agreement to do this.

3 Anyone want to allow customers to disable HTTPS?
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/39006
See also
https://lore.kernel.org/openbmc/8156dcbe-42d3-76f9-ba41-5998d3da6199@linux.ibm.com/
ANSWER:
Yes, we have use cases to disable the BMC's HTTPS interface. For example, a BMC controlled via the KCS interface (although these BMCs typically have their HTTPS interface removed entirely).
For the gerrit review: Allow HTTPS to be disabled, but don't make it easy for the admin to remove their only access to the BMC (bricking).
The BMC's service configuration manager (xyz.openbmc_project.Control.Service.Attributes at /xyz/openbmc_project/control/service/) shall issue an error message like "Cannot disable the %1{HTTPS,IPMI,etc} interface from a request via that same interface because that might brick the BMC. Make the request from some other interface."

An alternative to the above, we discussed having a behavior like "You cannot disable the last remaining interface".

We discussed enhancing the BMC's service configuration manager with a built-time option to disable the ability of the BMC admin from enabling and disabling the BMC's interfaces. For example, have a build-time block list (CANNOT_CHANGE_RUNNING_ATTRIBUTE_OF_THE_FOLLOWING_SERVICES) = "HTTPS" so any attempt to enable or disable HTTPS will be blocked and fail with a nice message like, "You cannot change the running state of the %1{HTTPS} service." In this way, the person who configures the BMC image can ensure that certain services are always running.

We discussed what happens to existing SSH sessions when SSH interface is disabled?
What happens to existing Redfish sessions when HTTPS interface is disabled?
What happens to existing IPMI LAN+ when IPMI/RMCP+ interface is disabled? (RMCP. No current use case to disable the KCS IPMI interface. Compare with KCS restricted mode.)

4 Linux-PAM dropped support for pam_cracklib and pam_tally2. These are being removed from OpenBMC usage because they are no longer available from yocto, but the function is not yet replaced. See https://github.com/openbmc/openbmc/issues/3750.
ANSWER: This work is happening now. Reviews appreciated.

5 The Intel security is planning to focus on penetration testing (an internal hackathon).

BONUS TOPIC:
6 Update on Linux process isolation.
ANSWER: Still working on solutions for common cases.
Difficulties: file permissions, testing other people's code, wrong architecture need to be upgraded
Hard to take the first step because you'll need dbus permissions working which is difficult.
Example: difficulties when the (downstream) nbd launches another process.
Idea: Have a new image feature to enable process isolation. Grow over time to encompass additional BMC services.

Meeting not held **2021-01-06**
This meeting was not cancelled but was also not held.

Meeting cancelled **2020-12-23** - cancelled
Agreed on 2020-12-19 to cancel this due to US holidays

Meeting held 2020-12-09:
1 Discord discussion #webui: Dumps and logs may contain sensitive information as documented here https://github.com/ibm-openbmc/dev/issues/1531#issuecomment-642238544 and https://github.com/openbmc/openbmc/wiki/Configuration-guide
Discussion.
Need to document sensitive info? Yes, worthwhile. Topics like: Dump and log handling. Where are dumps stored? Encrypted? Who *should* have read access to dumps and logs that may contain sensitive information? Note different use cases with different details in terms of what information is present, how sensitive it is, if it needs to be encrypted as it sits in the BMC, and who should have read access.
Interest in moving this from the wiki into the docs? The consensus was to keep this in the wiki for now.

2 Joseph: Proposed PerformService privilege enhancement to BMCWeb
https://lore.kernel.org/openbmc/1bfe87ea-9fc5-8664-d1de-d3138616a427@linux.ibm.com/T/#u

Discussion. Ed will send email.
The direction is to consume the Redfish-published privilege registry at compile time. Then it will be easier to have customized or multiple registries.

3 Cancel the next meeting 2020-12-23?

Yes, please cancel the Dec 23 meeting, and schedule the next 14 days out from that.

Meeting held 2020-11-25:
There was relatively low attendance. The US Thanksgiving holiday was the next day.
1 Phosphor-user-manager default group roles (email)
https://lore.kernel.org/openbmc/ec923bf7-d23d-bc45-9c31-2aded4b1fa68@linux.intel.com/
DISCUSSION:
Richard and Joseph went through the email thread and agreed on the solution for the ssh group. This includes the use case where SSH is enabled, but only special pre-created users are allowed to access it (such as manufacturing and service accounts).

We also discussed an image feature to disable SSH. Is there such an image feature in yocto/OpenEmbedded? If so, use it; otherwise add an option to openbmc. Specifically, if SSH is not present, then remove the “ssh” group privilege from the image (such as phosphor-user-manager).

We discussed the concept of “image type” as an image feature. A “development” image would have features such as SSH enabled and is intended for developers. A “production” image would have fewer (or different) features enabled and is intended for production servers. This might simplify testing. However, we did not discuss any specific features (beyond SSH).

Joseph mentioned that changing the SSH default was one of several desired changes...

Joseph is moving forward with a proof of concept (PoC) for a special pre-created “service” account that has a custom OEM “ServiceAgent” role that has the custom “PerformService” privilege. I believe all agreed that this privilege is needed to perform operations such as change a permanent MAC address or a FRU serial number.

(Joseph introduced the way we plan to authenticate the special-privilege pre-created users. Having a default password is problematic. The service user (person) will create a certificate pair, and work with the BMC admin to install the “public” copy onto the BMC. Details pending.)

(Joseph mentioned the “service” account is “special” in several ways: special authentication as mentioned above, and there are no APIs to delete or modify the account. The main idea is to prevent the admin user from escalating into the special account.)

We discussed if the OEM ServiceAgent role would be (A) a superset of the Administrator role, or (B) if it should be a subset of Administrator privileges plus the custom PerformService privilege. Option A is the use case currently needed. Option B may be more difficult to design, implement, document, test, and reason about.

We discussed the idea of making all these changes in BMCWeb and user-manager, and which would become image features.

The meeting went over the hour by a couple of minutes.

Meeting held 2020-11-11:
1 Is OpenBMC ready to move from root to an admin account? See
https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/33847
ANSWER:
Please change the design to add an image feature in meta-phosphor to add the "admin" account. Adding the "sudo" package is sufficiently independent that OpenBMC does not need to handle it specially. (As in: just add the sudo package and configure the wheel group if your image needs it.)
We discussed what privileges and accesses to assign to dynamically created users. For example, when a client creates a new admin or operator account, what groups should that user have access to (e.g., SSH, wheel)? See also: existing phosphor-user-manager D-Bus APIs.

2 The PAM_ABL module https://github.com/deksai/pam_abl is no longer supported. We had discussed using PAM_ABL to help prevent DoS.
No discussion.

3 The CSIS published a paper "A Case for a Trustworthy BMC" that gives recommendations for security. A section analyzes how well the OpenBMC project meets these recommendations.
I've added this to the OpenBMC security wiki.
ANSWER:
No discussion. Plans are to track OpenBMC's efforts in the security wiki.

4 Anton's progress in running daemon processes as a non-root user.
Success making a sandbox that launched multiple daemons (BMCWeb and ipmi-network) using less-privileged "namespace'd users". These daemons communicate with the rest of the system via D-Bus.
This uses Linux groups to carry the authority to make D-Bus API calls.
Please look at gerrit reviews. (1 | 2)

New question. Does this daemon work have any tie-ins or complication with the work to login with a non-root admin or operator account?

- Ipmi-network d - drop auth after connection established?

We discussed what should happen when a network user successfully authenticates:

- Given that we need root authority to be able to become another user.
- Authenticate - switch user into that user account (which has the privilege group needed to make D-bus calls)
- What model to use? Fork and then drop privilege, vs CGI model

Meeting held 2020-10-28:
We inserted a new topic as agenda item 1 and moved the rest down. We skipped from item 5 to 8 due to time constraints. We went over time. And the moderator lost the internet connection at the end of the meeting.

1 Voltage regulator (VR) email - security implications.
https://lists.ozlabs.org/pipermail/openbmc/2020-October/023760.html
OpenBMC currently supports a fixed voltage. Given that improper VR use can damage the host, looking for a safe way for the BMC to control the voltage (from an enum, or within a range) when requested by the host or the BMC admin
ANSWER:
Idea: Put access within an ARM TrustZone.
Do not want the full power of the i2c control command: ipmi-i2c passthrough or equivalent OEM.
Proposal: Access is provided by a proposed D-Bus interface. The safe voltages ranges are determined by entity-manager.

2 Gerrit review BMCWeb - DoS - maximum number of persistent sessions
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/37501
ANSWER: Need to cite best practices.

3 OpenBMC list of security topics - email
https://lists.ozlabs.org/pipermail/openbmc/2020-October/023606.html . The main idea is to reorganize the security wiki around this list.
ANSWER: No objections.

4 BMC Configuration wiki - https://github.com/openbmc/openbmc/wiki/Configuration-guide
(Guide for BMC system integrators and BMC admins). What is the best way to proceed? Get this into docs repo?
ANSWER: Leave in wiki

5 Security implementation of Linux kernel livepatch.
https://lists.ozlabs.org/pipermail/openbmc/2020-October/023723.html
ANSWER:
Alternative: kernel dynamic update. kexec
We discussed a use case: For very large scale deployments where quick deployment is required. This mechanism is for specific targeted fixes. When a livepatch is needed, it is applied temporarily in-memory only and is always accompanied by a firmware update that includes the patch; this update applies on the next BMC reboot.
Consensus: Seems like a good feature to get patches out quicker. Nobody has experience with this. Re-ask the embedded Linux community (OE/Yocto)? TODO: Joseph to re-ask yocto email list DONE -
https://lists.openembedded.org/g/openembedded-core/topic/experiences_using_livepatch/77875346?p=,,,20,0,0,0::recentpostdate%2Fsticky,,,20,2,0,77875346

6 skipped over - will leave on agenda for next time

7 skipped over - will leave on agenda for next time

8 status update on daemon privilege separation
ANSWER:
Cover privilege separation with distro-wise feature flag. Will use it to limit flash consumption as well.
Next step is to create PRs with root-oriented busconfig ACLs for smooth transition to unprivileged space.

Meeting held 2020-10-14
1 Follow up from 2020-8-19: Gerrit code review: BMCWeb webUI login change: https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/35457
It seems like we agree on having two configuration flags (to disable /login, and below). What are the security risks of using the proposed config flag BMCWEB_INSECURE_ENABLE_UNAUTHENTICATED_ASSETS=YES?

a. Fingerprinting (leak information about the BMC's manufacturer and version).
b. Attackers have an easier time getting the code to find and exploit security bugs.
c. May make DoS easier.
d. More?

ANSWER:
Yes, those are the main risks we talked about. And it seems reasonable for some environments to accept these risks. We discussed fingerprinting, and the desire to minimize this surface going forward. We discussed how the Redfish standard requires files to have unauthenticated access to static files while the OpenBMC project has uses cases that don't want to allow that, for example, discussion in https://redfishforum.com/thread/375/mtls-enforcement-openbmcs-redfish-implementation

2 Per https://lists.ozlabs.org/pipermail/openbmc/2020-October/023530.html do we agree on the approach? What security categories seem most important?
ANSWER:
The Microsoft, IBM, and Common Criteria schemes each have topics that seem appropriate. No other high-level scheme was proposed, so we'll go with these for now.
In particular, will someone please articulate topics from Microsoft Security Development Lifecycle (SDL), and we'll add them to the list.
⇒ It was agreed that the list of topics have information that can be leveraged by various security development processes. For example, a team that uses OpenBMC in their project and wants to follow a security scheme/process/evaluation should be able to use these topics to find what they need in the OpenBMC project documentation.

⇒ We agreed in principle to organize OpenBMC security work in (a subset of) the following topics:
- Security Audit (audit logs)
- Communication
- Cryptographic Support
- User data protection
- Authentication
- Security Management
- Privacy
- Protection of the BMC
- Resource Utilization
- BMC access, Trusted paths
- Document BMC architecture and configuration
- Development (process: architecture, functions spec, implementation)
- Internal representation (source code)
- Guidance documentation
- Life-cycle support
- Tests
- Vulnerability Assessment.

Development process: protect source code, planing, testing
Product lifecycle management: vulnerabilities, fixes
Secure Engineering Framework:
- Education and awareness
- Project Planning
- Risk assessment and threat modeling
- Security requirements
- Secure coding
- Test and vulnerability assessment
- Documentation
- Incident response
- Supply chain
- Assessment
- Threat Model
- Code Scan
- Security Tests
- Penetration Test
- Vulnerability Management

The list above has duplicates because the topics were pulled from multiple sources.
NEXT STEPS: Massage this into a list appropriate for the OpenBMC project.
We did not attempt to prioritize the list (but did talk about how we pull in security bug fixes).

We reviewed the security reporting and bug fixing process. Specifically:

- The OpenBMC security response team: https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team.md
- This is what github advocates using: https://github.com/openbmc/openbmc/security/advisories
- What tools do we use to:
    - Identify which open source pkgs are used in an openbmc build,
    - Identify security bugs in those packages, and
    - Ensure that we pull in fixes or otherwise mitigate the problem.

Given that OpenBMC is a Linux Foundation project, what resources does the Linux Foundation offer? Specifically, we want a private secure bug tracker for the OpenBMC security response team to use.

3 Anton update on privilege separation work
ANSWER:
Progress on ipmi-net & bmcweb -- working on dbus config, sockets; which areas to sandbox.
To make the migration work (changing from root user to another user), we will need to migrate the process's environment, for example: bmcweb uses files in /home/root and it won;t have permission afterward.
We discussed how to do the source bump to help CI go more smoothly.
See - https://gerrit.openbmc-project.xyz/c/openbmc/meta-phosphor/+/37366

Meeting held 2020-09-30:
1 Call for "Additional Topics for Learning Series" includes a security topic: *how project report/handle CVEs, designing for security, secure boot, privileges etc*. (A) What topics should this cover? (B) Who wants to help write the talk? (C) Who wants to present?
ANSWER:
Joseph will email an outline for the talk.

2 Do we want to look at items from our "security assurance workflow" linked above? For example, what items from the CSIS paper are high priority for OpenBMC?
DISCUSSION:
Which processes should the OpenBMC project prioritize? Example:
- Follow the code review process to prevent malicious code being inserted.
- Inadequate project docs.
- Use interface docs to move toward threat modeling.
- What will OpenBMC do if github fails and loses the source code? How do we implement secure disaster recovery? (Ideas discussed were to establish a secure server and then collaborate to merge our private copies into the "official" source.)

NEXT Step: Joseph to send email.

3 Getting mTLS-only option to be supported by Redfish standard:
https://redfishforum.com/thread/375/mtls-enforcement-openbmcs-redfish-implementation

ANSWER:
There is interest in OpenBMC supporting mTLS-only use case. This is a good example of disabling interfaces that are not needed (specifically, password authentication).
Please contribute to the Redfish thread. Attend the private Redfish forum meeting to push this forward.

You can find out how to join the DMTF Redfish forum here: https://redfish.dmtf.org/ (or ask your company if they are already a member). First, you must join the DMTF. Second you must become a member of the DMTF Redfish forum. Following that process allows you to participate in Redfish's private discussions and access to the Redfish calendar. Two of the Redfish forum meetings I (Joseph) regularly attend are:

- The Redfish Forum Meeting, every Tuesday. This meeting triages items in https://redfishforum.com/ such as the mTLS issue linked above.
- The Redfish Discussion Meeting, every Thursday. This meeting reviews the exact changes to the Redfish specification.
- These meetings are both private. The exact meeting time and access information is available to Redfish forum members under https://members.dmtf.org/.

4 Short update on privilege separation progress
ANSWER:
Anton walked us through his progress, including:

- D-bus broker has support for ACLs.
- Enable systemd-nss - Use supplementary groups for dynamic users.
- Working on net ipmid privileges, next is bmcweb.

Start a wiki to track daemons capabilities needed, sandboxing models, file access, etc. v
DONE: here
https://github.com/openbmc/openbmc/wiki/Security---Privilege-separation-&-Sandboxing

Meeting held 2020-09-16:
1 Common Remote API for TLS certificate management?

a. Certificate management = installation, **rotation, revocation**

ANSWER: OpenBMC desire manage certs via Redfish APIs.
Please create a design; start with email discussion.
Some difficulties were foreseen with cert rotation; need to work out issues.

2 BMCWeb Code review: Admin-configurable session timeouts
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/36016
No discussion.

3 BMCWeb core review: moving to Meson build system (from cmake): A security concern is ensuring project defaults are preserved so that builders get the same options when they use the new build system. https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/32816

No discussion.

4 BMCWeb code review: WIP toward HTTP-HTTPS redirect:
https://gerrit.openbmc-project.xyz/c/openbmc/meta-phosphor/+/36245
No discussion.

5 Interest in implementing Redfish ManagerNetworkProtocol properties: HTTPS, IPMI, SSH, VirtualMedia, KVMIP, HTTP (redirect), Oem.OpenBMC.TFTP, and Oem.OpenBMC.mDNS? This allows the BMC admin to enable and disable these services. Previous discussion on 2019-11-13.
ANSWER: Joseph intends to add pieces we need to the existing implementation.

6 Interest in implementing Redfish ManagerAccount.AccountTypes. This allows the BMC admin to control which users are allowed to access specific BMC interfaces (like SSH or IPMI). See https://redfishforum.com/thread/219/account-groups-property and email https://lists.ozlabs.org/pipermail/openbmc/2020-September/023080.html
ANSWER: Working out many issues; see links above. Joseph wants to implement.
Richard T: followup on issues with password change, and with backward compatibility.
When the user account is granted access to use IPMI (via PATCH to their account), the order of operations should be: add IPMI group (and exit if error), then change password.

7 Protect BMCWeb against password guessing attacks. See
https://lists.ozlabs.org/pipermail/openbmc/2020-September/023054.html
Delay a few seconds vs fail2ban.
ANSWER / DISCUSSION:
Do we have different use cases within OpenBMC? Different use cases:

- Protected datacenter.
- Connected to less-well protected network or to internet.

Connection limit: multiple simultaneous connections. [ref. Issue or email]. Desire is to limit max concurrent bmcweb sessions. Auth/nonauth connections. Server busy.
Intention: keep support for account lockouts, and add support for rate limiting so the BMC admin can use lockouts, rate limiting, both together, or neither.
Need to defend attacks against multiple interfaces: Redfish and IPMI -- will lockout and rate limiting happen for both?
RMCP+ could be enhanced to throttle via pam_tally2, but the design may not be straightforward because it does not rely on Linux-PAM.
How well does Linux-PAM and RMCP+ handle password guessing from simultaneous attacks?

8 Gerrit code review for “EventService: https client support”
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/31735/
No discussion.

9 PoC work for daemons' privilege separation
Use systemd features for privilege drop & sandboxing.
ANSWER: Anton debriefed efforts to make this work.
Running Linux processes as users created on-demand.
Hit problem: Systemd access check (not running root or capability sysadmin).
Solution approach: Partition processes into Linux groups. We believe a process in the same group will be able to send the message to another process in that same group, even when the processes have different effective userids and the sending process is not root.
Idea how to partition processes into groups: Create a group for network-facing processes to handle services such as network ipmi and bmcweb. This group would have access to the files it needs, but not have access to device files.
Next steps: List the daemon processes and characterize capabilities each of them need.
Joseph is interested in helping and adding this to the nascent OpenBMC threat model.

10 Heads up on alternatives to the filesystem overlay.
ANSWER:
Desire to move away from the overlayfs and use a better feature to handle mutable files.

Meeting held 2020-09-02:
1 Common Remote API for TLS certificate management?
b. Certificate management = installation, **rotation, revocation**
NO DISCUSSION. Leave on agenda.

2 Email: stable branches and security fixes - https://lists.ozlabs.org/pipermail/openbmc/2020-August/022762.html
DISCUSSION:
In the context on a downstream project using OpenBMC release 2.8.0 for a product, some of those product's customers read the OpenBMC release notes, e.g., https://github.com/openbmc/openbmc/wiki/Releases and become confused or concerned that the product was not built on top of a stable OpenBMC release. Specifically, the release notes uses the terms "stable" and "development" which implies "unstable". What can we tell such customers? What is the value in a release like 2.8.0? Can we tell customers "we are on 2.8+" which reflects that we are on stable release 2.8 and also some more commits were picked up.

For a downstream project in production, how do we relate this to OpenBMC fixes from other projects? How do we get common fixes?

3 Per 2020-08-05 meeting, how can we use security alerts from other repos? For example: https://github.com/openbmc/openbmc/security/advisories and all of the other github repos that building the OpenBMC project uses.
DISCUSSION: This is nice to have, but who will actually do the work? And how do we (as security incident responders) consume the list of alerts and apply them to our specific projects? That work is hard to share.

Idea: Tell downstream openbmc users what resources are available and how to find what vulnerabilities are written and how to get the fixes. Add this to https://github.com/openbmc/openbmc/security/policy as mentioned in the 2020-08-05 meeting.

Meeting held 2020-08-19:

1 Chris Svensson from Google presented GLOME: https://github.com/google/glome , and demonstrated the glome login protocol, and we discussed it.
This is a challenge-repsonse protocol similar to https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-16-12/fundamentals-xe-16-12-book/consent-token.html
Some of the items we discussed include:

- Subject to replay attacks.
- Similarities between the ephemeral key and one-time-use keys
- Using GLOME in dark sites. A typical dark site has a network, but does not have internet access. This presents difficulties in handling the challenge URL and response.
- The client side of the protocol is not sensitive to wall-clock time (but challenges may time out).
- When used on a BMC, the BMC does not authenticate the user. Instead, the glome server does that, and the BMC authenticates the response (which may include the user account name).
- Use a Linux-PAM pam_glome authentication module indratd of glome-login.
- Use GLOME with a Radius server.
- How GLOME could be used to replace BMC's password authentication vectors: serial, SSH, REST API Basic Auth, POST Redfish username+login to SessionService.
- How the web application (built on top of the Redfish and REST APIs) could use GLOME: Issue HTTP status 403 (forbidden) with a response that says "please use GLOME" and the link to GET the challenge, etc.

Other items were discussed that I just didn't take notes on.

Alternatives to this protocol were discussed. Here are the very basic ideas (and I apologise for mangling the details):

- IBM POC uses the BMC firmware image's public key (or equivalent) to validate login requests (which must be signed by the private key to be valid).
- Intel BMC: if there are no login credentials available, the BMC generates a key pair.

Please open issues in the globe repository.

At this point, there were 5 minutes left in the meeting, and we quickly covered the following 2 "boring" code reviews:

2 Gerrit code review: BMCWeb webUI login change:
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/35457

ANSWER:
There is some contention about whether this is the right direction. See comments in the review.
TODO: Joseph to agitate.

3 Gerrit code review: BMCWeb HTTP redirect to HTTPS:
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/35265
ANSWER:
This is pending tests and issue resolution. See comments in the review.

Bonus item 4 was added.
We did not get to item 4. It remains on the agenda for next time.

4 Common Remote API for TLS certificate management?
Certificate management = installation, **rotation, revocation**
DID NOT DISCUSS.

Meeting held 2020-08-05:
We discussed meeting emails and result emails. - Parth Shukla (timevortex@google.com) volunteered to do this starting next meeting.

1 Review GitHub / OpenBMC security policy.
https://lists.ozlabs.org/pipermail/openbmc/2020-July/022331.html
ANSWER: Sounds good.

2 How do we make our existing and new security advisories show up in https://github.com/openbmc/openbmc/security/advisories ? This gives our process to create security advisories:
https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md and here are GitHub's docs:
https://docs.github.com/en/github/managing-security-vulnerabilities/about-github-security-advisories
ANSWER: Sounds good.

3 Do we need a followup discussion to last meeting's "HTTPS site identity certificate" discussion based on the emails? Can someone summarize those email threads? :-)
ANSWER: The email thread consensus is good. Next steps: gerrit code review.

4 Large image uploads: Should we use Redfish-specified "multipart HTTP push updates" (that is, support the `MultipartHttpPushUri` property)? See Ed's comment in https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/34972 and in https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/30994. Are there other considerations?

ANSWER: Sounds good. Then we discussed a related topic: what images the BMC stores, how it updates those images, and vulnerabilities related to those choices. I did not record the entire conversation. This is what I got:
Discussed factory(aka golden)/primary/active/alternate images. An attacker who can boot from the golden image can exploit vulnerabilities known to be in the image.

5 Email: Call for BMC board vendors to collaborate with OCP security - https://lists.ozlabs.org/pipermail/openbmc/2020-July/022413.html
ANSWER: There was some interest and discussion about the definition of “platform” and about how to define the trust domains.

6 For next time (19 August): Chris from Google will talk about GLOME: https://github.com/google/glome
ANSWER: Parth introduced the Glome server for discussion next time.

- See ‘Read world applications’: https://github.com/google/glome/blob/master/docs/protocol.md

Real world applications

An example of a real-world scenario fitting the description above is authorizing a human operator to access a device with the following constraints:

- The device does not have a network connectivity (e.g. due to a failure or by design).
- The device does not have a synchronized time (e.g. no real-time clock).
- The device does not store any secrets (e.g. all its storage is easily readable by an adversary).
- The device accepts input from a human operator via a very low-bandwidth device (e.g. a keyboard).
- The device provides output to a human operator (e.g. via display).

With the constraints above, the operator effectively provides a low-bandwidth channel for the device and the authorization server to communicate by passing the messages back and forth. While there are ways to increase the bandwidth from the device to the operator (e.g. via matrix codes), we must assume that the opposite direction requires the operator to type the message manually on the keyboard, so minimizing the protocol overhead in that direction is crucial.

To address this problem, the GLOME login protocol based on GLOME was invented.

BONUS TOPICS not on the original agenda:

7 Surya: Can we have a new “security” label for GitHub issues and for Gerrit?
ANSWER: Yes.
Update 2020-08-06: Joseph created https://github.com/openbmc/openbmc/labels/security .

For gerrit reviews you can add any “topic” to your reviews and search by topic, for example: https://gerrit.openbmc-project.xyz/q/topic:%22security%22+(status:open%20OR%20status:merged)

8 Eric: CSIS (Cloud Security Industry Summit) wants feedback on improving BMC security. Meets every other wednesday (Aug 12) noon EST. Joseph volunteered to attend the meetings.

Meeting held 2020-07-22:
1 The OpenBMC interface overview is merged into the docs repository here: https://github.com/openbmc/docs/blob/master/architecture/interface-overview.md . Is there interest in building a threat model on top of this?
ANSWER: No discussion

2 Merged gerrit review: rework authorization flow:
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/30994
ANSWER: No meaningful discussion

3 Gerrit review: Firmware minimum ship level (can help with host firmware anti-rollback protection) https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-bmc-code-mgmt/+/29914
ANSWER: No discussion

4 Question: If BMCWeb finds an unusable HTTPS site identity certificate, it DELETES it and self-generates one. This has caused problems for certificates that are not valid until a future date. In general, what certificate management support should we have for BMCWeb? What is needed?
ANSWER:
There were two discussion threads: The BMC’s notion of time of day (TOD), and how BMCWeb should handle certificates.

Does the BMC have a battery backed TOD clock? Depends on BMC model. Can it validate if it has access to its NTP server (when configured)? Does the BMC know if its time was set correctly?

How does the BMC know if the BMC has the correct time? Have a BMC flag that says, “Look like the BMC TOD clock is not working.” Does the BMC know if we got a good time from an NTP server? Can we read the GPS signal? What is the industry solution?
Should the BMC store its idea of what date it is? So it can report if the time changes significantly. Or will this lead to a bigger problem? Is it better/simpler to check for TOD = beginning-of-era-1/1/1970? → start an email thread

BMCWeb configuration? Configure option: delete cert and generate self-signed -vs- use defective certificate. What is the purpose of deleting the unusable cert? Should “out of date”

not be part of the “unusable” definition? ⇒ Ideas: 1. If bmcweb finds a usable cert but is out of date, that cert can still be used. 2. Leave the defective certificate (do not delete it) and log an error.

The group consensus was that BMCWeb should treat its HTTPS site identity certificate like this:
1 certificate is perfectly good - Use the certificate
2 certificate is good but expired or not yet valid - Use the certificate and log a warning
3 certificate is missing or bad format or algorithm too old - Use another certificate or self-generate a certificate (and log that action)
There are no cases where BMCWeb should delete any certificate.

Next steps: discuss on email list, write patch.

5 Fuzzing. We briefly discussed the existing test infrastructure https://github.com/openbmc/openbmc-test-automation/ and previous calls for fuzzing.

NOTE: The host dropped during this discussion, and several participants left the call at that point. The call was continued a few minutes later in a more subdued fashion.

6. Can we fill out the information in https://github.com/openbmc/openbmc/security ?

Meeting 2020-07-08 - CANCELLED

Meeting held 2020-06-24:
1 Document privacy considerations? See comments in
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/32911
TODO: Joseph add to openbmc docs.

2 Dropbear release has new ciphers. The dropbear 2020.79 release adds new ciphers and drops older ones. Do we need to update our configuration, and which ciphers do we want?
https://matt.ucc.asn.au/dropbear/dropbear.html
ANSWER: Probably. Followup in the email list.

3 Do we want to create a new email for security announcements?
https://lists.ozlabs.org/pipermail/openbmc/2020-June/022040.html
ANSWER: We agreed this is a good idea if Joseph does all the work for it. To make it useful for subscribers, we need to moderate the content to actionable items (such as CVE fixes, significant security relevant configuration changes, and the like).
TODO: Joseph to move forward to the email list.

4 Are the **OpenBMC 2.8 security audit results** useful?
https://lists.ozlabs.org/pipermail/openbmc/2020-June/022085.html

DISCUSSION: Yes, the exercise has a benefit. It prompted some points for the release notes. It shows the facts (example: which ciphers are supported) and relates them to OpenBMC project defaults. This can help downstream projects understand security aspects of the BMC code when they consume it.
Consider replacing partitions of the custom shell script with open source tools such as:

- Lynis https://cisofy.com/lynis/
- Vulscan https://github.com/scipag/vulscan
- testssl.sh https://github.com/drwetter/testssl.sh

5 We are using PLDM (https://github.com/openbmc/pldm) over MCTP (https://github.com/openbmc/libmctp). Is there interest in SPDM? https://www.dmtf.org/content/dmtf-releases-security-protocol-and-data-model-spdm-architecture-work-progress
ANSWER: Yes, and SPDM is new.

Meeting held 2020-06-10:
1 See NIST SP 800-63B appendix A. Can we follow NIST simplified password guidelines? Some of our users are having trouble choosing passwords that pass the pam_cracklib requirements. Appendix A.3 “Complexity” suggests enforcing password complexity is not helpful. Can we remove complexity requirements and have only length requirements? https://github.com/openbmc/openbmc/blob/master/meta-phosphor/recipes-extended/pam/libpam/pam.d/common-password ← For discussion (not yet a proposal).
ANSWER:
Joseph mentioned users stumbling over complexity rules, for example, pw=0penBmc1234 has a pattern (too many digits in a row) but 0penBmc123 is accepted. The group consensus: leave defaults as-is. Integrators can configure whatever rules they want in the Linux-PAM common-password pam_cracklib module.
Additional discussion:
There is a bmcweb patch to say why pw was rejected. It is waiting for a better message to send back to the REST API user. https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/27503
What about non-latin characters in the password? How well does pam_craclib handle those?
We discussed the ipmi 20 char limit. TODO (joseph): Check message sent for ipmi 20 char limit.
Multiple steps may be needed to add an existing user to the ipmi group: no user interface to add/remove user from ipmi group, but backend support exists. When adding user to ipmi group, you need to change the password so the encrypted password gets stored in the ipmi file.
One of the (recent) gerrit reviews in this area suggested: if user changes pw>20 chars, that auto-removes user from ipmi. We agreed that seems like a bad idea.

2 Email proposing new Redfish ServiceRep role and privilege - https://lists.ozlabs.org/pipermail/openbmc/2020-June/021948.html
ANSWER:

Joseph touched on highlights of the new Role, privilege, and use cases for open systems vs enterprise systems. The details are explained in the original emails. Joseph will move this proposal forward to Redfish.

3 Idea: Build an OpenBMC threat model on top of the RunBMC spec (https://dropbox.tech/infrastructure/runbmc-ocp-hardware-spec-solves-data-center-bmc-pain-points). <-- Previous efforts toward an OpenBMC threat model are in the wiki: (https://github.com/openbmc/openbmc/wiki/Security-working-group#where-to-find-more-information). One difficulty was to describe what a BMC is, as no specs are publicly available and BMC's are abstract. It seems like the RunBMC spec solves this problem as the RunBMC spec is similar to the BMC models actually supported by the project (examples: ASPEED AST2x00 and Nuvoton models). => Even if we had no intention of supporting RunBMC, would it be worthwhile to create a threat model based on OpenBMC running on RunBMC that would cover the BMC/host interfaces?
ANSWER: This seems worthwhile. Add to the security wiki wish list. DONE: https://github.com/openbmc/openbmc/wiki/Security-working-group#model-openbmc-security-functions

4 Input to OpenBMC 2.8 release? Ref: https://lists.ozlabs.org/pipermail/openbmc/2020-June/021918.html
ANSWER: Publish security audit results for release notes? There was no discussion.

Meeting held 2020-05-27:
1 We talked about the OpenBMC Security response team's recent responses. (No specific problems or responses were mentioned.)
2 (Joseph) Talked about a Service login idea and the requirement to exclude admin access from service functions. We agreed for the OpenBMC project to have a new ServiceRep role. This might be a Custom Redfish role.
We discussed some related issues we need to solve to move forward:

- Move away from root login, and create an admin user. Agreed.
- Admin (ConfigureUsers privilege) should control which users get ssh access.
- A related issue is https://github.com/openbmc/openbmc/issues/3383 Daemons should not run as root.

Joseph to send email followup with the proposal.

Meeting held 2020-05-13

1 Decided to hold the security working group meeting regardless of concurrent OCP virtual summit.

2 Discuss SELinux email use cases -
https://lists.ozlabs.org/pipermail/openbmc/2020-April/021477.html

Manoj led us through SELinux email use-cases. SELinux can help control access so we (OpenBMC contributors) restrict access to those processes that should have access:

(Joseph disclaimer): I tried to summarize the use cases as Manoj walked through them. This is a summary only. Please refer to the email chain.
Use cases:
2-1 NBD (network block device) is used to offload dumps on POWER systems. It reads from PLDM source and writes to NBD device. Control who has write access to the NBD device.
2-2 All processes running root can write to config files under the /etc directory.
2-3 All processes can control use of systemctl command.
2-4 All processes can write to the journal (journald).
2-5 All processes can use network tcp and udp ports - port-based firewall capability.
2-6 D-Bus service names (paths under /xyz/openbmc_project/*)
2-7 D-Bus message passing - hardening D-Bus communication
2-8 Map existing roles (Administrator, Operator, etc.) to SELinux. Assign SELinux label based on ingress vector (serial line vs SSH vs REST login). Uses PAM-selinux config files.
2-9 System calls. For example, disable ptrace.
2-10 Run user executing capabilities. executables only from specific paths, for example, don't allow running programs from /tmp

Next steps: Compare AppArmor vs SELinux. Consider Cost/benefit.
- Prioritize the benefits (as listed above).
- Consider costs including: developer time (person-months), BMC resources (flash size and memory requirements, BMC performance).
- Also consider the cost of future development, for example consider the complications for a developer who is not skilled in security practice: adding a security-relevant function (or entirely new service) or adapting a service for different use cases. They can either struggle with getting the security controls correct, or accidentally create a security hole.

U-Boot focus: Interaction between SELinux and U-Boot (commands like fw_setenv)? For example: functions for factory reset and select BMC boot source (such as for BMC firmware update) use the fw_setenv command (or underlying mechanism). Are these functions the only ones who should be allowed to access the fw_setenv function?
Related side topic: Protect unattended BMC boot. Can we harden U-Boot itself?

Anton is considering an alternative to apparmor and selinux: KRSI: Kernel Runtime Security Instrumentation

Next steps: prioritize which benefits we want. Followup in email.

3 Experimental bmcweb prototype for authentication rate-limiting
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/31841
Joseph briefly walked through the review and talked about Linux-PAM issues and alternatives like pam_abl.

4 Added links to OpeBMC Threat Model docs to the security wiki
https://lists.ozlabs.org/pipermail/openbmc/2020-May/021551.html

5 Fwupd tool support - https://lists.ozlabs.org/pipermail/openbmc/2020-May/021573.html.

6 Requirements for crypto deprecation? - That is, allowing the BMC admin to disable ciphers
https://lists.ozlabs.org/pipermail/openbmc/2020-May/021619.html
Drawbacks: implementation cost. For example: do we try to prevent the admin from removing all supported algorithms so that are none left to connect to?

7 Requirements for security audit log -
https://lists.ozlabs.org/pipermail/openbmc/2020-May/021640.html
Joseph walked through the email.
After the meeting: Can we work this into the approved audit log design?
https://github.com/openbmc/docs/blob/master/designs/phosphor-audit.md

8 (Bonus topic) We need a better meeting time for India, Zurich, and others
Joseph: will revive email thread - DONE: see
https://lists.ozlabs.org/pipermail/openbmc/2020-May/021641.html

Meeting held 2020-04-29:
1 Cancel next week? OCP Virtual Summit - Skip May 13 meeting?
https://www.opencompute.org/summit/global-summit
ANSWER:
We'll decide later.

2 IPMI over DTLS. IPMI over DTLS https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/31548 - create a new de-facto protocol to address (1) weak crypto algorithms and (2) the need for the server to produce cleartext passwords. Doing so, plus retiring all previous protocols (RAKP cipher suites 3 and 17) would remove much security weakness from network IPMI. (This will not address other limitations, for example, single byte values limit IPMI to 255 sensors.)
https://lists.ozlabs.org/pipermail/openbmc/2020-April/021255.html as part of a more general "ipmi password" thread, with the anchor message in the archive here:
https://lists.ozlabs.org/pipermail/openbmc/2020-April/021232.html
ANSWER:
Still working in the email list. Vernon is still working on design.

3 Security audit logs. Handling security audit logs. The Redfish logging service has an API to delete logs or selected log entries. What should happen for audit logs?

c. Should we allow the Admin to clear audit log entries? Clearing defeats the purpose of the log. Is there a use case to allow audit logs to be cleared?
d. Alternatively, should clearing the audit log just add an entry that says “admin X cleared the log”.
e. Or really clear the log but store it on the BMC in a form accessible only by the ServiceRep?
f. Both the ServiceRep and a security auditor will want to see all the log entries and never be informed that someone deleted entries.

ANSWER:
There was general agreement to enhance OpenBMC with a special purpose security audit log (versus scraping security items from the logs from various services). And there is no reason to allow the security logs to be cleared.
There were questions about if clearing the security log should survive a factory reset; no they must be deleted in that case. Ideas: Add an entry in the security logs after logs are cleared to indicate the logs were cleared.
There was a question about storing the log locally on the BMC’s flash vs sending it to a remote logging service. Joseph indicated security logs could use the remote logging service just like any other kind of log.

4 How to use mTLS. More questions about how to use mTLS for HTTPS bmcweb:
https://lists.ozlabs.org/pipermail/openbmc/2020-April/021361.html
ANSWER: Contact the authors of the patch that created the mTLS feature, and ask them.
TODO: Joseph - Followup May 6: I waited too long and Zbig sent the email:
https://lists.ozlabs.org/pipermail/openbmc/2020-May/021547.html

5 Rate limiting. Joseph presented ideas to rate-limit Redfish authentication failures because he doesn't like lockouts. https://redfishforum.com/thread/311/rate-limit-authentication-attempts
ANSWER: The concept was favorably received and there were discussion around the topic including lock-out vs rate-limits, creating an account enumeration vulnerability, progressively longer lockouts, existing pam modules such as pam_abl, and what layer inside the BMC this would go. Joseph intends to push an experimental BMCWeb patch.

6 Dropbear SSH ciphers. Is there interest in reviewing dropbear SSH settings? Example:
https://github.com/mkj/dropbear/pull/94
ANSWER: Yes, and we should review which ciphers to drop because they are no longer considered strong.

7 OWASP dependency checkers. Use OWASP dependency checker -
https://lists.ozlabs.org/pipermail/openbmc/2020-April/021426.html
ANSWER: (The discussion was not recorded -- sorry -- allergies. I think the next item covers it.)

Agenda item added during the meeting:

8 What do we do for dynamic scans? Some scanners are privately licensed and the output of them is copyrighted which means it cannot be shared with the OpenBMC community.
ANSWER:
TODO: Joseph will writeup the paradigm for running scanners that produce copyright reports and add that to the security wiki.
Some examples of scanners used by community members include: Nessus, HCL AppScan and ASoC.
OpenBMC is a Linux Foundation project. Can we get access to scan tools from that? (Ask Kurt Taylor.) Synopsys: https://www.synopsys.com/software-integrity/security-testing.html Snyk: https://snyk.io/product/ scan tool.
What environment to run the tests? Private resources? CI systems?
New usage pattern: can we share the results from the scan tool?

Meeting held 2020-04-15:

1 Remove default private image signing key from openbmc - https://github.com/openbmc/openbmc/issues/3615
ANSWER:
Note: There may be two different signatures: Signing for development images vs production images.
We may want an un-signed image, for example, to sign via HSM after the Yocto build.
Alternate signing processes: If using a separate signing service (like using a HSM) happens after yocto bitbake build, then how do we get the public key into the image. IBM has open sourced this approach as part of open-power consortium.
Wrinkle: When the image signing process is separated from the build process, we need to insert the public signing key into the image.
Idea: Disable the recipe that signs the image, leaving it as an example.

3 [discussed out of order] Which algorithm should sign OpenBMC images? More generally, input to https://github.com/openbmc/openbmc/wiki/Security-working-group#security-end-of-release-checklist or email about OpenBMC audit tool, archived here: https://lists.ozlabs.org/pipermail/openbmc/2020-April/021193.html
ANSWER:
Yes, worth discussion. Followup in email list. TODO: Joseph
Not clear which algorithm to choose.

2 Discuss issues from the “ipmi password storage” email thread. The initial email in that thread is archived here: https://lists.ozlabs.org/pipermail/openbmc/2020-April/021232.html
ANSWER:
We discussed most of the ideas from the email thread.

Also: If the BMC has a TPM available, can we store the RMCP+ private key there? And use that as part of a TrustZone?

4 (Ofer) Use Yocto CVE as vulnerability scan for OpenBMC repos - https://www.cvedetails.com/google-search-results.php?q=openBMC&sa=Search
ANSWER:
Idea is to run the Yocto cvecheck command as part of OpenBMC's CI.
Intel runs something like this in their private CI, and handles results.
Do we do this in the project level Jenkins jobs? Suggest: a nightly build will generate a report.
See also minutes from **2019-07-24.**
Can invoke something like, via: bitbake -c cvecheck obmc-phosphor-image
Followup in email.

Meeting held 2020-04-01:

1. SELinux or AppArmor integration status & plans - see email by Anton Kachalov: https://lists.ozlabs.org/pipermail/openbmc/2020-March/021059.html
    a. Would also want to move away from all processes running as root. https://github.com/openbmc/openbmc/issues/3383
        i. TODO for 3383 - create issue for each repo. Note that BMCWeb has tried this ⇒ Corrected 2020-04-03 via email: Work out technical issues, then ask all daemons to move away from running as root.
    b. Criteria for selecting SELinux or AppArmor. SELinux was first. AppArmor is easier to deploy. Needs work to decide.
    c. There is interest, but no active work.
2. Admin-controlled security settings -- Discuss plans for BMC admin-controlled security settings. See IBM's plans here: https://github.com/ibm-openbmc/dev/issues/612 . Access per NIC. Disable ipmi cipher 3. -- there are a few changes and clarifications from issue 612
    a. Can control each NIC individually. Example: data-center wide network, vs, private management network.
        i. Users can control which network ports they plug cables into.
        ii. Users can control which of the BMC's NICs that bring up. There are existing REST APIs for that.
        iii. Shared NICs?
    b. With each NIC, can control which services are offered:
        i. For example, how can we provide oob RMCP+ service to a private network, but not to the data-center-wide network.
        ii. ANSWER: OpenBMC does not have a mechanism to do that in the general case. For example, REST APIs to directly model if service X is enabled from network Y.

iii. For the near team (a year), we'll work on allowing the admin to disable and enable services. But we won't be able to discriminate based on which network is using the service.
iv. Use case: IPMI access (SSH Access, etc.) allowed from host-NIC but not from management interface. Limiting access to IPMI per NIC is a higher priority, compared to other services.
v. How to design/implement? Does OpenSSH offer a way to do this?
vi. Asked Redfish about direction for channel based restrictions. This is copied from OpenBMC security WG notes (below) 2020-02-19 entry: https://redfishforum.com/thread/279/channel-privilege-support-direction-redfish ANSWER: Redfish direction is to NOT change Role based on channel, and suggests implementations can offer a different set of accounts based on ingress channel (for example, based on which ethernet device (eth0, eth1, etc) the accessed the BMC).

c. Can control: allow admin to block KCS or BT commands, also IPMB -- That is, allow the admin to disable those bridges or protocols. As far as I know (Joseph) this is a new request.
d. Want to allow the admin to disable RMCP+ cipher suite 3, leaving only 17. Is there an IPMI command to do that? Is it implemented in OpenBMC?
e. Note: difference between OOB network IPMI access -vs- inband IPMI -- should be separately controllable.

3. James created a google spreadsheet to track problems reported to the OpenBMC security response team (SRT). This is private, and access is given only to the SRT members See https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md

Meeting held **2020-03-18**:

1. Certificate dates beyond 2038 - https://lists.ozlabs.org/pipermail/openbmc/2020-March/020906.html ⇒ Wait for glibc or whatever.
2. Emergency shell (BMC boot failure) password - https://gerrit.openbmc-project.xyz/c/openbmc/meta-phosphor/+/30260 ⇒ Do not merge this. Discussed use cases for the BMC COM ports. Are UART pins removed? Are the resistors removed? Are any other ports used?
3. (Joseph) end-of-release scans - https://lists.ozlabs.org/pipermail/openbmc/2020-March/020924.html ⇒ Go head and email the shell script. It sounds useful. We discussed if it would help attackers more than it would help us. Ideas:
    a. Also check if AHB bridges are disabled (CVE-2019-6260)
    b. Run CHIPSEC on BMC/arm. Then work toward adding it to our Jenkins/CI.
4. (Nancy) OCP wants to publish BMC firmware feature requirements. Ideas:

    a. OpenBMC working with OCP security.
    b. Can we publish use cases together with their security requirements?
    c. Use cases for:
        i. Data center owner-operator, vs third party use (bare metal rental). Recovery, firmware validation, downgrade protection. Unique bmc id. Shared TPM between bmc/host.
5. Discuss progress in fixing older items ⇒ Send emails to the maintainers with a call for action. TODO: Joseph
6. Discuss priorities for 2020 ⇒ No discussion (and out of time)

Meeting held for **2020-03-04**:
(Agenda item 4 was discussed first.)
There was a communication problem near the start of the meeting. The audio failed and recovered and the meeting may have failed for some users.

1 (Joseph via email): New Redfish roles ServiceRep & OemRep - https://lists.ozlabs.org/pipermail/openbmc/2020-February/020540.html
DISCUSSION:
I (Joseph) think we agreed that ServiceRep and ManufacturingRep Privileges are useful to articulate. We discussed if this should go into the Redfish spec or be an OpenBMC OEM thing.
I (Joseph) think we have to first try to get it into Redfish before considering an OEM extension.

For reference: See the Redfish spec DSP0266 > Security details > Authentication > Privilege model/Authorization > Roles:
https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.8.0.pdf

There are two use cases:

Use case 1: The BMC admin is also the ServiceAgent and the ManufacturingRep. In this use case, the Administrator role could include the ServiceRep and ManufacturingRep Privileges.
I (Joseph) think we need to support this use case.

Use case 2: The system manufacturer, service organization, and owner/admin are all separate entities. This design is an attempt to articulate these separate roles.

- The Administrator role does not include either the ServiceRep or ManufacturingRep Privileges. The admin should be locked out of service.
- The new ServiceRep role includes the same privileges as the Operator role, plus the ServiceRep privilege.
- The new ManufacturerRep role includes the same privileges as the Operator role, plus the ServiceRep and ManufacturingRep privileges.

In both use cases, the BMC admin retains the ConfigureUsers privilege which means they have control over all accounts on the BMC, and the new roles do NOT have this privilege.

The ServiceRep privilege is required to perform the following operations:

- Operations involving FRU replacement, for example, calling an API to re-enable a locked out field replaceable unit (FRUs) after replacing a defective unit.
- The ServiceRep may be called upon to restore access to an admin who is locked out of their account. For this to work, the admin would set up a ServiceRep account and leave it enabled all the time. (Naturally, this may be a way for the ServiceRep to escalate privilege to Admin.)
- The ServiceRep may need to diagnose and recover a malfunctioning BMC which may involve more than merely factory reset.

The ManufacturingRep privilege is required to perform the following operations:

- Put the system into stop-on-error mode, so the manufacturing process can validate the system had no errors (as contrasted with tolerating errors or failed-but-still functional units) at the time the system was manufactured, or similar testing modes.
- Set Media Access Control (MAC) addresses, and similar data.

An open issue/problem with the approach outlined here is well-known to Redfish: the BMC admins can create a ServiceRep account for themselves, and thus escalate their privilege. A good solution for that was not proposed. One idea is to allow ServiceRep access only via mTLS where the BMC admin installs the public cert in the BMC which accepts only certificates that have a signature accepted by the BMC firmware. Since the Manufacturer controls the firmware image, it also controls who gets ServiceRep access. (This idea is not yet fully formed.)

Nevertheless, separating the Service and Manufacturing Roles and Privileges seems like a step in the right direction.

We discussed an alternate design (also referenced in the email thread) where the BMC is put into a mode that allows additional operations related to servicing and manufacturing the system. This is already implemented in OpenBMC. My feeling (Joseph) is this design does not follow the Redfish spec and is not as clean. For example, who controls what mode the system is in?

We discussed an alternate approach. Create a super-admin role that can create regular Admin accounts and ServiceRep accounts. This design separates the user world from the service world. However, then you have the problem of who controls the super-admin account: the customer or the manufacturer. My feeling (Joseph) is that security sensitive customers (for example, processing HIPPA or PCI-DSS data) would not want an account on their system they could not control.

2 (Joseph email): Implement the Redfish PasswordChangeRequired property
https://lists.ozlabs.org/pipermail/openbmc/2020-February/020554.html

DISCUSSION: This is work in progress. Joseph is working on a phosphor-user-manager D-Bus property to retrieve the “UserPasswordExpired” boolean fact so it can be used within BMCWeb and exposed as the equivalent Redfish property.

3 (Joseph email): delete BMCWeb sessions after some kinds of account changes
https://lists.ozlabs.org/pipermail/openbmc/2020-February/020555.html
DISCUSSION: This sounds like the right direction. Next steps: create a design or propose changes. Any volunteers?

4 James: Intel hackathon (pen test, code reviews, etc) results
DISCUSSION:
Intel held an internal security hackathon and is ready to share the results. What is the right way to present these to the OpenBMC community?
Answer: See the openBMC security working group wiki > link to Report an Issue > https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md
Use your best judgment if the problem can be simply reported via the open email list, or whether to report it via the openbmc-security email list.
We discussed renaming the OpenBMC project’s security response team to “Project Security Incident Response Team” (PSIRT) to be more consistent with member companies usage.

5 BMCWEB_ENABLE_DBUS_REST=ON enables information leak
https://github.com/openbmc/bmcweb/issues/114
DISCUSSION: The consensus is: def default should be OFF, but wait for code that currrently uses these APIs to migrate to the replacement Redfish functions. Specifically, the webui and automated tests should be working. See the discussion in the code review comments (https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/29344) for details.
We want to understand the timeline for changing this default and definite plans for moving forward; for example, an email stating the goals and timeline.
How to document the vulnerabilities? The BMCWeb config file (https://github.com/openbmc/bmcweb/blob/master/CMakeLists.txt)
BMCWEB_ENABLE_DBUS_REST option links to the docs:
https://github.com/openbmc/docs/blob/master/rest-api.md
The BMCWeb config file or docs should mention the risks of enabling this set of interfaces.
How to determine which BMCWeb flags were used? Scan the BMC for the presence of the URI associated with that option. For example, when authenticated as the admin, curl -GET /xyz/openbmc_project will succeed only when BMCWEB_ENABLE_DBUS_REST=ON.

6 (Chatter in IRC): Input to May 2020 release planning per https://github.com/openbmc/openbmc/wiki/Security-working-group#security-end-of-release-checklist
DISCUSSION: Joseph will send an email to the list with ideas for a very basic security scanning tool (per the end of release checklist) to report facts about a running BMC that are needed for security audit. The idea is to put the tool into https://github.com/openbmc/openbmc-tools/ , run

it for each release, and tighten up any security areas needed. A counter argument is that the tool would give bad actors information about security weaknesses in the OpenBMC project….but we would fix any items we find before adding them to the tool.

Meeting held **2020-02-19**:
The first 7 agenda items were covered. The remaining items will remain on the agenda for next time.

1. (Joseph): Is OpenBMC affected by the Chrome browser's SameSite cookie changes (https://blog.chromium.org/2020/02/samesite-cookie-changes-in-february.html)? Do we want to enhance BMCWeb (https://github.com/openbmc/bmcweb/blob/master/include/token_authorization_middleware.hpp#L430) to create cookies with `SameSite=None; Secure` when BMCWEB_INSECURE_DISABLE_XSS_PREVENTION is also used, to allow the BMC to be used by the Chrome browser. Perhaps by default BMCWeb should generate cookies with `SameSite=Strict`?
    a. ANSWER: Don't know, didn't discuss in depth. Joseph created bmcweb issue 115. https://github.com/openbmc/bmcweb/issues/115
2. (Joseph, follow up to agenda item 3 from 2020-02-05): Redfish Privilege updates: https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/28881 and https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/28878 Update Feb 11: See https://redfishforum.com/thread/281/manageraccountcollection-change-allows-account-enumeration clarified the intention to NOT enumerate all accounts (unless you are the admin)
    a. ANSWER: Consensus was to leave OpenBMC as-is (only admin can enumerate users) until Redfish releases a new spec.
3. (email) FYA. BMC aggregator - includes a security topic. https://lists.ozlabs.org/pipermail/openbmc/2020-February/020433.html
    a. ANSWER: Nancy plans to follow up.
4. (email) FYA - BMC Secure Boot / U-Boot - use dm-verity or alternate IMA? https://lists.ozlabs.org/pipermail/openbmc/2020-February/020452.html
    a. ANSWER:
        i. Need BMC threat model to understand what threats dm-verity protects against. Note that integrity protection is a defense in depth against an attacker who can run code on the BMC which writes to the BMC's file system.
        ii. Is the BMC filesystem writeable? ANS: It uses read-write overlay filesystem on /etc. Idea: Could discontinue using overlays and use soft links to fs on read-write partition.
5. Redfish forum question: Direction for channel based restrictions - https://redfishforum.com/thread/279/channel-privilege-support-direction-redfish
    a. ANSWER:

        i. Redfish direction is to NOT change Role based on channel, and suggests implementations can offer a different set of accounts based on ingress channel (for example, based on which ethernet device (eth0, eth1, etc) the accessed the BMC).
        ii. OpenBMC community may have multiple use cases where either the mgmt network or host is more secure, and the other is less secure.
        iii. Idea: expose the list of channels within OpenBMC, and allow Account-Channel associations. For example, an interface to allow "admin2" to access the BMC only from "eth0" or "eth1" but not "eth2".
        iv. This topic is related to Redfish host-based authenticated access.
6. (Bruce via email): BMCWeb Cert valid for 10 years - https://lists.ozlabs.org/pipermail/openbmc/2020-February/020488.html
    a. ANSWER:
        i. Change BMCweb's default self-signed cert to 825 days. Recommend 30 days.
        ii. If BMCWeb starts with and generates a self-signed cert, and it is not replaced, and the BMC's time is sane, the browsers that connect to BMCWeb will start to complain after 30 days. The recovery is: The BMC admin should install a valid BMCWeb site identity cert, then clients can re-connect to the BMC. (This will serve the updated cert and make the browser happy.)
        iii. The "BMC Admin guide" should talk about installing your own cert.
        iv. See https://github.com/openbmc/bmcweb/#configuration and https://github.com/openbmc/bmcweb/blob/91243c3b28b1df66e682f5a3ee96341fdc516b5a/include/ssl_key_handler.hpp#L205
        v. Will there be a warning for the BMC admin? (And don't rely on a warning from the browser itself.)
7. (Joseph / James / Richard email): Rate limiting, use pam_abl - https://lists.ozlabs.org/pipermail/openbmc/2020-February/020430.html
    a. ANSWER:
        i. There was concern about any account lockout mechanism locking out legitimate users; throttling is safer.
        ii. Next step is to design how this would be used.

Meeting 2020-02-05:

1. Followup from previous meeting - Joseph: Review review initial Security Assurance Workflow. How do we know we are covering all the areas we should be?
    a. I propose the first candidate item on this list: How to balance the ability of an attacker to guess user passwords (brute force) against the response of the BMC (account lockout vs slow responses). I am interested in both:
        i. How we relate this conversation to the OpenBMC security assurance work so we can find it later. See

https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/28213/3/security/denial-of-service-considerations.md

ii. The direction we should go to solve this problem. It is clear that OpenBMC should implement a delay for auth failures and not account lockouts. Or should we have a design?

b. Do we want to list areas we think are high priority? YES - we started, see below.

c. DISCUSSION: The list of assurance schemes is a good start. The next step is to apply it to OpenBMC and work out how to proceed. I (Joseph) didn't record all of the questions, but many related to specific security areas that we would cover, how we plan to move forward, if or how we would cover ALL security assurance areas. In particular, it seems important to come up with a threat model (that covers the architecture, interfaces, actors, risks, and threats to an operational BMC) as one of the higher priority items to cover. The initial list of areas can include:

i. Secure boot - work in progress including links to design and implementation, user docs for signing and key handling, etc)

ii. CWE-307 brute force password guessing balanced against denial of service.

iii. Transport Layer Security (TLS) - security features already present in BMCWeb

iv. Threat modeling

2. Emails about BMCWeb intermediate site identity certificates - https://lists.ozlabs.org/pipermail/openbmc/2020-January/020321.html

a. DISCUSSION: Next steps are to try this, push up an enhancement if needed, and document how users can provision the BMC with their intermediate certs

3. BMCWeb privilege changes for account management: https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/28881 These allow anyone with Login privilege to "enumerate usernames" as in CWE-200. Do we care? I think so Should we ask Redfish to change the standards to disallow this?

a. DISCUSSION: One other person was concerned. Post to the Redfish forum: https://redfishforum.com/thread/281/manageraccountcollection-change-allows-account-enumeration

4. Email address CWE-307 via rate-limiting authentication attempts. https://lists.ozlabs.org/pipermail/openbmc/2020-February/020429.html

a. DISCUSSION:

i. The project currently has no such protection, so this seems like a good approach.

ii. Have we considered blocking by IP address? Considered progressively longer timeouts? Considered the pam_abl module or PAM modules that require MFA?

iii. If an LDAP server is used, it may not allow enumeration of its users, which would make this a non-issue for this use case. Does this apply only to local users?

        iv. There are various disparate use cases including: rate-limiting (as proposed here), account lockouts (traditional pam_tally2 solution), password reset required, and notifying the admin … just to name a few use cases. I (Joseph) am going for a default least-common-denominator solution into the project that the BMC can provide without requiring additional elements such as 2FA servers.
5. Joseph: alternate meeting times (initial email): https://lists.ozlabs.org/pipermail/openbmc/2020-January/020335.html
    a. DISCUSSION: Joseph will followup in the email list. I (Joseph) think an early morning (like 2am CDT) would work for Australia, China, India, and Europe. (See subsequent emails.) The next step is to identify core individuals and set up a meeting time.

Meeting 2020-01-22 held:

1. (From previous meeting): Discuss BMCWeb's certificate handling, specifically intermediate certificates. See https://github.com/openbmc/bmcweb/#configuration
    a. Other web servers have directives to concatenate the intermediate certificates (excluding the root CA certificates) and send that. What does BMCWeb do?
        i. What is the default? Self-generated private key? public cert? concatenated?
        ii. Need better docs for BMCWeb, for example: How to replace BMCWeb site cert? Okay to concatenate intermediate certs? TODO: Alexander will investigate and email.
2. Design discussions about aggregation broached the security topic : https://lists.ozlabs.org/pipermail/openbmc/2020-January/020142.html
    a. We are not sure what security help is needed.
3. Per Alexander: Revisit Daemons should not run as root - https://github.com/openbmc/openbmc/issues/3383
    a. There is definite interest. Who can work on this? Possible initial goal: convert bmcweb so it runs as a non-root user. BMCWeb is selected because it is higher risk because it implements a network interface.
4. Merged BMCWeb commit to allow slower image uploads: https://github.com/openbmc/bmcweb/commit/2b5e08e2915d886655a78aaabff40745dca6b517 See also commit: 0e1cf26b1cd98e0ec069e6187434fcabf1e9c200 "Make the max http request body size configurable".
    a. Minimal discussion.
5. Merged BMCWeb commit that added new messages for security events: https://github.com/openbmc/bmcweb/commit/8988dda41319950476ebb146df06c2e7b3fbf44d
    a. Minimal discussion.
6. Joseph: How do we bring security assurance work into the OpenBMC project? Is there interest in considering Protection Profiles that apply to OpenBMC? We can use these as

a systematic way review security topics. For example, the Operating System Protection Profile (OSPP) talks about cryptographic functions, audit logging, network security, secure boot, etc. The Virtualization Protection Profile (VPP) considers the BMC to be part of the platform management system.

a. There was agreement that these security schemes are good starting points to use as a guide. Other applicable schemes include Common Criteria and Center for Internet Security (CIS) . (Joseph after the meeting: We had previously discussed OWASP.)
b. There was agreement for the following idea. Do this in the Security wiki: (1) Reference the representative security schemes. (2) Use them to generate a list of topics. (3) Prioritize the importance of each area.
c. From there we can explicitly prioritize cost/benefit, file defects against the project, etc.
d. DONE (Joseph) - Added new "Security Assurance Workflow" section - https://github.com/openbmc/openbmc/wiki/Security-working-group#security-assurance-workflow

Meeting held 2020-01-08:

1. Gerrit review: Overview of BMC interfaces which either (1) someone might want to dynamically enable or disable, or (2) form an interesting part of the BMC's attack surface. https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/27969
    a. We briefly reviewed this. The consensus was that this doc would be useful and mergeable. The discussion of the BMC-host physical interfaces needs work.
2. Gerrit review: Prompted by IRC #openbmc discussion: Idea: List applicable security standards and best practices which might apply to OpenBMC for folks who want to use OpenBMC in their higher-security project which needs to meet security standards.
    a. See https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/28207
    b. TODO (Joseph): This should be merged into the "Security assurance wish list", "best practices from upstream projects", and "keep learning" in the OpenBMC security working group wiki (https://github.com/openbmc/openbmc/wiki/Security-working-group).
    c. We briefly reviewed this: The consensus is that the material that relates directly to the BMC seemed worthwhile keeping.
3. Review composition of the openbmc-security email list per https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md#team-composition-and-email-maintenance
    a. Some changes to the list were made. No discussion.
4. Code review to redirect HTTP to HTTPS (via nc netcat) - https://gerrit.openbmc-project.xyz/c/openbmc/meta-openpower/+/28099 This is currently scoped to OpenPOWER; can it be moved to meta-phosphor (as an IMAGE_FEATURE? Are there security concerns with adding the "netcat" (nc) command?

    a. We briefly reviewed this: Corrected link: (https://gerrit.openbmc-project.xyz/c/openbmc/meta-phosphor/+/28257). There were questions about:
        i. The use case for this.
        ii. This is a new attack vector for volume-based attacks (either many requests or very longer headers) and netcat (nc) application protocol based attacks.
        iii. Can we run as non-root (but still have the capability to listen at port 80).
        iv. All of the sed and awk commands.
    b. I understand this is currently planned as a bitbake recipe which platforms will have to enable, if they want it.
5. Gerrit review: Denial of service (DoS) considerations - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/28213 (Joseph:) Specifically, I want to know if this is mergeable, and I want to start with the BMCWeb rate-limiting defences.
    a. We briefly reviewed this: The general consensus was to abandon this review and move the material into the BMC threat model and network threat model (https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md). Also, the review talks about the host as a threat vector; this should be recharacterized as platform-level threats (for example, including threats from the host and PCIe cards, etc.).

Meeting on 2019-12-25 is cancelled.
Cancelled

Meeting held on 2019-12-11:

1. BMCWeb patch to allow BMC admin to disable authentication methods - https://github.com/openbmc/bmcweb/commit/78158631aeab5b77ea9a5f566508285cb839fadf
2. Gerrit code review to “Provide feedback from Linux PAM about why the new password is not accepted” - https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/27503
3. Gerrit code review to “lockout a user account for 5 minutes after 5 login failures” - https://gerrit.openbmc-project.xyz/c/openbmc/meta-phosphor/+/27527 and email https://lists.ozlabs.org/pipermail/openbmc/2019-December/019726.html
    a. Yes, abandon this. Have delay after unsuccessful auth. Follow OWASP guidelines for security practices. TODO: Joseph will write up design points in new review package.
4. Gerrit code review to implement the Refish ConfigureSelf privilege correctly, which lets non-admin users change their own password and log out of their own sessions. - https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/27595
5. Email about TFTP vulnerabilities: https://lists.ozlabs.org/pipermail/openbmc/2019-December/019725.html

TFTP. MITM downgrade attack. Perhaps this is lower priority because of mitigating circumstances: digital signatures checked at download time and (future) at boot time.

Do we need a NetBoot capability for a recovery mode?

The discussion went into firmware upgrade and downgrade scenarios:
See https://tools.ietf.org/html/draft-ietf-suit-architecture-08#section-3.4
We discussed the "full" firmware image being composed of multiple smaller pieces (BMC, host, etc.) and some of those components may be updated by the host via PLDM.

See also: text in the SUIT CBOR Manifest -
https://tools.ietf.org/html/draft-ietf-suit-manifest-01

Idea: Use the firmware package's manifest's version to detect downgrades.
Idea: Add a capability for the customer to put together their own download package (from components provided by the manufacturer) and sign the manifest with their own key.
Note that OpenBMC currently has the public key baked into its firmware image (not as a file). [Added after the meeting ended:] See details in the doc review here:
https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-dbus-interfaces/+/9025/2/xyz/openbmc_project/Software/README.md

Which techniques are needed for the BMC to access its firmware images? Pull from an SFTP or SCP or HTTP or HTTPS server? Via Redfish (which pushes via HTTPS)?
Note that via Redfish would not require the BMC to have a client certificate.

[Added after the meeting:] OCP 2018 Summit talk "Ownership and Control of Firmware in Open Compute Project (OCP) Devices" - discusses the problem of initializing, maintaining, and transferring ownership of a device (via its firmware) such as a BMC -
https://146a55aca6f00848c565-a7635525d40ac1c70300198708936b4e.ssl.cf1.rackcdn.com/images/827b72776863a3e3988138d53a332e0ba9150f72.pdf and
https://www.opencompute.org/documents/ibm-white-paper-ownership-and-control-of-firmware-in-open-compute-project-devices

6. Trivial PAM bmcweb config file change -
https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/27764
7. Merged code to add privilege=NoAccess to BMCWeb -
https://github.com/openbmc/bmcweb/commit/d7e080295f1f3c2517a440e3911600cec0c190fa This helps implement the OpenBMC privilege role of "no-access" per
https://github.com/openbmc/docs/blob/master/architecture/user_management.md#supported-privilege-roles
8. Next meeting in 4 weeks, January 8 2020.

Meeting held (with very limited attendance) 2019-11-27:

1. Continue discussion: BMC Admin enable & disable interfaces discussion?
    a. We rehashed the discussion from the previous week, with no new content.
    b. Joseph and Jandra intend to follow up with email.
2. BMC SecureBoot design - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169
    a. No discussion.
3. Disable SSL Renegotiation (merged Nov 12, 2019): https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/26992 issue: https://github.com/openbmc/openbmc/issues/3624
    a. The HTTPS BMCWeb fix has merged. This vulnerability does not apply to SSH.
4. Joseph's BMCWeb auth primer (email) : https://lists.ozlabs.org/pipermail/openbmc/2019-November/019422.html
    a. This was discussed further on the email thread. Will follow up with (a) doxygen style comments in the code, and (b) Gerrit review of a new doc anchored by the "Authentication" section of https://github.com/openbmc/bmcweb/blob/master/DEVELOPING.md
5. Are these applicable to OpenBMC? https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00313.html Update (Joseph): I understand one CVE relates to blocking unauthenticated IPMI access from the host to the BMC.
    a. The meta-ibm layer addresses this by giving the user an API to limit host IPMI access to whitelisted commands. However, that solution is not generally applicable to the overall project.
6. Discuss how the "NIST Digital Identity Guidelines" (NIST Special Publication 800-63B - https://pages.nist.gov/800-63-3/sp800-63b.html) apply to OpenBMC. The passwords are called AAL1 "Memorized Secret". OpenBMC also has SSH certificates and LDAP certificates to consider, and is working on mTLS (certificate based auth).
    a. Done: Added this to the wiki.
7. Joseph: Discuss the need for two more Redfish Roles (Privileges) and how they relate to the existing BMC Administrator or Operator roles:
    a. ServiceRep - Using BMC functions to service the host system in ways the BMC admin would not normally do, for example, replacing FRUs.
    b. ManufacturingRep - Using the BMC functions to service the host system in ways even the ServiceRep would not normally do.
    c. Discussion items:
        i. This is in the early planning stages, will follow up with email.
        ii. The service agents will not have all the Admin privileges. For example, service agents should not be allowed to manage users or configure network settings. And Admin users should not have access to the innards on the host. So the privileges between the Admin, ServiceRep, and ManufacturingRep may overlap but will not be subsets. We'll have to work out the privilege model.

iii. Service agents will authenticate via network interfaces, such as via HTTPS to REST APIs (not necessarily Redfish, could be OEM).
iv. An idea is the service organization will create a certificate pair, with an expiration date, and give one cert to the BMC Admin to install on the BMC, and the other to the service agent who will use it to access the BMC.

d. Joseph added on 2019-12-16: I think the root user should also be part of this same discussion. The root user is more powerful than Admin due to its Linux heritage, specifically, when root has shell access, many interfaces behave differently. For example, the root user can access any file on the BMC's flash contrasted with an Admin user who cannot.
    i. There are multiple use cases:
        1. Allow root access for advanced debugging that cannot be provided by the other kinds of login (ServiceRep and ManufacturingRep above).
        2. Lock out and disable root. If root access is ever needed, simply replace the BMC.
        3. Allow root initially, for example, for development work and debug, then lock out root access, for example, during provisioning.
    ii. Access to the `sudo` or `su` commands should be handled similarly. These commands can allow a non-root user who has BMC shell access to gain effective root access. (Note: I believe the `sudo` command is not installed on the BMC by default, but the `su` command is installed.)

Meeting 2019-11-13 held:

1. We discussed only the first item: Allow BMC Admin to enable & disable BMC interfaces: https://lists.ozlabs.org/pipermail/openbmc/2019-November/019287.html -- See also https://redfishforum.com/thread/248/solssh-ssh-serialconsole-disabling-provision
    a. See also (Email thread): in-band management after IPMI: https://lists.ozlabs.org/pipermail/openbmc/2019-November/019406.html
    b. Alejandra presented a spreadsheet listing BMC interfaces. This covered a wide range of interfaces including those mentioned by the Redfish ManagerNetworkProtocol, interfaces OpenBMC offers as either client (like DHCP) or server (like SSH), and physical interfaces such as USB.
    c. The question is: OpenBMC should offer the capability to the BMC Admin to dynamically enable or disable which set of interfaces? An obvious answer is: all of them. The ability to disable any unneeded interfaces has utility value. The point is: We want to find out which subset is a higher priority; which ones we would actually implement in the project.
    d. For the Web GUI, we discussed the idea of having a single page view that shows all of the controllable interfaces and their status (enabled/disabled). This can have links to pages with more detail, for example, detailed network configuration settings.

e. For the REST or Redfish API backend support, we can have various places, for example, the Redfish ManagerNetworkProtocol might be one such place. We're looking for standards for how to do the other pieces.
f. We will continue the discussion in the openbmc email list. An idea was to push a gerrit review containing the list of interfaces, and information about each (such as exactly what the interface is, if OpenBMC offers that interface, if it is enabled by default, how the BMC Admin can enable or disable it, etc.)
g. We discussed the core set of interfaces that might be enabled by default. I believe they were: the BMC's network interface, HTTPS, and Redfish APIs. Also network IPMI and SSH access featured in some use cases. Currently most interfaces are enabled by default (except not telnet or FTP which OpenBMC does not have, or TFTP which is enabled by static compile/build time flag BMCWEB_INSECURE_ENABLE_REDFISH_FW_TFTP_UPDATE (https://github.com/openbmc/bmcweb/blob/master/CMakeLists.txt#L110), etc.)
h. We discussed the difficulty of determining which interfaces should be enabled by default. This gets at questions about BMC discovery and how to provision the BMC. There may be multiple use cases for how to discover and provision BMCs.
i. Next steps:
    i. Add more information to the list of interfaces. Show the structure (examples):
        1. network -- HTTPS -- BMCWeb -- Redfish // this shows that Redfish requires the HTTPS interface, which requires the network interface
        2. REST API -- firmware upload via TFTP -- TFTP client -- network -- TFTP server // This shows that the firmware upload via TFTP uses the BMC's TFTP client to access the firmware image via the network from the TFTP server
        3. (Joseph says: I don't know if this is the right way to show the structure. For another idea how to structure this, see https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md#services-provided-on-tcp-and-upd-ports)
    ii. Identify the core set: network, HTTPS, Redfish, etc.
    iii. (Joseph, after the meeting:) We may need to start talking about different use cases: BMC managed by IPMI, BMC managed by Redfish, BMC network not used at all and managed by its host vias inband interfaces, etc.
j. Did we discuss more sub-topics?

Meeting 2019-10-30 held:

1. Development items:
    a. AST2600 secure boot design - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26169

        i. Interest in collaborating
    b. BMCWEB_ENABLE_MUTUAL_TLS_AUTHENTICATION BMCWeb server TLS based authentcation - https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/23588
        i. This is ready to merge.
        ii. Joseph mention working on an email (WIP) that describes BMCWeb's authentication and authorization flows. The mutual TLS (when merged) is a new authentication technique.
    c. Changed BMCWeb server persistent data (including session data) permissions - https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/23480
        i. This prompted a discussion to move away from the default root user and the default password.
        ii. Joseph sent an email that talks about how to administer the BMC, topics like the BMC's genesis boot and discovery of the BMC in the network (https://lists.ozlabs.org/pipermail/openbmc/2019-October/018794.html) - We further discussed how to configure OpenBMC build settings, such as for the HTTP server BMCWeb - https://github.com/openbmc/bmcweb/blob/master/CMakeLists.txt
    d. OpenBMC 443 port renegotiation attack (CVE-2011-1473) - https://github.com/openbmc/openbmc/issues/3624 Questions:
        i. How to handle this kind of report? Should it be redirected to the security response team? ⇒ Answer: This problem is old, so we can address it in the issue itself and do not need a confidential response. Joseph will dump excerpts from the OpenBMC security response team emails into the issue, and proceed to resolve that issue.
        ii. How important is preventing DoS attacks to the OpenBMC community? ⇒ Answer: We'll add this as an OpenBMC Security WG initiative. We want to prevent script-kiddie attacks, such as this one, and attacks that can be prevented by rate limiting, etc.
        iii. The direction for OpenBMC is to require client access to the BMC to use modern software (such as recent versions of OpenSSL). Older clients will not be able to connect to the BMC, and that is okay.
2. Add an initiative: Change defaults to secure by default:
    a. Change D-bus API config to OFF
3. James: Disable BMC/host bridges such as KCS and BT because these are not authenticated. The problem is the host firmware and BMC use these to communicate. Reasons to shut these off (especially after the host is booted):
    a. Prevent vulnerability chaining (if an attacker gains access to the host, they may be able to get root access, then use the bridges to get BMC access)
    b. use case: renting a bare metal server, so host root access should not give you access to the BMC

Meeting held 2019-10-16

1. Items:
    a. Doc updates to describe signing the image https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-dbus-interfaces/+/9025/2/xyz/openbmc_project/Software/README.md or search for SIGNING_KEY https://github.com/openbmc/openbmc/search?q=SIGNING_KEY&unscoped_q=SIGNING_KEY
        i. Separate parts: Image signing, secure update, and secure boot process
        ii. need better documentation
        iii. Helpful to have reference implementation?
    b. Enforce minimum 2048 bit certificates? https://gerrit.openbmc-project.xyz/c/openbmc/phosphor-certificate-manager/+/25760
        i. Yes, 2048 is minimum
        ii. We discussed why an admin-level control (of the minimum acceptable certificate strength) would be needed
    c. Avahi service discovery - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/23484 Hmm, see also the Redfish spec https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.8.0.pdf section 12.4 Service Details > Discovery.
        i. We discussed trying to solve this problem: Having both service discovery (or just scanning the network) AND default credentials AND a non-secure network → would be a security risk. This pattern is used for large scale deployments, like thousands of systems.
        ii. No conclusions were reached.
    d. network security considerations (threat model) review - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/26025
        i. Joseph to continue work, see 2019-09-18 entry below
    e. Email how to provision and admin the BMC - https://lists.ozlabs.org/pipermail/openbmc/2019-October/018794.html
        i. Subtopics worthy of documentation:
            1. Building and signing a firmware image.
            2. Admin and provision your BMC. ← does not exist today
            3. Using the BMC's interfaces.

Meeting held 2019-10-02

1. Current development items:
    a. https://github.com/openbmc/docs/blob/master/designs/redfish-resource-supplement-for-pfr.md - Redfish Platform Firmware Resilience - is about RAS, not security per se
    b. LDAP authority model questions - https://lists.ozlabs.org/pipermail/openbmc/2019-September/018611.html

    c. CA Law ~ Do folks know they are affected by the law? https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
2. Rust - We discussed using the Rust language.
    a. Benefits: memory safety which gives better security, for example, by making it harder to have buffer overflows (which are popular security exploits).
    b. Previous discussions of using Rust in OpenBMC (samples):
        i. https://lists.ozlabs.org/pipermail/openbmc/2018-December/014328.html
        ii. https://lists.ozlabs.org/pipermail/openbmc/2018-June/011971.html
        iii. https://lists.ozlabs.org/pipermail/openbmc/2019-May/016405.html
    c. Performance of Rust.
    d. Using Rust recipes downstream from the OpenEmbedded Yocto/Poky releases
    e. Prospects for rewriting various OpenBMC daemons using Rust.
3. Discuss CSIS Secure Firmware Development Best Practices, currently in development here (goo.gl/uEoAh4) .

Meeting held on 2019-09-18:

1. Current development items:
    a. IPMI authority may not be implemented correctly - https://lists.ozlabs.org/pipermail/openbmc/2019-August/017905.html
    b. Multiple security questions about Role=admin - https://lists.ozlabs.org/pipermail/openbmc/2019-August/017910.html
    c. Discuss expired password design: https://github.com/openbmc/docs/blob/master/designs/expired-password.md and https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/25146
        i. This led to discussions of the Redfish authority model, and to the OpenBMC Phosphor user-management design (https://github.com/openbmc/docs/blob/master/user_management.md) which is built on top of Linux PAM
        ii. Questions about how to change an expired password led to the Network threat model (approved here: https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md) and to the overall the threat model in review here: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22404
        iii. Joseph mentioned his plans to partition the overall threat model into these categories:
            1. Threats from the BMC's management network.
            2. Threats from the host system.
            3. Threats from physical access to the BMC.
            4. Threats from the BMC supply chain (software and hardware).
    d. There are multiple mutual TLS (mTLS) reviews in progress

        i. https://gerrit.openbmc-project.xyz/q/TLS
        ii. Example: https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/23588
2. Some ideas came out of the discussion:
    a. Ask about plans to deprecate out-of-band IPMI network access to the BMC. Ideas for a progression: UPDATE: sent email 2019-09-18 https://lists.ozlabs.org/pipermail/openbmc/2019-September/018321.html
        i. Tell everyone the plans (examples: emails to the group, mention in the release notes, update https://github.com/openbmc/phosphor-net-ipmid/blob/master/README.md).
        ii. Implement the Redfish ManagerNetworkProtocol - defined in the DMTF Redfish Resource and Schema Guide DSP2046 https://www.dmtf.org/dsp/DSP2046 (IBM intentions: https://github.com/ibm-openbmc/dev/issues/612). This allows the BMC admin to disable out-of-band network IPMI.
        iii. Change the IPMI Network protocol to disabled by default. This removes network IPMI access by default.
        iv. Remove IPMI from the default OpenBMC configuration. This makes it an explicit choice for OpenBMC's downstream based project to use network IPMI.
        v. Remove the IPMI https://github.com/openbmc/phosphor-net-ipmid repository from OpenBMC. Done! :-)
3. Ben talked about the progress, plans, and content for the CSIS Secure Firmware Development Best Practices, currently in development here (goo.gl/uEoAh4) . This has sections directly applicable to OpenBMC. We discussed ideas to evaluate OpenBMC against these recommendations. ⇐ TODO

Meeting on 2019-09-04 is cancelled

1. This will not be held.
2. See notes from 2019-08-21 as to the reason why.

Meeting held **2019-08-21** :

1. Current development items:
    a. Expired password design: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/23849 and email -- joseph discussed - no comments
    b. Auditing user actions: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/23870 -- no comments
    c. Prevent overlay filesystem corruption: https://lists.ozlabs.org/pipermail/openbmc/2019-August/017704.html -- general agreement that filesystem overlays are problematic, and we should move to a

model where we don't need overlays, and just mount read-write file systems as needed.
    d. Nancy mentioned they are reviewing security features related to the Nuvoton BMC boot ROM and boot block.
2. There was a question about flashing the firmware (host, and similarly BMC).
    a. The current OpenBMC firmware update is described here: https://github.com/openbmc/docs/blob/master/code-update/code-update.md
    b. There is interest in using Redfish support for this. (Check the email list.)
3. We discussed "verified boot" and "One Time Programmable" (OTP) memory needed to hold secret keys needed to establish a root of trust. We talked about Aspeed's AST2500 and AST2600 support for this.
4. Joseph: Review level of effort in handling CVEs (https://lists.ozlabs.org/pipermail/openbmc/2019-August/017578.html).
    a. Dick mentioned how this works in the UEFI project. We can freely discuss CVEs, issues, and fixes when fixes are available. However, if someone asks about a CVE or an issue for which we don't have a fix, ideally we would not respond to the problem, not even to say that we were invoking the OpenBMC security response team (https://github.com/openbmc/docs/blob/master/security/how-to-report-a-security-vulnerability.md). Then followup with the response team.
    b. Dick mentioned that the information embargo period for security fixes is 6 months. This gives time for the fixes to be built, tested, deployed, and activated.
    c. TODO: Joseph will propose similar guidelines for the response team.
5. Joseph: Added web security wish list items. There were no comments.
6. We elected to cancel the next meeting (Sep 4) and meet again on Sep 18 because of the Open Source Firmware Conference (OSFC ~ https://osfc.io/schedule)
7. Joseph gave highlights from attending the Blackhat conference (https://www.blackhat.com/us-19/) related to firmware security. He plans to send an email with details.

Meeting Aug 7 - cancelled - not held

Meeting held 2019-07-24 at 10:00am PDT:

1. Standing item: no comments
2. SPDM (work in progress) interest:
    a. This is an emerging standard from the PMCI workgroup and Redfish. It negotiates security with other endpoints via MCTP/PLDM or similar.
    b. SPDM relies on MCTP, and OpenBMC will use both.
    c. Use cases: firmware measurements (TPM). Possibly communicating with host firmware.
3. Design to re-do openbmc defaults for example, root/0penBmc is in the IPMI group - Joseph TODO
    a. This is separate from the expired password design (will be derived from https://github.com/ibm-openbmc/dev/issues/947).

4. Chittari: Tracking Yocto Linux security fixes tracking
    a. Wanted: Yocto fix branches (warrior=2.7) get into OpenBMC fix branches
    b. Wanted: Visibility / tracking of high severity CVEs
    c. Yocto security email list; patches for CVEs sent to yocto email list
    d. Yocto cve-check class (https://git.yoctoproject.org/cgit.cgi/poky/plain/meta/classes/cve-check.bbclass) helps track CVEs, but this takes a lot of work to keep up to date.
    e. Yocto CVEs - https://bugzilla.yoctoproject.org/buglist.cgi?quicksearch=cve
    f. Inhibitors: Private security databases such as IBM X-Force reduce interest in open source security bug repos
    g. Inhibitor: Bugs are fixed in various projects and may be reported in that project's release notes, but the bug reports are typically not copied into Yocto. Yocto picks up the fixes, for example, as a package version bump, without ever knowing there was a security bug.
    h. Interest in Yocto long term support (LTS)? Match up with Linux LTS. Yocto would take our patches into their old release branches (but we would have to do all the work). ⇐ We generally agreed this would be desirable for the OpenBMC community, but have no plans to make it happen.
5. Remember to review the BMC threat model https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22404

Notes meeting held 2019-07-10:

1. (pre-populated by joseph): Joseph mention these:
    a. The network security considerations guide gas merged into the project
    b. The BMC security considerations document is still under review.
2. Joseph: links to BMC Threat models.... I am removing agenda item 2 and plan to move forward discussing this with the BMC threat models:
    a. Network Security (Threat Model) Considerations (merged into the project) - https://github.com/openbmc/docs/blob/master/security/network-security-considerations.md
    b. BMC Threat Model considerations (in review) - https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22404
    c. Related design - Host-facing setup mode (in review): https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/21195
    d. Please contribute to these either in the gerrit code review, or in the email list, or in the security working group meeting. (Or in IRC if anyone is listening.)
3. We discussed the https://github.com/openbmc/openbmc/wiki/Security-working-group#security-end-of-release-checklist and talked about a new wish list item to run a tool like chipsec during CI, but otherwise there was no input. Joseph will email his ideas to the email list.
4. We discussed moving away from default passwords:

a. what the CA law says - https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
b. We discussed complying with the law by having an unique password per device.
c. We discussed complying with the law by having either (a) an expired password which must be changed before the BMC can be used, or (b) a "setup mode" which requires the BMC user to enter a password before the BMC can be used.
d. Joseph is working on the "expired password" or "setup mode" design.

Notes 2019-06-26 at 10:00am PDT:

1. (pre-populated by Joseph): Changes from approx mid May until June 12:
    a. **Redfish User Auth** [#security] https://lists.ozlabs.org/pipermail/openbmc/2019-February/015237.html Are the authorities correct; is everyone admin? https://github.com/openbmc/bmcweb/issues/62
    b. **Don't offer a default user account or password** [#security] https://lists.ozlabs.org/pipermail/openbmc/2019-March/015488.html For IPMI: https://github.com/openbmc/docs/blob/master/user_management.md#deployment---out-of-factory
    c. **mTLS HTTP authentication** [#security] https://lists.ozlabs.org/pipermail/openbmc/2019-January/014861.html) Design: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22410
    d. Security test plan https://github.com/openbmc/openbmc-test-automation/issues/1853
    e. New https://github.com/openbmc/openbmc/wiki/Platform-telemetry-and-health-monitoring-Work-Group Joseph's ideas:
        i. Is there a website for telemetry security? I didn't find one …
        ii. Joseph's ideas (CIA triad) were moved to the telemetry wiki
    f. Joseph's BMC threat models:
        i. Network https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22106
        ii. BMC https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22404
    g. Redfish accountService password limit 20 chars - https://gerrit.openbmc-project.xyz/c/openbmc/bmcweb/+/19574
2. Did not discuss. Leave on the agenda.
3. Discuss the Threat Model review. Mentioned briefly. Will use this review to collect notes
4. Discuss Network Security Considerations. Joseph will continue to push on this review.
5. What input will the security working group contribute toward the OpenBMC 2.7 release process (https://github.com/openbmc/docs/blob/master/release/release-process.md#freeze) - Consensus - yes, talk about the facts of what security features were implemented. Always try to get bug fixes for security items, and is okay to mention them or release with

bugs still present. Okay to get consensus of the Security WG (that is, of the members of a particular WG meeting) and email that.

6. How to move away from default password? The direction is: Leave the default OpenBMC behaviour to have the default password; this will result in no change for any OpenBMC users. Then enable a use-case to comply with the "no default passwords" rules, which OpenBMC downstream forks can enable. One of the leading ideas is to set the root user password to "expired", with the idea that it (ref: CA Law SB-327) "requires a user to generate a new means of authentication before access is granted to the device for the first time". Specifically, ensure that when the password is expired, the IPMI and REST authentication fails, and SSH can be used to change the password, which then re-enables the other network interfaces.
7. Redfish Host Interface and related security model -- Paul explained the background and recent history of IPMI and Redfish access to the BMC from the host BIOS and Kernel. We also discussed passing credentials via UEFI variables from the BMC to the host kernel and similarly passing separate credentials to the host user space. These credentials, for example, would be for the host kernel to use Redfish to contact the BMC to retrieve error logs about the host hardware. Or in general, use Redfish to do anything host IPMI is currently used for. Redfish's usual authority model would be used.
8. We agreed to switch to Joseph's Webex to host the next meeting. 2019-06-28 update: Joseph changed the wiki, will send email to the list

Agenda 2019-06-12 at 10:00am PDT:

The meeting was not held.

Agenda 2019-05-29 at 10:00am PDT:

1. Would like to scrub the security wiki -- did not get to … ran out of time.
2. Review end-or-release security assurance activity: draft https://github.com/openbmc/openbmc/wiki/Security-working-group#security-end-of-release-checklist-draft-wip and formalizing it as part of release process.
    a. Joseph to create gerrit doc review -- DONE: being reviewed here: https://gerrit.openbmc-project.xyz/c/openbmc/docs/+/22110
3. Create a simplified BMC picture that other designs can be mapped onto.
    a. Joseph to create gerrit doc review
4. How well is the cppcheck going? venture@ used it initially and found lots of issues that were fixed. Not scored in gerrit so it's on the maintainers to take actions. First step could be to discuss with maintainers. Scoring could be a barrier to new comers to OpenBMC. AI: venture@ to reach out to maintainers.
5. Interest in removing ssh access? Specifically, giving the owner or administrator the capability to lock out access.
    a. stoltz@ disable any external interface so that it can't be turned on at runtime.
    b. We agreed on: Have a way for the BMC owner(?) to disable unwanted interfaces. For example: (a) IPMI, (b) Web, (c) ssh port 22.

    c. Joseph: Technical ways to do this are: (1) build it out of the image, (2) build it in but disable it, or (3) leave it in, but then use ssh 'systemctl disable ssh' to disable it.
    d. stoltz: interested in specifying an idealized bmc architecture. For example, a video capability is not needed.
    e. We discussed having a way for the operator to re-enable interfaces, perhaps requiring a second factor such as an owner key or physical presence.
6. Use joseph.reynolds1@ibm.com for HTML or jrey@linux.ibm.com for plain text emails.

Agenda 2019-05-15 at 10:00am PDT:

1. Spillover chat from Eclypsium…
    a. Presentation on BMC attacks.
    b. (Joseph) Rick and Jesse presented. Here are my incomplete notes of parts that most interested me:
        i. attacks from the host and from the management network, recent DOS attacks, modifying the BMC's firmware, how the BMC and host share a NIC.
        ii. Trust model assumptions and the "BMC's odd privilege space" which we TODO should document. [joseph: In our security assurance docs.] The use case for the BMC not trusting a bare metal host also applies to a compromised host.
        iii. Hope for using the OpenBMC project to have a correct {access, authorization, privilege} model design and implementation.
        iv. We talked about how secure booting the BMC and using a TPM on the BMC might be used.
        v. We talked about the need to reliably show the BMC's firmware (that is, not filtered through the BMC itself).
2. No other topics

Agenda 2019-05-01 at 10:00am PDT:

1. Eclypsium presentation and demo by Alex, Rick, and Jesse -- disclaimer (Joseph): These are my outline notes about the discussion; they are not intended to be complete.
    a. Presentation: Eclypsium Management Console
        i. This tool runs on the host (e.g., via netbooted host) to collect data, and sends it to a server for further analysis
    b. How to validate firmware and BMC system configuration. Demo: Use Pantsdown to read BMC's firmware image.
    c. Alex advocated for the BMC to offer a way to read its firmware image so that image can be validated
        i. Notwithstanding any secrets held on the BMC's flash
        ii. Suggested memory mapped the flash image to support faster reading speeds and help prevent spoofing

    d. Please contact them with questions (how? Openbmc email list?)
2. No other topics were discussed.

Notes 2019-04-17 at 10:00am PDT

1. Tests for LDAP support are missing and must be added, driven by Joseph.
2. Eclypsium - presenting chipsec.
3. Ack
4. We need tests that verify authentication works as expected, or doesn't when it shouldn't.
    a. TODO: Joseph will publish the original documentation he wrote for this.
5. Can we put secrets onto dbus?
    a. Password authentication is bad, but maybe the dbus file descriptor thing works IFF the information is never written to a real file. [Meaning: a file in the file system.] See https://lists.ozlabs.org/pipermail/openbmc/2019-April/015797.html .
    b. We didn't get to an answer.
6. Continuous testing of security features will help avoid regressions when rebasing onto newer poky, etc.
    a. How do we track monitoring of when cyphers are no longer valid? Or when http headers should be upgraded?
    b. Perhaps **a human process done after a real freeze and before a formal release of OpenBMC.**
        i. ^-- this is the thing we need to do. Check the security posture of what's in place and what has happened, such as cyphers being broken or security bugs (OWASP, CVE).
        ii. https://github.com/openbmc/docs/blob/master/release/release-process.md. Perhaps an end-of-release checklist which reminds us to validate which ciphers, http headers, etc. to validate. TODO: Joseph -- DONE - added https://github.com/openbmc/openbmc/wiki/Security-working-group#security-end-of-release-checklist-draft-wip
7. Matrix.org was hacked. Reminded us to look at https://lists.ozlabs.org/pipermail/openbmc/2019-March/015488.html aka "default passwords are bad".
8. (and 9 together): Logging of customer data, or sensitive information is bad, or we require permission (such as for GDPR's opt-in requirement), very specific
    a. obmc-console-server logs a period of time (or lines) to the BMC as a temporary log file.
    b. When on a management network and use redfish - - the BMC redfish application will log that someone on the management network talked to it.
    c. To make progress:
        i. We need a lawyer to really answer the questions about data usage.
        ii. We need to have a security review of the information logged.
9. See 8.

10.

2019-04-18 Notes by Joseph:
Per agenda item 8 from 2019-04-17, the OpenBMC-based system collects information about its users (from the host console and from logs about Redfish REST API access, SSH access, etc.). My understanding of this data:

- Users typically have a pre-existing relationship with the BMC, typically the user's ID is granted access to the BMC as part of a job role within a larger organization.
- OpenBMC does not have any kind self-service account creation. Instead, the BMC's administrator (or the administrator of the BMC's authentication server) must authorize users.
- No OpenBMC functions collect sensitive personal information beyond username and IP address. Specifically, OpenBMC functions do not collect telephone numbers, email addresses, or other personally identifiable information.
- The BMC logs information about user access. Example log entry: userid, the access facility, and the access time.

The OpenBMC-based system may incidentally handle sensitive or personal data. For example, such data may flow through the BMC's host console or be stored on the BMC's flash within host event logs. However, the BMC does not understand or interpret this data, and merely serves as a storage area or channel for this data. The BMC makes this data available via its functions such as host console access, or log retrieval.

Notes 2019-04-03 at 10:00am PDT
1. **[AI: Joseph]** Creating a separate wiki page that summarizes the relevant security related work.
Nancy: would like to see some discussion in this forum on important topics
2. API Authentication
    - manufacturing use cases - https://lists.ozlabs.org/pipermail/openbmc/2019-March/015485.html
3. Default regular user
    - forcing users to create a user during first boot or install - https://lists.ozlabs.org/pipermail/openbmc/2019-March/015488.html
4. [James] chipsec: it's on their roadmap but it's low priority.
[Supreeth]: Arm could help contribute
[Nancy]: Will arrange for someone from Eclypsium to come and present
5. Joseph discussed an approach to getting an OpenBMC Security Assurance Guide
    - outline containing the different interfaces/areas
    - Joseph will email the idea to the openbmc list
6. SE Linux
    - space is an issue, need to get rid of Python
    - meta-selinux pulls in a lot of stuff, need to prune it out

7. Wish list for security features or security changes [AI: Joseph - DONE] copy to security wiki page:

- Remove IPMI (RMCP)
- SE Linux
- Remove default password / mTLS/ passwordless systems
- RUST language
- Replace host IPMI with PLDM & MCTP

Joseph will re-structure the wikis as follows:
ALL DONE - see https://lists.ozlabs.org/pipermail/openbmc/2019-April/015759.html

1. Change the existing wiki/Security-working-group: (a) DONE move security-related development work into its own wiki. (b) DONE: start a "security function wish list" within the security WG wiki -- all DONE
2. Created new https://github.com/openbmc/openbmc/wiki/Work-in-progress DONE
3. Create new https://github.com/openbmc/openbmc/wiki/Changelog DONE

Notes 2019-3-20 at 10:00am PDT

1.
2. Interest in the Yocto Project Security Response Tool (srtool): https://wiki.yoctoproject.org/wiki/Contribute_to_SRTool. It is a database/tool to organize & track how the OpenBMC project's response to security vulnerabilities. ⇒ No discussion recorded.
3. Followup from 2019-02-20: the cve-2019-6260 (pantsdown) test tool is here: https://github.com/amboar/cve-2019-6260 ⇒ chipsec is a more generic tool. Not restricted to x86. Requires python.

- uefi and os pieces, can be executed from either space
- should be able to add what's tested by IBM's tool into chipsec
- per arch/platform support needs to be added, arm support missing
- stefano@intel, eclispym?
- James will put together plan/proposal

OCP

- https://www.youtube.com/user/OpenComputeProject/videos
- Here's the link to James' presentation: https://www.youtube.com/watch?v=s7SLXhjQCbA
- OSF: certification? TSC to discuss and will report back next meeting
-

Notes 2019-3-6 at 10:00am PDT

1. Any new comments about the standing items?
    a. Maybe the list should be pruned more aggressively
2. Published articles talking about BMC as an attack vector for bare metal type cloud providers
    a. Just for your information

3. Default passwords are a no-go (new California law, apparently: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327). How do we know a password if it wasn't built into the image at the start -- Ed has some ideas, and Redfish is looking at it.
    a. Provisioning mode
    b. Technically this law only applies to consumer products.
    c. By default, change the root password to be log-in-once-and-change-only.
        i. Companies can do what they need within their infrastructure
4. Per https://github.com/openbmc/openbmc/issues/3383, why does everything run as root?
    a. Ed: Difficult to fix, no policy manager, systemd -- evil bugs, not yet resolved.
    b. Brad has gotten it working at some point - old experiments
    c. Does dbus-broker have the same bug
5. Joseph suggests having another meeting?
    a. Nobody seems to object. Ed and Patrick will just read the results.
    b. Update: 2019-03-13 joseph: On the other hand, emails may be more effective.
6. Can we listen in to OCP sessions?
7.

Notes 2019-2-20 at 10:00am PDT

1. Reviewing items:
    a. Backup & restore BMC settings
    b. Firmware update over Redfish
2. Secure Boot vs Firmware Update Conversation - basically reviewed points of validation of the image.
3. Flash-side switching as a vulnerability
    a. A/B booting, on failure the BMC can automatically try the other "side."
        i. An option: once the boot has gotten to some point, it'll update the other side of the flash, to avoid this.
        ii. "Am I running what I think I'm running?" Software Attestation.
        iii. Enabling of attestation if possible within the hardware (Looks like it may be available in the ast2600 - maybe (+Chris Engel)
4. The test tool for ASPEED is available - should it be in an openbmc repo?
    a. The tool uses /dev/mem to check - It can be used for testing on a release image, but it requires /dev/mem (which is normally disabled on a release image).
        i. U-boot passes parameter to enable (`setenv bootargs mem.devmem=y`), would need to then send the tool over.
    b. I think we should have the tool in the openbmc repo (maybe in a tools repo?) so we can all use it.
        i. Joseph will follow-up on getting this code released so we can all just use it :D
        ii. The testing procedure would like:
            1. Boot your bmc with devmem. From u-boot: `setenv bootargs mem.devmem=y`
            2. Build the tool and copy it your BMC.

3. Run the tool the probe which interfaces are open.

c. Update 2019-02-26: Tracked in email https://lists.ozlabs.org/pipermail/openbmc/2019-February/015190.html

5. Have the security patches for CVE 2019-6260 been merged into v2.6?
    a. Joseph, says, "in the meta-ibm layer", for example: https://github.com/openbmc/meta-ibm/commit/e98ac73825bddbd95a4b931073c4481fe535cff8
    b. Set of patches, to disable all the bridges. Example: openbmc/meta-phosphor / aspeed-layer/recipes-bsp/u-boot/files/**0001-aspeed-Disable-unnecessary-features.patch**
    c. meta-ibm layer grabs those patches. Other machines are encouraged to use these security patches.
6. ASPEED AST2400, AST2500 PCI-to-AHB bridge nearly out for review (misc/aspeed-p2a-ctrl).
7. Security Assurance Work at IBM - architecture docs about host and BMC and network and BMC, gerrit reviews -- characterizing the data IO for the BMC.
    a. What needs securing? Attack vectors. People are working on it.

Notes 2019-2-6 at 10:00am PDT

1. (Really item 2, we skipped item 1) Reviewed openbmc-security email list.
2. Discussed idea of having other email lists related to security, security-announce and or security-discuss, etc. (Joseph:) The problem is folks are attempting to subscribe to openbmc-security to get security announcements, and there is no obvious place for them to get such announcements.
3. Going back to item 1.
    a. Dropping the DWF CNA piece (Joseph:) Abandoned the review.
    b. Secure Boot of the BMC - who plans to work on it -- collaboration available.
4. Firewalls
    a. On the BMC, use native (iptables) firewall
        i. The purpose of running a BMC-based firewall is defense in depth.
        ii. The BMC's Linux kernel run netfilter modules which provide the native firewall service. The iptables command is the command line tool to interact with the kernel. The question is what package to use to set up firewall rules. (That task is fraught with peril.)
        iii. The rules should not be handwritten
        iv. Joseph found a package that uses a bash script to set up the rules via iptables calls. We can then dump the configuration once that's run and restore it.
    b. There was interest in some netfilter use cases: logging IP traffic, redirecting ports, dropping malicious packets,
5. Basically IBM will be pushing software assurance pieces upstream to OpenBMC per their own requirements to have such matters resolved for their products.
    a. Data flows throughout OpenBMC need to be understood, .e.g. bmcweb as an admin interface.
        i. Joseph is planning to drive these requirements -- check out the previous meeting's notes for the details. AI's for him to push code review for the documents.

6. Currently there isn't a high level plan or proposal for secure boot.
7. We agreed to add an ARM (arm.com) representative to the security response team. (done)

Notes 2019-1-23 at 10:00am PDT

We acknowledged and briefly discussed the Pantsdown security vulnerability before beginning the agenda.

1. Standing item: review security-related development work (see wiki)
   - 15621 - Proposed answers to the DWF CNA Registration form: Easy to just go through Mitre directly
   - email Certificate upload via Redfish
   - email mTLS HTTP authentication

2. Joseph: Discuss the ARMv8 TrustZone use cases:
   - black & white list in each application, application needs to request authorization from authorization manager first
   - couldn't this be done using SELinux?
   - right now apps are run as root, switch to using non root with access to necessary resources, trust zone is another layer
   - trust zone good for protecting hardware resources though, and partitions and for encryption keys
   - what are the use cases for what needs to be protected?
   - (Joseph summary): Use TrustZone for things like (a) securing private keys and (b) the BMC's access to sensitive hardware. Use features like SELinux to secure applications.

3. Joseph: FYI, the openbmc-security@lists.ozlabs.org email group added a new header: "This is CONFIDENTIAL. See: https://github.com/openbmc/docs/blob/master/security/obmc-security-response-team-guidelines.md". And review https://gerrit.openbmc-project.xyz/#/c/openbmc/docs/+/17270/ adds guidance about widening the circle of people who know.
   - Everyone needs to review and +1 please

pantsdown: Everyone needs to review Stewart's draft response by EOD and reply with comments. Publish OpenBMC response 1/24

4. Joseph: In general, how to handle security fixes such as the recent systemd problems: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866. Our default answer is: wait for the fixes to get picked up by Yocto and for us to use Yocto, but we have picked up more recent systemd fixes.

   - protocode or cve scanner will help keep these fresh
   - Brad: want track yocto master

- Ed: Yocto recommends building with both master and release, master breaks a lot
- Brad: Weekly merge with master
- Do we backport fixes? Depends on severity and which branch
- (Joseph summary): Yes, the intention is to keep up with security fixes in upstream projects such as systemd, and do so at least weekly. Although companies using OpenBMC in their projects may be already doing this, there is interest in doing it in the OpenBMC project.

5. Joseph: How do we get started with software security assurance? Can we start with threat modeling? Specifically documenting the BMC's assets along with threats to those assets.

- James and Joseph have both started this effort before. I (Joseph) this new format has a better chance of being reviewed and approved and built upon.
    - Document a bmc's assets
    - Document threats to assets
    - Why two separate docs? (No answer. :-).)
- James has a security analysis md patchset under review
- (Joseph as discussed during the meeting:) Here are the documents I am proposing, with an indication of the scope of their initial content:

  docs/security/assurance/README.md:

  Purpose: Material in this directory is for security assurance, so OpenBMC can be used in higher-security applications. Uses are to inform development effort and to provide assurance to users.

  docs/security/assurance/assets.md

  Purpose: This lists BMC assets that need to be secured. Specifically for BMCs in typical operational environments.

  Includes: Data stored on the BMC, the BMC's access to its host, the BMC firmware, the host firmware

  Data includes: logs, sensor data, fru inventory, etc.

  Security-relevant data includes: firmware images, public and private keys and certificates, HTTP session credentials, memory dumps

  How you can help: This starts at a high level and ideally decomposes hierarchically according to how the BMC is configured, listing all of OpenBMC's common elements with links into development docs: your help is needed to do that work. Identify which assets are more valuable: we'll spend more time protecting them.

  docs/security/assurance/threats.md:

  Purpose: This lists threats to the BMC's assets.

  Threat vectors: BMC management network, BMC operator, BMC firmware updates, physical access to the BMC, the host access to the BMC.

  Threats are to the confidentiality, integrity, and availability of assets.

  How you can help: Think like an attacker, and list more threats. Help prioritize

threats: we'll spend more time of them. Help assess threats, for example, using CVSS scores. Learn about threats and apply solutions to your technical area.

6. How to handle blacklisted components. That is, for whatever reasons your company cannot use a specific open source project that OpenBMC pulls in, for example, busybox.

- Nancy: Busybox has a serious history of litigation behind it and it's maintainers are unpredictable
- Joseph (after the call): Can we Propose to the OpenBMC project a different implementation?
- Nancy: It's Google's requirement to ban it. I don't want to impose it on OpenBMC unless the community agrees with the conclusion.

Agenda 2019-1-9 at 10:00am PDT:

1. We skipped the standing item to review development work.
2. Supreeth presented the ARM v8 Trust Zone and Secure Partitions presentation. Thank you Supreeth!
3. Joseph spoke briefly about security testcases for the openbmc/openbmc-test-automation Robot test bucket. Joseph is writing tests mostly for phosphor-rest-server, with 1 or 2 tests for Redfish.
4. Joseph will ask about agenda items 5-7 (a-c below) on the openbmc email list:
    a. (Joseph) How do we move forward with REST server authentication? Specifically Phosphor WebUI both (A) uses Phosphor-rest (/login session cookies) and (B) wants to use Redfish (SessionManager X-Auth-Tokens). Having to authenticate both places is bad. Do we change Phosphor-REST to use X-Auth-Token, or what is the solution?
    b. (Joseph) Can we enhance BMCWeb to redirect http://$bmc/ to https: for the web app?
    c. (Joseph) Add to the OpenBMC Security wiki: https://cwe.mitre.org/top25/index.html

Note we did not meet between 12-12 and 1-9.

Agenda 2018-12-12 at 10:00am PDT:

1. Standing item: review security-related development work (see wiki)
    a. Deleted items that are merged.
2. Will likely cancel the 2018-12-26 meeting and meet again on 2019-01-09.
    a. Motion carries, blah blah blah, meeting cancelled.
3. Joseph: Coordinate plans for release-end activity (release slated for 2019-02-04 per https://github.com/openbmc/openbmc/wiki/Release-Planning) Reviews or testing?
    a. What should we do? Should we review configurations or?
    b. Test configurations --
        i. Bmcweb authentication verification test cases. (IBM)

        ii. Penetration testing, code analysis (Q1) (Intel)
    c. Can task security team with code analysis, bmcweb, net-ipmid, host-ipmid, etc (Google)
4. Joseph: See project-level security testing https://docs.google.com/spreadsheets/d/1TW706qauln3EPQNd11IOzvnRVM8_-II-WCvdxm5NR6Y/edit#gid=784275422. See https://github.com/openbmc/openbmc-test-automation/blob/master/tests/security/test_ssl.robot.
    a. Designs should focus on testability as well as functionality, and designs need test review as well as any normal review.
5. Joseph: Interest in a firewall? Yocto uses iptables.
    a. Default disable everything not enabled? Example: enable ssh but not telnet
        i. Provide configuration or recipes for disabling further ??
        ii. meta-security is a good place for additional configurations. (Joseph:) My understanding is to use the firewall infrastructure in the meta-openembedded meta-security layer, then customize it via BBAPPENDs from the meta-phosphor layer.
    b. Where would a security phosphor patch?
        i. meta-phosphor -- per Brad
    c. Review dropbear patch for upstreaming, with v2.6
    d. Joseph submitted a patch to dropbear to drop the ciphers from the default dropbear configuration.
    e. Arno-iptables-firewall - open-embedded
        i. Not presently being built.
        ii. Customized shell script to set-up the firewall for us.
    f. Discussion warranted, what tool is best?

Agenda 2018-11-28 at 10:00am PDT:

1. Standing item: review security-related development work (see wiki)
2. Joseph: Add TARGET_MACHINE to /etc/os-release to help establish provenance. See email https://lists.ozlabs.org/pipermail/openbmc/2018-November/014085.html.
3. Joseph (per 11/26 Community Call): Default passwords (root - ssh, ipmi user). How to ship with secure defaults, and yet enable automated testing? Using ssh-keygen && ssh-copy-id.
4. Joseph: FYI - Added to the Security WG wiki: https://airbus-seclab.github.io/ilo/ZERONIGHTS2018-Slides-EN-Turning_your_BMC_into_a_revolving_door-perigaud-gazet-czarny.pdf
5. Ed: NPM event-source package vulnerability

Add TARGET_MACHINE to /etc/os-release to help establish provenance.

- uname -a will work
- Joseph will respond to original post - update 2018-12-05. This was pushed for review here: https://gerrit.openbmc-project.xyz/#/c/openbmc/meta-phosphor/+/16489/.

Default passwords (root - ssh, ipmi user). How to ship with secure defaults, and yet enable automated testing?

- enforce password is changed when someone builds their image?
- change at first login
- passwords can be leaked
- passwords are per system, default password is time limited
- passwords for manufacturing? manufacturing sets one like serial number and the exits manufacturing by resetting to default
- passwords for automated testing like CI? If it's a server, assume host is trusted and host would set the password.
- moving to untrusted hosted, but currently host is trusted
- future directions: certificates, ldap, http based certificates

NPM event-source package vulnerability

- someone got ownership of package and injected malicious code
- ed to post to mailing list
- GunnarM has a patchset out for it, in security wiki - https://gerrit.openbmc-project.xyz/#/c/16215

Build target that provides minimial external access (no gui, no remote console, etc).

- done per machine
- good to have such a target but how would this look?
- Observation: Perhaps build targets correspond to use cases: enterprise, cloud-scale doesn't offer the webui, etc.

CNA Application draft:

- We generally agreed that the OpenBMC CNA should cover "The OpenBMC project, not including vendor, company, or hardware specific elements covered by another CNA." See Nov 27 comment here: https://gerrit.openbmc-project.xyz/#/c/openbmc/docs/+/15621/1/cna-request.md
- We started discussing what should happen for upstream and downstream bugs, but ran out of time.
- Joseph will put up another patchset and ask for re-review on the email list.

Agenda 2018-11-14 at 10:00am PDT:

1. Standing item: review security-related development work (see wiki)
2. Joseph: CNA update, "all new open source CNAs go through DWF" (https://github.com/distributedweaknessfiling/DWF-Documentation) and specifically: https://cna-form.distributedweaknessfiling.org and in review here: https://gerrit.openbmc-project.xyz/#/c/openbmc/docs/+/15621/
3. Open Compute Project (OCP): has a security topic https://www.opencompute.org/projects

4. Joseph: Discuss phosphor-webui. It uses AngularJS which requires either ngCsp/ng-csp or HTTP response headers 'unsafe-inline' 'unsafe-eval'. Also phosphor-webui seems to use inline styles, but I am not sure. We need a plan to enable using phosphor-webui without requiring unsafe directives.
5. Joseph: Began work to enable OpenBMC security reviews. Started bmcweb config guide; will continue work.

Meeting Notes 2018.11.14

1. Standing item: review security-related development work (see wiki)
   - use security tag to generate list of reviews dynamically
   - hashtags are available but have to use noteDB
2. CNA update, "all new open source CNAs go through DWF"
   - github org account: create a OpenBMC user
   - should OpenBMC create PGP keys?
3. Open Compute Project (OCP): has a security topic
   - known project: includes Cerberus and Titan
4. Discuss phosphor-webui
   - code needs to be reviewed by someone versed in CSS and javascript security
5. Began work to enable OpenBMC security reviews
   - started with bmcweb config
   - auto generate doxygen docs. where to host? question for infrastructure group

Agenda 2018-10-31 at 10:15am PDT:

1. Standing item: review security-related development work
2. Joseph working on CVE/CNA
3. Joseph: Move "development work items" into the security working group wiki.
4. Joseph: Plan a security review of network interfaces as part of the 2.6 (2/2019) release

Meeting held 2018-10-31 at 10:15am PDT:

1. Security item reviews -- incoming problems, public or private.
    a. Do we know when it's going to be in sumo? (yocto upstream?)
    b. We might set a clock, and if it's not in yocto within ${severity_calculation} days
        i. We do it ourselves
        ii. Rotation or lottery
    c. Separate discussion -- how do fixes get assigned or owned?
        i. Merged idea into general security idea -- how do groups own it, take responsibility.
    d. Mature process takes time.
        i. Could better define a maintainer's role.
        ii. Maybe a public SLO --
2. Joseph is working with IBM's internal teams to sort out the CVE/CNA for OpenBMC
    a. More specifically, if problem in OpenBMC brought to Joseph's attention through the private openbmc-security mailing list is ok to be sent up the chain.

        i. Information sent to the mailing list is allowed to be reported up to each company on the mailing list versus through a more restricted method.
3. Could we move it into the wiki?
    a. Popular opinion: 6 yays
4. Joseph: Plan a security review of network interfaces as part of the 2.6 (2/2019) release
    a. Security review of bmcweb
        i. How to enable/disable endpoints and services?
        ii. Basic testing? Documented for each feature (item).
        iii. Currently documentation lives in the bmcweb repo, but maybe it should be combined into the docs repo.
        iv. Documenting how you use versus security issues associated with those ports and services
    b. Preferably start with a configuration guide… as a jump off point for any security review.
    c. Doxygen for browsing code to find actual pieces of an implementation… might help -- automatic references to code that is searchable.
    d. (Joseph summary:) Add a link from the openbmc/bmcweb/README to a configuration guide which introduces various topics and then (ideally) refers to doxygen-generated docs.
5.

Agenda 2018-10-17 at 10:00am PDT:

1. Standing item: review security-related development work
2. Discuss removing support in SSH (secure shell) for the MD5 MAC algorithm.
3. Security announcement for phosphor-host-ipmid changes.
4. Joseph: discuss GUI design workgroup is starting
5. cppcheck is staged in CI, hopefully merged soon.

Meeting held 2018-10-17 at 10am PDT

1. Current documents under review are pending updates.
    a. Certificate management daemon underway
    b. Phosphor-host-ipmid user management underway.
2. Removing MD5 MAC from SSH by default?
    a. Off by default, force customer who want it to re-enable it in their own recipe.
    b. Ed to look into dropbear vs openssh
3. Image size?
    a. Maybe a build target piece, or machine_Feature can make intelligent choices about what packages or variations to prefer.
4. Features on or off
    a. How to know what's on or off for an image, documentation automatically generated?
    b. Should security features have some variable name that's easy to detect? E.g. SECURITY_CONFIG
5. Security announcement for phosphor-host-ipmid changes.

    a. How to announce?
        i. Once announced, we can mark something as non-private.
        ii. Joseph is meant to write the security announcement.
        iii. Handing off CVE generation to Joseph.
    b. How to deal with CI not running?
        i. The author can run the CI locally and post the results to the review.
            1. This should be part of the contributing process.
6. GUI design workgroup is starting

    a. IBM design team, phosphor-webui, the images will be posted envision app - for visual reviews.
        i. Gerrit review, describes the items being reviewed in envision.
        ii. Into openbmc/docs ? or **phosphor-webui** repository?
7. cppcheck is staged in CI, hopefully merged soon.
    a. Any slower parser will need to run periodically if not presubmit.
    b. Ed is looking into Coverity which is a slower, larger, mechanism.

Agenda 2018-10-03 at 10:00am PDT:

1. Standing item: review security-related development work
2. Joseph: Discuss responsibility for reviews. Specifically, if an attacker pushes code and has their friends +1 it, what mechanism ensures review? How do we make it harder for attackers to push bad code?
3. Joseph: Discuss "it should be easy to request a CVE number by e-mailing cve-assign@mitre.org to ask for the number, linking to the commit of the fix, and adding some description". Is okay? Are we ready to create a security advisory? See related https://github.com/openbmc/openbmc/issues/3359.

HELD Agenda 2018-09-19 at 10:00am PDT:

1. Standing item: review security-related development work
2. Joseph: Discuss security response team
3. Joseph: Discuss code scanners: Code Climate vs SonarQube
4. Joseph: Discuss running daemons as non-root
5. Joseph: Discuss documentation efforts

Notes

Discuss security response team

- First report received, routed to IPMI maintainers
- high vulnerability but no known exploit
- expectation that maintainers attempt to resolve

Discuss code scanners: Code Climate vs SonarQube

- Code Climate doesn't work with gerrit only github
- SonarQube is popular in Open Source communities, could be integrated into CI

Discuss running daemons as non-root

- create a github issue for it
- Created - https://github.com/openbmc/openbmc/issues/3383 "daemons should not run as root"

Discuss documentation efforts

HELD 2018-09-12 at 10:10am PDT

Agenda 2018-09-12 at 10:00am PDT: (Started 10 minutes later)

1. Standing item: review security-related development work
2. Joseph: Discuss code scanners:

    a. Codacy scanner (https://www.codacy.com/)
    b. Code Climate quality tools (https://codeclimate.com)
    c. Cppcheck
    d. Clang (https://clang.llvm.org) used today to check OpenBMC C++ formatting. Note that Clang is open source. Is Clang static analysis used by OpenEmbedded? Yes -- meta-security layer
3. Joseph: Proposal: Hold OpenBMC security show & tell sessions with the purpose of bringing together developers and security pros to identify and document each area's security considerations. The documentation will be usable by new developers (and to encourage peer review) and by security professionals (as a starting point for more thorough analysis). Main ideas of this proposal are:
    a. Candidate areas: bmcweb, Redfish, rest-server, phosphor-webui, using PAM+LDAP, ipmid, AST2500, the digital signing and code update process, github source repos, the review process, etc. TODO: prioritize the list.
    b. The documentation for each area may include: identify the area, list related areas, identify assets to protect, interfaces, threats, risks, controls. Also: link to OpenBMC docs and implementation, external links, standards, recommendations for users (aka best practices), etc. TODO: Identify appropriate docs for each area. Idea: Propose a template to the mailing list and refine it before each session.
    c. Before each show & tell session:
        i. Organizer: Set up a schedule: date + area + technical presenter. Avoid holidays, hackathons, release dates, etc.
        ii. Developers: Gather your docs and attend the meeting.
        iii. Organizer: Announce the event in the openbmc email list.
        iv. Everyone: invite security pros, users, testers. TODO: grease the skids
    d. During each show & tell session:
        i. Introduce the area.
        ii. Agree where to document the results (for example, in the area's OpenBMC repo README file). Identify the scribe. Sign up reviewers.
        iii. Talk about your area. Please begin as if you were introducing a new software engineer to the area. Start with basic function and how it relates to other areas in OpenBMC. See the "documentation" section above for more ideas about what areas are needed for security.
        iv. Answer questions and collaborate.
        v. The scribe takes notes.
    e. After each show & tell session:
        i. The scribe pushes updated docs for review.
        ii. Participate in the documentation review.
    f. TODO: Create a new wiki: openbmc/openbmc/wiki/security-show-and-tell to track the schedule, briefings for participants, pre-review comments, reviews, and results
4.

Notes 2018-09-12 at 10:10am PDT
Attendees: Joseph Reynolds, Brad Bishop, Subraswami, Supreeth Venkatesh, Nancy Yuen
Should names to openbmc security mailing list be secret?

- Not a secret, but not going to announce it publicly. In particular, we can discuss names in public forums like the security working group.

Discuss code scanners

- IBM investigating Codacy & Code Climate
- Codacy will scan Open Source for free
- Yocto/OE uses clang
- In general, OpenBMC will take any usable work in this area, whether the scanner is open source or not. For example, see use of valgrind in https://github.com/openbmc/sdbusplus.

Security Show & Tell

- Joseph to create the show-and-tell wiki
- The previous efforts to document various security-relevant areas had issues. Chiefly:
  - They covered too many areas, making it hard to get +1s
  - The effort did not have buy-in from the technical leads
- In contrast, the show & tell effort:
  - Is target to a specific area/repo, so a developer in that area can +1 the overall document
  - Buy-in is created when the technical leads signs up for the show & tell session, and then participates in the discussion. They would naturally want to follow up by reviewing documentation which was created based on that discussion.
- Idea: Hold a model show & tell session at the Hackathon Oct 9-11.

Agenda 2018-09-05 at 10am PDT

1. Standing item: review development work that has security questions
2. Three security bugs found by our security team reviewing ipmid -- how to proceed.
   a. We don't yet have patches ready.
3. Joseph: Review gerrit 11665 “Security response team guidelines” and its associated email: openbmc-security@lists.ozlabs.org
4. Housekeeping - new header for this file?
5. New meeting time discussion.

Agenda held - 2018-09-05 at 10am PDT
Attendees: Patrick Venture, Brad Bishop, Joseph Reynolds, Subraswami, Supreeth Venkatesh,

1. Docs under review
2. Three vulnerabilities found in IPMId
3. The security process.
4. Joseph volunteered to make the document easier to engage.
5. Email going out to discuss having the meeting at a different time.

Notes

- Related to gerrit review 12027: Services have policies under SELinux -- orthogonal to groups and authorizations of people. So this is unrelated to what is discussed with the groups and roles dbus interfaces.
- SELinux may be too large to fit within the 32Mb kernel partition.
- Currently under review is the process 11511 - email the details to openbmc-security@lists.ozlabs.org -- that is a private response team.
    - Currently, Joseph, and the TSC members.
    - Having Google security email the group.
- The new process detailed in the 11665 was reviewed and it made sense.
- Joseph to add new header on the Google docs file to declutter.

Agenda held - 2018-08-29 at 10am PDT
Attendees: Brad Bishop, Joseph Reynolds, Subraswami, Supreeth Ventatesh, Ben Stoltz, Patrick Venture, Nancy Yuen

1. See CVE-2013-4037, CVE-2013-4786 re IPMI 2.0 RAKP password hashes.
2. Joseph: What does an OpenBMC security program look like? Should we have one?
3. Joseph: How to influence development work? Focus on discussion and reviews
4. Joseph: Documenting security controls → how to handle different features

Notes

See CVE-2013-4037, CVE-2013-4786 re IPMI 2.0 RAKP password hashes

- Some people still use IPMI, best strategy is to move to Redfish
- Need to make it harder to do the wrong thing
- Documented, part of review, can test for it…
- Need configurability, opt-in approach (feature encapsulated code)
- offer clearly defined configurations for different needs (can use meta subtree layers to manage)

Documenting security controls → how to handle different features

- identify the controls and knobs, which config files control it
- bitbake supports machine and image features (and distro features?)
- be careful to document only OpenBMC specifics (and point to Yocto when needed)
- everything in phosphor is opt-out today, need to change to opt-in?
- when new recipes are added, security needs to be involved about which configs it belongs to
- distro, machine, image features: https://www.yoctoproject.org/docs/2.0/ref-manual/ref-manual.html#ref-features-machine
- https://github.com/openbmc/openbmc/blob/master/meta-phosphor/conf/distro/include/phosphor-base.inc

- Idea: Work toward documenting/offering sets of feature groups, including {normal, paranoid, compliance} security configurations. For example, obmc-phosphor-image would be the normal (out of the box) secure

What does an OpenBMC security program look like? Should we have one?

- **Rename this topic: do activities that promote security**
- The overall answer is “yes” and here are the activities:
- Follow the current feature development process and inject suggestions where appropriate.
- Maybe monitoring certain repositories, ones with obvious attack vectors: ipmid net-ipmid
    - Consider bringing the maintainers onboard to know to keep an eye out and bring us into the fold.
- Meeting to discuss development work with security implications
- penetration and other security testing
- educate contributors (during discussions and reviews), other times?
- audit configurations and images
    - What configurations are set, what values, versus what we expect.
    - Design idea: use $(bitbake -e | grep … | diff ...spec...)
    - However, this approach doesn’t help, for example, for hard-coded use of DES3.
- Agreed: Review selected development items in each security workgroup meeting. Selection is at the discretion of meeting participants. Idea: focus on repos that offer BMC attack vectors.

Agenda held: 2018-08-22 at 10am PDT
Attendees: Joseph Reynolds, Brad Bishop, Sub, Supreeth,

1. Review: Map LDAP group to role - review 12027 above - email
2. Joseph: Where to document security stuff? Answer: in the docs repo
3. Joseph: Highest priority items?
4. User Management IPMI (IPMI features as configurable pieces)

Notes
Review: Map LDAP group to role - review 12027 above - email
Critical need for IBM
Not well explained
ldap server backend maps each user to a set of groups, bmc maps group to roles. Roles are used for authorization functions
Existing user function isn't well understood

Where to document security stuff?
docs repo and wiki existing already
Prefer wiki for things like meeting notes. Technical docs should be revisioned under docs repo.
Format has been hard to be reviewed by one person. May need to break it down smaller pieces
Hard to view the doc without seeing all the comments initially

command line interface to gerrit: gertty

Joseph is documenting: how to turn off ssh, ciphers, etc

Highest priority items?
Main idea: Use existing tools first: source code scanners, penetration testing tools
How to keep up to date with reported vulnerabilities, security updates, etc.

- Highest vulnerability packages - openssl, busybox, dropbear, …
    - Configuring the packages for secure modes by default.
    - Documentation for community members on how to configure the core packages.
- Identifying kernel security modes / patches to enable.
-

Action Items

1. Identify core security packages (and document their modes) (*joseph*)
    a. Examples: busybox, openssl, dropbear
2. Identify configurations that are secure by default and provide mechanism (default recipe or add-on layer that sets them).
3. Identify kernel security mode patches (configurations we can enable with 32-bit).
    a. Kernel address randomization, etc
4.

User Management IPMI (IPMI features as configurable pieces)

- rakp authentication protocol being used
    - 2013 that protocol would expose salted hash passwd to remote console
    - it's not default
    - Witherspoon specific change

Agenda held: 2018-08-15 at 10am PDT
Attendees: Joseph Reynolds, Sub, Nancy Yuen, Ben Stoltz, Supreeth Venkatesh, James

1. Discuss CVE-2018-5390 as a test of https://gerrit.openbmc-project.xyz/#/c/11511. See https://github.com/openbmc/openbmc/issues/3359
2. Discuss the unbearable lightness of being a BMC: https://www.blackhat.com/us-18/briefings/schedule/index.html#the-unbearable-lightness-of-bmcs-10035
3. Joseph: Prioritize security initiatives. See the wiki section “Initiatives”. They are all important, but what do we work on first? For example: https://gerrit.openbmc-project.xyz/#/c/openbmc/docs/+/7095/6/interface-https.md.

Notes
Joseph walked through the test run of the security response team.
Discuss the unbearable lightness of BMC blackhat conference talk

- Nothing surprising

- Focused on Dell and HP systems
- Joseph putting together a presentation for IBM management that covers OpenBMC security topics.
- how to keep up with vulnerabilities for all the packages that go into openbmc image
    - Automate? The openBMC Yocto/bitbake build process can generate a Bill of materials (BOM) that includes information about all packages it retrieves. That is the starting point for Open source license compliance and security work: we want to know best practices and security advisories for packages we are using. The OpenSource community uses SPDX packages and is still working toward a better solution.
    - Joseph notes two distinct shades of BoM:
        - (BOM-1) includes all the source packages
        - (BOM-2) includes the subset of source packages that are built into the final image (e.g., not including build tools)
        - For license compliance work we might want BOM-2, but for security/vulnerability work, we need to use BOM-1
    - Ideally check for security advisories regularly ie weekly
    - Check the BoM against whitelist/blacklist.

Prioritize Initiatives

- code coverage directed fuzzing
- we need come up with security requirement for OpenBMC
- PMCI work group DMTF forum, security requirement for MCTP

Joseph: My impression of higher-priority items after hearing from the group:

- Automated security testing during the code review process. OpenBMC uses the Gerrit code review server which uses a Jenkins server to check the source code. This should be leveraged to perform additional scans.
- There is strong interest in following best practices from upstream projects. See notes above.
- There have been multiple independent efforts to document various aspects of the security architecture, but the work is difficult, and time limited. Perhaps a “fix it” week for this effort?

Agenda held: 2018-08-08 at 10am PDT

Attendees: James Mihm, Sub, Brad Bishop, Joseph Reynolds, Patrick Venture, Ben Stoltz, Nancy Yuen

1. New design (11840 above) for certificate management (SSL, LDAP, etc).
2. Joseph: Is this a good goal for OpenBMC: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Power%20Systems/page/Power%20Systems%20Flexible%20Service%20Processor%20(FSP)%20Security

New design (11840 above) for certificate management (SSL, LDAP, etc).

Should private key be downloadable?
We should not export private keys in plaintext.
Answer: No

Everyone please review #11840

List of cls to review at the top of meeting notes, maybe add a topic in gerrit so they're easy to find. Will need to remove the topic from a cl when it's time to submit.

Patrick emailed the CVE person again, cc'd more people, to get CNA.

Is this a good goal for OpenBMC: Power Systems Flexible Service Processor (FSP) Security?
Attack surfaces and mitigations are good. Good for education.
Talk about case histories separately, github issues.

Why we care about supply chain security:
https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Create a page on OpenBMC wiki and collect examples [TODO Joseph Reynolds] DONE: See https://github.com/openbmc/openbmc/wiki/Security-motivation.

Blackhat presentations are today.

Agenda held - 2018-08-01 at 10am PT
Attendees: Nancy, Patrick, Ben, Joseph, James, Sub

1. New call-in number for week starting 2018-08-08.
2. Discuss secure boot aka verified boot, multiple implementations. Verify u-boot, then the firmware image.
3. Discuss "`SSL Certificate management proposal`" from 7/31 openbmc mailing list.
4. Updates on reviews?
5. Reached out for CVE CNA, still haven't heard back, will ping again and rope in others to email.

Notes
Discuss secure boot aka verified boot, multiple implementations. Verify u-boot, then the firmware image.
Ben's requirements

- Signature verification prior to flashing update
    - Still prone to supply chain attacks and ?

    - Intel: verified and measured (less restrictive, digest hash stored in tamper resistant location) boot
    - Verified is a policy, if it doesn't validate, then do something like not run the code
    - Intel's verified boot will brick the system if it doesn't validate
    - Prefer some kind of self repair
- Titan project: measures boot flash
- BMC processor may support some kind of signature verification and policy
- Owner of machine owns and signs

Need the option of owner being able to use their own keys to sign
Is key replacement support be sufficient?
Needs to be tamper resistant, physical presence, …
Need to capture these in a document
Need first instruction validation, establish root of trust, u-boot or something else
…

Runtime sw doing checks on ports and assets, how do you trust it?
Figuring the top level query, attest to verified measured boot, various stages to chain of trust

Intel is working on to secure boot, a/b update, separate spi part that validates

Ast 2600 will provide hw verification…

Discuss "`SSL Certificate management proposal`" from 7/31 openbmc mailing list.
Signing request takes place on BMC or some other secure server get all the signed certs and loads them on the BMC.

Oauth2.0?

Some designs are in progress.

Updates on reviews?
Joseph: OpenBMC channels were talking about a proposal for a documentation workgroup.
Answer: A workgroup may be more trouble than it is worth. But we do need some way to give focus to documentation.

Agenda held - 2018-07-25 at 10am PT
Attendees: Brad, Joseph, Jayanth, Sub, Nancy, Patrick, James, Jubin, Sai

1. Joseph: Discuss the security response team: -- see the review above
    a. Who should be on the team? The *main idea* is the security response team must privately and directly contact the developers who need to address the problems. So we are looking at people who know the project's technical leadership.

    b. Collect guidelines for the team's role. The current draft is:
        i. interact with the submitter, contributors, and other stakeholders
        ii. coordinate with upstream and downstream projects, including vendors
        iii. Get onto http://oss-security.openwall.org/wiki/mailing-lists/distros
        iv. Handle the process for information embargo and announcement
    c. Decide how to document vulnerabilities. The current direction is to use https://github.com/openbmc/openbmc/issues/. Perhaps use a "security vulnerability" label. These issues should use a template that includes a brief description, CVEs, affected repositories, when mitigated or fixed, etc. including elements of CVSS.
2. Joseph: Decide when to open up this meeting (the security working group) to anyone. Can we do it once a security response team is in place?
3. Joseph: Discuss suitability of the OpenBMC architecture docs (review 11645) for use a reference material by the security documentation. Specifically, can Joseph and James reference the new "OpenBMC architecture" docs from their security docs so the security docs can get right down to business? The model would be for the security doc to reference (or include?) the OpenBMC's architecture doc and immediately establish its security relevance.
4. Joseph: Discuss TLS certificate management (2018-07-25 clarification: This is for transport level security.). How should OpenBMC generate certificate signing requests and install certificates onto the BMC?

Notes:
1. The overall agreement was to think about 1a and 1b (team composition and activity guidelines)
1c. Decide how to document vulnerabilities.
Vulnerabilities reported about first party owned code/applications are handled by our Security response team. We won't know about third party vulnerabilities ahead of times but we can link it in to our github issues. Security response team uses private emails and writes description, CVEs. Publish at the agreed to time by all parties (Joseph added:) into https://github.com/openbmc/openbmc/issues/.

Linux Foundation has best practices for how projects deal with security concerns. From Michael Dolan @ Linux Foundation:

> ---
> I would highly recommend taking a look at the CII Best Practices. They embedded them into a badging process. It covers everything from disclosure to reporting.
>
> There are basic "Passing", Silver and Gold levels.
>
> You can view the details on the Linux Kernel (Passing level) here as an example: https://bestpractices.coreinfrastructure.org/en/projects/34

The main website is here: https://bestpractices.coreinfrastructure.org/en

---

2. Agreed: open up the next meeting to all. DONE: Joseph created new wiki page under https://github.com/openbmc/openbmc/wiki/Security-working-group.
3. Sounds good.
4. Certificate Management -- specifically TLS certificates

How does BMC get it's certificate?

James: we provide the mechanism that allows manufacturers to do this

Brad: the person buying the server will want to upload their own cert

James: Different types of certificates

Brad: This is for TLS

Brad: (1) BMC generates the CSR and uploads and download the signed cert or (2) provide an interface to download it

Effort is about the same. Need to make sure the right private key and an cert are uploaded in the (2). (1) private key doesn't leave system

Uses cases for both

Joseph: My overall impression is that OpenBMC needs this and it will be implemented soon. My understanding of the 2 approaches Brad outlines are:

- Approach 1 is for the BMC to create a key pair, create the CSR (certificate signing request), and send the CSR to get signed by the CA (certificate authority), and install the CA-signed certificate.
- Approach 2 is for OpenBMC to have APIs to add/remove/revoke certificates. The signed certificates would have to be created by someone else.

Either way, whoever provisions the BMC would be responsible for this.

Book: Zero Trust Networks mentions Google's Low Overhead Authentication System.

Held 2018-07-18 10am PT
Attendees: Joseph, Brad, Ben, James, (other?)
0. Before the meeting properly started, we discussed the state of the current security documentation reviews. There is push back because of the non-security-specific background included in the document. Joseph will start an OpenBMC architecture documentation effort. It should be usable by new OpenBMC team members and in a form consumable by the security documentation.

1. At the 2018-07-16 OpenBMC Community call we agreed to create a private email list for people to privately report OpenBMC security vulnerabilities. BradB to create the email list initially populated with e-mail addresses, exactly one per TSC member (i.e., member or delegate). JosephR proposed guidelines for the project, here: (https://gerrit.openbmc-project.xyz/#/c/11511). Note the nomenclature:
    a. The OpenBMC security working group (this group) will remain completely open.
    b. The OpenBMC security response team works privately to resolve security issues.
    c. Brad will proceed with getting the email address.
2. Update on OpenBMC participation in the CVE process.
    a. No update.
3. Joseph: Does the OpenBMC team need a vulnerability database even if we use CVEs?
    a. Discussion:
    b. Can we use this?: https://github.com/openbmc/openbmc/issues/
    c. We want each commit message to be high quality. It should explain why the change is needed and what it is accomplishing.
    d. We discussed a mechanism that requires each commit message to point to a github issue (similar to the “resolves” line). Requiring this would be a barrier to entry for new developers.
    e. We want traceability, a way to link issues with commits. A use case: when working a security problem, then locate a line of code that is the proximate cause of a security vulnerability, we can use git blame to trace that to a commit. It would be more helpful if we could trace it to a github issue.
    f. "Tooling needs to make the right path also be the easy path." Talking about requirement to have commit message link to an issue.
4. Common tooling with the release work group: need to get information about upstream projects: license.manifest and packages.manifest that shows versions. Our security team would want to investigate security aspects.
5. Brad: Will not be getting security vulnerability reports at this time.
6. We discussed opening up this group’s meetings, for example, by announcing in the email list. Joseph: Probably want at least a prototype vulnerability reporting process in place first.

Comment that OpenWall mailing list would show, in part, how to deal with CVEs.

Held Date: 2018.07.11, 10 AM PT

Attendees: Joseph, Patrick, Emily, Scott, Brad

1. Quick overview/intro for Scott
    a. Joseph: explanation of documentation & process goal behind security WG
    b. Scott works on fw security arch @ Lenovo. Here to get an understanding first
2. Brad: Once we define a process for sharing vulnerabilities, we will be flooded with vulnerability reports. MS Security has a review waiting for us. What will we do with all these reports? We don't have headcount to fix it all. (Maybe cover next time)
    a. Patrick: if we collate all that info we can put it on a release schedule and alleviate the crush of bugs.
    b. Depending on reporting/mitigation process, that might not be a problem. So we should build the process thoughtfully.
    c. <Picking up during meeting 7/11. Notes before this are from previous meeting 6/27>
    d. How does the security WG work together with release WG?
    e. Brad: Blackhat conference, there will be talk on BMCs. Probably disclosing a number of vulnerabilities. So we'd better hurry on the process, these reports are coming, we need to deal with them. James M attending, Ben Stoltz, maybe another Googler.
    f. Brad: CVE process? Is this worth pursuing? Suggested by someone (James)
    g. Patrick: There is value in following existing FOSS process to insulate from mistakes during roll-your-own. But OBMC is 100s of Yocto packages, we need a process to coalesce bugs/patches/etc for those in addition to ones we find in OBMC specifically.
    h. Joseph: OBMC documentation today has a sentence about Yocto packages, grabbing security fixes. We should focus on this esp for releases. We should also focus on how to report problems specific to OBMC layer
    i. Brad: No, let's not roll our own, bad idea. But how to go from A) vulnerability disclosed at sec conference to B) CVE process & actions
    j. Brad: MS have done security review of OBMC and has lots to disclose, but is waiting for a process to be defined.
    k. Patrick: If we say we will use CVE database, MS wants to know whether there's additional process - internal disclosure first? What key for db? Once we agree to use CVE, we have a process that's well-defined to have people refer to. Maybe not much value in holding reporters back from disclosing vulnerabilities, since the source is open already, it's probably fine to have it out in the open.
    l. Patrick trying to figure out where to request to create new project for CVE. OK to do offline. **Who wants this as action item??** Patrick TODO
    m. Joseph: Once we have process, place for CVE to go, have MS report a few, tire-kick the process, write some Github issues, documentation etc.

n. Joseph: But, we need maybe different process for high-impact (easy to reproduce, and creates a large hole) vulnerabilities. We probably want to request that people let us fix the vulnerability before the CVE gets written.
o. Patrick: We should probably look over the list of vulnerabilities from MS to rate what's high-impact or not, and use this as good training data etc for figuring out our process/rating system
p. Action item: Get somewhere where people can write CVE against our OBMC project (Patrick)
q. Action item: Privately get list of vulnerabilities from MS, IBM, etc. How to do this? Can't publish it openly… but maybe can just email a handful of people, TSC? I.e., have one rep from each company disseminate the list as necessary. And then, once we have process set, we can name the right POCs on website. (Brad)
    i. Brad: Is it necessary for Brad to do introduction to MS security rep? Who should do that? Brad will send introductory request.
    ii. Joseph: As an alternative, we can establish a process first, then kick the tires on our new process?
    iii. Brad: I'll just send an email and ask the list to be forwarded to company reps. Ali probably will want to wait for another couple weeks/next TSC meet. No rush. Will send email today.

3. Status of security documentation reviews:
    a. Joseph: https://gerrit.openbmc-project.xyz/#/c/11120/
    b. James: https://gerrit.openbmc-project.xyz/#/c/11164/
    c. Joseph: Pending firmware architecture (Linux: device files, D-Bus object, REST URIs) review which describes the architecture and identifies elements. The idea is to commit/approve/merge this framework first, then engage developers to focus on their specific element as time and interest allows.
    d. Should we break the existing reviews into smaller pieces, or can we move forward? Answer: Go ahead an advertise that the review is outstanding.
4. Status of user management work. Docs are approved, implementation is in review.
    a. Nobody on call to discuss this. :(
5. Patrick: Maybe we should integrate FOSS static analysis tools (like valgrind, code coverage tools, static code analysis) & include as part of release process? Worth considering. Patrick offered to look into it further.
    a. Joseph: We have a Gerrit-initiated Jenkins process that performs a limited set of static analysis on each patch set such as clang-format.
    b. Brad: It's related, easy to add to the process that exists now.
    c. So, this is good low hanging fruit. Yay.

Notes
Date: held on 2018.06.27, 10 AM PT
Attendees: Sossy, Emily, Patrick, Brad, Sub, Joseph, James Mihm, Ed Tanous

1. Update on security documentation reviews. Is help needed?
    a. James has review of architecture on Gerrit, partly complete

        i. Haven't had time to look at comments yet. Later this week will review comments etc
        ii. Joseph: Overall comments are positive, value-add
        iii. Joseph: HW aspects first? When talking about web server/rest/ipmid, why not bring in area developers? Is this an option? -> Sure
    b. Joseph has functional assurance stuff, also partly complete. Update: 2018-07-09: This was pushed to gerrit for review: https://gerrit.openbmc-project.xyz/#/c/11120/
        i. Will scope out TODOs from the first draft and hope to finish the partial first cut.
        ii. Have buyin for overall structure
        iii. Probably worth checking in at this point, and adding on later
2. ~~Joseph: What external standards could/should apply to OpenBMC? Including development standards (such as https://bestpractices.coreinfrastructure.org) and functional standards (such as OCP, HTTP and web-apps, etc.).~~
3. Joseph: Propose a model for how the security working group works with other OpenBMC development areas. See immediately below.
    a. Development team needs to own their own security items. How will Joseph and James engage other development areas? Bring in who owns the components under scrutiny
    b. Copied proposal to google doc below. Thoughts?
    c. Emily: How is this going to work for staffing? Joseph: The security team is me. Given time budget from management to create some of this doc. James owns other document but doesn't have as many cycles to work with developers. So mostly Joseph using script below to engage devs, to try to get some effort but understand async nature of FOSS. But basic security documentation is important!
    d. James: This kind of parallels internal work too; my time upstream/downstream ebbs and flows. Couple times a week finding time for upstream.
    e. Joseph: How to prioritize which team to bring first? Talked to Gunnar some (web interface) Trying to get consensus on moving forward. Which teams first, what to do, how much participation etc
    f. Brad: Only way to make people do stuff: 1) fix content already there (vulnerability, doc) and 2) moving forward (don't leave a gap in the first place). Can't just tell people what to do w/ FOSS model. But can define a process for the project, for new features to ensure they are sec compliant. Embed into workflow. Should we start by defining what developer workflow is?
    g. Ed: Once we get there, process is code -> update doc. But we don't have any bootstrap security doc. Need that doc from each team. James's doc is sketched out for web server, rest, etc, but how do we flesh out each section w security considerations? Update 2018-07-10 Joseph: See agenda item 2c above.
    h. Brad: As a developer, I don't want to think and just write code, and it's easier to follow an example. Is that the goal of the security documentation? Joseph: Yes,

in my opinion, the security docs must be written primarily for the development team to use (with extra landmarks for outside teams like security professionals); that is what we are aiming for. When there are written, the docs can be consulted for design considerations. The docs should be updated at the same time as the code, ideally(?) in the same review. Any new repos could be documented by following the pattern.

i. Joseph: not quite at a level of detail like, for power control, do x. But we should have doc for higher-level tasks, how to fill out security doc, etc. Eventually, a checklist for developers to go through as part of release cycle to check whether known threats mitigated
j. Big pieces are involved in writing upfront doc. We don't really need a lot of work every release.
k. Brad: This checklist is a big goal for the working group, please. Can we add an empty list to the release process, and then fixup the checklist as we go? Update 2018-07-09: This checklist was added (with a single placeholder item) to the security documentation review.
l. Ed: Incremental changes are easier to suss out disagreement than big blocks of stuff
m. Brad: functional security (checklist) vs documenting how to write security doc? Security process vs security documentation process. Which one do we need? Brad's rec is to do the checklist first or instead of the per-project documentation.
n. Everyone is in agreement to define a process for release (release planning WG), starting with empty checklist. But we want to put something on to come up with general security ideas. I.e., check against yocto, openssh for security concerns. Obmc-specific stuff that's not part of upstream yocto we can worry on. (Joseph can own looking upstream etc?)
o. James: Will you document how security doc lifecycle can gate release lifecycle? How will we block releases for security? Will we document that linkage?
p. Joseph: yeah, there is a section for security/release planning. Will add more today based on this conversation.
q. It sounds like we agree we want a per-release process for OpenBMC overall to cover security topics. Security README? New file? We probably want separate document for the concise checklist. "This doc is where the release considerations go."
r. James: need reviewers. But consider that most of dev team hasn't done a lot of these docs before, the content/form is new.
s. Maybe it'll be better to put up an empty outline and then a commit per section, and invite stakeholders for each area. (Each section is a different set of stakeholders, i.e., section for REST, section for web server, etc). Pushing empty framework into doc repository, is this ok? Brad: Yeah, sure, LGTM, push it
t. Brad: Every patch series should tell a story - i.e., it's ok to have atomic commits that just do one step of the way. So a skeleton doc is fine. No difference in end product but localized chunks are easier to digest.

4. Joseph: The following topic came up in my security doc review. Perhaps we can discuss briefly and create a github issue for it?: I propose that the OpenBMC project identify security considerations for any projects it pulls in, and explain how it configures each item and why. ⇒ An example identification and how and why: OpenBMC uses Dropbear for SSH instead of OpenSSH because Dropbear has a much smaller memory footprint. However, dropbear release schedules are different than OpenSSH which may affect which cryptographic ciphers are supported for TLS/SSL connections to the BMC.
    a. Can we see an example end-to-end for a single component explaining all the configuration, what's different, what's a risk etc first?
    b. Sounds like we do want a document like this. Can do this as smaller reviews, and then others can follow along with the pattern
5. Brad: Once we define a process for sharing vulnerabilities, we will be flooded with vulnerability reports. MS Security has a review waiting for us. What will we do with all these reports? We don't have headcount to fix it all.
    a. We can possibly collate the information from teams about security with the CVEs we pull in -- if there's a process in place to handle these things we can peg items to a list.

Joseph: My proposed collaboration model (in markdown syntax): Update 2018-06-27: This is not the model. We are the model of using a series of short, focused commits.

~~# The OpenBMC security documentation collaboration model~~

~~Here is what to expect when working with the security group on an initial review of your area:~~
~~- We'll work on a mutually agreed timeline prioritized with all the other work.~~
~~- We'll work together to understand your area's security considerations. We need to learn about your area, and you many need to learn some security concepts.~~
~~- We'll help you write your security documentation. When done, it will clearly state all of your area's security considerations. The security area will ideally maintain only an index into your documentation which binds together multiple areas, for example, referring to (area A:) web server documentation and stating its relationship to (area B:) the reverse proxy server.~~
~~- The documentation may suggest additional work items. High-impact security vulnerabilities will remain confidential until they are mitigated.~~

~~How can a security review help you? It can help:~~
~~- focus another set of eyes on security~~
~~- write security documentation accessible by new developers and~~

~~- security experts~~
~~- provide assurance that all security topics are covered~~
~~- identify security vulnerabilities~~

~~So what is security?~~
~~The [definition we use](https://gerrit.openbmc-project.xyz/#/c/11120/3/security/README.md) is:~~
~~- Security is broadly defined to mean avoiding negative impacts to the confidentiality, integrity, and availability of the BMC's resources. Resources include information stored by the BMC and its capability to control itself and its host server.~~
~~- So the review will be looking at all the places where vulnerabilities generally appear.~~

~~How we get started:~~
~~1. We'll start by telling you what we know about your area's function, interfaces, and security considerations.~~
~~2. We'll establish a conversation. We'll be interested in what you consider to be security functions and external interfaces. We will ask follow-up questions about areas that may have security relevance, for example, internal interfaces an attacker can use.~~
~~3. We'll summarize your area's security story. The story should become part of your area's documentation and clearly explain all security considerations.~~

~~For higher levels of assurance, we can continue inspecting and documenting your area, including:~~
~~1. The internal design, to identify interfaces an attacker can exploit such as network connections, what files you read and write, dbus objects you work with, what shared object (*.so) libraries or programs you provide or use. Other internals include places where you gain or lose privileges or capabilities, or switch users. The idea is to understand the basic architecture and identify vulnerabilities.~~
~~2. The implementation, for example, tracing code that takes a password to the point it is validated. The idea is to explain the implementation and why it is correct.~~
~~3. The testing effort. The idea is to explain the overall testing architecture and how it provides complete coverage.~~

Agenda:
Date: 2018.06.20, 10 AM PT

1. Status of Joseph's security documentation review - https://gerrit.openbmc-project.xyz/#/c/11120/

2. Status of James' OpenBMC security documentation - https://gerrit.openbmc-project.xyz/#/c/11164/
3. Status of User management spec - https://gerrit.openbmc-project.xyz/#/c/8440/
4. Determine what elements are needed in the BMC product lifecycle (see 2018.06.11 item 4) and how OpenBMC talks about downstream development activity such as build and provisioning.
5. Sub: interaction with the Trusted Computing Group (TCG) and OCP Security Group

2018.06.20

Attendees: Patrick Venture, Brad Bishop, Joseph Reynolds, Sub, Ratan, Ben Stoltz, Christopher Engel, Sossy

1. Status of Joseph's security documentation review - https://gerrit.openbmc-project.xyz/#/c/11120/
   What OpenBMC team does, best practices
   Question for reviewers: Is this the right structure for the security team?
   Joseph's notes: We'll move forward on this topic with the Gerrit review process.
2. Status of James' OpenBMC security documentation - https://gerrit.openbmc-project.xyz/#/c/11164/
   Describes interfaces and protocols and assumptions made on these
   Needs a section for Nuvoton?
   How does the document scale for the number Soc?
   a. OpenBMC Software stack versus the hardware on which it runs (Aspeed BMC, Nuvoton BMC, etc)
      i. Software interfaces exposed
      ii. Hardware interfaces exposed
   b. In order to have a full security story, one has to make security descriptions for each hardware configuration.
      i. A fully secure design needs requirements.
   c. Need a hardware design to handle specific requirements, this is vendor/chip agnostic.
   d. Joseph: As requested, created https://github.com/openbmc/openbmc/issues/3265 titled "What approach to document security considerations for various BMC hardware?" to track this item.

   Describe goals, non-goals, security objectives
   Assets and objectives for protecting the assets
   Brad: Would there be consensus on objectives?
   Venture: Yes, a subset.
   James: Some of the non-goals for now, would like them to be goals later. For example, detecting that a chip swap has happened.
   Ben: Another discussion needed: code integrity. Signature needs to be out of attestation.
   Ben: We need a method for verifying the code and bugs that are running on the chip are what we expect. TODO: Ben please correct as necessary

Joseph: The beginnings of how to track issues are being developed (how to use openbmc doc) (Joseph: see https://gerrit.openbmc-project.xyz/#/c/11120/2/security/obmc-development-practices.md topic “issues” and https://gerrit.openbmc-project.xyz/#/c/11120/2/security/obmc-downstream-best-practices.md topics “obtain source code”, “build”, and “provisioning”)
Venture: Are you talking about CVEs?
Joseph: (revisionist history:) The “development practices” doc mentions the issues database, but the OpenBMC team does not yet have a formal process for bug tracking.
James: We will do that for Intel. Goes to keeping some things under wraps until the mitigation is in place.
Joseph: need the OpenBMC team to do that
James: security team that looks at CVEs all the time and we need to interface to open source project
Joseph: Need someone who can put that together, independent of a release.
James: Need to consider smbus/i2c, protect access from outside access
James: There’s a risk level associated with assets that need to protected, it’s subjective.
Joseph’s notes: We’ll move forward on this topic with the Gerrit review process.

3. Status of User management spec - https://gerrit.openbmc-project.xyz/#/c/8440/
   Joseph: very similar to a AAA server, could this interface be used for an enterprise class management solution? (answer: not perfectly suitable, no)
   Ben: If it has any passwords, user and roles, we’d probably object to it.
   Joseph: We’re moving forward with this, is there a better solution for enterprise
   Brad: Leave objections soon, this has been out there since Jan.
   Ben: If you decommission, information can be harvested, better to rely on external service, certificates
   Brad: What about servers not in data centers
   Ben: Not saying there shouldn’t be a choice, just one we can’t use
   Brad: Next up is for someone to propose an alternative solution
   Ben: Everything on BMC must be something that consumed by public
   (Service users and login users are equivalent in this conversation.)
   Brad: User module can be excluded from image
   Brad: i2c linux kernel example: started with multiple versions, but eventually merged common code into i2c-core. Envision the same for OpenBMC. A framework will fall out from what we’re here.
   Joseph’s notes: Summary: We’ll move forward with the User management spec with the Gerrit review process. We are accepting other AAA proposals. We can offer downstream development teams a choice of AAA models from (a) basic Linux login, (b) the current User management spec, and (c) a solution that does not store *any* secrets on the BMC.
4. Determine what elements are needed in the BMC product lifecycle (see 2018.06.11 item 4) and how OpenBMC talks about downstream development activity such as build and provisioning.

Joseph's notes: Summary: Review with the Gerrit review process.

5. Sub: interaction with the Trusted Computing Group (TCG) and OCP Security Group
   High level set of requirements. Doesn't get into specific details of design. Takes TC workload in a PC environment and adapting to a BMC environment. Focused on TPM, trusted/measured boot.
   Joseph's notes: The OpenBMC security working group has members who call in to the OCP meetings, so we'll stay in contact.

Action Items from Meeting:

1. We need a method or process associated with CVEs.
2. All parties leave feedback on:
   a. https://gerrit.openbmc-project.xyz/8440
   b. https://gerrit.openbmc-project.xyz/11164
   c. https://gerrit.openbmc-project.xyz/#/c/11120/
   d. https://github.com/openbmc/openbmc/issues/3265
3.

2018.06.11

Attendees: James Mihm, Joseph Reynolds, Brad Bishop, Ed Tanous, Sub, Christopher Engel, Jayanth, Supreeth Venkatesh

Agenda

1. The group needs an online forum for agendas, meeting notes, and discussion. I had created an #openbmc_security IRC room, but a topic-based collaboration tool would be better. I hope someone will look into that and and propose something to the group. Objective: choose a forum to use.

2. The "meeting in secret" topic came up several times. I propose we make a list of items to keep secret, publish that list to the overall OpenBMC group, then get all secretive only when discussing items on that list. Here is my starter list:
   1. High-impact vulnerabilities (high-impact means: easy to exploit, has large consequences), until mitigation is available (examples: workaround documented, fix merged into github.com/openbmc master branch and tested).
   2. Results of vulnerability analysis, until high-impact vulnerabilities are mitigated.
   3. Results of penetration testing, until high-impact vulnerabilities are mitigated.

Objective: agree to this approach to secrecy.

3. I think OpenBMC may need multiple security frameworks to address different concerns. Certainly network security (authentication, supported ciphers, etc). Probably open source security. Maybe device security?? I would be happy supporting the Common Criteria framework which is perfectly happy deferring to other standards, so I don't see that work duplicating anybody else's.

Objective: agree that multiple frameworks may be needed.

4. Protection Profiles.
Objective: Determine if the group thinks the OpenBMC Protection Profile is a good way to move forward, or what the alternative is.

5. Authentication, Authorization, and Auditing. I think enterprise data center customers will want OpenBMC to offer a good way to manage AAA functions. I would like to find out more about the requirements, open source models, and how much work it would be for the OpenBMC team.
Objective: Share concerns and issues in this area.

Notes

1. The group needs an online forum for agendas, meeting notes, and discussion.
    - Use #openbmc_security IRC chat and git/gerrit for threaded topic conversations Joseph: ...and use google docs (this document) to add agenda items and meeting minutes.

2. The "meeting in secret" topic came up several times.
    - cve.mitre.org
    - Some secrets, if there's a vulnerability that doesn't have a mitigation, keep it secret until there's a fix
    - Need to provide a process that allows external reporting of vulnerabilities
    - Difference between vulnerabilities in deployment and in development
    - AI: read up on cve.mitre.org processes Joseph: Where in this website does it describe how a project like OpenBMC should set up a process for its users to report vulnerabilities? The closest things I found was: https://cve.mitre.org/compatible/guidelines.html x

3. I think OpenBMC may need multiple security frameworks to address different concerns.
    - Need different frameworks for different things
    - Joseph: We need stories for functional security, product lifecycle, functional security requirements implemented by development team
    - Ben: agreed, but CC isn't the right approach
    - Joseph: Backing off CC. Joseph: 6/14/2018- I've written the OpenBMC lifecycle security story and pushed it for review at https://gerrit.openbmc-project.xyz/#/c/11120/. Please add yourself as a reviewer if interested. I plan to abandon the previous security review (but refactor the material -- thanks for your comments!).

4. Protection Profiles.
    - Joseph: Not the right person to work on protection profiles
    - Ensuring OpenBMC is following the requirements to enable certification is important, not everyone is getting certifications though
    - OpenBMC protection profile could be a piece of a larger certification
    - James: will upload Intel security architecture document

- Joseph: No need to publish the CC work since it's covered by James' effort, but will still pursue it

5. Authentication, Authorization, and Auditing
   - Joseph: Is there a way to put in a AAA server that could be used by an enterprise datacenter?
   - It's being worked on…
   - Who and what's the solution like?
   - There's a mailing list post on user management, Richard (from Intel?)
   - Brad: There isn't any code in OpenBMC, we need something
   - Ed: dBus wrapper around PAM,
   - Brad: dBus allows you to make a data model, proposal for data model for AAA (user management)
   - Look for things by Richard in gerrit
   - How do we get people to review things?
   - Cc ppl on reviews directly, could use a mailing list
   - AndrewJ maintains the tools repo but there's no group for general OpenBMC tools (gerrit for auto adding reviews)
   - AndrewJ wrote a tool, wrapper around doing git pushes that will automatically cc people in maintainers file.
   - Ben: the tool promotes best practices
   - Gerrit support running this automatically, just needs to scripted
   - Brad: ok but no one is volunteering
   - AndrewG is the person to talk to about getting admin privileges for anyone who wants to tackle it

Let's meet weekly, some day 10AM PT

Sub: Trusted Computing Group (TCG) and OCP Security Group, what do we want to see being discussed. Maybe check out their minutes or get someone from these groups to come to our meeting

2018.05.31
Attendees:

- Ben Stoltz, Nancy Yuen, Patrick Venture, Brad Bishop, Joseph Reynolds, Ed Tanous, James Mihm, Sub, Ratan Gupta, Jayanth, Supreeth Venkatesh

Agenda:

- Introduction round table: what you're interested in and why
- Joseph Reynolds: OpenBMC security documentation project https://gerrit.openbmc-project.xyz/#/c/10443/
- Ben Stoltz: CC as it applies to design and implementation phases. Separation of policy and mechanism in BMC lifecycle, including product lifecycle manufacture, provisioning, deployment, operations and maintenance, recovery, and disposition. Joseph Reynolds: The CC model ALC assurance class ("Lifecycle support") talks about these topics. I've started to sketch them out in the framework on gerrit: https://gerrit.openbmc-project.xyz/#/c/10443/15/security/obmc-security-framework.md E.g. repairs: {Low-/Med-/High- touch} x {manual-/automated-self-/automated-assisted-repair}. Joseph Reynolds: I'll add a Protection Profile Module for automated repairs.
- Security topics that need to be investigated/discussed for future meetings
- Private vs public meetings
- Regular meeting times

Propose a separate protection profile for each authorization method

- IPMI user/password
- Pluggable Authentication Modules (PAM) https://en.wikipedia.org/wiki/Pluggable_authentication_module
- Redfish security http://redfish.dmtf.org/schemas/DSP0266_1.1.html#security ← note incorrect link in the document, you probably want Chapter 9: http://redfish.dmtf.org/schemas/DSP0266_1.1.html#protocols

Followup notes from Joseph Reynolds: Here are my notes and followup ideas from the OpenBMC security working group meeting.

I recorded the following information in the OpenBMC security documentation, indexed by Common Criteria (CC) chapters and security classes. References into the CC pubs are provided for more details about each topic. The references to CC are to "v3.1. Release 5," and can be found here: https://www.commoncriteriaportal.org/cc/.

OpenBMC Protection Profile

The OpenBMC Protection Profile (PP) content is in rough shape. The group is just getting started.

The "Objectives" section has statements about multiple users, authorization, auditing, etc. These were all straw-man proposals for a minimum function BMC. In particular,

OpenBMC already supports multiple users, effectively those with root/sudo access and those who don't.

I am adding the following ideas to the OpenBMC security documentation:

- Idea: OpenBMC should offer a role-based authorization model like RedFish: redfish.dmtf.org/schemas/DSP0266_1.1.html. [ref: CC part 2, FDP User data protection]
- Idea: OpenBMC should offer a pluggable AAA (authentication, authorization, accountability) service. When enabled, functions (like REST APIs, Web Apps, IPMI) must use this service. The service provider can be a stub (local linux userid authentication), something like LDAP, or something more sophisticated. If an external server is used, [ref: CC part 2, "Inter-TSF TSF data consistency (FPT_TDC)"] applies.
- Idea: OpenBMC should anticipate functions that require trust between 2 or more BMCs, for example, to move a virtual machine from one host to another. [ref: CC part 2, "Internal TOE transfer (FDP_ITT)"]
- Idea: if the OpenBMC is configured for secure boot (of itself) and cannot securely boot itself, it functions with limited privileges, for example so it can reinstall its firmware and reboot itself. (IP concerns??)

The OpenBMC Protection Profile meta-discussion

Much of the discussion about security features was based on the OpenBMC Protection Profile. And nobody said using a PP was a bad idea. And teams who use OpenBMC to create commercial products with security certification may choose to pursue CC certification. So I will continue to favor the PP format.

I strongly prefer to use the basic PP format [ref CC part 1, section B.2, "Mandatory contents of a PP"]). That format is: {assets,users} -> threats -> {objectives,assumptions} -> requirements. However, until we get these in much better shape, I don't think it is worthwhile cost/benefit to do the formal cross referencing required by the CC standard. So I propose we leave that for later (much later), and catch problems in the spec with a review process.

How much detail should we put into the OpenBMC PP? My opinion: Follow the CC guidelines in [ref: CC Part1, "B.3.1 How a PP should be used"]: a statement of need, a specification, a baseline for developers. The standard also talks about [ref: CC part 1, section B.3.2 "How a PP should not be used"], but it is okay with me if we give a more detailed specification than is strictly needed and if we talk only about only the OpenBMC.

My idea for what to include in the initial OpenBMC PP is: exactly the set of security features OpenBMC has now. I think we can also put in features that the OpenBMC team is currently implementing. Then we would enhance the PP as OpenBMC adds features. But I don't see much value in creating a spec for more than a release away. That's what the PP Modules are for.

I am collecting ideas for PP Modules (in the protection-profile-modules file). These are very informal now, with the idea to incubate ideas now, and in the misty future to either (a) merge them into the base PP or (b) make a formal PP Module.

I will create a PP Module for the pluggable AAA service. Are any IP concerns with this? Reference material?

End of notes from Joseph Reynolds.

Product lifecycle outline

Here is a rough DRAFT outline of the OpenBMC product lifecycle security assurance topics based on my (Joseph Reynolds) limited understanding of OpenBMC development; it and may contain errors and omissions. [Cut/paste from Word.] Joseph: As of 6/14/2018 this has been moved into a gerrit review at https://gerrit.openbmc-project.xyz/#/c/11120/

~~0) Notes~~

~~a) OpenBMC is a toolkit to make it easy for downstream development teams to build BMC firmware for their project. This document outlines practices and procedures the OpenBMC team uses to support the use case of using OpenBMC in highly secure installations, and provides guidance for such development teams.~~

~~b) References are to OpenBMC and the OpenBMC development team except where downstream and upstream development teams and project are specifically mentioned.~~

~~1) OpenBMC Development~~

~~a) Project identification. OpenBMC development refers to the project described by https://github.com/openbmc/openbmc and includes the git project, all contributors to the code, participants in meetings, etc. This does NOT include any upstream projects (that OpenBMC uses), and does not include downstream development projects (that use OpenBMC).~~

~~b) Source code identification – There are multiple source code repositories under https://github.com/openbmc. The primary repository is github.com/openbmc/openbmc which contains the top-level build instructions. It must be configured for a specific target architecture before it can be used to create an install image. Based on this configuration, the build process pulls in various repositories from github.com/openbmc and from other open source projects. All the repositories under github.com/openbmc are under source code control.~~

~~c) Overview: OpenBMC is open source and changes can be submitted by anyone. However, code review, continuous testing, and source code maintainer processes accepts only high-quality changes for merging into the project. The project's "contributing" page explain this.~~

d) Code review process – Anyone can develop material (code, documentation, etc.) for OpenBMC in their private repositories and submit their material for review using gerrit or emailed to the team's email list. A review is conducted by the OpenBMC development team which includes subject matter experts for each repository. Comments are recorded and responded to. Re-worked material is seen in context with previous versions. The review results in the proposed change being accepted, rejected for reworking, or abandoned. Each repository has a small list of maintainers who accept only high-quality material and merge it into the public repo.

e) Development team education – The development team consists of anyone who submits material to the project (whether that material is accepted or not). There are no education requirements.

f) Development review team education – The development review team consists of the people names as reviewers (and maintainers) for each of the OpenBMC repos. (TO DO: that list is controlled by each repo maintainer?) Their opinion matters in the decision to accept the changed material. The OpenBMC team maintains contributing guidelines, including source code formatting, etc. The reviewers are highly-skilled software engineers who are aware of software and hardware security practices and accept only high-quality contributions.

g) Source code repository maintainers – Each of the github.com/openbmc repos has a small list of maintainers. Github prevents others from making changes to the code. Generally, the changes are merged into these repos from a Gerrit review process. (to do: The gerrit website is managed by whom? And configured how?) NOTE: The github.com/openbmc project uses git's fast-forward merge strategy to avoids all merge conflicts.

h) Use of open source projects and toolchains – The OpenBMC build process pulls in other open source projects, including Yocto, OpenEmbedded, and many others. The exact list depends on how OpenBMC was configured to build (and can be found by the development team using the bitbake -e command). The open source packages are from reputable sources, specific releases are used, and the secure hashes (?) are validated during the build process. All such hashes are stored in the OpenBMC build repository (originally github.com/openbmc/openbmc or as cloned) which means the exact set of packages can be controlled.

i) External development tools: OpenBMC relies on web-based tools such as Gerrit, Jenkins, and Github to provide their own security. The OpenBMC developers who have administration access to these sites protect that access.

j) Secure development environment

    i) OpenBMC contributors are not expected to have a secure development environment. See the code review process.

    ii) OpenBMC maintainers are authorized to make changes to the source code and generally have secure development environments. To-do: this is weak! Can we strengthen this statement?

k) Work items including defects are recorded under github.com://openbmc/openbmc/issues. (TO DO: Who can close issues?)

2) Downstream Development

a) Identification. Downstream development is any project that uses OpenBMC as part of its function. A simple application is building a firmware image from the example OpenBMC configuration and loading it onto a BMC device.

b) The expected use case for the downstream development team is to:

i) Create a secure development environment: controlled access to the hardware, storage, command-line interfaces, etc.

ii) Fork (copy) an OpenBMC release and place that under source code control in a private repository into the secure development environment. Only this copy is used for validation or further changes.

iii) Optionally create a private mirror site within the secure development environment to contain all the packages pulled in by OpenBMC.

c) The downstream development team is expected to modify OpenBMC code and configure OpenBMC's behavior, including:

i) Userids: OpenBMC defaults to a Linux image that has the root userid set to a well-known password.

ii) Web server: OpenBMC uses Nginx as a reverse proxy to serve web apps and REST APIs. The OpenBMC REST API is currently a Python Bottle app. TO DO: Check this: The OpenBMC web app is

iii) IPMI server: An IPMI server daemon starts. You may want to configure it to respond only to white-listed functions, provide additional authorization and access controls, or not start the daemon.

iv) Configure the build process to digitally sign the firmware images.

v) Etc. TO DO: More work is needed here.

3) Test

a) OpenBMC functional test cases are part of each repository. In addition, a Jenkins server at https://openpower.xyz run a continuous integration test which compiles, starts up the a QEMU-based BMC, and runs tests.

b) The OpenBMC team has an active community including downstream development teams that submit fixes back into the OpenBMC project and its upstream projects (such as the Linux kernel).

c) Downstream development teams are expected to have their own testing agenda.

4) Release

a) As of 6/2018, the OpenBMC project is beginning to plan regular releases, with the first release around November 2018, and continuing twice per year following the Yocto project release schedule.

b) I expect OpenBMC releases to be identified by code name, semantic versioning, or git commit id.

c) I expect the OpenBMC team will generally consider upgrading package versions (Yocto/Linux, OpenSSH, web servers, etc.) to pick up updates once per release.

d) I expect OpenBMC release notes to include a statement of what open source projects it was built from, including release level. (Note that Yocto helps provide that.)

e) I do not expect OpenBMC to identify flaws (security or otherwise) that were fixed in the release. Interested parties can review OpenBMC's source code commit history.
f) Downstream development teams are expected to have their own release schedule which may involve more frequent security updates.

5) Build
   a) OpenBMC is a toolkit for creating firmware. A primary part of the toolkit is a build process based on bitbake/Yocto. The build process begins with source code and creates a firmware image that can be installed. However, the OpenBMC release process does not invoke the build process nor does it build firmware. The steps in this section are provided as guidance for downstream development teams building OpenBMC images intended for use in a highly-secure environment.
   b) It is expected that a secure build environment be established for building the installation image (like the secure development environment). The build environment is typically separate to keep the source code clean, restrict access to the private keys for digital signatures, etc.
   c) Build process – The build process begins in a secure environment with a git clone from a private repository. All other code is pulled in (as described above) from the internet or from mirror sites that can be controlled by the build environment and directed to private repositories. The gcc-based tool chains are built and used to target the specified architecture (aka cross compiler).
   d) Digital signing – It is expected that the resulting install images will be digitally signed as part of the build process, presumably using a private key within the secure build environment. TO DO: Explain how you can digitally sign the firmware during the build process.

6) Provisioning
   a) The OpenBMC team does not provision firmware. This section is provided as guidance for downstream development teams provisioning devices built from OpenBMC intended for use in a highly-secure environment.
   b) OpenBMC has a few ways to update its firmware.
      i) TO DO: How to install firmware on a blank device? Like an empty flash drive.
      ii) TO DO: Can OpenBMC guarantee updates validate the digital signature?
   c) Installation image: Something more than installing the OpenBMC image onto the BMC device and checking the digital signature?

7) Operation
   a) TO DO: Operation is via the REST APIs. Maybe IPMI is needed?

8) Repair
   a) The only way to repair flaws in the OpenBMC firmware is to replace the overall image. OpenBMC has several ways to replace its firmware. TO DO: Enumerate the interfaces (scp, REST API, ./bmc_update.py, more?).
   b) TO DO: Which of these validate the digital signature?

c) The OpenBMC team is just beginning (as of 6/2018) to think about supporting releases. It does not have a plan for providing urgent fixes, for example, involving branches under the github.com/openbmc/openbmc repository.

d) TO DO: I expect developers will want to diagnose OpenBMC or OpenPOWER firmware problems by getting onto the system and entering Linux shell commands. I expect developers will want to provide test fixes and data collection instrumentation by installing custom-built programs to replace functionality.

9) Decommissioning

a) OpenBMC stores host data on nonvolatile storage. It has the capability to erase this data. TO DO: Enumerate the interfaces.

b) TO DO: Are passwords (/etc/passwd) stored on the system?

c) TO DO: If private keys are stored, for example, for ssh access.

d) TO DO: Are web site certificates stored?

e) TO DO: Other credentials?

Why we care about supply chain security:
https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/
Why we care about coding style and code reviews (missing semicolon):
http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/att_collapse.html