OpenSSF Supply Chain Integrity WG Notes

We are helping people understand and make decisions on the provenance of the code they maintain, produce and use. We have great projects like GUAC, SLSA and gittuf that you can work with.

Meeting Times: OSSF Public Calendar
Charter: https://github.com/ossf/wg-supply-chain-integrity
Meeting recordings: https://www.youtube.com/channel/UCUdhiXNEBEayowJXY_v7AXQ/videos
Discussion group: https://lists.openssf.org/g/openssf-supply-chain-integrity
Projects: SLSA; S2C2F; GUAC; gittuf; Zarf; (FRSCA)
Slack Channel: #wg_supply_chain_Integrity
MEETINGS: Log in to your LFX Profile and go to MEETINGS to see your upcoming and past meetings. For help, Sucontact support@openssf.org

Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws. Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuhttps://www.youtube.com/channel/UCUdhiXNEBEayowJXY_v7AXQ/videosxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Code of Conduct

All OpenSSF meetings are subject to its code of conduct. See https://openssf.org/community/code-of-conduct/

Working group chairs

- Co-chair: Nicole Bates (Microsoft)
- Co-chair: Justin Cappos (NYU)
- Co-chair: Michael Lieberman (Kusari)

Apr 8, 2026

Attendees

-
- Kris Borchers (OpenSSF)
- Vishal Jindal (Apple Inc)
- Arnaud Le Hors (IBM)
- Mike Lieberman (Kusari)
- Jonatan Männchen (Erlang Ecosystem Foundation)
- Adolfo García Veytia (Carabiner)
- Justin Cappos (NYU)
- Nick Tait (Red Hat)
- Nell Shamrell-Harrington (Microsoft, Rust Foundation)
- Igor Ageyev (Wind River)
- axel simon (StackHPC)
- Rithikha Rajamohan (EQTY Lab)

Regrets:

-

Agenda

- Introductions
    - Nick Tait - Red Hat Product Security
    - Nell Shamrell-Harrington - Microsoft
    - Vishal Jindal - Apple, manages a supply chain security team
    - axel simon - StackHPC, helping with security for the company doing OpenStack deployments
- [Mike] - Low priority, but I have a neat little demo of how to protect against stuff like the axios and other attacks.
- [Puerco] Ramping up the AMPEL donation
  Ref: Sandbox Application Draft

Mar 25, 2026

Attendees

-
- Rithikha Rajamohan (EQTY Lab) -
- Nicole Bates
- Nell Shamrell-Harrington (Microsoft, Rust Foundation)
- Igor Ageyev (Wind River)
- Gwen Burchell (CloudSmith)
- Kris Borchers (OpenSSF)
- Laron J (

Regrets:
-

Agenda

- Introductions
    - Gwen Burchell - CloudSmith, team is building out policy engine for management of artifacts, rego.
    - Rithikha - hardware provenance - how SBOMs evolve for agent consumption. Hardware root of trust, TPM.
    - LJ- Laron - on defend pen testing company.
- Working Group 2026 Goals
    - Nicole will reach out to current projects to build connective tissues. Adding demo pieces.
- Does this timezone work? Kris will send out doodle poll.

Mar 11, 2026

Attendees
- Arnaud Le Hors (IBM)
- Mike Lieberman (Kusari)
- Kris Borchers (OpenSSF)
- Brandt Keller (Zarf / Defense Unicorns)
-

Regrets:
- Marcela Melara (Intel)

Agenda
- 2026 Priorities Review

- Next meeting:
    - Come with ideas - think outside the box - what should we focus on in 2026
    - IE - “Here are the projects that fall under WG SCI - here is how they could work with other OpenSSF projects”
    -

Feb 25, 2026

Attendees

- Judie Muhrez (EQTY Lab)
- Justin Cappos (NYU)
- Igor Ageyev (Wind River)
- Ivan Chubb (ARCYER)
- Arthit Suriyawongkul (Trinity College Dublin)

Agenda

- Could there be a common place to list GitHub repos, etc. on programming language repos? (Ivan) Preferably a field in a packages metadata containing a link to the VCS URL.
- Means of trusting in-toto attestations and scans results from closed-source vendors (Ivan)
- How to capture buildtime dependencies for multi-stage builds? (Ivan) -> SBOMIT

Feb 11, 2026

Attendees

-
- Kris Borchers (OpenSSF)
- Mike Lieberman (Kusari)
- Patrick Zielinski (NYU)
- Justin Cappos (NYU)
- Nell Shamrell-Harrington (Microsoft, Rust Foundation)
- Rithikha Rajamohan (EQTY Lab)
- Marcela Melara (Intel)
- Sunil Ravipati(Yottasecure)
- Ivan Chubb (ArCTIC)

Agenda

- Chair Election
    - Nominations closed, interim chairs were the only nominees

    - Should we continue with 3 co-chairs or should we hold an election
        - Agreement to continue with 3 co-chairs
- [Mike] - Quarterly update!
    - https://hackmd.io/3jmLRrVISjisemknt6gHjw –please update here if you are a maintainer of an SCI project or have anything you want to highlight

Jan 28, 2026

Attendees

- Justin Cappos (NYU)
- Mike Lieberman (Kusari)
- Marcela Melara (Intel)
- Nicole Bates (Microsoft)
- Gilbert Martin
- Brandt Keller (Zarf / Defense Unicorns)
- Igor Ageyev (Wind River)
- Sunil Ravipati (Yottasecure)

Agenda

- Chair Election
    - Nominations are open - https://github.com/ossf/wg-supply-chain-integrity/issues/84
    - WG Guidelines - https://github.com/ossf/tac/blob/main/process/wg-lead-R%26Rs.md
- [marcela] FYI: CoSAI Model Signing Maturity Model (paper, needs access permissions)
- Latest project updates - new projects ?
- Md Niaz Morshed - University of Alabama - Code review in OSS security survey https://universityofalabama.az1.qualtrics.com/jfe/form/SV_03zTHf83SiO01f0
- [Brandt] Zarf bias - pitch for zarf integration
-

Jan 14, 2026

Attendees

- Justin Cappos (NYU)
- Kris Borchers (OpenSSF)
- Brandt Keller (Zarf / Defense Unicorns)
- Marcela Melara (Intel)
- Adolfo Garcia Veytia (Carabiner)
- Sunil Ravipati(Yottasecure)

Agenda

- Chair Election
    - Kris will kick off the call for nominations by end of week
        - Self nominations are great. If you nominate someone else, please discuss it with them first.
- What do we want to accomplish?
    - White paper? Specific topic?
    - Supply Chain Integrity Working Group Discussion - Google Docs
    - What does the group do?
        - Current objective in the repo ossf/wg-supply-chain-integrity: Our objective is to enable open source maintainers, contributors and end-users to understand and make decisions on the provenance of the code they maintain, produce and use.
    - We could create a supply chain threat model
    - Darnit is trying to be toolbelt 2.0, etc.
    - Can we apply “all the right tools” somewhere, like this WG’s website or a hello world?

Dec 17, 2025

Attendees

- Mike Lieberman (Kusari)
- Justin Cappos (NYU)
- Kris Borchers (OpenSSF)
- Igor Ageyev (Wind River)
- Marcela Melara (Intel)

Agenda

- Discussed what we should focus on in the coming year.
    - Perhaps a white paper about what tooling to use

Dec 3, 2025

Attendees

- Zach Steindler (GitHub)
- Justin Cappos (NYU)
- Mike Lieberman (Kusari)
- Kris Borchers (OpenSSF)
- Igor Ageyev (Wind River)
- Marcela Melara (Intel)
- Adolfo Garcia Veytia (Carabiner)

Agenda

- [Justin] Let's update interim chairs in this doc ✅ and on GitHub repo ✅
    - PR for GitHub update Update WG chair information in README by kborchers · Pull Request #82 · ossf/wg-supply-chain-integrity
- [Zach S] Project survey!
    - SLSA Specification meeting
        - Ways in which things are signed
        - How should attestations be stored / distributed (specifically for Homebrew)
        - What's going on with Trusted Publishing
    - SLSA Dependency meeting
        - Looking for participants!
    - SLSA meetings are a bit confusing today - should SLSA Dependency track attend SLSA Specification meeting?
        - SLSA Specification meeting rotates through tracks, community, and other topics
        - Dep track could definitely benefit from lessons learned in 3 build track releases (as well as upcoming source track release)
- [Zach S] OpenSSF Working Group consolidation
    - Would y'all consider taking on ~~Zarf~~ OpenBao, SBOMit, Protobom, Fuzz Introspector, and Bomctl?
        - Zarf has been sponsored under WG SCI
            - Let's update https://github.com/ossf/wg-supply-chain-integrity?tab=readme-ov-file#activities!
            - [Brandt K] Agree - I will take this action item
        - Kris AI: work with Nicole to attend project meetings to start discussions about moving over to SCI WG
            - OpenBao - Dec 4 @ 9am EST

        - Kris attended this meeting and those present thought the change made sense. Alex will take the update to the TSC and they will reach out if they have any questions.
    - SBOMit - Dec 10 @ 9am EST
    - Protobom - Dec 17 @ 10am EST
    - Fuzz Introspector - only meets monthly, next meeting is Jan 6 @ 11:30am EST
    - Bomctl - only mention the Security Tooling WG meeting, next meeting is Dec 12 @ 10am EST
- [Mike L] Darnit

Nov 19, 2025

Attendees

-
- Kris Borchers (OpenSSF)
- Zach Steindler (OpenSSF/GitHub)
- Nicole Bates (Microsoft)
- Brandt Keller (Defense Unicorns)
- Mike Lieberman (Kusari)
- Marcela Melara (Intel)
- Deanna Medina (United Airlines)

Agenda

- Welcome new attendees
    - Deanna Medina
- Chair elections (Kris)
    - Nominations open now - Chair and Co-chair Nominations · Issue #81 · ossf/wg-supply-chain-integrity
        - Extending the call for candidates to next Wednesday
    - Chair + co-chair voting process
        - Separate votes vs ranked-choice vs something else?
            - Strongly recommend ranked-choice vote; top two vote-getters are the co-chairs
        - Do we need a chair and co-chair?
            - Leaning towards two co-chairs
    - Who is eligible to vote?

        - Is there a membership list somewhere that is up to date? If not, should we require some sort of registration process similar to TAC elections?
        - Should we ask for registration? Should we ask for evidence of participation in the WG and member TIs? Or evidence of participation in the OpenSSF in general?
            - Recommend pre-registration for anyone who has participated in OpenSSF in the past year
    - Alternate proposal: have the 3 people who have expressed interest be interim co-chairs until we can run an election in 2026.
        - We'll check with Cappos but this is the most likely outcome
- Future best practices for the working group
    - Consider meeting at APAC and EMEA friendly times
- [Nicole] Supply Chain Integrity Working Group Discussion - Google Docs to support brainstorming purpose of the WG.
    - How do we balance community feedback of open source maintainers with feedback from people who are consumers of open source maintainers?
    - Let's not be beholden to the charter, but let's use it as inspiration / make sure we learn from the past
    - Let's also look at the OpenSSF MVVSR
- Introductions?
    - Deanna Medina - has worked previously with Issac and SBOMs; compliance & GRC for United Airlines
    - Zach Steindler - GitHub + npm supply chain security for open source and enterprise users
    - Nicole Bates - supply chain security focused on transparency and ledgers at Microsoft
    - Brandt Keller - maintainer of Zarf (part of this WG) at Defense Unicorns; supply chain security advocate for public sector
    - Marcela Melara - Leads software supply chain research at Intel; maintains in-toto
    - Kris Borchers - technical project manager for OpenSSF

Nov 5, 2025

No attendance - cancelled

Oct 8, 2025

Attendees

- Mike Lieberman (Kusari)
- Ben Cotton (Kusari)

- Adolfo García Veytia (Carabiner)
- Marcela Melara (Intel)
- Kris Borchers (OpenSSF)
- Nicole Bates (Microsoft)
- Brandt Keller (Zarf/Defense Unicorns)
- Prince Oforh Asiedu
- John Andersen (DigitalOcean)
- John Kjell (ControlPlane)

Agenda

- Working Group revamp!
    - What is the role of the group?
        - Facilitators vs Tactical Executors
            - Maybe not be mutually exclusive and we can do both
            - Consider
        - Communication
        - Collaboration
            - Cross-project collaboration
    - Staff is making recommendations for how to improve groups and scope
    - Focus on the personas involved and how does that influence the work we do
    - “Does this time still work for everyone?”
        - Keep this open as an opportunity to explore
    - WG should not be solely focused on delivering project updates
        - Unify support, collaboration, use-cases
        - Share ideas ++
    - What are the current and future challenges?
    - Where can we begin building this knowledge?
        - Whitepaper
        - 2-pager
    -

Sep 24, 2025

Attendees

-

Agenda

- OSS Rebuild presentation

Aug 13, 2025 & Aug 27, 2025

No agenda — canceled

Jul 30, 2025

Attendees:

- Jay White (Microsoft)
- Mike Lieberman (Kusari)
- Zachariahcox (github)
- Marty Haught (Ruby Central)
- Marcela Melara (Intel)
- Kris Borchers (OpenSSF)
- Victor Lu
- Robert Martin
- Brandt Keller
- Ejiro Oghenekome

Agenda

- Welcome new attendees
    - Ejiro Oghenekome
- New workstreams (Mike)
- Meeting agenda [sigs reporting] and cadence (Jay)
- Guac updates (Mike)
- in-toto/SLSA updates (Marcela)
- Bundler policy layer (Marty)
-

Jul 16, 2025

Attendees:

- Isaac Hepworth (Google)
- Marty Haught (Ruby Central)
- Brandt Keller (Defense Unicorns)
- Bob Martin (MITRE)
- Nicole Bates (Microsoft)
- Adolfo Garcia Veytia (Carabiner Systems)
-

Agenda

- Welcome new attendees (Isaac)
    - Bob Martin (MITRE)
- Zarf & GUAC Integration (Brandt)
    - Quick Highlights from OpenSSF Community Days
    - Recording
    - https://docs.zarf.dev
    - Proof-of-concept GUAC/Zarf integration demo
- Package repository policy support (Marty)
    - License restrictions, security minimums
    - Prior art?
        - Mitre's SAF
        - CNCF's Policy as Code similarities
        - OpenSSF security baseline
        - In-toto attestations as a base
        - SCITT and Sigstore
        - ssci.io/attestations-deck — 101 on attestations and their use for policy
    - Write a 1 pager

Jul 2, 2025

[canceled]

Jun 18, 2025

Attendees:

- Isaac Hepworth (Google)
- Kris Borchers (OpenSSF)
- Brandt Keller (Defense Unicorns)
- Arnaud Le Hors (IBM)
- Tom Hennen (Google)
- Michael Lieberman (Kusari)
- Lee Preimesberger (HP)
- Rohan Sen

Agenda

- Welcome new attendees (Isaac)
    - nobody today

- SLSA Source Track preview (Tom Hennen)
    - [see recording]
    - Feedback to Tom on email or Slack :)
-

May 21, 2025

Attendees:

- Isaac Hepworth (Google)
- Kris Borchers (OpenSSF)
- John Kjell (ControlPlane)
- Nicole Bates (Microsoft)
- Patrick Zielinski (NYU)
- Marcela Melara (Intel)
- Rohan Sen
- Marty Haught (Ruby Central)
- Mike Lieberman (Kusari)

Agenda

- Welcome new attendees (Isaac)
    - Welcome Rohan!
- TI Audit Review (Kris)
    - WG Items
        - No TAC lifecycle document. Please review tac/process at main · ossf/tac
    - GUAC
        - Technical charter is not in the repo. Kris can provide a PDF version if needed.
            - https://github.com/guacsec/governance/blob/main/CHARTER.MD
        - Meeting agenda/notes should include the antitrust policy and code of conduct at the top. Use the WG notes as an example here
          OpenSSF Supply Chain Integrity WG Notes
    - gittuf
        - Meeting notes link on this README needs to be updated to the latest document gittuf/community: Governance and community aspects of gittuf
    - S2C2F
        - Technical charter is not in the repo. Kris can provide a PDF version if needed.
    - Security Insights Spec
        - Objective/motivation/scope missing from README
        - Unable to find any information about meetings
        - Technical charter is not in the repo nor in OpenSSF project management.

        - No TAC lifecycle document. Please review tac/process at main · ossf/tac
    - SLSA
        - SECURITY.md is not in the repo
        - TAC lifecycle doc is missing but there is an open PR to move to graduated state. Apply for SLSA graduation by lehors · Pull Request #415 · ossf/tac
    - Zarf
        - Need to add date/time of meetings and links to meeting notes to the README and/or website.
- Discussion on Audit items
    - Mike: Tie-up here with (a) security baseline; and (b) Security Insights itself, which can help index some of these assets in a standard way
- Relevant open CFPs and possible submissions (Marcela)
    - OpenSSF Community Day EU (deadline May 26, event Aug 28, co-lo with OSS EU)
    - Open Source Security Con (deadline June 30, event Nov 10, co-lo KubeCon NA)
    -

Apr 23, 2025

Attendees:

- Isaac Hepworth (Google)
- Justin Cappos (NYU)
- Brandon Mitchell (Independent)
- Eduardo Gonzalez
- Ben Cotton (Kusari)
- Michael Lieberman (Kusari)
- John Kjell (ControlPlane)
- Brandt Keller (Defense Unicorns)
- Brandon Lumb (Google)
- Marcela Melara (Intel)

Agenda

- Welcome new attendees (Isaac)
    - Justin Cappos — hi
    - Ben Cotton — hi
    - Eduardo Gonzalez — hi
- Demo of “Chainsights” (mike@kusari.dev)
    - “A PoC Supply Chain Transparency Protocol”
    - Context:

        - Producers
            - How do I tell the world what supply chain metadata I'm providing
        - Distributors
            - How do I make it easy for package publishers to declare what metadata they provide and consumers to easily discover that?
        - Consumers
            - What supply chain metadata is an organization providing?
    - See https://github.com/kusari-oss/chainsights
    -
- Any questions on GUAC/Trustification merge? (Ben Cotton)
    -

Apr 9, 2025

Attendees:

- Isaac Hepworth (Google)
- Daniel Moch (Lockheed Martin)
- John Kjell (ControlPlane)
- Cristian Urlea (University of Glasgow)
- Kris Borchers (LF)
- Marcela Melara (Intel)
- Laura Voinea (University of Glasgow)

Agenda

- Welcome new attendees (Isaac)
    - n/a
- SLSA Build Environment Track update (Marcela)
    - Extend SLSA build integrity concerns to build environment itself
    - Mitigates new threats related to compromise of build platform
        - Compromised admins in cloud provider hosting build
        - Compromised build platform admins
        - Rootkits and bootkits
    - Specific requirements, incrementally
        - provenance of build platform itself
        - measured boot of build platform
        - move root of trust into hardware, below hypervisor
    - Fleshing out threat model and working on detailed requirements

    - tl;dr: SLSA Build Track anchors trust in the builder; SLSA Build Environment Track *substantiates* this trust
    - Track is coming together in draft form over the coming weeks
        - Timelines beyond that depend on extent and nature of feedback on drafts
    - How does this work with self-hosted runners in GHA-land?
        - It's complicated! Provenance of runner needs to be factored in here
        - There's some interplay here with SLSA L2 as well… requirement is that build is "hosted" but what does that mean specifically?
    - We begin to get more optionality here about which specific components in the SDLC are/aren't trusted
    - How applicable is this work to the Solar Winds attack example?
        - Unclear; we don't know enough about the specific platform architecture for SW, and the details of the attack (e.g., was the control plane compromised)
-
-

Mar 26, 2025

Attendees:

- Cristian Urlea (University Of Glasgow)
- Mike Lieberman (Kusari)
- Jay White (Microsoft)MS
- Michael Winser (Alpha-Omega, Eclipse Foundation, XWind.io)
- Marty Haught (Ruby Central)
- Bob Martin (MITRE)
- Nicole Bates (Microsoft)
- Patrick Zielinski (NYU)
- Brandt Keller (Zarf, Defense Unicorns)
- Kris Borchers (OpenSSF)
- Daniel Moch (Lockheed Martin)

Agenda:

- Welcome new attendees
    - Nicole Bates (Microsoft)
    - Michael Winser (Alpha Omega,
    - Patrick Zielinski (NYU)
    - Brandt Keller(Zarf, Defense Unicorns)

    - Daniel Moch (Lockheed Martin)
    - Robert Martin (The MITRE Corporation)
- Publish repository for BEAR (Behavioural Enforcement & Attestation Runtime) project proposal.
    - Current home: https://github.com/DSbD-AppControl/bear
    - Draft Application for Sandbox stage: https://github.com/DSbD-AppControl/bear/blob/main/project-lifecycle-documents/beast_sandbox_stage.md
    - Next steps:
        - Raise PR with TAC
- Kubecon?
    - Who's going?
    -
    - 1-4 April 2025, London, England

Feb 26, 2025

No agenda — canceled!

From Isaac Hepworth in Slack:

> *I'd like to figure out with folks in this group how we might best use our regular meeting time. I don't want to gather just for the sake of meeting, but I do suspect that if we got together we'd have interesting things to talk about. I have an inkling that there's a sweet spot somewhere in between "pointless agenda-less meeting" and "fascinating free-range discussion" and we might see if we can locate it.*
>
> *Anyway — **meeting canceled today**. I'd love to hear y'all's thoughts on the above ahead of next time.*

Feb 12, 2025

No agenda — canceled!

Jan 29, 2025

Attendees:

- Jay White (Microsoft)
- Cristian Urlea (University Of Glasgow)
- Laura Voinea (University of Glasgow)
- Nathan Menhorn (AMD)
- Matt Suozzo (Google)
- Marty Haught (Ruby Central)
- Tracy Ragan (DeployHub / Ortelius OS (CDF))0
- Kris Borchers (LF)
- Arnaud Le Hors (IBM)
- Abdullah Garcia (J.P. Morgan)

Regrets:

- Marcela Melara

Agenda:

- Welcome new attendees
    - None
    - Tracy Ragan (DeployHub) did drop in to say hi and share an update. She reported that Ortelius has been released with OpenSSF Scorecard Dashboarding. She also announced the formation of the CI/CD Cybersecurity SIG at the CDF.

- Cristian Urlea lead an Open Discussion on "Behavioural Enforcement and Attestation Framework" or behavior specifications. The following is a list of discussion starting points, time permitting. Observationally Reproducible Builds ~ Predictable Builds
        - Matches goals and informal definition of "Predictable Builds"
            - "focuses on ensuring the outcome and behavior remain consistent, verifiable, and aligned with an organization's security expectations."
                - Consistent: What is the appropriate abstraction level such that behaviour can be consistently specified (i.e. implementation agnostic).
                - Verifiable: Discuss implications on verification tools that must support verification of the "build process behaviour" as well as the predicted artefact behaviour
                - Aligned w/ Org security expectations: Discuss integration with threat modelling tools and processes

- Tackle the need to “define what behaviours are, not necessarily how those behaviours are executed”:
    - (Theory) One approach : Define behaviours as effects (as in Type and Effect Systems) or Resources
        - Walkthrough FileIO example on page 4
    - (Practice): Discuss highest value effect handlers, such as:
        - Network: Integrate L7 Firewalls
        - Storage: Instrument Filesystem in Userspace (FUSE) or reuse networking approach (above) alongside a distributed/networked filesystem
        - IO: Instrumenting system calls: Seccomp BPF, SystemTap, etc.

Comments on above:
Tracy Ragan asked for clarification on what ‘build process’ included. Cristian indicated that it represented the entire DevOps workflow. Tracy also mentioned CDEvents.dev, https://github.com/cdevents/ and indicated that work has been done in event specifications that may contribute to this specification effort.

Jay White brought up the signing process, where does signing fit, and how is the verification completed. Cristian indicated that the verification would be completed in real-time, based on ‘credentials’ across the build process. Jay indicated that he is assuming that work on this specification would be done by the OpensSF.

Matthew Suozzo asked what the end goal would be. Cristain indicated the goal is to have the components of the build the would have communications and verification to strengthen the overall process. And the ability to package of behaviors with dependencies to predict behaviors. Matthew also asked if there was a way to define an expected behavior of a piece of software, and mentioned the challenges around different languages.

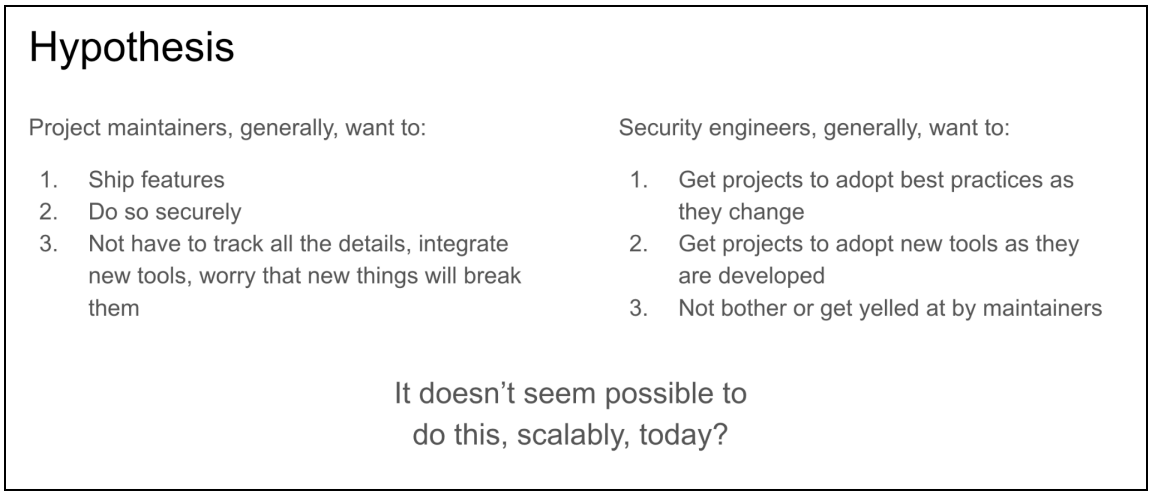
- capability analysis
    - golang has done some work on this: capslock
- remote attestation
    - SLSA has track in development for this
- observability/instrumentation
    - OSS Rebuild instruments network and syscalls for its builds
    - reasoning about the syscalls has been difficult
        - separating out the sub-components of this
    - we don't make the syscall dataset public (yet)

Jan 15, 2025

Attendees:

- Isaac Hepworth (Google)
- Tom Hennen (Google)
- Laura Voinea (University of Glasgow)
- Cristian Urlea (University of Glasgow)
- Christopher Robinson (LF)
- Kris Borchers (LF)
- James Carnegie
- Abdullah Garcia (J.P. Morgan)
- Ben Cotton (Kusari)
- Marty Haught (Ruby Central)
- Marcela Melara (Intel)
- Cassie Crossley (Schneider Electric)
- Mike Lieberman (Kusari)
- Jay White (Microsoft)

Agenda:

- Welcome new attendees (Isaac Hepworth)
    - CRob (OpenSSF)
    - James Carnegie
    - Cassie Crossley (Schneider Electric)
- “Wrangle” proof-of-concept introduction and walkthrough (Tom Hennen)
    - Can we make maintainers’ lives much easier (and make security better too)
    - 

Proposal

Provide a common framework/library/whatever that

- Provides “1-click” adoption of CI/CD best practices for project maintainers
- Allows new tools to be “plugged in” without bothering project maintainers
- Allows new best practices to be adopted without bothering project maintainers
- Doesn’t *depend* on official ecosystem support

Next steps?

- Feedback on the concept?
  - Does this already exist elsewhere?
- Feedback on what I did wrong?
  - Roast me
- Should we find a better home for this work?
  - For something that people might actually use ‘for real’?
- Initial applications
  - Can this to make the OpenSSF security baseline easier to meet?
- Could it use a better name?
  - “streetlights”?

- Potential additional challenges
  - Heterogeneity of brownfield environment
  - Being able to establish/maintain input/output invariants

- OpenSSF MVSR (CRob)

- 

- Move forward on "Behavioural Enforcement and Attestation Framework" (Cristian Urlea)
  - One-page description of idea and opportunities in the SCI WG slack channel
  - Please provide feedback, ideas, opinions, thoughts, roasting for Cristian
- Working Group Lifecycle documentation and approval is needed for Incubating status (Kris Borchers)
  - Lifecycle update process: tac/process/working-group-lifecycle.md at main · ossf/tac · GitHub
  - Incubating stage template: tac/process/templates/WG_NAME_incubating_stage.md at main · ossf/tac · GitHub
  - Example document from Securing Critical Projects WG for reference: tac/process/wg-lifecycle-documents/securing_critical_projects_incubating_stage.md at main · ossf/tac · GitHub

Dec 18, 2024

Canceled — no agenda

Dec 4, 2024

Attendees:

- Isaac Hepworth (Google)
- Mike Lieberman (Kusari) (OpenSSF TAC)
- Sean McGinn (AMD)
- Abdullah Garcia (J.P. Morgan)
- David A. Wheeler (Linux Foundation)
- Cristian Urlea (University of Glasgow)
- John Kjell (TestifySec)
- Daniel Moch (Lockheed Martin)
- Jay White (Microsoft) (OpenSSF TAC)
- Marty Haught (Ruby Central)
- Victor Lu
- Laura Voinea (University of Glasgow)
- Nathan Menhorn (AMD)
- Marcela Melara (Intel) (OpenSSF TAC)
- Aditya Sirish (NYU / Bloomberg / in-toto)
- James's AI Notetaker (Otter.AI) 🙄

Agenda:

- Welcome new attendees
    - Laura Voinea (University of Glasgow)
- Want to start a TI: Behavioural Enforcement and Attestation Framework (Cristian Urlea)
    - Looking for a Sponsor and Mentor for to traverse the TI lifecycle
    - Need a short description of what this is
        - E.g., "We are working to develop a set of tools to use static analysis of source code management and build processes to enforce and attest behavior" <- if it's something different, please write that instead!
        - Actual: We are working to develop a specification language based on Multiparty Session Type Theory and Capability-based security concepts, and a set of tools integrating the specification language, static analysis techniques and run-time monitoring and enforcement. Collectively, these will allow for compositional reasoning about, and monitoring/enforcement of, application behaviour before, during and after execution.
    - Gather more context on future SIC WG direction and scope, particularly on:
        - Verifying build platforms Track
        - Source-code Track
        - Dependency Track
        - Secure Hardware Support
    - Examples

        - E.g., maybe the compiler starts to read other files or writing something other than .o files, such as accessing the network
        - Capsicum can do some of this
    - Find interested parties / time for technical discussions on applications, including:
        - Clean Dependency Project
        - Verifying build platforms
- Clean Dependency Project
    - [Mike Lieberman] - Spoke to clean dependency project about a shift that might attract more of a community and contributors

Nov 20, 2024

Canceled — no agenda

Nov 6, 2024

Attendees:

- Isaac Hepworth (Google)
- Jay White (Microsoft)
- Mike Lieberman (Kusari)
- Sean McGinn (AMD)
- Nathan Menhorn (AMD)
- Cristian Urlea (University of Glasgow)
- John Kjell (TestifySec)
- Raghav Vema (Fannie Mae)
- Toni Pereira (Google)
- Marcela Melara (Intel)
- Jeff Diecks (OpenSSF)
- John Mark Walker (Fannie Mae)
- Abdullah Garcia (J.P. Morgan)

Agenda

- Welcome new attendees (Isaac Hepworth)
    - Hi Raghav Vema (Fannie Mae)
    - Hi Brittany Istenes (Fannie Mae)
    - Hi Cristian Urlea (University of Glasgow)
    - Jeff Diecks (OpenSSF)
- Vulns, patching, and maintenance in regulated environments (Isaac Hepworth)

    - See background
    - VEX is partially relevant here
        - Yes, from the perspective of exploitability assessments
        - No, from the perspective of end-customer risk (which is a problem downstream of this one)
    - CVSS itself has issues, as we all recognize
        - It's not a measure of risk
        - It's a very coarse measure in the context of most threat models
        - BUT we need to find a way to work with the regulations we have
    - We suspect that regulators may be receptive to exploitability arguments
        - But this kind of detailed risk-modeling and per-issue assessment is expensive and hard to scale
    - Some of the relevant CVEs are highly environment-specific and configuration-specific
        - May make them easier to mitigate locally, but upstream interest in general could be lower
    - Reachability analysis is fraught
        - Needs reassessment with every release
        - Hard to automate where language doesn't support static analysis
    -

Oct 23, 2024

Attendees:

- Isaac Hepworth (Google)
- Marcela Melara (Intel)
- Sean McGinn (AMD)
- Marty Haught (Ruby Central [RubyGems])
- Nathan Menhorn (AMD)
- Mike Lieberman (Kusari)
- Tom Hennen (Google)
- James's AI Notetaker (Otter.AI) 🤔
- [add yourself]
-

Agenda

- Welcome new attendees (Isaac Hepworth)
    - Tom Hennen (Google)
- SLSA Attested Build Environment Track (Marcela Melara)

    - Marcela and others have been collaborating on this new track for SLSA
    - Extend provenance to the build environment itself
        - e.g., VM, container, cloud provider, etc.
    - Take advantage of existing tech, e.g., TEEs and TPMs
    - Draft is at https://slsa.dev/spec/draft/attested-build-env-levels
    - Levels 0 through 3 are specified (0 is ~no-op)
    - Gradual reductions in trust of the build stack
    - Can think of this as substantiating trust in the build platform, which for Build Track is ~assumed
        - Including evidence production etc.
    - Timeline?
        - v1.1 is first in line for SLSA v.next
        - After that, Source Track
        - After that, Attested Build Environment
            - mid-2025 for v0.1? No promises!
    - For folks wanting to help, the project board is maintained
        - gives jumping-off points, many ready for contribution of PRs
    - Will there be some interesting challenges in making this broadly accessible… e.g., expensive hardware needed for some parts
        - Perhaps… but main target is CI services not individuals or individual projects
        - fwiw, prototype/demo is in flight
- SLSA Source Track (Tom Hennen)
    - Draft is at https://slsa.dev/spec/draft/source-requirements
        - “The SLSA source track describes increasing levels of trustworthiness and completeness in a repository revision’s provenance (e.g. how it was generated, who the contributors were, etc…)”
    - Three levels L1, L2, L3
        - L1: Use version control
        - L2: Branch history (“how did this revision come to be”)
        - L3: Source provenance attestations
            - ideally, attestations issues contemporaneously with source revisions
    - Key principle: source track doesn’t require the use of any particular platform, or even *a* platform
        - GitHub and GitLab may offer native support, but it’s not required
        - potentially gittuf has a role to play here. Aditya has been involved in track development
        - Should be possible to meet these new levels whatever source control technique you’re using
    - Timeline?

        - Draft out now
        - Hoping for release this year
        - Ideally, release would have example code etc.
    - As a go-to-market consideration, need to think about things folks can pick up and use, play with, see in action, fork, etc.
    - Source Track has been in touch with Scorecard team to collaborate on attestations and “making it real”
- SLSA Dependency Track (Jay White)
    - Re-working S2C2F to make it a good fit for SLSA
        - (Using AI, no less)
    - Timeline
        - First-draft target ~mid-Nov
        - Would love to finalize by EoY

Oct 9, 2024

Canceled — no agenda

Sep 25, 2024

Attendees:

- Isaac Hepworth (Google)
- Mike Lieberman (Kusari)
- Nathan Menhorn (AMD)
- Jeff Diecks (OpenSSF)
- Marty Haught (Ruby Central [RubyGems])
- Scott Hissam (CMU/Software Engineering Institute)
- Arnaud Le Hors (IBM)
- Sean McGinn (AMD)
- Daniel Moch (Lockheed Martin)
- Kirk Rasmussen (RTX)
- Abdullah Garcia (J.P. Morgan)
- Marcela Melara (Intel)
- Jay White (Microsoft)
- William Burton (Google)
- … and “James’s AI Notetaker (otter.ai)” 🤔

Agenda:

- Welcome new attendees (Isaac Hepworth)
    - Jeff Diecks, OpenSSF
    - Marty Haught, Open Source Lead, Ruby Central
- Post OSS EU update (mike@kusari.dev)
    - Lots of good feedback on GUAC, SLSA, S2C2F and other SCI WG projects
    - A few talks referencing SLSA, an OpenSSF supply chain panel
    - Keynotes mentioned SLSA, S2C2F, and GUAC
    - OpenSSF booth saw steady traffic. Interest in S2C2F, GUAC, gittuf
    - End users/consumers very interested in S2C2F for safe consumption
    - Some questions about FRSCA… even though it's archived
        - In general, folks looks for practical examples, real-world implementations, detailed case studies
    - Some potential collaborators, e.g., landlock
    - Opportunities
        - Awareness of SLSA, still work to do
        - Practical examples for folks to help them grok
        -
- Public Sector UG S2C White Paper (Daniel Moch)
    - Working on a white paper slated for introduction around Kubecon
        - → how should public sector consumers work with open source
    - CNCF Slack channel: #ug-public-sector
    - Meetings on Thursdays
    - Panel discussion at SigstoreCon, possible BoF discussion at Kubecon
    -

Sep 11, 2024

Attendees:

- Mike Lieberman (Kusari)
- Sean McGinn (Advanced Micro Devices)
- Abdullah Garcia (J.P. Morgan)
- Daniel Moch (Lockheed Martin)
- Nathan Menhorn (AMD)
- Arnaud Le Hors (IBM)
- Mike Silverman (FS-ISAC)
- Matthew Suozzo (Google)
- Scott Hissam (CMU/Software Engineering Institute)

- .

Agenda:

- Welcome new attendees
- OSS EU
  - Arno and Mike have a panel with Tom Hennen and Aeva Black
- Reproducible builds is having a workshop around the same time as OSS EU
  - Event details: Hamburg 2024

Aug 28, 2024

Attendees:

- Isaac Hepworth (Google)
- Xander Grzywinski (Defense Unicorns)
- Zachariah Cox (github)
- Ben Cotton (Kusari)
- Mike Lieberman (Kusari)
- Scott Hissam (Carnegie Mellon/Software Engineering Institute)
- Aditya Sirish (NYU)
- Nathan Menhorn (AMD)
- Mike Silverman (FS-ISAC)
- Adrian Diglio (Microsoft)
- Daniel Moch (Lockheed Martin)
- Marcela Melara (Intel)
- Arnaud Le Hors (IBM)
- John Kjell (TestifySec)
- … and “James’s AI Notetaker (otter.ai)” 🤔

Agenda:

- Welcome new attendees (Isaac Hepworth)
  - Zachariah (GitHub)
  - Scott (CMU)
  - Ben (Kusari)
- Project round-up:
  - gittuf (Aditya)
    - With plumbing work behind us, working on usability
    - Worked on building a GitHub application
    - Aditya working on piloting gittuf and incorporating feedback

        - Requested funding from OpenSSF to host app
        - Aspirations for EoY
            - Driving adoption
            - Heading to next maturity phase
    - SLSA (Zachariah)
        - 10–15 active participants in docs/meetings/issues
        - recent work
            - Hardware attestations track making progress. No longer an extension to the build track. Focused more on incremental integrity objectives for the build environment.
            - SLSA 1.1 is now out of draft and is a release candidate
                - mostly minor changes, clarifications
                - some leftover TODOs
                - PSA: everyone please review
                - https://github.com/slsa-framework/slsa/pull/1117
            - collaboration with S2C2F looking positive
            - Source track making good progress; clearer collective understanding of objectives and positioning
                - focus on “making trustworthy claims”
                - separating claims made from evaluative judgments based on those claims
                    - Here’s a (beta) list of those qualitative claims and how they might be described: https://github.com/slsa-framework/slsa/blob/main/docs/spec/draft/verifying-source.md
                    - Here’s Tom’s PR describing the relationship between SLSA attestations and VSAs: https://github.com/slsa-framework/slsa/pull/1094
                - Please take a look at the current source-requirements draft! https://github.com/slsa-framework/slsa/blob/main/docs/spec/draft/source-requirements.md
                - New source track project board: https://github.com/orgs/slsa-fram%20work/projects/5/views/7
            - Working on refreshing/updating the governance structure
                - Steering committee has been somewhat MIA, for example; needs new membership and clearer role
    - S2C2F (Adrian)
        - Incorporating suggestions and proposals for language updates
            - Adding flexibility here and there

        - Pausing standardization via ISO; may revisit
        - Threads of work moving forward
            - Aligning S2C2F with SLSA's desires for a "dependency track". There's a lot to explore here, but seems at a high level like a promising direction
            - Working with Scorecard on overlap of concerns. Scorecard could become a part of the tooling solution for S2C2F attestations 🙌
                - Adjacency here with SLSA Source track; Scorecard could be useful here also
            - Working on S2C2F web site, s2c2f.io
            - Exploring possible applications of S2C2F to AI/ML domain
                - Open question as to whether S2C2F in this context would apply to data as well as code
                - Mike Silverman interested in collaboration here
    - GUAC (Michael)
        - Current status
            - Version 0.7 and 0.8 releases:
                - Clearly Defined integration completed
                - CycloneDX SBOM license parsing
                - Improved S3 collector
            - In progress
                - Additional REST API routes… not everyone wants to learn GraphQL
                - Postgres performance improvements
            - Onboarding experience survey
        - Up next
            - Planning 1.0 release
            - Stabilizing API
            - Improved demo flow
            - Additional documentation
    - Security Insights (Eddie Knight)
        - Tidying up specification and auditing existing data
        - Aligning with the Baseline SIG, to work on required values for SI specification
            - Eddie also leading Baseline with Dana's departure
    - Zarf (Xander Grzywinski)
        - "The big thing" is 1.0 release by EoY (~Kubecon, November)
            - Stabilization
            - Production-readiness
            - Tech debt
        - Aiming for release candidate at SOSS Fusion (October)
        - Onboarding to OpenSSF

    - Seeing more folks showing up to community meeting, as well as a lot of DU folks
    - Repo migration
-

Aug 14, 2024

Canceled — no agenda topics.

Jul 31, 2024

Canceled — no agenda topics.

Jul 17, 2024

Attendees:

- Isaac Hepworth (Google)
- Abdullah Garcia (J.P. Morgan)
- Mike Lieberman (Kusari)
- Robat Williams (Scott Logic)
- Andrew Lilley Brinker (MITRE)
- Emilio Escobar (Datadog)
- Sean McGinn (AMD)ƒ
- Nathan Menhorn (AMD)
- Daniel Moch (Lockheed Martin)
- John Kjell (TestifySec)
- Salve J. Nilsen (CPANSec)
- Scott Hissam (CMU Software Engineering Institute)
- Arnaud Le Hors (IBM)
- Adrian Diglio (Microsoft)
- Matthew Suozzo (Google)
- Kirk Rasmussen (RTX)

Agenda:

- Welcome new attendees (Isaac Hepworth)

    - hi Emilio
    - hi Robat
    - hi Scott
    - hi Salve
- Adding Trusted Repo Security TI to SCI WG (Isaac / Mike Silverman)
    - Show of hands following review of proposal doc
        - No objections in the meeting
- Adding Security Insights to SCI WG (Isaac / Eddie)
    - No objections in the 7/3 meeting; review any mailing list feedback
    - No further input; moving on!
- P4 Framework briefing (Scott Hissam, Carnegie Mellon Software Engineering Institute)
    - Presentation Deck (ossp4r-overview-DistA-vJun2024)
        - **Objective**: To develop an automated approach to capture information about Open Source Software supporting Software Supply Chain Risk Management under Software Assurance.
        - **Challenge**: Unlike Commercial/Proprietary software, there is no "supplier" accountable for Open Source Software to provide such information yielding no insight into SCRM concerns.
        - **Solution**: Using Open Source tools and Open Source data sources assemble relevant data and information and identify potential risk items that would need to be mitigated for use in a production system.
    - Question: in separating project from product do we lose information about actual contributors, which is in scope of government interests? E.g., we've seen interest in whether foreign nationals are involved
        - P4R generalizes to "malicious actors"
    - ABC → Adopt, Buy, Create
    - Question: might we be concerned too about the "bus factor" of a given project/product? And can we gather "missing metadata" directly from project principals in collaboration with them?
    - Might we be concerned about 'gatekeeping' around projects which don't 'meet the bar'?
    - How well are the score inputs to P4R (e.g., Scorecard) correlated with real-world risk?
    - https://github.com/cmu-sei/scir-oss
-

Jul 3, 2024

Attendees:

- Isaac Hepworth (Google)

- Brittany Istenes (Fannie Mae)
- Mike Lieberman (Kusari)
- Sean McGinn (AMD)
- Kirk Rasmussen (RTX)
- Mike Silverman (FS-ISAC)
- Toni Pereira (Google)
- Andrew Lilley Brinker (MITRE)
- Jay White (Microsoft)
- Nathan Menhorn (AMD)
- Marcela Melara (Intel)
- Abdullah Garcia (J.P. Morgan)
- Arnaud Le Hors (IBM)
- Eddie Knight (Sonatype)

Agenda:

- Welcome new attendees (Isaac Hepworth)
    - Andrew Lilley Brinker (MITRE)
- Welcome Zarf to SCI WG
    - Now formally a member!
- Review the Clean Dependency Project - FNMA to determine if it should move into the WG
    - Brittany = OSPO Strategist at Fannie Mae
    - CDP originally developed in 2022
        - Move from a reactive to a proactive stance wrt vulnerability management
        - See tech talk at OSS NA
    - Intent is to make patches available to regulated industry ahead of upstream availability
        - Making vulnerability window shorter
        - Not intended to be permanent substitution
    - CDP would love to find additional maintainers and contributors from within OpenSSF
    - From mike@kusari.dev
        - Note, TAC requirement is to have maintainers from orgs in addition to Fannie Mae
        - How does this scale over time? What types of principles for what packages are in/out of scope? Does this get to 100 packages? 1,000? Etc.
    - From Marcela
        - Can we get additional value by identifying patterns we see in the types of things we're fixing?
        - Check out the Critical Projects working group in OpenSSF too
    - Good next steps

        - Publicize this project via meeting notes and Slack
        - Make connection to Critical Projects WG
        - One-pager with vision for the project outlining what great success (12–18 months) looks like
- Security Insights looking to join SCI (Eddie Knight)
    - No objections noted in the meeting; next step mailing list
- SLSA Update (Isaac Hepworth)
    - Source track is getting close! Draft just merged
        - Was removed from 0.1 to ship 1.0
        - Now, along with Build L4, coming back
    - Specification working group is heading towards a 1.1 with some more minor updates…
        - …and then land new Source and Build requirements
    - Specification group will be making more noise about progress around specification
        - It's been difficult to detect activity from outside to-date
- Trust in Open Source
    - As discussed, xz undermined a key part of the prevailing threat model: that maintainers are trusted
    - In an upcoming meeting we'll be looking at a research proposal for modeling and measuring trust networks in open source communities
    - https://docs.google.com/document/d/1a38KHaot0JSoGygzFQLRd5OaV61991fkf3Tstgehsdo/edit
    -

Jun 19, 2024

Meeting canceled owing to Juneteenth Federal Holiday in United States.

Jun 5, 2024

Attendees:

- Isaac Hepworth (Google)
- mike@kusari.dev (Kusari)
- Xander Grzywinski (Defense Unicorns)
- Eddie Knight (Sonatype)
- Abdullah Garcia (J.P. Morgan)
- Nathan Menhorn (AMD)

- Adrianne Marcum (OpenSSF)
- Sean McGinn (AMD)
- Amanda Martin (Linux Foundation)
- Matthew Suozzo (Google)
- Mike Silverman (FS-ISAC)
- Aeva Black (CISA)
- Dana Wang (OpenSSF)
- Mike Thompson (Datadog)
- John Kjell (TestifySec)
- Toni Pereira (Google)
- Marcela Melara (Intel)
- William Burton
- Arnaud Le Hors (IBM)
- Namit Deshpande (Amazon)
- Jay White (Microsoft)

Agenda:

- Welcome new members (Isaac)
    - Hi Amanda (LF)
    - Hi Aeva (CISA)
    - Hi Matt (Google)
    - Hi Mike Thompson (Datadog)
    - Hi Dana (OpenSSF)
    - Hi Namit (Amazon)
- Zarf — follow-up from below; proposal to add to SCI WG (Isaac)
    - Show of hands — no objections
    - Next up: PR and call for final objections on the mailing list
- Security Insights (Eddie Knight)
    - TI is leaving Metrics and Metadata
    - Looking for a new home…
    - Trackability for things that can't be automated
        - (Over time, as more can be automated elements will be deprecated)
    - Currently, primary adoption in CNCF
        - SI is now a part of CNCF hygiene standards
        - Projects use SI to declare non-automatable conformance elements
    - GUAC is investigating consumption of SI also
        - SI could be a useful discovery tool
        - GUAC could highlight gaps in security metadata
    - Utility for S2C2F e2e story too

- Trusted Repo Security SIG Proposal (SCI #80) to join SCI WG (Mike Silverman)
    - Call for objections? None heard
        - However, Aeva flags that more definition is needed
    - Next steps: add definition and create a PR to join
- 👋 OSS Rebuild (Matthew Suozzo)
    - Previously presented to SIG, following up post-launch (though still early days)
    - No imminent action here but feedback would be much appreciated
    - No intent for OSS Rebuild to join the SCI WG (yet!) but an interesting project in an adjacent problem area
    - Feedback from mike@kusari.dev
        - Not super-clear from documentation what the project is "for" and how best one might engage
        - Is the current output info intended to be actionable? Informational?
            - Matthew Suozzo : For now, informational. We do believe there are actionable signals to be derived but that's a product question.
        - Do we imagine a constellation of rebuilders operated by various organizations?
            - Matthew Suozzo : Certainly one possibility. For now, we're shouldering the operational cost.
        - Might we rebuild OpenSSF's projects? Maybe even run additional security checks? Etc.
            - Matthew Suozzo : Additional security checks are a really interesting application since they can be decoupled and not block the release process. Golang projects are already generally in a very strong place re: build integrity but interesting for distributing binaries and projects in other languages.
    - Isaac Hepworth : Think of it more as a capability with many possible product applications
        - Functions as a pure overlay, no CI/process changes required
- Plug for Software Supply Chain Workshop (Marcela)
    - SCORED workshop; see CFP
    - Mostly academic, but building bridge to industry

May 22, 2024

Attendees:

- Isaac Hepworth (Google) ← regrets, in Sydney this week
- mike@kusari.dev (Kusari) ← regrets, Kubernetes Community Days NY

- jaywhite@microsoft.com (Microsoft) ← regrets, OOO
- John Kjell (TestifySec) ← our Chair this week
- Xander Grzywinski (Defense Unicorns)
- Brandon Mitchell (independent)
- Aditya Sirish (NYU)
- Kenny Paul (LF)
- Nathan Menhorn (AMD)
- Arnaud Le Hors (IBM)
- Ovidiu Ghinet (UBS)
- Marcela Melara (Intel)
- Eddie Zaneski (Defense Unicorns)

Agenda:

- Welcome new members (Chair)
    - Kenny Paul (LF)
    - Eman Abu Ishgair (Purdue, Intel Labs intern)
- Zarf demo (Eddie / Xander)
    - Zarf is specifically targeted towards air gap environments and the unique problems those propose.
    - Zarf has been seen anywhere from nuclear submarines, rockets, and vehicles.
    - CLI tool to package up a variety of software artifacts (containers, VMs, binaries).
    - Start with bootstrapping a kubernetes cluster. It includes its own registry. Many things are packaged as config maps.
    - Many optional components can be included with a Zarf deployment (logging, its own k3s cluster, and others)
    - Based on configuration it retrieves contents from external locations, such as container registries, and generates an SBOM for those contents.
    - Currently looking at support for protobom, another OpenSSF project, for a meta-SBOM
    - Actual transport over the air gap is an exercise left to the user (sneakernet, one-way diodes)
    - What are the unique challenges faced in the type of air-gapped environments Zarf sees?
        - Oftentimes very limited bandwidth on deployment side. There's lots of logic to gracefully handle retries.
    - Many tools built directly into Zarf: kubectl, helm, everything you should need to deploy
    - How far down the stack can Zarf deploy? How close to bare metal?
        - Can include k3s and VMs
        - Current work with "actions" concept to deploy full k8s stack directly onto RHEL
    - Zarf is at a fairly stable point. Looking for future feature request from end users

    - Includes cosign to perform verification of image signatures, interested in future support of generic in-toto attestations
    - Use stereoscope to visually SBOMs
    - Looking to donate to OpenSSF under the SCI Working group
    - How does Zarf relate to all of the other SBOM tooling work in OpenSSF
        - Collaborating and working closely with the protobom and bomctl groups
    - End user consumption of SBOMs is an open question. They're looking for guidance on how to really leverage the information
        - Example: how to scan for vulnerabilities based on SBOMs
        - A lot of interest in the way that tooling like protobom can help problems in that space
        - Current state for many customers is a checkbox exercise
    - PR ready to go against the TAC repo for entering as a sandbox project
        - Issac Hepworth listed in the sponsor.
        - Waiting for approval from all WG leads based on today's demo and conversation
    -
- Supply Chain Integrity TAC Update (Chair)
    - SLSA Status
        - Discussion focused on two main topics:
            - Supply chain threat model - how to expand & edit, is the model broad enough and well understood? Basing conversation on feedback from users since 1.0
            - Source track work stalled due to recent layoffs of several contributors
            - Dependency track in progress
            - Additional integrity requirements for build tracks - focus are hardware based attestations and integrity measurements. Proposed to be level 4 of build track. Current track places requirements on the build platform itself. These requirements do the same.
    - S2C2F Status
        - Recently reached Incubating Project lifecycle stage
    - GUAC Status
        -
    - gittuf Status
        - Getting to a good state with underlying plumbing based on recent release
        - Focusing on end user experience and improvements
            - Looking to create a good experience in a "typical" developer workflow
            - Hoping to increase adoption with an upcoming release

May 8, 2024

Attendees:

- Isaac Hepworth (Google)
- Xander Grzywinski (Defense Unicorns)
- mike@kusari.dev (Kusari)
- Kyle Kelly (CramHacks/Semgrep)
- James Artis (JibChain)
- Kirk Rasmussen (RTX)
- Arnaud Le Hors (IBM)
- Zach Steindler (GitHub)
- Brandon Mitchell (independent)
- Nathan Menhorn (AMD)
- Aditya Sirish (NYU)
- John Kjell (TestifySec)
- John Klein (CapitalOne)
- Abdullah Garcia (J.P. Morgan)
- Marcela Melara (Intel)
- Jay White (Microsoft)
- Sean McGinn (AMD)
- Abhishek Chowdhury

Agenda:

- Welcome new members (Isaac)
    - Mike Silverman (FS-ISAC)
    - Xander Gyzywinski (Defense Unicorns)
    - James Artis (JibChain)
    - Kirk Rasmussen (RTX)
- GitHub Artifact Attestations (Zach) 🙌
    - Free to use for public repos
    - Paid users can use with private repos
    - Simple stanza for GHA workflow to create SLSA provenance attestation and sign
        - with Sigstore public good instance (public repos)
        - with internal Sigstore instance (private repos)
    - gh CLI can download/verify/actuate policy on attestations
    - Also support for other attestation types (e.g., SBOMs)
        - e.g., in-toto CycloneDX/SPDX predicates
    - Standardization on in-toto seems like a productive direction

    - Question (mike@kusari.dev): we don't yet have broad consensus on where attestations live long-term and how they're discovered. Any thoughts?
        - GH provides REST API endpoints to download attestations, as Sigstore bundles for easy offline verification
        - cf. GitHub OCI Registry — artifacts have a temporary home here but it's not the "final resting place"
    - Question (Marcela): thoughts on attestation piece being a standalone reusable workflow rather than an attribute on top of existing steps
        - Approach was informed and constrained by the SLSA provenance design itself, where the attestation is defined as the final disposition of the build process — not of interim steps
        - Generally, GH is interested in fleshing out this story in collaboration with OSS community
- Concepts from TF-TRSI Task Force (Mike Silverman)
    - TF was created coming out of the November summit in DC: "how can we get more trust from repos in general"
        - "Trusted Repository Security Initiative" (TRSI) Task Force (TF)
    - Various proposals about identity verification, KYC-style
    - Exploration of trusted communities, crowdsourced reputation, etc.
        - Inter-community trust super-difficult!
    - xz, where maintainer trust is brought into sharp focus, catalyzed this initiative
    - New approach, conceptually: layering with defense in depth
    - Idea: volunteers outside a project do periodic "QA-type" checks
        - A lightweight guided "audit" of a repo; are the right things happening?
        - Validation against an existing checklist
    - General concern would be additional maintainer burden
        - Will there be pressure to "conform" or to "be certified" in some way?
    - (Related concept, via Zach: https://mozilla.github.io/cargo-vet/)
    - Some elements here can be rather granular
        - e.g., you may just not trust the build process, and hence decide to build the source yourself
    - Folks can join the #tf-trsi channel in OpenSSF to connect with the initiative and learn more
    - Task Force would be interested in joining forces with an OpenSSF WG (maybe this one!) to move this initiative forward
        - SCI would be a great fit! But so perhaps might be other WGs
        - Per Jay: this may not be the perfect place, but it'd be a great place
- Make project updates a regular thing in this meeting (Mike Lieberman)

    - Lots of valuable projects in SCI but we don't have a great roll-up view or a way to connect dots systematically
    - How about every other meeting (i.e., monthly) we pull the various projects together into a round of updates?
        - GUAC
        - gittuf
        - SLSA
        - S2C2F
        - …
- Call to action for toolbelt PoC (Mike Lieberman)
    - The 'security button' which makes the right thing happen across various tools and technologies
    - How do we make best practices easier? Easiest, even?
    - Interested in collecting folks with opinions/contributions in this space
        - e.g., who would make a GHA to ensure the correct gittuf policy? Etc.
    - Question (Marcela): how many projects are you targeting for the pilot?
        - Probably 3–5 in the first instance
        - Possibly start with some projects in SCI, even
    - Folks can start here and pull on linked threads etc.: https://github.com/ossf/toolbelt/issues/11
-

Apr 24, 2024

Attendees:

- mike@kusari.dev (Kusari)
- Abdullah Garcia (J.P. Morgan)
- Sean McGinn (AMD)
- Arnaud Le Hors (IBM)
- Matthew Wood (Intel)
- Aditya Sirish (NYU, right at the end)

Agenda/notes:

- [Mike] Open Source Summit/SOSS updates
- What's next for SCAI?

Apr 10, 2024

Attendees:

- Isaac Hepworth (Google)
- Toni Pereira (Google)
- mike@kusari.dev (Kusari)
- Bobbie Chen (Anjuna)
- Jay White (Microsoft)
- Marcela Melara (Intel)
- Kyle Kelly (Semgrep / CramHacks)
- Nathan Menhorn (AMD)
- Brandon Mitchell
- John Kjell (TestifySec)
- Jeff Borek (IBM)
- Sean McGinn (AMD)

Agenda/notes:

- [Mike] Update on GUAC PoC, as part of Toolbelt
    - Approved to run the PoC
    - Working with LF on approved mechanisms for containing costs
    - Received great feedback from various folks, e.g., OpenTelemetry
    - Data scope
        - SBOM
        - SLSA provenance
        - other in-toto attestations
        - OSV
        - deps.dev
        - VEX
    - PoC will allow us to construct a feedback loop back into data generation
    - Sidebar: what is SCAI?
        - Goal is to be able to bind evidence to ~arbitrary attestations (think: key/value pairs)
        - Over time, common usages/patterns will emerge for which we may want to build first-class semantic support
        - See Summary attestation reqs/design
- [Marcela] Hosting a rebuilderd service for OpenSSF projects and broader ecosystem?
    - Originally an idea in CNCF Slack
        - tl;dr: could OpenSSF host a rebuilderd for OpenSSF projects?

    - We could begin with something best-effort
        - e.g., closer to GUAC PoC than to Sigstore
    - Over time, better operationalize and offer SLAs etc.
    - fwiw, GUAC found securing the funding ~easy compared with actual mechanics of spending the money, controlling costs, etc.
        - Would be good for OpenSSF to make this easier
    - Could potentially start with a pilot focused on a few OpenSSF projects
        - GUAC? Fulcio? Rekor?
    - GB has been clear putting production services in general out of scope for OpenSSF in 2024
    - What would the rebuilderd service output? Attestations only? Binaries? Pass/fail?
        - Begin with just attestations perhaps
        - Could even store attestations in Sigstore
        - Could GUAC PoC play a role in distributing the data?
        - Archivista angle maybe?
            - archivista.testifysec.io
    - Next steps: quick one-pager summarizing idea, scope, starting point…
- [Isaac] OASIS Supply Chain Information Modeling WG
    - See Supply Chain Information Modeling (SCIM) TC DRAFT Charter
    - Jay is a proposer of the TC
        - Main thrust is standardization of core information concepts, independent of specific serialization formats
- [Isaac] Perspectives on xz
    - Some thoughts from Isaac
        - Subversion of the predominant threat model; what do we do if we can't in fact trust maintainers
        - Where are the other attacks? Seems desperately unlikely that xz is a one-off, even from this threat actor
        - Did supply chain security succeed here, because the attack was so expensive? Or did we fail, because we got very lucky and the RoI would've been enormous for the attacker
    - Mike: reminder that the human aspect is super-important
    - Kyle:
        - fascinating new vector
        - relationship with OSS Fuzz
        - analysis of binary contributions to packages

Mar 27, 2024

Attendees:

- Mike Liebemerna (Kusari)
- Sean McGinn (AMD)
- Ovidiu Ghinet
- Jay White (Microsoft)
- Matthew Wood (Intel)
- John Kjell (TestifySec)
- Arnaud Le Hors (IBM)
- Dmitry Raidman (Cybeats)

Agenda/notes:

- Project updates
    - S2C2F will inform TAC of intent to enter PAS process
    - GUAC trying to stabilize for 1.0
    - SLSA
        - Working on multiple new tracks: dependencies, source, and hardware attested builds.
- KubeCon updates
    - Biggest LF event ever…12k people
    - Panel discussion with a nice full room. Many questions asked.
        - Beyond SBOM talk
    -
- Upcoming Open Source Summit

Mar 13, 2024

Attendees:

- Isaac Hepworth (Google)
- Michael Lieberman (Kusari)
- Eddie Zaneski (Defense Unicorns)
- Will Bierbower (Autodesk)
- Sean McGinn (AMD)
- Toni Pereira (Google)
- Jay White (Microsoft)
- Adam Shamblin (Digital Ocean)
- Marcela Melara (Intel)

- Kyle Kelly (Semgrep / CramHacks)
- Nathan Menhorn (AMD)

Agenda/notes:

- Welcome new folks
    - Welcome Will! Security engineer with Autodesk. Application security engineering, and more attention to supply chain
    - Welcome Adam! Digital Ocean, looking at supply chain security
- GUAC's accession to OpenSSF is complete!
    - Everything squared away and it's official now
- [Mike Lieberman] - GUAC+Toolbelt PoC
    - Security toolbelt = assembling OpenSSF tools into a coherent toolset, working together towards known security outcomes
        - Ideally, simply to pick up and use
    - Context:
        - Maintainers: "how should I use Scorecard? How does this benefit me or my users?"
        - OSS Consumers: "how can I contain and mitigate risk from my upstream dependencies?"
    - Looking for participation!
    - Looking for end users and maintainers
        - 3–5 maintainers to work closely with
        - 3–5 OSS consumers to work closely with
        - How can GUAC substantively help?
            - Use cases
            - Example queries
            - Data sources
            - Particular risk examples
        - What's missing from our datasets?
        - Are there valuable questions which are hard to answer with GUAC?
    - POC plan is approximately one year of elapsed time
        - Considerably less in terms of effort-time
        - Meetings are Tuesdays at noon ET
        - See https://openssf.slack.com/archives/C057BN7K19B
- [Abdullah Garcia] - Is it possible to produce a FAQ document/page?
    - → next time
- [Isaac Hepworth] Ad-hoc discussion about attestations, trust, and policy
    - Start from slide deck ssci.io/attestations-deck
    - Scorecards adjacency

    - in-toto adjacency
    - GUAC adjacency

Feb 28, 2024

Attendees:

- Mike Lieberman
- Sean McGinn (AMD)
- Nathan Menhorn (AMD)
- Toni Pereira (Google)
- Tom (DHS)
- Arvind Singharpuria
- Matthew Wood (Intel)

Agenda:

- Welcome new folks
    - Tom - Department of Homeland Security interested in supply chain security
    - Arvind - Interested in learning more about supply chain security
    -
- [mike]: Explained gittuf, slsa, guac, s2c2f and group focus
- [tom]: Ask more information about s2c2f
- [tom]: What kind of info guac needs to work?
- [tom]: Vendors concern about different SBOMs formats generated by XYZ tools
- [toni]: What are the improvements to Guac that need immediate attention for wider adoption?
    - [mike]: guac foundation, 1 1/2y old initiative, focus to solve the problem of dependency graph understanding, answer - make it easier - solving the hard problem, step back and focus on small/trivial problems people have today - Could guac expand its capabilities?
- [ardind]: Can you share some issues to start contributing to guac / which expertises guac needs
    - [mike]: front-end, info consumption, info insights - user needs focus

Feb 14, 2024

Attendees:

- Isaac Hepworth (Google)
- Zach Steindler (GitHub; TAC)
- Adrianne Marcum (LF, OpenSSF)
- Mike Lieberman (Kusari)

- Eddie Zaneski (Defense Unicorns)
- Sean McGinn (AMD)
- Marcela Melara (Intel; TAC)
- Brandon Mitchell
- Toni Pereira (Google)
- Jay White (Microsoft)
- Jeff Borek
- [add yourself here]
-

Agenda:

- Welcome new folks (Isaac Hepworth)
    - Hey Zach
    - Hey Eddie
    - Hey Toni
- Open Source Integrity and Standardization Task Force readout <link to TAC update> <link to TF notes summary> (amarcum@linuxfoundation.org)
    - What is this task force?
        - Establish consistency across open source ecosystems
        - Improve repository security and transparency
        - Enhance community engagement and user education
    - OpenSSF seeks to establish a relationship/partnership with US FedGov
        - DC Summit was a part of that
        - Not directly tied to funding — we think? — but funding-adjacent
    - Opportunities remain for better internal coordination in OpenSSF around these types of events
        - e.g., making sure that hands-on-keyboards folks in the TIs are well represented
        - e.g., making sure that plans, outputs, etc., are written up and socialized sufficiently
    - Task force “suggested roadmap” output was intended to be suggestive/illustrative, not prescriptive
- [eddiezane] Intent to donate Zarf to the OpenSSF and looking for a WG sponsor
    - Zarf = “tool for deploying into an airgapped environment”
    - Originally designed for deployment of k8s onto nuclear submarines (!!)
    - See GitHub repo and zarf.dev
    - Would like to land in a good WG in OpenSSF; SCI looks like a plausible fit?
    - mike@kusari.dev : one of the interesting things about Zarf is that it’s complementary to pieces of SCI which are on the “production” side of things

        - i.e., Zarf is in some senses downstream, a consumer of software and attestations
    - Next steps here: Zarf to develop opinions about which WG it thinks would be best, and share that with TAC etc.
- [add your items here ^^]

Jan 31, 2024

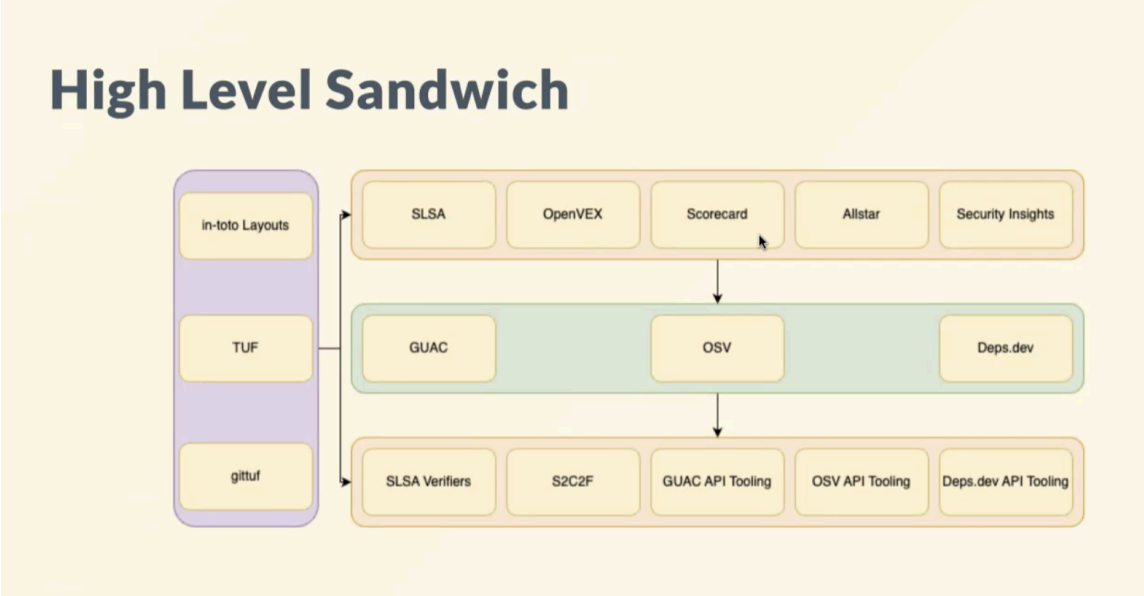
Attendees:

- Isaac Hepworth (Google)
- Mike Lieberman (Kusari)
- Nathan Menhorn (AMD)
- John Kjell (TestifySec)
- Sean McGinn (AMD)
- Ovidiu Ghinet
- Arnaud Le Hors (IBM)
- jaywhite@microsoft.com (Microsoft)
- Abdullah Garcia (J.P. Morgan)
- Bobbie Chen (Anjuna)
- Yotam Perkal
- Adrianne Marcum (LF OpenSSF)
- Marcela Melara (Intel)
- Matthew Wood (AWS)
- Brandon Mitchell (independent)
- Raghav Kaul

Agenda:

- Welcome new folks (Isaac Hepworth)
    - Hi Sean! (AMD)
    - Hi Ovidiu! (back after a year of absence!)
    - Hi Bobbie! (Anjuna)
    - Hi Yotam!
- Demo of Skootrs (mike@kusari.dev)
    - Theme: ever-increasing burden on devs and maintainers
    - Hard to keep track of recommendations and obligations across multiple dimensions of concern — especially as the bar is continuously being raised
    - Skootrs: make it easy to get security right, starting from a new repo. “Easy button” for the creation of a secure-by-design/secure-by-default project

        - creates a GH repo
        - fires a CDEvent
        - creates README, LICENSE, .gitignore for the language, etc.
        - sets up branch protection
        - enabled vulnerability reporting
        - sets up security insights
        - sets up Anchore SBOM action
    - “Security Sandwich”



    - Question: if Skootrs is an encoding of best practices in a tool (for creation) and Scorecard is an encoding of best practices in a tool (for assessment), should they be the same thing?
        - Possible consolidation across
            - creation
            - assessment
            - policy
            - remediation
    - Question: can we somehow link the tool to the set of OpenSSF best practices? So that as they evolve, the tool keeps up?
        - Yes, active area of exploration
- Runtime service verification (@bobbie.chen@anjuna.io)
    - See doc Improving trust in Sigstore using TEEs
    - Core idea: much of supply chain thinking is about software being packaged and distributed. But what about services?

        - What if I want to verify that [service foo] is running the code that it should be? e.g., that it's actually running the SLSA-attested build
    - Execution would be in a TEE, and an attestation about the code being run is signed by an enclaved private key
        - Existing mechanisms for TEE verification can be used
    - How is this different from RATS?
        - Think of it as a specialization of RATS for a particular use case
    - Has any work been done to demonstrate this end to end?
        - Not with Fulcio specifically, but yes with other services
        - Bobby will add some detail to the doc about specifics on verification
    - PR to run Fulcio inside the environment would be a useful proof point
        - Should be possible to produce a byte-for-byte reproducible build in this case
- Future of "SCI Positioning" WG (Isaac Hepworth)
    - Low attendance for the last few months
    - Possibly we could migrate some of the work to the cross-WG "community" working group?
        - Remainder could be folded into this SCI WG call?
    - Jay: Some things in SCI Positioning which should have a home
        - Blogs
        - Talks
        - Panels
        - general outbound and evangelism
    - Arnaud: There were good reasons for the Positioning SIG to exist… let's make sure we keep an eye on those motivations and that today's needs are being met
    - Mike: definitely let's lean on Toolbelt and Devrel groups to take up some of this work
    - Jay: need to balance Devrel as a horizontal concern against SCI as a vertical one
    - Marcela: positioning has a broader audience than just devs… another factor when considering Devrel as a home for some of the work
- Highlights for TAC presentation next week (Isaac Hepworth)
    - [no suggestions]

Jan 17, 2024

Attendees:

- Isaac Hepworth (Google)
- Jay White (Microsoft)
- Mike Lieberman (Kusari)

- John Kjell (TestifySec)
- Marcela Melara (Intel)
- Brandon Mitchell (independent)
- Barry Greene (Qubit Cyber)
- Kirk Rasmussen (Raytheon)

Agenda/notes:

- New meeting attendees
  - Barry Greene
  - Kirk Rasmussen
- Update from jaywhite@microsoft.com on SupplyChainSecurityCon, Apr 16–18
  - Jay is chairing
  - Number of good submissions have arrived; haven't started reviewing yet
  - Volunteers to help with the program are welcome
- Input from OpenSSF event in DC in September; see doc SOSS Task Force: OSIS-TF
  - "Proposed roadmap"
    - Q1
      - Initiate the process to standardize build instructions in a universal, machine-readable language.
      - Define associated problems and challenges within the open-source software supply chain.
    - Q2
      - Conduct a technical survey to understand current practices and gaps in the supply chain.
      - Delve into enabling third-party (3P) builds, with platforms like Nix and Portage being explored. (Note: Eric will be seeking additional assistance in this domain).
    - Q3/Q4
      - Engage users and enhance the adoption of new capabilities developed and introduced in the previous quarters.
      - Assign Cheuk to focus on the adoption of these new capabilities by open-source consumers.
  - Some hesitation around the value and feasibility of standardized build instructions
    - Why this group?
    - Why/how might we succeed where others have failed?
  - We have no real context about any of the above
    - Would be useful to have more background
    - Who asked for this stuff? Who's the customer, etc?

- This meeting: we've been agenda-light recently. Any thoughts or ideas on how best to use this time?
    - Sub-groups (e.g., SLSA, S2C2F, gittuf, GUAC) are certainly active and productive
    - Some things we could usefully do in this group
        - Review progress and blockers from sub-groups
        - Demos from other projects and working groups
        - Presentations from actual in-the-field practitioners
            - e.g., "Corporation [foo] on implementing SLSA internally"
            - e.g., "I'm at company [bar] and I'd like to use GUAC to do [baz]"
        - More coordination within the OpenSSF
            - e.g., invite End Users WG to come present

Dec 6, 2023

Attendees

- Isaac Hepworth (Google)
- Nathan Menhorn (AMD)
- Kyle Kelly (Semgrep/CramHacks)
- Arnaud Le Hors (IBM)
- Jay White (Microsoft)
- John Kjell (TestifySec)
- Abdullah Garcia (JP Morgan)

Regrets:

- Marcela Melara (Intel) – working towards a paper deadline tonight

Agenda/notes:

- Direction and priorities for 2024
    - Reprised the quarterly TAC review, ssci.io/sci-deck
    - Directions in 2024:
        - SLSA, new tracks
        - S2C2F, attestation format
        - gittuf, enabling SLSA Source track
        - GUAC, continuing supply chain metadata aggregation and synthesis
    - For the TAC
        - WG landscape: current WGs have evolved organically and split simultaneously by audience (e.g., End Users), by approach (e.g., Tooling), and by domain (e.g., Supply Chain Integrity). Some centrally-guided refactoring could be useful.

        - Technical and architectural biases: could be good to have more formal and deliberate biases in technology and architecture across OpenSSF, e.g., in-toto should be a default choice for attestation format.
    - Note that there is now a “WG Leads” meta-WG for better coordination, information sharing, etc., across the OpenSSF
- OpenSSF Elections are upon us
    - TAC is expanding from 7 seats to 9 seats
    - Going forward, elections will be staggered to split up TAC turnover
    - TAC election timeline
        - Nominations Open: NOW
        - Nominations CLOSE: Dec 15
        - Voting Starts: December 16
        - Voting Stops: December 30
        - New members seated: January 1
    - To request a ballot that we sent through OpaVote please fill out this google form.
    - To run for the TAC:
        - SCIR Member GB Nomination Form
        - TAC Community Seat Self-Nomination Form
- SCI WGs inventory and possible refactor
    - Probably time that we take a look at various WG meetings in SCI-land
        - e.g., SCI Positioning was originally chartered with creating clarity wrt various in-motion standards and frameworks last year. Is it still needed?
    - SCI Positioning now very active driving blogs, conferences, papers etc.
        - Perhaps this is now “SCI Evangelism” or such? Confusion between SBOM, SSDF, SLSA, S2C2F, etc., seems to have diminished
    - We could start by listing out what we have and going from there
- CFP just dropped for OSS NA
    - Closes 1/14
    - https://events.linuxfoundation.org/open-source-summit-north-america/program/cfp/
    - jaywhite@microsoft.com is chairing SupplyChainSecurityCon component
- DevRel community is spinning up… opportunity for collaboration here

Nov 22, 2023

Attendees

- Mike Lieberman (Kusari)
- John Kjell (TestifySec)
- Kyle Kelly (Semgrep/Cramhacks)
- Jon Williams (NSA ESF)

- Adam Shamblin (DigitalOcean)
- Jay White (Microsoft)
- Adrianne Marcum (OpenSSF)

Agenda

- Note that this meeting was on Thanksgiving eve which impacted attendance and production
- Mostly working session to clean up some stuff and chat about future work

Nov 8, 2023

Meeting canceled to accommodate KubeCon attendance

Oct 11, 2023

Attendees

- Isaac Hepworth (Google)
- Kyle Kelly (Semgrep)
- Aditya Sirish (NYU, in-toto, gittuf)
- Nathan Menhorn (AMD)
- Dana Wang (OpenSSF)
- Brandon Mitchell (IBM)
- Mike Lieberman (Kusari)
- Patricia Tarro (Dell)
- John Kjell (TestifySec)
- Matthew Wood
- William Burton (Google)
- Matt Suozzo (Google)
- Matthew Wood
- Chad Kimes (GitHub)
- Joshua Lock (Verizon)
- Tom Hennen (Google)
- Luiz Carvalho (Red Hat)
- Jay White (Microsoft)

Agenda:

- :03 Welcome new friends (Isaac Hepworth)
    - Hi Dana!

- :05 New project additions to SCI WG 🙌 (Isaac Hepworth)
    - Welcome gittuf 🎉
    - Welcome GUAC 🥳
- :10 Rebuilding OSS (Matthew Suozzo)
    - [link to slides]
    - Question about reuse of existing reproducible build work
        - Matt's in touch with maintainer of https://github.com/kpcyrd/rebuilderd
            - Presented earlier version of this work at reproducible builds workshop last year
            - Foundational work has been vital to enable the plausibility of this project
        - For language packages, much of the complexity is in the inference/heuristics side, where existing work on OS packages has limited reuse value
        - Long-term, plausibly makes sense to converge the projects
    - Question about how much of the 67% reproducible required human intervention
        - 67% is "semi-automated" with light human review of heuristically-derived build process
        - Human inputs were as it happened ~reliably recreatable using COTS LLM
    - Question about the distribution story for attestations coming from rebuilds
        - Intent to reuse as much of Sigstore/Rekor/Cosign as possible
        - BUT indeed rebuilder can't push provenance to the original package location
    - Question as to whether "rebuild" attestations are special/custom
        - It's implemented as SLSA Provenance
        - In more detail, it's actually several since the 'build' is run separately from the 'compare' for isolation purposes so both of them get provenance.
    - Question re: "when can we play with this?!"
        - Talk at PackingCon coming up; hoping to have code published shortly
    - "I feel like there's an opportunity for rebuilders to add scorecard like checks, running vulnerability scans on the source, checking for PR approvals, git commit signing, etc." - Brandon Mitchell
- :40 in-toto across OpenSSF (John Kjell)
    - Many of the security properties of interest could be captured as in-toto attestations; do we see as a group that as the right general direction?
    - Desire for more specificity as to shared schemas, common semantics, etc. to make machine readability more tractable
    - How can we evolve standardized predicates over time?
        - some core standard set
        - some set of vendor extensions (like "X-" HTTP headers)
        - some set of loosely experimental etc.

        - This is encoded today in https://github.com/in-toto/attestation/blob/main/docs/new_predicate_guidelines.md#vetting-process
    - How do we settle on in-toto across OpenSSF?
        - Perhaps driving via the TAC? mike@kusari.dev could help here.
    - Need to settle on a consumption story, too. Generation of in-toto is just one part

- :45 tbd

Sep 27, 2023

No agenda! — canceled

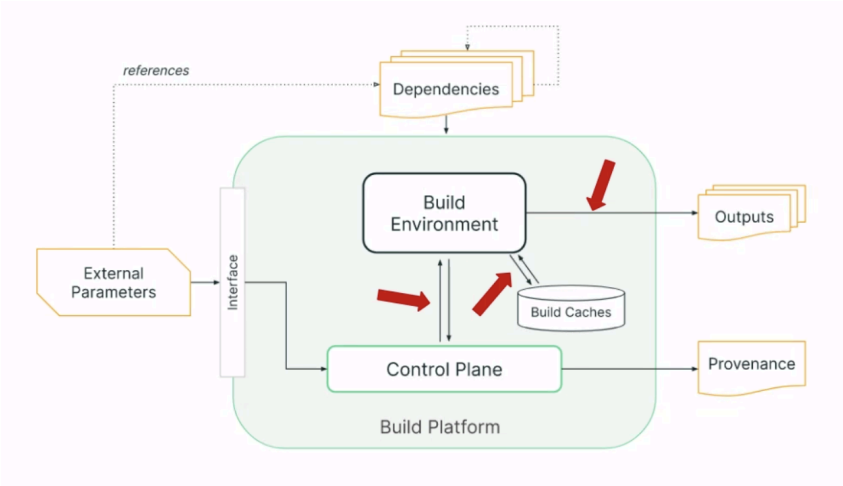
Sep 13, 2023

Attendees

- Isaac Hepworth(Google)
- Seth Larson (PSF)
- John Kjell (TestifySec)
- Chad Kimes (GitHub)
- Marcela Melara (Intel)
- Bruno Domingues (Intel)
- Mike Lieberman (Kusari)
- Byron Nevis (Intel)
- Kris Borchers
- Matthew Wood (Intel)
- Aaron Bacchi (Verizon)
- John Andersen (Intel)
- Tricia Tarro (Dell)
- Aditya Sirish (NYU, in-toto, gittuf)
- Shripad Nadgowda (Intel)
- Luiz Carvalho (Red Hat)
- Brandon Mitchell (IBM)
- Kris Kooi (Google)
- Jay White (Microsoft)

Agenda

- :03 Welcome new friends 👋
    - Chad Kimes (GitHub)
    - Patricia Tarro (Dell)
- :05 SCI and SLSA Scope (Isaac)
    - Thoughts on trajectory of SLSA expanding to “fill” SCI WG scope
    - Questions about S2C2F and dependency track of SLSA
    - Attempt of ‘control plane’ concept to pull together raw materials into a more coherent whole
- :15 Build environment attestations (Marcela / Chad)
    - Slides
    - Framing: Threats to the Build Environment
        - SLSA defines trusted build platforms
        - Assume build platforms are not malicious
        - Build platforms are not perfect
        - Assuming temporary breach, what are the possible threats?
        - How can we protect against those?
    - Threats to the Build Environment
        - Tampering with
            - image generation or boot process
            - build init or build execution
            - control plane
            - build cache
        - Install malicious bootloader or kernel
            - Very difficult to detect without hardware measurement
        - Modify/compromise build software (compilers, package managers)
        - Install persistent backdoors
        - Poison build outputs or inputs
        - Attacker goals:
            - Poison build outputs
            - Access CI/CD secrets



- (Very High-level) Trusted Hardware Background
  - Static attestations:
    - Capture launch-time state
    - Examples: Intel SGX, AMD SEV
  - "Dynamic" attestations
    - State can be re-measured as new code is loaded onto the platform
    - Examples: TPMs, Intel TDX
  - Confidential compute platforms:
    - Memory is encrypted and integrity-protected during execution
    - Some provide remote attestation features (including via RATS)
    - Examples: Intel SGX, AMD SEV, Intel TDX, ARM TrustZone
- Providing Build Environment Integrity
  - Goal: To provide build integrity *even in the face of control plane compromise*
  - UEFI Secure Boot + TPM Attestation
    - Remotely validate Secure Boot parameters
    - Remotely validate bootloader, kernel, initramfs
    - Validate build environment image
      - Currently limited ecosystem support, possible with dm-verity
  - Confidential Computing (Intel SGX, Intel TDX, AMD SEV-SP)
    - Fully encrypted execution environment
    - Remotely attestable
    - Provides hardening against control plane attacks
    - Caveat: Intel SGX mostly suitable for smaller-scale, highly sensitive operations like signing

- PROPOSAL: A new SLSA track for Attested Build Environment

Level	Threat addressed	Requirements
L1	Tampering with build of build environment	Attest to provenance of build environment
L2	Tampering at boot time	Run build env on secure boot-enabled compute
L3	Tampering during build init	• Run build env on run-time measured HW • Attest to binding between build environment and build ID
L4	Tampering during build execution	Attest to policy enforcement: dependency ingestion, external resource accesses

    - Question about trust anchor and who makes/signs attestations
        - Trust would be delegated to the platform provider
    - Question about intersection/overlap with “Build L4”
        - View of hermeticity as a property of the build environment rather than the build process
    - Question about what is realizable today with common hardware capabilities
        - Validate bootchain
        - Support needed on both hardware and software sides
    - “Trust but verify” approach
- Need to figure out how to ‘land’ this in SLSA itself
    - We don’t yet have a set of principles to guide creation of new tracks etc.
    - Good next step could be discussion in SLSA Specification WG

Aug 30, 2023

Attendees

- Isaac Hepworth(Google)
- Aditya Sirish (NYU, in-toto, gittuf)
- Lindsay Newton (VMware)
- John Kjell (TestifySec)
- Mike Lieberman (Kusari)
- Seth Michael Larson (PSF)
- Melba Lopez (IBM)
- Kris K (Google)
- Brandon Mitchell (IBM)
- Mark Lodato (Google)

- Eddie Knight (Sonatype)
- Kyle Kelly (Semgrep)
- Marcela Melara (Intel)
- Jay White (Microsoft)
- Tom Hennen (Google)
- Luiz Carvalho (Red Hat)
- Billy Lynch (Chainguard)

Agenda

- :03 Welcome new friends 👋
    - Aditya, NYU, working on software supply chain
    - Kyle, security consultant and researcher
- :04 SSP
    - Group consensus to invite Omkhar to come tell us more
    - We'll gather questions for the session async
- :08 Supply Chain Control Plane (Isaac Hepworth)
    - Trying to establish some conceptual anchors for our space, and identify patterns we're seeing from various contributors
        - ssci.io/control-plane
    - Please read and comment on the doc!
    - Feedback from the meeting
        - Would be useful to have a crisper idea of the universe of tools fitting together in this space
        - How is policy consistently applied left-to-right across the SDLC?
- :10 Generic SDLC Architecture (Tom Hennen)
    - Slides
    - Discussion
        - Admission control as a broad concept
            - Runtime, yes, e.g., "traditional" k8s admission control
                - Although for runtime, *evaluations* should occur to the left, ahead of time (and be captured in a signed VSA, for example)
            - But also for artifact registries, source management, dependencies etc.!
        - Kusari sees things similarly, and is building in this space
- :40 gittuf (aditya.sirish@nyu.edu)
    - Slides: gittuf @ OpenSSF SCI WG
    - Resources
        - Repository: https://github.com/gittuf/gittuf
        - Website: https://gittuf.github.io/
        - Demo: https://github.com/gittuf/demo

        - Roadmap: https://github.com/gittuf/gittuf/blob/main/docs/roadmap.md
    - Discussion
        - Show of hands; no objections to adding to SCI WG in Sandbox
        - AI: Isaac to help coordinate work with TAC etc. to land gittuf in OpenSSF
            - (follow-up Sep 5, 2023, see here)

Aug 16, 2023

Attendees

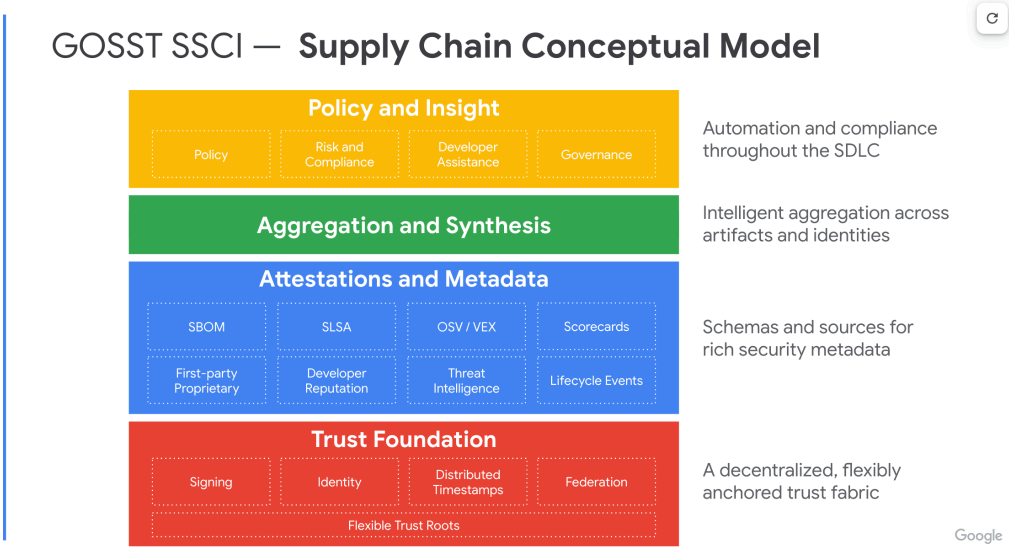
- Isaac Hepworth (Google)
- Joshua Lock (Verizon)
- Seth Larson (PSF)
- Michael Scovetta (Microsoft, Alpha-Omega)
- Nathan Menhorn (AMD)
- Lindsay Newton (VMware)
- Brandon Mitchell (IBM)
- Laura Seay (Red Hat)
- Jay White (Microsoft)
- mike@kusari.dev(Kusari)
- Marcela Melara (Intel)
- Arnaud Le Hors (IBM)
- Matthew Wood (AWS)
- John Kjell (TestifySec)

Agenda

- Welcome new friends
    - nobody today!
- Update on SSP
    - Since last time…
        - Isaac Hepworth wrote to the TAC/GB
        - Anecdotally, many many other folks in OpenSSF WGs have the same concerns, questions, frustration, and curiosity
        - Omkhar (OpenSSF GM) responded “a doc is going through a GC review that compares and contrasts OpenSSF and the proposed scope of SSP. Once this doc is relatively stable, we can share more with the community”
        - OpenSSF Governing Board will be discussing this Thursday Aug 17, 2023
        - Stay tuned!
    - Jay: we need to have patience; there are more moving parts here than meet the eye
- Michael.Scovetta@microsoft.com: Assurance Assertions (https://bit.ly/assuranceassertions)

- Pitch deck
  - Vision - make informed decisions around what OSSW is consumed
  - Reduce analysis on the consumer-side and provide consumable data to consumers
  - Assertion examples
    - CVEs
    - Actively maintained
    - Code was reviewed by <entity>
    - Isaac - what is this tied to? Is the Subject a project, a repo, a build artifact, a developer, etc?
    - Marcela - Is this the same as the in-toto attribute assertions? What are the differences? Intent is to align.
  - Architecture
    - Isaac - what's the Assertion Store look like? PS flat database. How to get data? REST API
  - Demo
    - You could set a policy where no CVEs are allowed versus specific CVEs
    - Wrapper around the tool itself in order to trust the tool?
      - Making the relationship between evidence and trustworthiness through assertions is definitely something that has been missing.
    - important point Michael S made there that matches my thought process: this should be separate, pluggable layers. The datastore and the policy layer as separate projects would give flexibility to keep the part that works as this project grows and experiments
  - Next step get a SIG. Michael to post further details in Slack
- Deep link

- c.f., SCI conceptual model



August 2, 2023

Attendees

- Isaac Hepworth(Google)
- mike@kusari.dev(Kusari)
- Brandon Mitchell (IBM)
- Melba Lopez (IBM) → thank you for whomever signed me in :)
- Lindsay Newton (VMware)
- John Kjell (TestifySec)
- Luiz Carvalho(Red Hat)
- Nathan Menhorn (AMD)
- Laura Seay (Red Hat)
- Mihai Maruseac (Google)
- Jay White (Microsoft)
- Marcela Melara (Intel)

Agenda

- Welcome new friends
- mike@kusari.dev: Update on GUAC, especially in light of SSP
    - Legal review done, and passed 🙌
    - We can move to OpenSSF but maintainers have concerns around support from OpenSSF

    - https://softwaresecurityproject.org/blog/the-software-security-project-is-coming-soon/
    - SSP is potentially giving pause to GUAC joining OpenSSF
        - Mainly, a desire for clarity as to the status and direction of SSP and OpenSSF
        - So far, the movements of LF and SSP don't appear particularly open
    - Isaac Hepworth to write up concerns and circulate to OSSF leadership
        - (UPDATE 8/7: DONE, see Slack)
- Isaac Hepworth: Quick reprise of TAC update
    - Question about terminology and framing of SLSA and S2C2F, see issue
    - Need clarity in terms of how we all pitch and position these projects
        - Security? Compliance? Best practice?
        - Framework? Implementation plan? Maturity model? Transformation playbook?
- jaywhite@microsoft.com: update on GitHub repo access and operations
    - Jay now has ✨admin access ✨ to OpenSF GitHub 🙌
    - Jay can now be a shortcut for common operations requests for this group
- Luiz Carvalho: Demo enterprisecontract.dev, https://github.com/enterprise-contract
    - Verification tool to track image verifications, signatures, etc.
    - OPA and Rego as policy definitions
    - GitHub action is in the works, to integrate easily into workflows
    - Question about relation to Seedwing and Trustification
        - Also from Red Hat
        - Seedwing could potentially define policies which are evaluated by EC
-

Jul 19, 2023

Attendees

- Mike Lieberman (Kusari)
- Patricia Tarro (Dell)
- Lindsay Newton (VMware)
- Claudia Ring (ActiveState)
- Brian Behlendorf (OpenSSF/LF)
- Jeff Borek (IBM)
- Brandon Mitchell (IBM)
- Luiz Carvalho (Red Hat)
- Shripad Nadgowda
- Melba
- Matthew Wood
- Joshua Lock (Verizon)

- Chad

Agenda:

- Welcome new friends
- [Mike Lieberman] Quick GUAC Update
    - Still waiting for LF legal review to finish
- Supply Chain Control Plane (Shripad Nadgowda, Intel)
- [Mike Lieberman] PURL spec questions (if there's time)
    - https://github.com/package-url/purl-spec/issues/190
    - https://github.com/package-url/purl-spec/issues/242
- [Claudia Ring] SLSA webinar - any interested co-presenters?
    - Me! (Mike Lieberman)
    - Joshua Lock (@joshuagl on GitHub) potentially interested, would like more context

Jul 5, 2023

Attendees:

- Isaac Hepworth (Google)
- Mike Lieberman (Kusari)
- Melba Lopez (IBM)
- Jay White (Microsoft)
- Abdullah Garcia (JP Morgan)
- Marcela Melara (Intel)
- Arnaud Le Hors (IBM)
- Matthew Wood (Intel)
- Brandon Mitchell (IBM)
- Nathan Menhorn (AMD)

Agenda:

- Welcome new friends
- GUAC inbound (mike@kusari.dev)
    - LF process
        - https://github.com/ossf/tac/pull/178
        - https://github.com/ossf/tac/issues/179
        - https://github.com/ossf/tac
    - SCI WG process
        - Adding a project to a WG is in itself something of a work in progress

        - GUAC is a fit nominally for SCI WG vision, per our vision doc OpenSSF SCI WG 2023 — EXTERNAL
            - "Upstream security practices universally evaluable by downstream automation"
            - No objections, +1 from Melba and Marcela and Arnaud
            - Isaac Hepworth will ping Slack and mailing list for feedback
                - Absent objections we'll consider adding GUAC to SCI WG the plan of record
- Next week's review with the TAC (Isaac Hepworth)
    - Isaac will build draft deck and circulate
    - We have a GitHub issue in the repo for TAC approval of Charter
    - SLSA — 1.0, futures (Build L4, and other tracks)
    - S2C2F — leave blank slide(s) for Jay and Adrian
    - GUAC — summarize where we're at
    - FRSCA —
        - It's a reference implementation, not a production tool
        - We still have lots of idea, but relatively few resources to move it forward
        - Possible ✨synergy✨ with Sterling Toolchain
            - FRSCA could be an implementation of the ST ref arch for Build
- [Melba] (5 mins) SCI Repo Changes + Charter Update
    - Melba did a bunch of cleanup in the repo
        - Cleaning up branches
        - Closing old issues
        - Posting/updating the charter
    - Melba also working with Jen Bly
        - We need to find folks who can help with content: copyediting, video production, etc.
            - OpenSSF doesn't have these skills on staff currently, but JBly looking into it
            - Feels like content production should be a core competency of OpenSSF?
    - Some continued operational challenges
        - Melba doesn't have edit access to calendar, e.g.
- [Mike Lieberman] SCI API
    - Might be related to some sterling toolchain stuff
    - This group is building some tools and standards and there's interest in helping define that unified API so that folks building SLSA, S2C2F, etc. tools can integrate.
    - Would be good to develop or settle on standards for pluggability of various capabilities in the supply chain
        - e.g., discovery of SLSA provenance, distribution of SBOMs, etc.

    - CDEvents could be interesting or relevant as a common language
    - Idea of a “supply chain control plane”
        - Metadata fabric spanning SDLC
        - Actors in the supply chain and add metadata
        - Actors in the supply chain can query metadata, then evaluate and actuate policy
    - Marcela has been working on supply chain control plane concept
        - Isaac Hepworth to schedule a look at it in a future SCI WG meeting

Jun 21, 2023

Attendees:

- Mike Lieberman (Kusari)
- Andrew McNamara (Red Hat)
- Nathan Menhorn (AMD)
- Brandon Mitchell (IBM)
- Chris de Almeida (IBM)

Agenda:

- New friends
- [Mike Lieberman] GUAC contribution status
    - https://github.com/ossf/tac/pull/178
    - https://github.com/ossf/tac/issues/179
    - https://github.com/ossf/tac

Jun 7, 2023 — No agenda, canceled

May 24, 2023

Attendees:

- David A. Wheeler (Linux Foundation)
- Laurie Williams (North Carolina State University)
- Adam Shamblin (DigitalOcean)
- Jonathan Leitschuh (Linux Foundation)
- Isaac Hepworth (Google)
- Jay White (Microsoft)
- Matthew Wood (Intel)

- Arnaud Le Hors (IBM)
- Joshua Lock (Verizon)
- Marcela Melara (Intel)
- Ben Edgar
- Kris Borchers
- Mikey Strauss (scribe)

Agenda:

- New friends
    - Laurie Williams — North Carolina State University
- Proactive Secure Software Supply Chain Risk Management (P-SSCRM) framework (lawilli3@ncsu.edu)
    - Slides
    - Focuses on *product*
    - So far, it's all on companies
    - Folks can contact Laurie directly (email above) for follow up
- Sterling Toolchain (sometime in May, dwheeler@linuxfoundation.org)
    - David: I've been sick so haven't been able to work on it recently
    - Issue: GB wants more *automation*. Mobilization plan identified a number of things to do. I started creating a proposal to square this circle.
    - David: Key issue: Developers generally will not *change* the tools they use. So in many cases we'll need to create plug-ins, integrations, etc. so that people can use their existing tools
    - Have started developing concept, others have been working on it: https://docs.google.com/document/d/1z4YxuT6yzbgrNlUpgTbJhuKv5ngdsd6O8Dz5yRTepgs/edit
- Next time: Next steps for vision doc OpenSSF SCI WG 2023 — EXTERNAL
    - Final call for comments!
    - By next meeting we'll have begun formalizing the adoption of this doc, including circulating with the TAC etc.

May 10, 2023

Canceled owing to OSS NA Vancouver.

Apr 26, 2023

Attendees:

- Isaac Hepworth (Google)
- Mike Lieberman (Kusari)
- Will Enck (NC State)
- Tim Pepper (VMware)
- Matt Wood (Intel)
- Jay White (Microsoft)
- John Kjell (VMware)
- Mike Thompson (AWS)
- Marcela Melara (Intel)

Agenda

- Welcome new friends!!
    - Matt Wood, working on internal adoption of SLSA at Intel. Motivations:
        - Goodness and light
        - Compliance too
- [Mike Lieberman] Updates from KubeCon EU
    - SLSA 1.0 announcement went over well.
        - Lots of excitement
        - Interest in the future roadmap with respect to evolution and addition of tracks
    - SLSA audits!
        - Prometheus and Argo had an audit through CNCF
        - They are looking to do more
        - They are looking to partner with OSTIF (also under LF) as the way CNCF pays for audits.
    - Some confusion around S2C2F. Folks have heard of it, but unsure where it fits in. Some folks have pointed out a lot of the documentation indicates it's a Microsoft framework instead of an OpenSSF framework: https://www.microsoft.com/en-us/securityengineering/opensource/osssscframeworkguide
        - All maintainers being Microsoft employees doesn't help
        - Some of the links point to: https://github.com/microsoft/oss-ssc-framework instead of https://github.com/ossf/s2c2f
            - jaywhite@microsoft.com is already on a mission to chase these down and fix them
            - Notably, folks finding this stuff is encouraging in the sense that people are reading the docs :)
    - Desire for OpenSSF to take a larger part in helping define end to end supply chain security

        - Some folks aren't ready for cloud native adoption yet, and want to better understand how to secure supply chain outside of cloud native tools.
        - Folks are asking for more diagrams and where SCI fits in.
        - Unclear if/when SCI will focus more on tooling.
            - We need to work out how we scope and drive this work in OpenSSF
                - slsa-tooling?
                - sci-tooling?
                - openssf-tooling?
            - Potentially we engage the TAC in helping to drive alignment?
- Question about when Hermeticity requirement will come back (removed in L4)
    - We need better definition around the precise requirement
        - "hermetic" has some wiggle-room with various interpretations
        - Request from Matt T for recognition of the nuance around network access being allowed, but under controlled circumstances (e.g., metered, whitelisted, logged, etc.)
    - Anticipate a "SLSA Build L4" draft in the coming weeks, for community feedback and comment
    - Other additions on the radar
        - Source track
        - Securing custom build infra (e.g., not using a COTS SaaS tool)
- OpenSSF SCI WG 2023 — EXTERNAL review and next steps
    - We need to be cognizant of high bar of requirements for smaller software organizations
    - incentives in open source are worthy of note and recognition
        - OSS rebuilding could be part of the solution here
        - Aspiration of OSS could be to make builds readily operable by others
            - Pain when OOTB OSS builds fail, should be easily buildable by someone with SLSA-conformant builders
                - Example of Apache OSS
            - Possibly this is table stakes for mature OSS, even
                - new SLSA practice?
        - Observation of the overall "accountability gap" in open source
            - Red Hat has a business here, others nascently so

Apr 12, 2023

Attendees:

- Isaac Hepworth (Google)

- David A. Wheeler (Linux Foundation)
- Joshua Lock (Verizon)
- John Kjell (VMware)
- Nathan Menhorn (AMD)
- Brandon Lum (Google)
- Tim Miller (Kusari)
- Aditya Sirish (NYU, in-toto)
- Melba Lopez (IBM)
- Sunny Yip (Kusari)
- Mike Lieberman (Kusari)
- Tazin Progga (VMware)
- Will Enck (NC State)
- Hossein Siadati (Datadog)
- Justin Abrahms (Looking for work? 😅)
- Parth Patel (Kusari)
- Mihai Maruseac (Google)
- Jeff Borek (IBM)
- Jay White (Microsoft)
- Matthew Wood (Intel)
- Farzaneh Sarafraz (Google)
- Hemil Kadakia (Yahoo)
- Adam Shamblin (DigitalOcean)
- Marcela Melara (Intel)
- Jeff Mendoza (Kusari)

Agenda:

- Welcome new friends!!
    - Aditya Sirish
    - Farzaneh Sarafraz
    - Sunny Yip (Kusari)
    - Hossein Siadati (Datadog)
    - Justin Abrahms
    - Tazin Progga (VMware)
    - Adam Shamblin
    - Tim Miller (Kusari)
    - Parth Patel (Kusari)
    - Jack K (ControlPlane)
    - Mihai Maruseac (Google)
    - Brandon Lum (Google) - on same team as Mihai

- [Michael Lieberman] (Kusari) - GUAC demo - approx 20 minutes
    - GUAC = Graph for Understanding Artifact Composition
    - Collaboration of Google, Kusari, Citi
    - Fundamental problem: transitive closure of dependencies affects you.
        - You may inject 10s of thousands of packages in an application, most won't hurt you but one might.
        - Need a way to understand your data, like a telescope, can zoom in/out
        - Have too much data (many many packages)
        - Yet in other ways have too little data (data quality problems, unknown unknowns)
        - Need to understand relationships of data
    - GUAC is a software supply chain observatory - lets you see information
    - E.g., see GUAC image - many Python packages, many depend on containers, etc.
    - SLSA provides a lot more information about how the package was built
    - GUAC is a knowledge graph, enables analysis & synthesis. Builds on:
        - Trust foundation (sigstore is here)
        - Software attestations (SLSA is here)
    - GUAC enables you to be proactive & reactive
    - GUAC ingests many data sources into a graph database, currently neo4j
    - Two kinds of queries:
        - Informational (learn more about it)
        - Evidence ("how do you know this claim is true?")
    - Two main kinds of uses
        - Use only public data
        - Use private data (for a specific organization)
    - Demo!
        - E.g., run a query. E.g., "what has SLSA attestations?"; "what do I know about the builder for kubernetes?"
        - Can query on specific vulnerability (e.g., Log4Shell) & starting point, & it can list nodes via terminal or create a visualization showing the sequence that gets you there.
        - Q: Day-to-day, how would you use this? This couldn't be done with so many vulnerabilities & packages.
        - Working on many other things as proof of concept
    - Follow-up
        - Project hosted at: https://github.com/guacsec/guac
        - GUAC Community mailing list: https://groups.google.com/g/guac-community
        - GUAC Community meetings monthly (Calendar Invite, Recordings: https://www.youtube.com/@guacsec)
        - We are looking for devs/contributors! (issue#1)

        - The project will have Technical Advisory Members which are to inform the project. It is still a developer first project. (issue#1)
        - Kubecon 2022 Talk: https://sched.co/182Jr
- Sterling Toolchains
    - OpenSSF governing board wishes to see more emphasis on automation
        - “Sterling toolchain” was an idea which came from this
        - David co-authored a document to connect the concept to the mobilisation plan and other efforts in the OpenSSF: Sterling Toolchain Concept
        - RFC from the TAC https://github.com/ossf/tac/issues/151
            - Though TAC is currently in transition from 2022 members to 2023 members (3 seats not yet filled)
        - Would b noe good to have some specificity about how Sterling Toolchain intersects (or doesn’t) with FRSCA
        - Let’s schedule a follow-up in May as the concept crystalizes
    -
- SIG Round-up
    - SLSA (esp. version 1.0)
        - On track for April 18th release
        - Comms out on April 19th
        - Companies can begin publishing their own blogs April 26
        - Blog by Mike on Tracks
        - Upcoming blog on deep dive on bld vs src,
    - S2C2F
        - RSA
        - OSSummit
        - SKF Training Modules
    - FRSCA
        - Needs developers! Please reach out to mlieberman85@gmail.com
- Reminder to review the OpenSSF SCI vision doc OpenSSF SCI WG 2023 — EXTERNAL
    - Isaac to review comments and discuss in next WG meeting (2 weeks)

Mar 29, 2023

Attendees:

- Michael Lieberman (Kusari)
- Jay White (Microsoft)
- Jeff Borek (IBM)
- John Kjell (VMware)
- Nathan Menhorn (AMD)

- Ixchel Ruiz (JFrog)
- Claudia Ring (ActiveState)

Agenda:

- Welcome new friends
    - John Kjell - In a lot of the other meetings and joining this one to see what we're working on.
    - Ixchel Ruiz - Also in a lot of the other different working groups. Very interested in supply chain security.
- SLSA 1.0 RC
    - RC2 coming out soon
    - SLSA talks at Open Source Summit
    - Distributing provenance - https://github.com/slsa-framework/slsa/pull/673
    - Depth and Breadth of SLSA blog - https://github.com/slsa-framework/slsa/pull/740
    - BLD vs SRC blog - https://docs.google.com/document/d/1W-oiua5somqp0vXnyCq9apGPyYz5mTj8TNSzZbsVNAE/edit
    - SLSA tooling meeting
- S2C2F is creating training modules
    - Adrian is giving a talk at RSA on S2C2F
    - Working on explanatory report
- FRSCA
    - What is FRSCA

-Mar 15, 2023

[meeting summary in Slack]

Attendees:

- Isaac Hepworth (Google)
- Jay White (Microsoft)
- Michael Lieberman (Kusari)
- Jonathan Leitschuh
- Tim Pepper (VMware)
- Benjamin Schmidt
- Melba Lopez (IBM)
- Joshua Lock (VMware)
- Arnaud Le Hors (IBM)
- Eddie Knight (Sonatype)

Agenda:

- Welcome new friends
  - Tim Pepper, Principal Eng in VMware OSPO
  - Benjamin Schmidt, Cybersecurity Eng in MITRE
- WG Leadership
  - Update the README in the openssf GitHub, currently shows Kim & Dan as WG leads
  - Dan stepped down when he joined the TAC; Kim stepped back from the meeting several months ago
  - What's the process for naming new/additional chairs?
  - (Joshua) Isaac has been facilitating meetings and driving 2023 vision, seems a strong candidate for WG chair
  - OpenSSF requires two chairs, nominating chairs is a simple WG vote with notification to the TAC
    - https://github.com/ossf/tac/blob/main/process/working-group-lifecycle.md
  - This WG's repo has governance doc which states only "TODO"
  - Proposal: Isaac as chair, Jay and Melba as co-chairs
    - No recorded objections in the meeting
  - Making it so: a PR on the README (done, 3/15), with thumbs up from stakeholders in this team
    - Note that there were no objections today
      - Done 3/15
    - Include a link to the meeting video
      - tk
    - Include a link to the Slack message publishing the proposal
      - Done 3/16
- 2023 Vision Proposal (Isaac)
  - Been incorporating comments, updating document, clarifying wording
  - Most comments to date have been clarification round the edges, not on the substance
  - Question for the group: is there a shared sense that the overall direction is ~right?
  - SCI Positioning group post-dates this document
    - Original framing of positioning group: "The relationship between adjacent technologies, frameworks, and methodologies in the SCI space is clear with appropriate cross-links established"
    - Possibly there's a chance to incorporate new structure we have into 2023 priorities
    - Question about whether SCI Positioning is a WG or a SIG or a Project… possibly it needs to be a SIG, in line with OpenSSF uber-structure
    - Updated/Commented on SIG naming change on the top of the meeting notes

    - Opportunity to adjust meeting cadence and schedule
        - This group (SCI WG) might instead meet bi-weekly rather than monthly
    - Next steps:
        - Isaac to continue to incorporate feedback on the doc
        - Isaac to add some detail on role of SCI Positioning (and tag Melba/Jay)
        - We'll move this forum to bi-weekly (*done 3/15 by* Melba.Lopez@ibm.com) and use it to land on a final doc we all nod along with
- SLSA Update
    - 1.0 RC Is out and open for comments
    - See #sci-positioning Slack channel for recent updates
    - **Very** interesting results from last year's SLSA survey
        - https://www.chainguard.dev/unchained/new-slsa-survey-reveals-real-world-developer-approaches-to-software-supply-chain-security
        - https://uploads-ssl.webflow.com/6228fdbc6c97145dad2a9c2b/640b6a455617000890bd79ba_SLSA%2B%2BWhitepaper_Design_Final.pdf
- S2C2F Update
    - Training modules under development
        - Eight hours total, in various blocks
    - Useful input from David W will likely be incorporated into the framework itself
    - Presentation to RSA is confirmed 🙌
- FRSCA Update
    - FRSCA is looking for more contributors/maintainers. Many of the current contributors and maintainers have either permanently or temporarily moved onto other priorities.
    - Could do with some more hands-on contribution and leadership/stewardship of the vision
    - Note that we have a FRSCA presentation in Vancouver in May @ Open Source Summit NA
    - FRSCA has huge potential as an e2e reference implementation of SCI practices and tools; could help with comprehension and ultimately adoption
        - Securing the pipeline definition
        - Secure the orchestration
        - Secure the build execution itself
    - mlieberman85@gmail.com has been writing a doc to frame FRSCA, where it is, its goals and ambitions. Will share with the group

Feb 15, 2023

Attendees:

- Isaac Hepworth (Google)

- Mike Lieberman (Kusari)
- Kathleen Goeschel (Red Hat)
- Caroline Cameron (IBM)
- Andrew McNamara (Red Hat)
- Jay White (Microsoft)
- David A. Wheeler (Linux Foundation)
- Arnaud Le Hors (IBM)
- Will Enck (NC State)
- Trevor Dunlap (NC State)
- Christine Abernathy (F5)
- Katherine Druckman (Intel)
- Melba Lopez (IBM)

Agenda:

- Welcome new friends
    - Caroline Cameron (IBM), works with Melba
    - Andrew McNamara (Red Hat), interested in usable security & privacy
- mlieberman85@gmail.com — Supply Chain Taxonomy (conversation topic)
    - I keep hearing about it, but not sure what's going on with it.
    - TAC has discussed adopting "Taxonomy of Attacks on Open-Source Software Supply Chains" by Piergiorgio Ladisa, Henrik Plate, Matias Martinez, Olivier Barais, https://arxiv.org/abs/2204.04008. TAC hasn't made any decision at this time. It's on a taxonomy of attacks, but of course you can map defenses to what you can defend.
    - MITRE has done some work, e.g., MITRE ATT&CK
    - See also pbom.dev, "Open Software Supply Chain Attack Reference (OSC&R)"
    - OpenSSF Diagrammer's Society OSSF Diagrammers Society Meeting Notes
    - S2C2F - front portion has a list. See: https://slsa.dev/spec/v0.1/threats
    - SLSA has a list too https://slsa.dev/spec/v0.1/threats
    - Others have starting doing this, e.g., in-toto, CNCF.
    - David: These tend to be taxonomies of the attacks. I could imagine a taxonomy of the defenses, but that's harder, and in the end we want to know what attackers are countered.
    - Take-away: Work with end user group. Encourage them to not re-invent the wheel unless needed.
- Melba - SLSA Positioning Update
    - 1.0 Spec Draft (pre-RC) https://github.com/slsa-framework/slsa/issues/606
    - SCI Panel for OSSNA submitted : **Ketchup, Mustard, and Relish of Software Supply Chain Security (panel)**
    - SLSA OpenSSF Landing Page (SCI - 10 point mobilization plan link)
        - SLSA, FRSCA, S2C2F sub pages

        - Focus on how it fits into the overall picture
        - c.f., https://openssf.org/community/sigstore/
    - Positioning upleveling?
        - Jay agreed to co-lead S2C2F
        - Mike (maybe) to co-lead FRSCA
        - Need to update charter- expansion of charter scope
        - Meetings renamed/slack channel renamed
        - David: If you change a WG charter, need to ask TAC to review/approve. As long as it's reasonable they are generally happy, but the goal is to try to make it so the WGs don't constantly bump into each other.

Reminder to review and comment on OpenSSF SCI WG 2023 — EXTERNAL

- Will this be presented to the TAC? And if yes, when?
- Need to ensure alignment with OpenSSF Charter/Mission for the year

Jan 18, 2023

Attendees:

- Isaac Hepworth (Google)
- Rob Szumski (EdgeBit)
- Joshua Lock (VMware)
- Jay White (Microsoft)
- Melba Lopez (IBM)
- Trevor Dunlap (NC State)
- Nathan Menhorn (AMD)
- Christine Abernathy (F5)
- Will Enck (NC State)
- Abdullah Garcia (J.P. Morgan)
- Randall T. Vásquez (Gentoo/Homebrew/SKF)
- Matt Rutkowski (IBM)
- Michael Lieberman (Kusari)

Agenda:

- (Isaac Hepworth) Review OpenSSF SCI WG 2023 — EXTERNAL — approach for 2023
    - Comments inline throughout the doc. Added follow-ups to each.
- (Melba.Lopez@ibm.com) 2023 Future Roadmap/priorities requested from SCI for SLSA, S2C2F, FRSCA
    - Once we have alignment on the vision (above doc), what can we make actual progress on?

        - e.g., how best to target conferences, marketing, outreach, etc.
    - Need to define actual streams of work and deliverables and so on.
- (mlieberman85@gmail.com) 2023 FRSCA Roadmap
    - Review next week in FRSCA WG

Chat:

Dec 14, 2022

Attendees:

- Abdullah Garcia (J.P. Morgan)
- Melba Lopez (IBM)
- Trevor Dunlap (NC State)
- Will Enck (NC State)
- Isaac Hepworth (Google)
- Jonathan Leitschuh (Dan Kaminsky Fellowship)
- Jay White (Microsoft)
- Arnaud Le Hors (IBM)

Agenda:

- Melba (5 mins): 2023 Future Roadmap/priorities requested from SCI for SLSA, S2C2F, FRSCA
    - Looking at what improvements we can make going into 2023
    - We can do a better job at drawing the joint picture across the various SIGs
    - We have a “missing middle” problem of insufficient structure and vision between the top-level OpenSSF direction and the work in individual SIGs
    - Single framework to provide standardization of Supply Chain Integrity (potential vision) in a scalable manner
        - Should also enable enterprise with this framework
        - Define scalable - all package ecosystems, distributions, etc
        - Framework would drive where the gaps are and who we need to reach out to
- **Next steps:** Draft up the new vision for SCI and share with broader stakeholders
- **Next Steps:** Review new draft and kickoff 2023 with new priority/alignment
- **Next Steps:** Bring new charter to TAC
- **Next steps:** Should pull in reps from NPM, PyPi, etc to get better access/collaboration from other organizations
- Melba (5 mins): Coordination between SLSA, S2C2F, FRSCA SIG Leads
    - Revisit after 2023 and consensus with vision

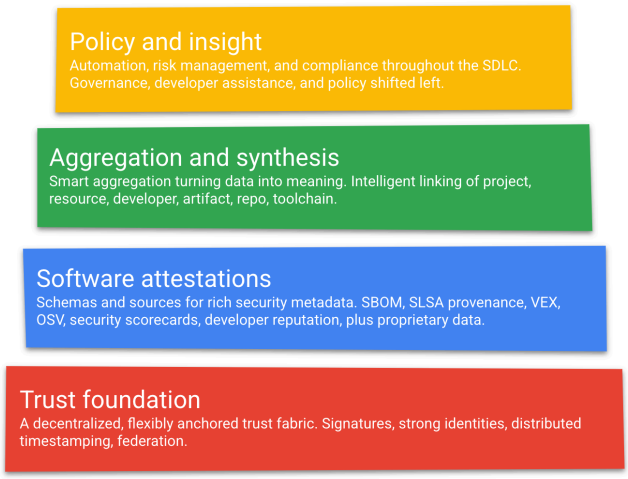
Nov 16, 2022

Attendees:

- Isaac Hepworth (Google)
- Aaron Bacchi (Verizon)
- Arnaud Le Hors (IBM)
- Mike Lieberman (Kusari)
- Randall T. Vasquez (SKF/Gentoo/Homebrew)
- Will Enck (NC State)
- Kim Lewandowski (Chainguard)
- Abdullah Garcia (J.P. Morgan)
- Trevor Dunlap (NC State)
-

Agenda:

- Aaron Bacchi to present Verizon case study
    - Link to blog post
    - Insights:
        - SLSA enables a scan of a binary to be strongly linked to a commit SHA
        - Current wave is about generation of provenance; next will be about consumption, e.g., policy decisioning and consumer risk assessments
        - Lots of opportunity to make security metadata actually *valuable* to various audiences



        - Current state of documentation, tutorials, guides, etc., are oriented around the happy path, and there's limited coverage of rainy day scenarios
- Project updates (mlieberman85@gmail.com)

    - Tooling:
        - Rather quiet recently with Kubecon, vacations, etc.
        - Exploring implications of recent changes in OCI
            - Distribution
            - Artifacts
        - Working on some details and nuance around conformance, interpretations of spec intent as applied to actual tooling implementations
        - Starting to investigate the “Aggregation and synthesis” layer (see diagram above)
    - Specification
        - Draft for 1.0 SLSA provenance spec is posted (Mark Lodato)
        - Working through some definitional minutiae (e.g., “ephemeral” versus “isolated” etc.), checking for prior art (e.g., standard NIST definitions)
        - Looking for opportunities to collaborate with SBOM community
            - particularly around SPDX “buildinfo” concept, which is rather similar to SLSA provenance
            - hoping to make interop and conceptual landscape simpler
    - Positioning
        - Blog post being drafted on problems solved by SLSA, ideally to accompany 1.0 spec launch
        - Some residual work around mappings to adjacent standards
            - Lots of surrounding pieces still in motion
    - FRSCA
        - Well received FRSCA talk at Kubecon
        - Lots of interest, including in how to make the framework simpler
            - Not the easiest thing to deploy today; looking at argo and flux as potential packaged deploy solutions
        - Interested in additional collaborators
        - Integrating SPIRE into Tekton, should be complete in a few weeks
        - Talk by mlieberman85@gmail.com next month in Japan
            - “Securing Your Supply Chain by Building with FRSCA”
    - S2C2F
        - Blog post going out today, both on the MSFT blog and OpenSSF blog (Adrian.Diglio@microsoft.com)
            - Announcing S2C2F’s addition to SCI WG in OpenSSF
- Open discussion topics if any
    - None!
        - Everyone gets 28 minutes back to stretch legs, drink water, pet a cat, enjoy sunshine, get fresh air, etc.

October 26, 2022

Attendees:

- David A. Wheeler (Linux Foundation)
- Isaac Hepworth (Google) - Facilitator today
- Sebastien Awwwad (Anaconda)
- Jay White (Microsoft)
- Christine Abernathy (F5)
- Melba Lopez (IBM)
- Trevor Dunlap (NC State)
- Joseph Gonzalez (USPTO)
- Arnaud Le Hors (IBM)
- Will Enck (NC State)
- Avishay Balter (Microsoft)
- Sarah Evans (Dell)
- Katherine Druckman (Intel)
- Matt Rutkowski (IBM)
- Nathan Menhorn (AMD)

Agenda:

- Status of SLSA - will be covered tomorrow
    - Specification - 1.0 Project underway. Narrowing focus on build, levels 1-3 (4 TBD), there is a separate “source” track
    - Positioning - Dev Blog underway - will include move to 1.0, have noted some discrepancies while writing the blog & will report that back
    - Tooling - (No tooling meeting last week due to KubeCon). Update pending from Mike L
    - Unclear how well SLSA working group will be attended this week due to KubeCon
- `Thoughts on slsa-positioning ⇒ sci-positioning (Isaac) - supply chain integrity positioning`
    - Maybe move SLSA positioning group up to supply chain integrity WG overall, in particular, make sure SLSA & S2C2F & Frsca map into the problem space so it’s clear
    - It’s made more pressing by the welcome addition to S2C2F, need to make it clear to all
    - Jay: There needs to be a bridge conversation, so we discuss what each does/doesn’t do so they work together. We could bring them out as 2 parts of an overall specification.
    - David: I propose working to create 1 slide that presents how SLSA & S2C2F work together. We’ll have to present it, let’s create it together.
    - Isaac: Agreed, maybe multiple people try to create that slide, then we compare & take the best ideas. Need a common conception/articulation on how they work together.
    - Jay: Melba created a diagram. We could overlay where SLSA sits, S2C2F sits.

    - Jay: 2 slides, figure + notes.
    - At least show SLSA & S2C2F, it'd be great to show other things too like Frsca.
    - Will try: Isaac, Melba, Jay - share in Slack within 2 weeks, discuss in a month.
- Status of s2c2f following adoption by this WG (Jay)
    - https://github.com/ossf/s2c2f
    - Had our first SIG meeting, finally got calendar fixed up so it should be correct.
    - May need to move some meetings due to holidays. Working on admin rights on m
    - We have made a few changes to the framework per some issues (brought from old repo)
    - Want to make sure repo looks proper, positioned as project under LF
    - Work done in the open
    - Come and help us! Be in meetings, comment, alleviate gaps, etc.
    - Already have a few organizations interested in adopting it.
    - Other links:
        - https://www.microsoft.com/en-us/securityengineering/opensource/osssscframeworkguide
        - https://www.microsoft.com/en-us/securityengineering/opensource
    - David: Once SLSA & S2C2F become more mature & we have a clear explanation of how they work together, I intend to update the fundamentals' course to explain their top-level concepts & point people to more.
    - Jay: Maybe have an sci.dev? One tab to SLSA, another to S2C2F.
    - S2C2F next meeting Nov 1, 3pm US Eastern Time
- Calendaring (David)
    - LF is working on improved calendar tooling - we let other foundations be the guinea pigs. Plan to slowly roll it out, making sure it works better than what we've been doing.
    - I haven't used it seriously, but I understand it has significant improvements, e.g., tracks who was at meetings automatically (e.g., so we can make sure that we have multiple organizations involved)

September 28, 2022

Attendees:

- Kim Lewandowski (Chainguard)
- Isaac Hepworth (Google)
- Jacques Chester (Shopify)
- Mike Lieberman (Kusari)
- Josh Bressers (Anchore)
- Nathan Menhorn (AMD)
- Jay White (Microsoft)
- Jeff Borek (IBM)

- Katherine Druckman (Intel)
- Chapman Pendery (Bloomberg)
- Randall T. Vásquez (Gentoo)
- Alan Miller (Bloomberg)
- Will Enck (NC State)
- Sarah Evans (Dell Technologies)
- Sebastien Awwad (Anaconda)
- Melba Lopez (IBM)
- Kim Lewandowski (Chainguard)
- Trevor Dunlap (NC State)

Agenda:

- New faces:
    - Sarah Evens from Dell
    - Alan Miller from Bloomberg
- [Sarah Evans] Where does the group fit in with the signing workstream of Mobilization Plan?
    - SLSA, FRSCA in this group
    - Sigstore as an OpenSSF project
- [Kim L] OSS SSC Framework - Do we want to adopt?
    - Call for objections
    - **No explicit objections**, group agrees to adopt SSC
    - Next stop: TAC blessing
- [Kim L] Meeting cadence
    - Should we move to monthly? Most of the work is done in subgroups.
    - Isaac: when we adopt SSC there will be a flurry of work for WG
        - Also we might want to expand scope of SLSA "Positioning" SIG to cover SSC
            - Jay: hesitant, want to ensure each has equal vigor, might be crowded with SLSA well underway and SSC still gaining momentum. But further down the line look at a single effort
            - Isaac: yes; we need to show how things map at least. This is SLSA, this is SSC, this is FRSCA. We don't have that yet.
            - Jay: yes, some sort of doc of how SLSA and SSC align and bridge together will be necessary
    - Mike: there has been some confusion on how to get engaged in supply chain. Is lack of topics because folks don't know where to start? Folks working on projects and want to demo but don't know where to go.
    - Jacques: feels like TAC responsibility to show what goes where and make clear policy of whether projects/efforts will be adopted. Less liberal than say CNCF.

    - Mike: CNCF is liberal but has a well-known lifecycle, info at the moment is unclear for folks coming to OpenSSF.
    - Decision: We'll change to monthly and we can always change back.
- [Mike L] FRSCA update
    - We have a logo!
    - Still poking at workload identity, hardware identity.
    - Will be reaching out to Jay / SSC to see how FRSCA fits or maps into that framework.

September 14, 2022

Attendees:

- Jacques Chester (Shopify)
- Shaun Lowry(ActiveState)
- Philipp Svehla (Safe Software)
- David A. Wheeler (Linux Foundation)
- Jay White (Microsoft)
- Isaac Hepworth (Google)
- Mike Lieberman (Kusari)
- Alasdair Nottingham (IBM)
- Lee Preimesberger
- Trevor Dunlap (NC State)
- Abhishek Arya (Google)
- Tom Hennen
- Nathan Menhorn (AMD)
- Wietse Z Venema (Google)
- Parth Patel (Kusari)
- Kim Lewandowski (Chainguard)
- Katherine Druckman (Intel)
- Vinod Anandan (Citi)

Agenda:

- New faces
    - Lee Preimesberger from HP
    - Deanna Medina from Honeywell
    - Philipp Svehla from Safe Software
    - Katherine Druckman from Inte
- [Jay White] and [Adrian Diglio] presentation on Open Source Software Secure Supply Chain (SSC) Framework
    - Aspirational end: becomes ISO standard (-1 developer focused, -2 consumer focused), complete in a way that's continuously improved

- First step: Contribute this to OpenSSF, work it through. Have already proposed to best practices WG. It can be home to one WG, but want multiple WGs involved in some way.
- David: LF is an ISO PAS (Publicly Available Specification) submitter - if creating an ISO standard is the eventual goal, the LF has mechanisms to make that easy to process.
- Adrian: We specifically chose the spec license to make it easy to send to ISO
- Adrian Diglio then began discussion.
- 8 different requirements, all based on specific supply chain threats. Sonatype noted 650% increase in supply chain attacks in 2021. We have links to the threats, then map the threats to requirements that mitigate the threats.
- Various levels, e.g.
    - Level 2: Need to adopt approaches to patch faster than adversaries
    - Level 3: Added mechanisms to protect themselves against dependency confusion, etc.
    - Level 4: More aspirational. Intended for OSS you deem critical.
- There's a questionnaire for developers
- There's a mapping to other specifications, e.g., SLSA
- https://github.com/microsoft/oss-ssc-framework
- David: There are some things that people would like to change, e.g., their definition of OSS. You're open to changes, yes?
    - Absolutely! We want community feedback!
- Is this applicable to organizations, or should I have a focus on a particular component/package/artifact? Or both?
    - Adrian Diglio: I imagine a future where an organization claims conformance to the framework at a particular level - some requirements are really leaning org-level, not just repo-level. E.g., disaster recovery.
- Isaac Hepworth: The title of the document seems much broader than the actual specification today. Might the title be changed, e.g., "Secure ingestion framework" or something?
    - Jay White: We're aspirational to bring it large. It starts with consumer-focus.
    - When you combine developer & consumer focus, you're complete.
    - Obviously we could change the name, but we'd like to bring them together.
- Jay White: Both SLSA & SSC can be developed in the open together. The conversations need to happen in the open.
- Isaac Hepworth: I share your excitement. It'd be good to map out the domain so we understand where each fits in. Someone could be easily confused. I don't object to bringing in SSC, but I want to make sure people understand how they work together. There's also CNCF, etc. It's incumbent on us to explain the problem domain & how these components work together to solve it.

- Jacques Chester: I like SLSA's limited/focused scope. There's room for complementary methods/controls. I'd be happy to have an allied framework to allow SLSA to be what it is, instead of trying to make SLSA be all things to all people.
- Who has contributed beyond Microsoft?
  - Some others have, many have been interested & had discussions
- Kim L: Anything that improves supply chain security is great by me. I want to make sure things are clear.
- Need to figure out how to work out SLSA/SSC relationship.
- Michael Lieberman: Need to work out "how things work together"
- David A. Wheeler: I did a mapping to the SLSA diagram of OpenSSF & non-OpenSSF activities; CRob has also tried to do some organizing.
- Jay White: Jonathan Meadows (Citi, chair end users WG) has something that might help.
- David A. Wheeler: Let's not leave Microsoft endlessly hanging. Don't need to vote TODAY, but need to decide if OpenSSF is accepting this, & if so which WG
- Jay White: We'll also present to End user WG tomorrow. Maybe this is a "bidding war"? :-)
- Abhishek: I think SSC would be better in this WG, that'll help align SLSA & SSC together. We're very excited about SSC.
- Adrian Diglio: I lead the Microsoft Supply Chain Team. We ID the scenarios, then work with various partners to scope out the parts.
- Michael L: That's a concern for OpenSSF as well - how do we best self-organize?
- Jay White: The sooner we get SSC into OpenSSF, the faster we can resolve how they work together.
- <Most people seemed to be very positive about SSC.>

August 31, 2022

Meeting canceled due to no agenda topics

August 17, 2022

*Please add your **agenda item**, **name** and **approximate time** allocation to the bottom of the list. Thanks!

Attendees:

- Kim Lewandowski (Chainguard)
- Jacques Chester (Shopify)
- Melba Lopez (IBM)
- Chapman Pendery (Bloomberg)

- Christine Abernathy (F5)
- Laura Seay (Red Hat)
- Trevor Dunlap (NC State)
- Sebastian Crane
- Matt Rutkowski (IBM)
- John Speed Meyers (Chainguard)
- Mike Lieberman (Kusari)
- Parth Patel (Kusari)
- Isaac Hepworth (Google)
- Jeff Borek (IBM)
- Randall T. Vasquez (Gentoo/Homebrew)
- Aaron Bacchi (Verizon)
- Piergiorgio Ladisa (SAP Security Research)

Agenda and Notes:

- RubyGems requires MFA!! Announcement
- OpenSSF Open Source Software Compromises Dataset [John Speed Meyers, 5-10 minutes]
    - Intend to begin the construction of a prospective dataset of open source software compromises
    - Based on this design document: jointly authored by myself, Brandon Lum, Jose Miguel Parrella, Piergiorgio Ladisa, and Abhishek Arya. Feedback and constructive critique welcome.
    - Began because of this GitHub issue
    - Feedback and ideas welcome.
- [Mike Lieberman, 10 minutes] - SLSA updates
    - 1.0 specification, positioning, tooling, adoption meetings
    - Requesting additional feedback on E2E Supply Chain Security "visualization" with regards to Supply Chain Integrity: https://openssf.slack.com/files/U035YK22V1U/F03R0EATU13/end-to-end_supply_chain_security_framework.pdf
    - https://docs.google.com/document/d/1L1gEJMBIvE0IbpFi23FOUByDYlItSYPPJmKdhvJQYsg/edit
- [Parth Patel, 30 minutes] - FRSCA demo and updates
    - SPIFFE/Spire
    - Runtime visibility
    - https://github.com/buildsec/frsca

August 3, 2022

Meeting canceled due to no agenda topics

July 20, 2022

Attendees:

- Kim Lewandowski (Chainguard)
- Mike Lieberman (Kusari)
- Melba Lopez (IBM)
- Brian Behlendorf (OpenSSF/LF)
- Adolfo García Veytia (Chainguard)
- Alasdair Nottingham (IBM)
- Brandon Lum (Google)
- Matt Rutkowski (IBM)
- Chapman Pendery (Bloomberg)
- Sebastien Awwad (Anaconda)
- Josh Bressers (Anchore)
- Hector Fernandez (VMware)
- Vinod Anandan (Citi)

Agenda:

- Mike Lieberman (Kusari) Frsca Updates
    - Looking for help on runtime visibility
    - Looking to back signing with hardware using tools like Sigstore, PARSEC, Spire, and Vault
    - https://github.com/buildsec/frsca
    - OpenSSF Calendar has info. Every other Wednesday at 10AM Eastern
        - #frsca channel in slack
    - Looking for contributors. Particularly looking at:
        - Runtime visibility
            - Looking at Tetragon, Tracee, Falco, others.
        - Confidential computing/Hardware root of trust
            - Looking at PARSEC
            - Looking at confidential containers
- Adolfo García Veytia preso on VEX
- Feel free to add any questions or comments Josh can bring back to the CISA VEX crew below
- Matt referenced that OWASP is defining an SBOM “Maturity model” and information taxonomy; see https://owasp.org/www-project-software-component-verification-standard/
-

07/06/2022

Attendees:

Agenda:

- Open Source Summit Updates
- Mike Lieberman (Kusari) SLSA Updates

06/08/2022

Agenda:

- [no items. meeting canceled]

05/25/2022

Attendees:

- Kim Lewandowski (Chainguard)
- Jason Hall (Chainguard)
- Bob Martin (MITRE)
- Eric Smalling (Snyk)
- Mike Lieberman (TBD)
- Arnaud J Le Hors (IBM)
- Alasdair Nottingham (IBM)
- Jacques Chester (Shopify)
- John Speed Meyers (Chainguard)
- Simon Kent (Google)
- Jon Meadows (Citi)
- Josh Bressers (Anchore)
- Gavin McNay (Bloomberg)
- Brandon Lum (Google)
- Matt Rutkowski (IBM)
- Wietse Z Venema (Google)
- Luis Saiz (BBVA)
- Jon Velando (Individual Contributor)
- Yehuda (Checkmarx)
- Matthias Weckbecker (Red Hat)
- Aaron Bacchi (Verizon)
- Jeffrey Borek (IBM)

- Mehdi Entezari (Unisys and Digital Bill of Materials (DBoM) project)
- Nico Thirion (Optum)
- Isaac Hepworth (Google)
- Camille Sarder (Bloomberg)
- Eric Tice (Wipro)
- Vinod Anandan (Citi)
- Jan Zerebecki

Agenda:

- Is it ok to move the threat model into the repo to polish it? Can this be merged?: Add attacker capabilities to threat model https://github.com/ossf/wg-supply-chain-integrity/pull/50/files (please ask these questions in my absence)
    - https://arxiv.org/abs/2204.04008 - Piergiorgio Ladisa et al paper
    - Let's figure out where this should live!
- SLSA(-inspired) Survey (https://forms.gle/5n8FfUU5fxpsJi269): Seeking constructive feedback and joint participation from organizations or individuals that want to jointly run the survey and present results (John Speed Meyers, jsmeyers@chainguard.dev)
    - Will describe motivation, mention questions, and proposed whitepaper
    - John Speed is looking for feedback and collaborators
    - Hoping to send out mid-June or July, keep it open for a month
    - Collect data, make it open (not the PII), turn into a whitepaper
    - Happy for this to be an OpenSSF effort or cross org
- Mike Lieberman (TBD) - Discuss WG scope - https://docs.google.com/document/d/1OJFlUV3jdhQ0aEgmkMx4J5cfSyViRHisOPQwr_6tf-M/edit
    - [Josh] TAC is working on something for wg structure etc but it's not ready yet
        - (notes from Josh): Not exactly. The TAC is going to defer to the working groups to determine their own purpose and structure. What a WG wants to consider in scope is up to the working group. The TAC will only weigh in when necessary (hopefully that never happens)
        - The TAC is putting effort into better understanding how and when to accept project donations. This is partially documented here https://github.com/ossf/tac/issues/78 and will be a future TAC meeting topic

04/27/2022

Attendees:

-
- Jacques Chester (Shopify)
- Jason Swank(Sonatype / Maven Central)

- Abhishek Arya (Google)
- Simon Kent (Google)
- Brad Beck (Citi)
- Christine Abernathy(F5)
- Patricia Tarro (Dell)
- Arnaud J Le Hors (IBM)
- Tim Miller
- Matt Rutkowski (IBM)
- Marcela Melara (Intel Labs)
- Jon Velando (Individual Contributor - Conda-Forge)
- David A. Wheeler (Linux Foundation)
- Michael Peters (Red Hat)
- Yehuda Gelb (Checkmarx)
- Yotam Perkal (Rezilion)
- Michael Winser (michaelwinser@google.com)
- Mike Lieberman (TBD)
- Bill Bensing (Red Hat - wbensing@redhat.com)
- Alasdair Nottingham (IBM)

Agenda:

- (April 27) Ploigos Ecosystem - Automated Governance (Bill Bensing - Red Hat)
    - Slides -> https://www.slideshare.net/BillBensing1/ploigos-how-it-works-and-whypdf
    - Demonstrate the automated governance feature of the upstream.
    - Would like to assess the community's thoughts on this as an OpenSSF Project.
    - Learn more on this 43 min video
    - Want to cover the technical details on this call.
    - Focuses on "SOLID"
        - S - Single Responsibility
        - O - Open-Closed Principle
        - L - Liskov Substitution
        - I - Interface Segregation
        - D - Dependency Inversion
    - Ploigos step runner: It's not like Tekton. It needs a CI tool (GitHub actions, Jenkins, etc.) to run it. It extends the underlying runner. It can unit test the logic (for example)
    - Problem: two different auditors might give different response
    - Instead, serializes process/results, signs it with sigstore rekor separately from its results, so that you have separate evidence that it was generated from this approach.
    - The evidence isn't stored in rekor, it's stored separately.
    - Serialized Material is key to externalized policy

    - David: (to be question): Can you talk about its potential relationship to Pyrsia, SLSA, Secure Software Factory, reproducible builds?
        - Not familiar with Pyrsia
            - https://github.com/pyrsia/pyrsia - “Zero-Trust Decentralized Package Network”
        - SLSA: Needs evidence. Ploigos lets you collect the evidence to show that you meet certain SLSA requirements. E.g., validate that you have 2 people. Ploigos lets
        - This can power secure software factory - that uses Tekton. Ploigos can work even when you aren’t using tekton
        - Reproducible builds: separates the RESULTS from the evidence of process. The results should reproduce, the evidence of running a specific process won’t reproduce (different time/datestamps) instead it provides evidence that process ran multiple times. Capture the config file with the what ploigos was running.
    - Jacques: I’d call this repeatable not reproducible, it’s not bit-for-bit reproducible
    -
- [Kim - May 11] Adopt WG charter template (10 min)
    - Jacques will open PR
        - Maintainers: > 3 attendances
    - Mike voluntold to work on scope/antigoals

03/30/2022

Attendees:

- Jacques Chester (Shopify)
- David A. Wheeler (Linux Foundation)
- Kim Lewandowski (Chainguard)
- Arlen Baker (Wind River)
- VM Brasseur (Wipro)
- Christine Abernathy (F5)
- Mark Lodato (Google)
- Jason Swank (Sonatype)
- Mike Lieberman (Citi)
- Nathan Menhorn (AMD)
- Yehuda Gelb (Checkmarx)
- Steve Lasker (Microsoft)
- Alasdair Nottingham (IBM)
- Brad Beck (Citi)

- Michael Komraz (Snyk)

Agenda

- New faces
    - Patricia Tarro - Dell. Dependency mgmt PM.
    - Christine Abernathy - F5. OSPO.
    - Jason Swank - Sonatype. Maven Central.
- Harden-Runner - security agent for GitHub hosted runner (Varun Sharma - StepSecurity)
    - Demo
    - Assess community's thoughts on donating project to OSSF

2022-03-16

Attendees:

- Kim Lewandowski (Chainguard)
- Zach Steindler (GitHub)
- Jacques Chester (Shopify)
- Jason Swank (Sonatype)
- Brandon Lum (Google)
- Dan Lorenc (Chainguard)
- Mike Lieberman (Citi)
- Amith K K (Unisys)
- Steve Lasker (Microsoft)
- Bob Martin (MITRE)
- Tracy Miranda (Chainguard)
- Jossef Harush (Checkmarx)
- Debashis Das (AWS)
- Matt Rutkowski (IBM)
- Sebastian Crane
- Andrew Martin (ControlPlane)
- Batuhan Apaydın
- Marta Rybczynska (OSTC)
- Yehuda Gelb (Checkmarx)
- Srikrishna Paparaju (Red Hat)
- Yotam Perkal (Rezilion)
- Mark Lodato (Google)
- Wietse Venema (Google)
- Nathan Menhorn (AMD)

- Hemil Kadakia (Yahoo)
- Bob Callaway (Google)
- Brian Russell (Google)
- Michael Winser (Google)

Agenda:

- Signing formats (continued) - comments inserted into document
- Supply Chain Catalog from CNCF (Brandon) - discussion issue here
    - It turns out that there are several such collections.
    - CNCF;s https://github.com/cncf/tag-security/tree/main/supply-chain-security/compromises
    - Backstabber's knife collection: https://drive.google.com/file/d/1Iz8ZhigIVOsX5DJDy35--4nCZXWUGoaq/view
    - In-Q-Tel: https://github.com/IQTLabs/software-supply-chain-compromises/blob/master/software_supply_chain_attacks.csv
    - Checkmarx would also be willing to contribute & would like to have a merged set
    - Many seemed to agree that it'd be really useful to have a merged database of all past software supply chain attacks, to enable future research, trend analysis, show what attackers are doing (and not currently doing), prove that this is real, etc. We could start with these existing datasets & work on merging them
- Next steps on SSF (naming) (Dan/Michael)

2022-03-02

Attendees (40) (please add yourselves):

- VM Brasseur - Wipro
- Michael Winser - Google
- Bill Bensing - Red Hat
- Ian McMillan - Microsoft
- Michael Peters - Red Hat
- Joshua Mulliken - Red Hat
- Brian Krell - Microsoft
- Nathan Menhorn - AMD
- Steve Lasker - Microsoft
- Jim Flanagan - AWS
- Yehuda Gelb - Checkmarx
- Debashis Das - AWS

- Asaf Karas - JFrog
- Ryan Haning - Microsoft
- Arlen Baker - Wind River
- Kay Williams - MIcrosoft

Agenda:

- Discuss Supply Chain Artifact Signing Envelope Format Comparison - Google Docs
    - This document originated as a Microsoft evaluation of signing envelope formats in preparation for signing SBOMs and other EO 14028 Attestations of Conformance. We've generalized the content, and are sharing with others for feedback and community discussion.

2022-02-16

Attendees (40) (please add yourselves):

- Dan Lorenc - Chainguard
- Kim Lewandowski - Chainguard
- Mike Lieberman (Citi)
- Jonathan Meadows (Citi)
- Jacques Chester (Shopify)
- Mikhail Swift (TestifySec)
- Josh Bressers (Anchore)
- Josh Mulliken (Red Hat)
- Bill Bensing (Red Hat)
- VM (Vicky) Brasseur (Wipro, she/her)
- Sebastian Crane
- Tracy Miranda (Chainguard)
- Arlen Baker (Wind River)
- Brad Beck (Citi)
- Bob Callaway (Google)
- Brandon Lum (Google)
- Brian Russell (Google)
- Bob Martin (MITRE)
- Michael Komraz (Snyk)
- John Naulty (Coinbase)
- Matt Rutkowski (IBM)
- Konstantin Ryabitsev (Linux Foundation)
- Kay Williams (Microsoft)

- Brian Behlendorf (OpenSSF / LF)
- Aeva Black (Microsoft)
- David A. Wheeler (Linux Foundation)
- Vinod Anandan (Citi)
- Yotam Perkal (Rezilion)
- Marcela Melara (Intel Labs)

Agenda:

- New README.MD
    - This is done and merged! Thanks Kay!
- Witness Presentation/Q&A - (TestifySec) - We would like to demo our modular, open source, attestation framework that implements in-toto current spec and proposed ITE-5, ITE-6, ITE-7 (~30min+Q/A)
- Michael Lieberman - SSF (Secure Software Factory)
    - Intention to contribute SSF as an implementation of SLSA to this Working Group as discussed last meeting
    - Can reach SLSA level 2 today, is close to SLSA 3 when and if spiffe/spire work gets merged upstream (outside 2 person review/social aspects)
    - Some examples of getting closer to SLSA 4 with specific tooling like bazel and nix
    - *Decision to adopt*
        - Lots of +1s in zoom chat
        - No objections
        - **Accepted !**
    - Name brainstorming next step
        - Naming the "Secure Software Factory"
- Sig v2 Intro+Discussion
    -

2022-02-02

Canceled

2022-01-19

Attendees (please add yourselves):

- Bob Martin (MITRE)
- David A. Wheeler (Linux Foundation)
- Nathan Smith

- Georg Kunz (Ericsson)
- Mike Lieberman (Citi)
- Sergio Rojas (Different Dimension)
- Nathan Menhorn (Xilinx, Inc.)
- Brad Beck (Citi)
- Josh Bressers (Anchore)
- Rémy Greinhofer (Citi)
- Marta Rybczynska (OSTC)
- Arlen Baker (Wind River)
- Bob Callaway (Google)
- Michael Peters (Red Hat)
- Wietse Z Venema (Google)
- Steve Lasker (Microsoft)
- Jacques Chester (Shopify)
- John Speed Meyers (Chainguard)
- Arnaud J Le Hors (IBM)
- Adolfo García Veytia (Chainguard)
- Tom Bedford (Bloomberg)
- Brian Russell (Google)
- Michael Komraz (Snyk)
- Santiago Torres-Arias (Purdue University)
- Kim Lewandowski (Chainguard)

Agenda:

- [30 min] Secure Software Factory/Reference Architecture presentation, Michael Lieberman, from CNCF Security Working Group (https://github.com/thesecuresoftwarefactory/ssf)
    - Showed demo with Tekton chains
    - Slides https://docs.google.com/document/d/1FwyOIDramwCnivuvUxrMmHmCr02ARoA3jw76o1mGfGQ/edit
    - cue is a configuration language looks like JSON+stuff, lets us easily add added functionality, can output to yaml, from some of the developers of Borg
    - GitHub actions works well for smaller tasks, but as workflows get bit need something else
    - Key abilities: Ability to define security policies at multiple levels (where each complies with the broader level), validating versions of tools (valid version of Tekton, etc.), making the secure software factory eventually pluggable (eventually!), using cue to configure things makes it easier - “while deploying Tekton, ensuring Tekton policies are linked (in)”
    - Intend to announce this more widely after a little while

- Review - Updated README.md
    - Supply Chain Integrity WG - Google Docs

2022-01-05

Attendees (please add yourselves):

- Kim Lewandowski (Chainguard)
- David A. Wheeler (Linux Foundation)
- Josh Bressers (Anchore)
- Alex Goodman (Anchore)
- Brian Russell (Google)
- Michael Winser (Google)
- Nathan Menhorn (Xilinx)
- Gavin Hindman (Intel)
- Santiago Torres-Arias (Purdue University)
- Steve Lasker (Microsoft)
- Mike Lieberman (Citi)
- Kay Williams (Microsoft)
- Bob Martin (MITRE)
- Debashis Das
- Medhi Entezari (Unisys)
- Henk Birkholz (Fraunhofer SIT)
- Arnaud J Le Hors (IBM)
- Santiago Torres Arias (Purdue)
- Moshe Zioni (Apiiro)
- Ryan Haning (Microsoft)
- Marta Rybczynska
- Roy Williams (Microsoft)
- Ria Schalnat (HPE)
- Ian McMillan (Microsoft)
- Michael (Miki) Komraz (Snyk)
- Mark Ryland (AWS)
- Laurent Simon (Google)
- Tom Bedford (Bloomberg LP)

Agenda:

- Update WG README.MD (including vision, scope) (Kay Williams)
    - Create an initial draft (Kay?)
    - Share with mailing list for discussion (or create a PR?) (Kay)

    - Discuss at next next meeting (all)
- Syft demo - SBOM generation ask from the last meeting (Alex Goodman from Anchore)
    - https://github.com/anchore/syft (Apache 2.0 license)
    - Analyzes containers & filesystems to generate SBOMs in SPDX & CycloneDX & its own format.
    - It creates probable CPE names as “best guesses”, Directly supports Grype (vulnerability matcher). Might be better to have *separate* process for CPE guessing.
    - David A. Wheeler: The OpenSSF Best Practices badge uses repo URLs and home page URLs to identify packages; we *record* CPEs when available, but URLs are much better for identification. SWIDs don’t work for this use case; they’re based on hashes, & can’t work in this case because since a recompile often causes it to fail (no longer match when it should)
    - David A. Wheeler: I’ve been trying get NVD to add home page URL, repo URL, maybe pURLs - many packages don’t have CPEs, but SWIDs can’t work in this use case. I have proposed version ranges for pURL.
- Josh: PURL has a proposal for version ranges https://github.com/package-url/purl-spec/pull/139
    - Moshe:
        - PCE/pURL/SWID are not tackling the dependency-inheritance issue.
        - Security Content Automation Protocol (SCAP) is an interesting effort by NIST to stitch together many formats and processes in a consistent and processable manner - https://csrc.nist.gov/projects/security-content-automation-protocol/
- Supply chain artifact signing (Kay Williams)
    - Context:
        - Microsoft and industry partners have been contemplating approaches to signing digital artifacts including SBOMs, containers, Digital Media metadata, IoT artifacts, etc. We would like to sync with others in this WG to see if there is interest in collaborating on an overall approach for digital artifact signing. In particular, we have a near term need to establish an approach for signing SBOMs, containers, and C2PA artifacts.
    - Goal: Supply chain participants across the industry can validate the authenticity and integrity of digital artifacts
        - Digital artifacts: code, packages, containers, attestations (including SBOMs), and policy
        - Authenticity: was the artifact provided by the expected entity?
        - Integrity: was the artifact altered between the time it was provided and the time it was received?
    - Problem: Multiplicity of signing formats impedes validation of authenticity and integrity
        - Producers and consumers must provide/validate artifacts in an array of formats.

    - Goal for this WG:
        - Develop recommendations to facilitate authenticity and integrity validation
        - Solutions might include one or more of the following:
            - Agreeing on a standard format for signing digital artifacts
            - Creating tooling to assist with signing and validation artifacts across a variety of formats
    - Next Steps?
        - Establish a subgroup for discussion (Kay/Ian)
        - Subgroup to create proposal outlining requirements, alternatives
        - Subgroup to bring proposal back to full WG for discussion
    - Santiago: Updated WG README might help capture
    - Michael: I'd rather this group be an authoritative voice to develop the answer, e.g., where the government can come to. Can't create results overnight.
    - (General agreement, create a subgroup to work this.)
    - Wheeler: Probably should first create a quick summary / links to existing formats (clearly document existing space, e.g., GPG), make sure it's clear what the problem is, make sure we understand how existing projects (esp. sigstore) connects
- New meeting time to accommodate new members (due to WG scope change) (Kay Williams)
    - Check the OpenSSF calendar for possible times that don't conflict with existing meetings?
    - Send a poll to the mailing list?

2021-12-08 Attendees (please add yourselves):

- Kim Lewandowski (Chainguard)
- Josh Bressers (Anchore)
- Abhishek Arya (Google)
- David A. Wheeler (Linux Foundation)
- Michael Winser (Google)
- Jeffrey Borek (IBM)
- Jacques Chester (Shopify)
- Adolfo García Veytia (Mattermost)
- Ashley Ellis Pierce (Shopify)
- Betty Li (Shopify)
- Walt Della (Teleport)
- Mike Lieberman (Citi, CNCF Supply Chain WG)
- Jenny Shen (Shopify)
- Swati Sharma(Amazon)

- Ryan Haning (Microsoft)
- Georg Kunz (Ericsson)
- axel simon (Red Hat)
- Marcela Melara (Intel Labs)
- Michael Komraz (Snyk)
- Steve Lasker (Microsoft)
- Matt Suozzo (Google)
- Matt Rutkowski (IBM), he/him. CST
- Ian McMillan (Microsoft)
- kpcyrd (Arch Linux, Reproducible Builds, Debian)
- Joshua Lucas (Citi)
- Moshe Zioni (Apiiro)
- Henrik Plate (SAP)
- Marc Ohm (University of Bonn)

Regrets:

- Mark Lodato (Google) - On-call shift so I won't be able to attend. I'll catch up on the video.

Agenda:

- [kpcyrd] reproducible builds
- [Marc and Henrik] Proposed: Presentation from "Backstabber's Knife Collection" researchers
    - Paper
    - Another related paper
    - https://github.com/crev-dev/cargo-crev
    - Long discussion on what could be done to address the problems they've identified
        - Verified reproducible builds
        - Disabling "run on install" by default
            - Some specific actions could be allowed if they're known-safe, to make this practical.
        - Making the secure way the easy way
        - Convincing people to stop doing installs with "curl http://some_thing | sh"
            - Companies could say "I won't use it then"
            - However, that probably won't affect behavior
            - Nix tools sandbox it all, so none of those things should affect parent environment
        - Jacques: This paper has been very influential at Shopify, thank you.
            - Repos have a centralizing position, so you don't need a denylist... you can just remove the package.
            - E.g., kix npm package.

            - Wielding that central authority is often something to be avoided much of the time, though. Needs to be confident that the result is correct.
        - Discussion of centralization vs. decentralization
            - I wouldn't want to be in a situation where someone can remove a package & take down my system""
            - There are vendors who provide repos
- [Adolfo] Revisiting SHAs in SLSA materials (follow up on slsa#214)
- "We should discuss more about SBOM generation, e.g., Syft, etc." - maybe we should have an SBOM generation tool here

2021-11-10

Attendees:

- Kim Lewandowski (Chainguard)
    - kim@chainguard.dev
- Kay Williams (Microsoft)
- Josh Bressers (Anchore)
- Matthew Wood (Intel)
- Abhishek Arya (Google)
- Mark Lodato (Google)
- Gavin Hindman (Intel)
- Adolfo Garcia (Mattermost)
- Ryan Haning (Microsoft)
- Michael Peters (Red Hat)
- Matt Rutkowski (IBM), he/him, CDT
- Marcela Melara (Intel Labs)

Agenda:

- Rename WG from Digital Identity to Supply Chain Integrity (Kim/Kay)
    - Most in WG are supportive
    - TAC is supportive (see previous TAC meeting)
    - DECISION: We will rename! New name "Supply Chain Integrity WG".
- Move the biweekly meeting earlier by 1 hour (8 AM Pacific)? (Kay)
- Adolfo García Veytia present on SBOM generation tool for Kubernetes
    - Built a tool to produce SBOMs (in SPDX format) for Kubernetes (k8s)
    - URL of tool:
        - https://github.com/kubernetes/release/tree/master/cmd/bom
        - Eventually it may split out, but that's where it is for now
    - Input formats it can handle:

    - Kay: Would this be better in OpenSSF or SPDX projects? I can see it'd be useful to have more general SBOM tooling in OpenSSF. Microsoft has some tools internally, too. There's also a dependency tree generator that's been used. Perhaps this WG is a good place to put SBOM generators, etc.
    - Adolpho: We've been in talks with LF SDPX teams. They already have an SBOM generator, looking for community maintenance. Perhaps the two projects could be fused. E.g., we only handle go. They have support for other languages. They were also concerned about creating an "official" SPDX tool, because that could be seen as the single tool & interfere with the development of other tools. One suggestion was to move it to OpenSSF. (ACT tooling as well.)
    - Overall issue: Where do SBOM tools go? Currently lots of people are working on them.
    - We want people to have a BOM, and we want that to be easy.
    - Abhishek: We also don't want to reinvent the wheel.
    - Matt R: We should have tools do better than minimum.
    - Kim: Also, where are the BOMs stored? Exchanged? How are they supposed to be consumed?
    - https://github.com/awesomeSBOM/awesome-sbom has list of tools
    - https://docs.google.com/document/d/1KT5QPCgVx_8UFIKv8-0k9GYjfcL3uvHmK4COOEGq_UQ/edit# - Aeva Black, "An Analysis of the SSC Landscape"
    - David to figure out location/home for SBOM tools, should they live in ACT or in OpenSSF. And in OpenSSF, it is easy to develop in a community (Josh).

2021-10-27

Attendees:

- Kim Lewandowski (Chainguard)
- Kay Williams (Microsoft)
- Neal McBurnett
- Kengo Suzuki
- Mark Lodato (Google)
- Sergio Rojas
- David A. Wheeler (Linux Foundation)
- Jeff Billimek (The Home Depot)
- Santiago Torres Arias (Purdue)

Agenda

- Discuss budget requests for 2022
    - Sigstore (proposed transfer to OpenSSF?)
    - Looking to approve budget for 2022

    - Preliminary budget review for Nov 5
    - SLSA
        - Swag?
    - Reproducible Builds - this is a good thing to do no matter what, helping projects do that is a good thing, helps to support SLSA
        - Make reproducible builds default in various ecosystems. E.g., Python isn't by default because its zip files include timestamps (among other issues?).
        - E.g., top N packages within various ecosystems (language-level; many Linux distros have managed to do a lot)
        - Related: https://discuss.python.org/t/introducing-asaman-a-tool-to-bulid-reproducible-wheels/10932
        - $100K to fix defaults, $100K to fix top N packages, $200K total? (rough estimates)
        - Kim to ping Chris Lamb to come chat again
        - We may want to include others from r-b project Holger Levsen, Kpcyrd (suggestion from Santiago)
    - New projects (assume 3?)
        - Website development
        - Swag
        - Potential future projects include:
            - SCIM - Supply Chain Integrity Model
                - microsoft/scim: Supply Chain Integrity Model (github.com)
            - Gluecose - Test suites and libraries for COSE signing -
                - gluecose (github.com)
                - Firmware transparency (Microsoft is looking at signing SBOMs, etc.) - COSE is being defined by IETF

- SLSA updates
    - Operation slsa video
    - Kubecon talks! Transparent compromise-resilience (in-toto + TUF + sigstore)
    - Website improvements doc
    - Site translation to Japanese issue
    - Improved threats and mitigations documentation #92
        - Backstabbers knife paper
        - CNCF tag-security list
        - Wikipedia edits
- Discuss re-scoping / renaming group to Supply Chain Integrity
    - Discussed in TAC on Oct 5

- ATT&CK-like matrix for CI/CD Pipelines - Kengo Suzuki discussed, heard presentation about this
    - There was a talk, recording not yet available (hopefully will be soon)
    - https://github.com/rung/threat-matrix-cicd
    - https://speakerdeck.com/rung/cd-pipeline

2021-09-14

Attendees:

- Kim Lewandowski (Google)
- Jeff Billimek (The Home Depot)
- Edoardo Tenani
- Casey Silver (Palantir)
- John Naulty (Coinbase)

Agenda

- [David] quick preso on yubikeys! / Multi-factor authentication (MFA) token use
    - David: I have to leave in a few minutes, I'm giving a presentation at a NIST workshop
    - Hot off the press: OpenSSF has been offered a large number of Yubikeys to distribute to OSS developers
    - We need to work out:
        - Who to distribute keys to
        - How to distribute (we need to give them confidence they're not subverted!)
        - EASY to apply guidelines/tutorials/best practices for using them in common uses for OSS. E.g., ((commit to GitHub|GitLab|?)|(release package on repo)) using my platform (Ubuntu|Fedora|MacOS|Windows)
    - Propose working this as a task within the best practices WG & using its mailing list [is that unreasonable?]], but we really need to coordinate with:
        - the Digital Identity Attestation WG (hi!) [to ensure we get confidence] AND
        - Critical projects WG (ID some projects we really want to use tokens)
    - Suggestions on how to take next steps?
        - Maybe create a Google doc for a plan, assign parts, start executing
        - https://docs.google.com/document/d/1Hhg4KcLCzEdd9ZcbdEviN0TIUTLyWDsIdF6B_hY3Xv0/edit
    - Let me know if you're interested, dwheeler@linuxfoundation.org
    - There is also a slack channel in OpenSSF Slack: https://openssf.slack.com/archives/C02EX4CE6KB
- [Matt] cosign keyless signing demo!
    - sigstore.dev

2021-08-18

Agenda

- SLSA bi-weekly meeting on OpenSSF calendar
    - Every other Wednesday at 9-10am Pacific (invitation).
    - ~~Video Call: meet.google.com/cfp-ywbh-cxz~~
- Update on the update framework in SigStore
    - TUF community meeting info: https://hackmd.io/jdAk9rmPSpOYUdstbIvbjw

Attendees:

- Kim Lewandowski (Google)
- Asra Ali (Google)
- Dan Lorenc (Google)
- Mike Malone (smallstep)
- Jacques Chester (Shopify)
- Kengo Suzuki (LayerX)
- Casey Silver (Palantir)
- Peter Wells (IF)

2021-07-21

Agenda

- New SLSA site preview: send feedback to peter@projectsbyif.com
    - ProjectsbyIF
    - sigstore discovery (which provided insights on audience)
    - New SLSA staging site (NB: content is still changing)
    - Research panel form
    - Current SLSA site: slsa.dev
    - Main SLSA git repo (for GH Issues): github.com/slsa-framework/slsa
        - Staging site is currently in a fork; will be merged soon
    - Any feedback on non-requirements related content on the staging site can be sent to peter@projectsbyif.com

Attendees:

- Kim Lewandowski (Google)
- Matt Rutkowski (IBM)
- Peter Wells (IF)

2021-07-07

Agenda

- [Appu Goundan] Maven Wrapper Validation.

2021-06-23

Attendees:

- Kim Lewandowski (Google)
- Matt Rutkowski (IBM)
- Mike Malone (smallstep)
- Peter Wells (IF)
- David A. Wheeler (Linux Foundation)
- Michael Peters (Red Hat)
- Matt Rutkowski (IBM)

Agenda

- [David A. Wheeler] Best Practices WG is creating document “Existing Guidelines for Developing and Distributing Secure Software” - please add what's missing!: https://docs.google.com/document/d/11bRB-Q_j9sj19EEC32-ijMiEHERPRwZRVWE9HwNr2pc/edit#heading=h.gxoel3nswm76
- [Mark Lodato] Update on SLSA
    - Many changes have been made
    - Recommend using Dead Simple Signing (DSSE), part of in-toto
    - As always, looking for feedback & contributions
    - Next step: SLSA 2 demo
    - Not yet determined: How does one show SLSA compliance? Self-attestation?
        - There are things that could be checked automatically at 1,2,4. Some aren’t easily checked unless there was some trusted computing thing (hardware attestation), that’d be a long-term.
        - David W: My experience with Common Criteria is that efforts that require a long time & lot of money won’t scale to the millions of OSS projects used today.
    - How to send comments? GitHub issues preferred, though there is a Google Group if you’d prefer to do that.
- David A Wheeler: I have a somewhat similar diagram that you might want to look at: https://docs.google.com/presentation/d/1sxJUO1Ap6NxpU8B4iHKzRxaIIQwB_dZ7lLK9G5dGuls/edit#slide=id.gcee7a21866_0_33

2021-06-08

Attendees:

- Kim Lewandowski (Google)
- Dan Lorenc (Google)
- Asra Ali (Google)
- Mike Malone (smallstep)
- Aditya Mahendrakar (Verizon Media)
- Muhammad Usama Sardar (TU Dresden)
- Edoardo Tenani

Agenda:

- [Asra] TUF and cosign integration demo https://docs.google.com/presentation/d/1Z2BLctUE57CX-B-av5p8R2DCOrgbAUN5Nb67Fv4w850/edit#slide=id.p

2021-05-12

Attendees:

- Kim Lewandowski (Google)
- Ryan Haning
- Konstantin Ryabitsev
- Mike Malone
- Matthew Wood
- Gavin Hindman(Intel)
- Vinod Anandan (Citi)
- Mark Lodato (Google)

Agenda:

- Patch attestation proposal [Konstantin]
    - Slides
    - GH: Is there a mailing-list configuration bkm for not mangling DKIM that we should capture for best-practices?

2021-04-14

Attendees:

- Gavin Hindman (Intel)

- David A. Wheeler (Linux Foundation), dwheeler@linuxfoundation.org
- Kim Lewandowski (Google)
- Mark Lodato (Google)
- Luis Villa (Tidelift, @luis_in_brief on Twitter, @tieguy on GitHub)
- Ryan Haning (Microsoft)
- Mike Malone (smallstep)
- John Warren (Verizon Media)
- Vinod Anandan (Citi)
- Matt Rutkowski (IBM)
- Andrew Lytvynov (Teleport)
- axel simon (Red Hat)

Agenda:

- Interesting survey about signing: “The state of package signing across package managers” by Tieg Zaharia, June 11, 2020, https://blog.tidelift.com/the-state-of-package-signing-across-package-managers
    - E.g., for some package managers there’s an API to determine whether or not there is 2FA. If there’s no API, we just have to take people’s word for it (not great)
    - ?: Maven/Java has signatures, but it’s hard to do, so it typically doesn’t happen. This report makes things seem rosier than it really is.
    - “The gap between what’s done & what’s possible is very large”
- WG goals/targets open discussion - Gavin
    - We had previously identified areas in the supply chain where Identity is relevant and some threat models where do we want to proceed from there?
    - Potential (non-exhaustive) Options:
        - Identify tool-agnostic minimum best-practices for each stage (the kinds of thing, not specific solutions)
            - Add to badging/scorecard projects?
                - CII Best Practices badge already has a signed release requirement at “Silver” - not at “passing” level because of its challenges - see https://bestpractices.coreinfrastructure.org/en/criteria/1?details=true&rationale=true#1.signed_releases
                    - It would be great if there was a paper that said “here’s recommended practices on how you do it” that others could point to (that paper could point to others)
                    - Recommended tools should be public OSS projects under neutral governance.
            - Whitepapers?

        - What's the relationship between this WG and SLSA? Is this the right WG for SLSA?
        - Recommended practices, perhaps including tools for each stage
            - Example identity tool chains?
            - Badging?
            - Whitepapers?
        - David A. Wheeler: No matter what, when writing criteria (requirements), it's good to:
            - Write higher-level criteria that aren't locked to specific tools
            - Provide rationales for each (WHY is that requirement there)
            - Provide guidance (suggestions on how to implement it for common cases.
        - For either/both, what recent/prominent supply-chain attacks might have been prevented? Solar Winds? PHP? Etc.
        - Others?
    - Note: per the README, we do not require revelation of real names. We also don't want to *require* revelation of other sensitive information (location).
    - Stephen Lauck: There's really no way around the problem that there's NO articulated policy of "what you're using" in Dockerfiles, etc. People are asking for transitive trust, but there's no way to get that information. There needs to be a way to declare what you use. Transitive closure is hard
    - How much overlap between projects/efforts is okay?
    - We could investigate how many SLSA requirements can be transitioned to the CII Best Practices badge. It might not be all of them, but it might be helpful

2021-03-31

Attendees:

- Kim Lewandowski (Google)
- Gavin Hindman (Intel)
- Sam White (GitLab)
- David A. Wheeler (Linux Foundation)
- Edoardo Tenani (Arduino)
- Matt Rutkowski (IBM)

Agenda:

- Note: Dave Huseby has begun work on git so that it can interact with other signing mechanisms (we've previously had discussions about this). The work will create a generic mechanism & then implement OpenSSH signing as a useful example
    - https://www.youtube.com/watch?v=L01E2yLQIBQ&t=16s
- SLSA - Kim Lewandowski 03-31 (pronounced "salsa")
    - "Supply-Chain Levels for Software Artifacts"
    - Slides are here: https://github.com/slsa-framework/slsa/blob/main/presentations/Intruducing_SLSA.pdf
    - David W: I suggest adding a 2.5 (no two-person, since many projects don't have 2 people) & a level 4 (verified reproducible builds)
    - Gavin: Having an exhaustive node build-out - it's sometimes necessary to build everything
    - Bootstrappable.org - starts with a few bytes, builds out
- https://blog.tidelift.com/the-state-of-package-signing-across-package-managers
-

🍀🍀2021-03-17🍀🍀

Attendees:

- Kim Lewandowski (Google)
- Dan Lorenc (Google)
- Mike Malone (smallstep)
- Ryan Haning (Microsoft)
- Priya Wadhwa (Google)
- Edoardo Tenani (Arduino)
- Sam White (GitLab)
- John Warren☕ (Verizon Media)
- Ned Smith (Intel)
- Steve Lasker (Microsoft)
- Asra Ali (Google)
- Jason Hall (Red Hat)
- Vinod Anandan (Citi)
- David A. Wheeler (Linux Foundation) - *respect* for the Shamrocks :-)

Agenda:

- Sigstore - Dan Lorenc - 03-17

    - Sigstore slides here: https://docs.google.com/presentation/d/1-XospFFdgR_vAE-ZA8IXvuciGSjfIVzjZ65jOoR3y_o/edit?ts=60522959
    - https://dlorenc.medium.com/how-to-sign-a-release-of-oss-e96ee94286fc

2021-03-03

Attendees:

- Kim Lewandowski (Google) 1st!
- Dan Lorenc (Google)
- Mike Malone (smallstep)Ryan Haning (Microsoft)
- Priya Wadhwa (Google)
- Edoardo Tenani (Arduino)
- Sam White (GitLab)
- John Warren (Verizon Media)
- Ned Smith (Intel)
- Steve Lasker (Microsoft)
- Asra Ali (Google)

Agenda:

- Notary v2 presentation! Steve Lasker
    - Containers are the next major virtualization stack, providing an easy means to build a deployment package that encompasses your code, binaries and dependencies. How do you know the container image you're deploying was built by a vendor, or even a team you trust? Notary v2 aims to solve this problem by enabling signing of all artifacts placed in an OCI conformant registry. As the artifact is promoted within and across registries, Notary v2 signatures can move with the artifacts, enabling secure validations, ensuring the content you deploy is the content you trust.

2021-02-17

Attendees:

- Kim Lewandowski (Google)
- Andrew Martin (ControlPlane)
- David A. Wheeler (Linux Foundation)
- Mike Malone (smallstep)
- Edoardo Tenani (Arduino)
- Konstantin Ryabitsev (Linux Foundation)

- Ned Smith (Intel)

Agenda:

- David Huseby (Security Maven, Hyperledger, The Linux Foundation) - his work to integrate OpenSSH and git. His presentation is here: https://docs.google.com/presentation/d/1eko1gUviMLj58vbMQPet0c-3BCEj9KjqablTePVo6oY/edit?usp=sharing
    - https://git.kernel.org/pub/scm/linux/kernel/git/mricon/patch-attestation-poc.git/plain/README.rst
    - Assuan protocol - where is that documented? What's the license of the spec (if any)?
        - https://gnupg.org/software/libassuan/index.html
        - Need to investigate. The CODE is GPLv3, but don't know about spec. May need LF legal to check on
    - No code for THIS version is written, but we have written code for previous versions, so probably 75% is already implemented. Should take ~2 weeks full time
    - Google FIDO team is interested in this
    - "I've already taken 2 years on this" - moving from Linux Foundation, indefinite period for personal reasons. Not sure have time to write the code.
    - Who else could write this? I can propose Hyperledger mentorships, could mentor someone for this summer.
    - Goal: Self-verifying git repos (where public keys are part of the git repository).
    - What about downgrade attacks? (In JSON web tokens, one of the headers was the algorithm you were using & could downgrade hash algorithm, including to algorithm none).
    - https://git.kernel.org/pub/scm/linux/kernel/git/mricon/patch-attestation-poc.git/plain/README.rst
    - David A. Wheeler: If you add support for a /etc/gitconfig.d file, then package managers could easily install the scripts to make it "just work" by default
    - This also allows digitally-checked pseudonyms ("Mickey Mouse")
    - "We don't have to solve all trust; we just have to bind digital trust to social trust mechanisms"

2021-02-03

Attendees:

- Kim Lewandowski (Google)
- Dan Lorenc (Google)
- David A. Wheeler (Linux Foundation)

- Ryan Haning (Microsoft)
- Justin Cormack (Docker)
- Mike Malone (smallstep)
- Sam White (GitLab)
- Jacob Rikerd (Cisco)
- Edoardo Tenani (Arduino)

Agenda:

- https://openssf.org/blog/2021/01/27/digital-identity-attestation-roundup/
- Crxcavator ("crex-cavator") - Chrome Extension analysis: https://crxcavator.io/ - presentation by Jacob Rikerd, jrickerd@cisco.com
    - programmatically calculates a risk score of chrome extensions
    - It's free but NOT open source software
- Signature best practices discussion: https://lists.openssf.org/g/openssf-wg-best-practices/message/40
- One more shameless plug: new blog post from google, touches on identity at the end

2021-01-06

Attendees:

- Kim Lewandowski (Google)
- David A. Wheeler (Linux Foundation)
- Mike Schwartz (Jannsen Project)
- Dan Lorenc (Google)
- Gavin Hindman (Intel)
- Ryan Haning (Microsoft)
- Zach Steindler (Cisco / Duo)

Meeting Recording

Agenda:

- Presentation from Mike Schwartz, Jannsen Project, gluu.org8
    - No formal slides, talked through github.com/JanssenProject/home
    - Mike Schwartz also hosts https://opensourceunderdogs.com/ podcast, on creating an OSS business
    - Focus: MultiParty Federation. Many autonomous organizations want to collaborate. Everyone's familiar with a centralized authority (e.g., GMail).
    - There are many kinds of federation, e.g., hierarchical, meshed, etc.
    - Many Universities use "InCommon" Federation

    - GTRI Trustmark: https://trustmark.gtri.gatech.edu/ - originally XML, now JSON. This was funded under the Obama administration, isn't funded any longer.

2020-12-09

Attendees:

- Kim Lewandowski (Google)
- David A. Wheeler (Linux Foundation)
- Mike Malone (smallstep)
- Dan Lorenc (Google)
- Luke Hinds (red hat)
- Konstantin Ryabitsev (Linux Foundation)
- Santiago Torres-Arias (Purdue University)
- Ryan Haning (Microsoft)
- Michael Peters (Red Hat)
- Gavin Hindman (Intel)
- Ned Smith (Intel)

Agenda:

- Housekeeping
    - Meeting schedule for EOY?
    - Probably cancel Dec. 23rd

- LF Announced Project Janssen -https://www.linuxfoundation.org/press-release/2020/12/the-janssen-project-takes-on-worlds-most-demanding-digital-trust-challenges-at-linux-foundation/ Can we get someone from the project to come present?
- Blog post recapping videos!
    - Kim
- Presentation: PKI/Certificates/Signatures 101 - Mike Malone
    - URL???
- Related URLs:
    - https://korg.docs.kernel.org/gitolite/transparency-log.html
    - https://github.com/projectrekor/rekor

2020-11-11

Attendees:

- Kim Lewandowski (Google)
- David A. Wheeler (Linux Foundation)
- Mike Malone (smallstep)
- Dan Lorenc (Google)
- Luke Hinds (red hat)
- Konstantin Ryabitsev (Linux Foundation)
- Santiago Torres-Arias (Purdue University)
- Ryan Haning (Microsoft)
- Michael Peters (Red Hat)

Agenda:

- Debian presentation 11/11 (Enrico)

2020-10-28

Attendees: (*Please sign yourself in*)

- Kim Lewandowski (Google)
- David A. Wheeler (Linux Foundation)
- Derek Ferguson (GitLab)
- Mike Malone (smallstep)
- Damien Miller (Google)
- Dan Lorenc
- Gavin Hindman
- Sam White (GitLab)
- Ryan Haning
-

Agenda:

- Damien Miller (Google) presented on "Git Signing with SSH" - a proposal about supply chain attribution to make it possible to attribute something back to its author. Ideally back to a hardware root of trust. Some points:
    - GPG signatures supported, but rarely used. GPG/PGP is famously hard to use, no trivial way to link GPG ID with repo ID. Another problem is to preserve attribution over common changes.
    - Proposal: Add support for SSH signatures to git (as a peer to GPG). Most developers already use SSH with git, already have some familiarity with this.

    - Steps already taken:
        - In 2019, added to OpenSSH 8.1 a signature mode (SSHSIG). Retains ssh's simple trust model, authorized_keys-like map between IDs and keys.
        - OpenSSH has long supported PKCS #11 but they're fiddly & expensive. Early this year added support for U2F/FIDO, which splits key into hardware part & rest part, which is MUCH cheaper. <$10 to get a FIDO key
    - Some work happened since in git, but didn't complete & go upstream - believe they ran out of time before it really completed. No objection from git developers in principle.
    - How can someone find a mapping between keys & iDs? GitHub as an API for querying this, the mapping can also be included in repo itself (so "git clone" can use it immediately)
    - Wider story of crypto & git: Some mutating operations destroy signatures (e.g., rollup commits).
    - What about expiration/revocation?
        - Revoking keys should be easy.
        - The system supports certificates which supports lifecycle control (e.g,. Timeframes allowed)
    - Damien will provide POCs to David Wheeler, who will try to contact those who partly implemented the next step to see what can be done next

2020-10-14

Attendees: (*Please sign yourself in*)

- Dan Lorenc (Google)
- Konstantin Ryabitsev (Linux Foundation)
- Sam White (GitLab)
- David A. Wheeler (Linux Foundation)
- Myles Borins (GitHub)
- Luke Hinds (Red Hat)
- Michael Peters (Red Hat)
- Mike Malone (smallstep)
- Wenjing Chu (futurewei)

Agenda

- Node.js identity management
- Review threat models doc, discuss diagram and interest.
- White Paper!

2020-09-30

Attendees: (*Please sign yourself in*)

- Dan Lorenc (Google)
- Sam White (GitLab)
- Derek Ferguson (GitLab)
- David A. Wheeler (Linux Foundation)
- Mike Malone (smallstep)
- Arnaud Le Hors
- Gavin Hindman (Intel)
- Kim Lewandowski (Google)
- Michael Peters (RedHat)
- Konstantin Ryabitsev (Linux Foundation)
- Kengo Suzuki (LayerX)
- Wenjing Chu (Futurewei)
- Santiago Torres-Arias (Purdue University)
- Ryan Haning (Microsoft)
- Eman Abu Ishgair (Purdue University)

Meeting Recording

Agenda

- Self Sovereign Identity presentation [~35 min] confirmed by Arnaud Le Hors (Open Technologist in IBM) (slides will be made available later)
- Review threat models doc, discuss diagram and interest.
- White Paper!
- heads up! we need to move 10/28 meeting to 3pm PT for a presentation on git signing

2020-09-16

Attendees: (*Please sign yourself in*)

- David A. Wheeler (Linux Foundation)
- Kim Lewandowski (Google)
- Ryan Haning (Microsoft)
- Justin Cormack (Docker)
- Kay Williams (Microsoft)
- Andrew Martin (ControlPlane)
- Dan Lorenc (Google)
- Santiago Torres-Arias (Purdue University)
- Gavin Hindman(Intel)
- Mike Malone (smallstep)

- Eman Abu Ishgair (Purdue University)
- Maya Kaczorowski (GitHub)
- Wenjing Chu (Futurewei)
- Michael Dolan (Linux Foundation)
- Chris Aniszczyk (Linux Foundation)
- Mike Malone
- Luke Hinds (Red Hat)
- Michael Peters (Red Hat)
- Konstantin Ryabitsev (Linux Foundation)

Agenda

- Calendars!
    - We had two let's use the OSSF-wide one going forward
- [Santiago Torres] presentation on In-Toto/TUF
    - Link to presentation https://docs.google.com/presentation/d/13LgoNSfbf1WG0GJ3qbh_ZWjN5ZalDFUnkBwg7Y3qdrU/edit#slide=id.p
    - Link from Michael Dolan: https://trustoverip.org/
- Next steps on threat models doc:
    - Review threat models doc, discuss groupings and which ones are most actionable/good starting points.
    - Who is interested in which ones? (Comment with a +1)
- Review/discuss name/scope PR: https://github.com/ossf/wg-developer-identity/pull/15

2020-09-02

Attendees: (*Please sign yourself in*)

- Kim Lewandowski [Google]
- Kay Williams [Microsoft]
- Dan Lorenc [Google]
- Jonathan Meadows [Citibank]
- Andrew Martin [ControlPlane]
- Derek Ferguson [GitLab]
- Mike Malone [Smallstep]
- Gavin Hindman[Intel]
- Sasha Levin [Microsoft]
- Michael Peters [Red Hat]
- David A. Wheeler [Linux Foundation]

- Luke Hinds [red hat]
- Lily Sturmann [Red Hat]
- axel simon [Red Hat]
- Santiago Torres-Arias [Purdue University]
- Eman Abu Ishgair [Purdue University]
- Matthew Thompson [Individual from FinTech]
- Konstantin Ryabitsev [Linux Foundation]

Meeting Recording

Agenda

- [Konstantin Ryabitsev] presentation for linux development (confirmed)
    - Presentation on LInux kernel developer identity verification from Konstantin: https://docs.google.com/presentation/d/1ouNX0MQc5PH9YozoTHkpYFu1ANZFW24gDwy7RcIGFQM/edit?usp=sharing
    - Many maintainers choose to use “trust on first use” (TOFU)
    - “If you’re in my keyring, I trust your signature”
    - Upside: Scales better, easier to understand compared to web of trust (WoT)
    - There is a kernel.org web of trust, it’s everyone with an account on kernel.org. https://korg.docs.kernel.org/pgpkeys.html - effectively this is my web of trust
    - Visualization: https://www.archlinux.org/master-keys/#visualization
    - “PGP isn’t hard because it’s PGP. It’s hard because delegated trust is hard. The problem is less with tools & more with the problem itself. It’s true that PGP’s CLI’s is complex. It’s gotten better, and they really need more funding.”
- Any other presentation ideas for future meetings?
    - KR: I can suggest we talk to David Huseby of Hyperledger, who is working on did:git (distributed identity and signing with git, as alternative to PGP): https://github.com/dhuseby/did-git-spec
- Follow-ups from Last time:
    - [Kay Williams] Collaboration with CDF security sig (confirmed)
        - CDF sec sig 3T sbom
        - https://www.it-cisq.org/software-bill-of-materials/index.htm
    - [Dan Lorenc/Luke Hinds] - Scope discussions with TAC pending. For now, assume we can expand scope.
        - Next steps is to put together a simple doc outlining the scope and present to TAC
- Plan for threat models doc:
    - Collect all threat models in the supply chain integrity space in the document
    - Review threat models to decide which are in scope and which are believable
    - Collect prior art/discuss how existing projects mitigate these threats
    - Prioritize/split into themes and start addressing them!

        - What should be in scope for addressing threats? We can:
            - publish documents, best practices, guides
            - Build tools
            - Operate services?

2020-08-19

Recording
Attendees: (Please sign yourself in)

- Kim Lewandowski [Google]
- Dan Lorenc [Google]
- Derek Ferguson [GitLab]
- Andrew Martin [ControlPlane]
- Matthew Thompson [Individual from FinTech]
- Chris Aniszczyk [Linux Foundation]
- Ivan Font [Red Hat]
- Lily Sturmann [Red Hat]
- Mike Malone [Smallstep]
- Sasha Levin [Microsoft]
- Sridhar Poduri [Microsoft]
- David A. Wheeler [Linux Foundation]
- Konstantin Ryabitsev [Linux Foundation]
- Michael Peters [Red Hat]
- Joshua Lock [VMware]
- axel simon [Red Hat]
- Srikanth Suresh [Individual]
- Luke Hinds [Red Hat]

Agenda:

- Intros (Name, Organization, Location)
    - Why are you interested in this topic?
- Logistics
    - Meeting cadence, time?
        - every other week at this time (16:00UTC, 9am PST)?
        - timezones?
        - Rotation to an Asia-friendly timezone once a month or so?
        - Decision: start with every other week, same time for now
    - Zoom/Hangouts/etc.?
        - Luke is happy to use hangouts
        - Matt says Teams is better than Zoom, maybe hangouts is too

        - Should we record these?
            - Yes, and remind people every time
    - GitHub Repo: https://github.com/ossf/wg-developer-identity

- Scope of WG
    - Kay Williams: Here is a document for discussion. This is a rather large scope expansion, aimed at first laying the groundwork for supply chain attestation and policy, and later building from it to support attestation and policy around developer identity (and other aspects of supply chain security and compliance)
    - Luke: Agrees with everything in here. It's a lot wider, not sure this is a bad thing
    - Joshua - not sure there is a place where the overall topic is being discussed, let's just expand the scope here
    - Luke - Identity could still be an inroad to this, start with this as a first goal
    - David - if we do expand, we do still need to pick a few areas to focus on
    - Sridar - pick a few goals to build an MVP
    - Ivan - For people not familiar with OSSF, what other WGs are there? is there overlap?
        - https://github.com/ossf/tac
        - Is there a community-wide meeting for the entire foundation? Could we check scopes then?
    - Luke - TAC meeting provides oversight for these
        - First TAC meeting Friday at Noon
        - David - scope changes could be discussed then!
    - Matt Thompson - reference to things like keybase.io stuck in his mind, enabling people to identify themselves in a secure fashion
        - Maybe this is just a facet
    - Andrew Martin - other organizations in this space
        - sig-security-supply-chain in CDF
        - SBOM working groups
        - David - if we decide to broaden scope we'll need to work with these other organizations
    - Matt - are we verifying companies or individuals?
        - Luke - yeah this is a topic we're tackling here, it's harder in open source than at a private organization. Risk could be involved for people to work under real names. Need to balance these concerns.
        - David - privacy is very important, this is a large concern
            - Could look at this as supplier identity (could be real name, or pseudonym, or organization)
        - Dan - other threat models to verify two identities are unique
            - David - very tricky

    - Luke - good we have people from in-toto here
        - Bad things do happen. Do we have some ways to verify/log all things that have happened later. Tamper proof record
- Next Steps
    - Start with Threat Models
        - David - stronger confidence that releases were done by the same organization/individual as the last one
            - Bitcoin - we still don't know who Satoshi Nakamoto is, but we can verify if that person made a change
            - Axel - actually we don't know, we just know it was signed by the same key. Could be multiple people
            - Matt - we have keys as identifiers
            - David - keys aren't perfect but are a good first step, the next step of associating keys to suppliers (organizations, pseudonyms, and real people) would be fabulous. Maybe we can split it into those 2 different problems (so we can work on them separately)
        - List of case studies. eg. Linux
        - From github repo:
            - Malicious/Nefarious individuals get maintainer permissions and starts making making commits or pushes to a registry
                - Making it more obvious that a different individual is involved could help recipients know there might be a higher risk
            - Duplicate accounts, self-reviewing code
            - Identity spoofing: claiming you work for a specific organization that you do not, or are a specific individual that you are not
        - Konstantin - would case studies be helpful?
            - Yes! He'll do a presentation on how this works in the linux kernel in a future meeting.
            - Linux has some things, not documented well, but they exist and are trying to address these things
        - Luke - different levels of projects, PyPi, NPM on one end, Golang on the other end
            - Varying levels of cryptographic guarantees
        - Luke - more hands on keyboards than powerpoints, should be able to find projects to try these techniques out in
        - David - subverted repo

        - People gained control of entire repos, verifying things in Repos. GitHub has had a few of these. It's happened several times in the past. E.g., 2003? - Linux kernel repo was subverted
        - GitHub/GitLab have done great jobs here, but no one is perfect
        - also subverted package managers repos - credential compromise & package manager repo compromise
    - Srikanth - subresource integrity
        - CDNs distributing things are part of the supply chain
        - Golang module transparency in this space
            - Also Brandon Phillips' new project https://www.transparencylog.com/
    - Andrew Martin - typo squatting
        - #1 supply chain problem right now (David can you link this?)
            - In Sonatype report
            - [Ohm 2020] Ohm, Marc, Henrik Plate, Arnold Sykosch, and Michael Meier, "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks", 2020-05-19, https://arxiv.org/abs/2005.09535
        - This could be viewed as verifying the identity of the *package* instead of verify the identity of the supplier
    - Axel - another issue: "not another account/set of credentials!"
        - One account to do everything (fedora has SSO)
        - Self-sovereign identity/decentralized identity
    - Joshua - need to keep in mind the amount of effort required to use these. If it's too hard no one will use it.
        - TUF integration into PyPI was scaled back because developers didn't want another secret to remember (see initial proposal in PEP 480 vs PEP 458, which is being implemented now)
        - Repository signed on upload
        - Must make it EASY to use
        - Make it a carrot instead of a stick (provide an advantage/incentive)
        - Andrew - ingestion of OSS into regulated environments is a nightmare. This could help as a carrot
- Next steps:
    - Dump all this into a doc and start having people contribute threat models. We can then curate, combine, agree
        - Dan to send out this doc
        - CNCF sig security has an attack catalog https://github.com/cncf/sig-security/tree/master/supply-chain-security/c

ompromises and https://github.com/cncf/sig-security/blob/e6dfeb2f767b36c747831850e2a3fdf4f9c26aea/supply-chain-security/compromises/compromise-definitions.md

- Luke Hinds and Dan Lorenc to discuss scope at TAC meeting Friday
- All: review Kay's document