2024 OpenSSF BEST WG Meeting Notes

Want to help drive open source security education or help develop best practices? We have a lot of projects and groups that are working towards these goals.

- We envision a world where software developers can easily IDENTIFY good practices, requirements and tools that help them create and maintain secure world-class software, helping foster a community where security knowledge is shared and amplified
- We seek to provide means to LEARN techniques of writing and identifying secure software using methods best suited to learners of all types
- We desire to provide tools to help developers ADOPT these good practices seamlessly into their daily work

This WG is chaired by Avishay & Georg (with some help from CRob)

BEST WG Meeting Details

: Repo | Discussions

📧📭: OpenSSF* (Mailing List)

* Join the Mailing List to receive the calendar meeting invite.

📅: Tuesdays, starting Jan 16, 2023 (occurs every 2 weeks)

🕖: 10:00a ET/7:00a PT

: LFX Zoom

▶: OpenSSF (New!)

→ **MEETINGS**: Log in to your LFX Profile and go to MEETINGS to see your upcoming and past meetings. For help, contact support@openssf.org

BEST Projects & SIGs

EDU SIG Meeting Details

:Repo 📅:Every other Wednesday 🕘:9:00a ET/1400 UTC zoom: LFX Zoom 📄: Meeting Notes

Scorecards Project Meeting Details

: Repo 📅: Every other Thursday : 4p ET/ xxx UTC zoom : LFX Zoom 📄: Meeting Notes

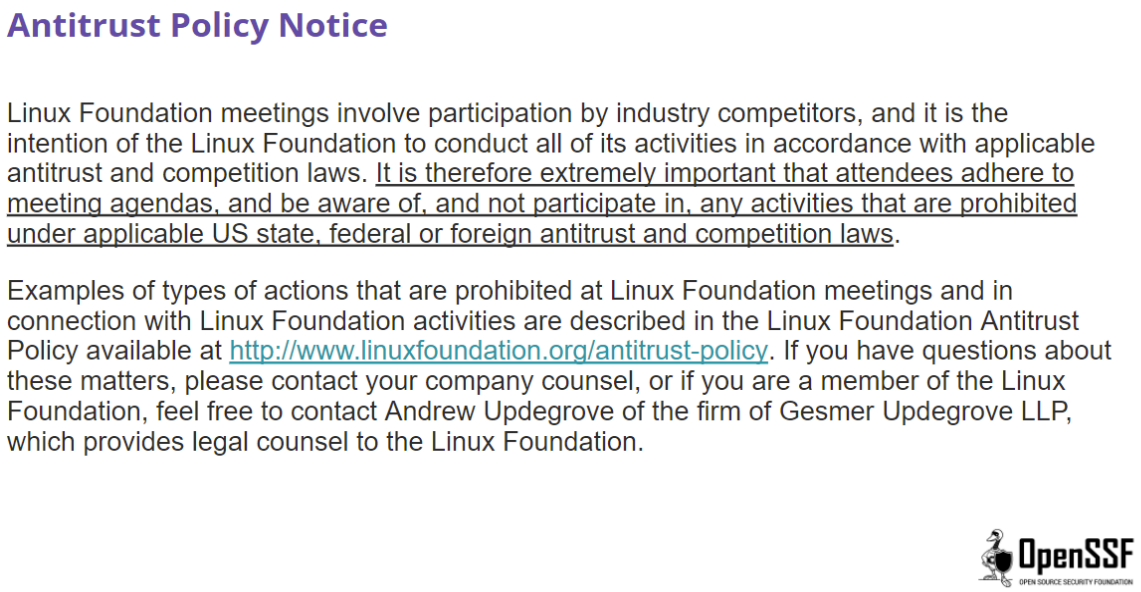
C/C++ Compiler BP Guide SIG Meeting Details

: Repo 📅: Every other Wednesday 🕗: 8:00a ET/1300 UTC zoom : LFX Zoom

Memory Safety SIG Meeting Details

:Repo 📅:Every other Thursday 🕐:1:00p ET/1700 UTC zoom: LFX Zoom 📄: Meeting Notes

Older 2023 notes are available at OpenSSF Best Practices WG Notes - 2023
Older 2022 notes are available at 📄 OpenSSF Best Practices WG Notes-2022
Older 2021 notes are available at 📄 OpenSSF Best Practices WG Notes-2021



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.linuxfoundation.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.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Antitrust Policy Notice

Python Hardening Guide - Meeting details

:Repo 📅:Every other Monday 🕗:1600 UTC zoom: LFX Zoom : Meeting Notes

→ **MEETINGS**: Log in to your LFX Profile and go to MEETINGS to see your upcoming and past meetings. For help, contact support@openssf.org

Code of Conduct

All participants in OpenSSF meetings are subject to the OpenSSF Code of Conduct. See: https://openssf.org/community/code-of-conduct/

Meetings

2025 Meeting Notes - HERE

2024-12-17 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Georg Kunz* Co-chair	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Daniel Appelquist* [TAC, Web]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Stefan Bavendiek		UHH		
x	Salve J. Nilsen		CPANSec		sjn

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)

New Friends

- Stefan Bavendiek - PhD student in Hamburg. Interested in Sandboxing. https://github.com/ossf/wg-best-practices-os-developers/issues/631

Opens

- TAC read-out scheduled for January 7
    - Please provide updates in this document or at https://github.com/ossf/tac/pull/423
    - We should collect info we’re going to present…
- Global Policy WG
    - https://github.com/ossf/wg-globalcyberpolicy
    - “The Global Cyber Policy Working Group seeks to assemble subject matter experts from many disciplines to collaboratively discuss legislation, regulation, and cybersecurity frameworks and standards that can help stakeholders of all background meet their compliance obligations.”
        - Awareness workstream: https://docs.google.com/document/d/1d0mHlmImMNJNKat7qd2binfxBINot7kMBaoQKTH9_b4/edit?tab=t.0#heading=h.untq66fszwdn
        - Tooling and processes workstream: https://docs.google.com/document/d/1EV4pNZXxiTGdo8tdA92ya16N8otCdLFvqedmqntF4lg/edit?tab=t.0#heading=h.ljy0cv72hwef
        - Standards and specs: https://docs.google.com/document/d/1ZgLv26CvN6JBYHguIpN9GzGj-yzE5U_tyQNbYxDCRF8/edit?tab=t.0#heading=h.he1hzvqvfnat
    - Meeting time
        - Is this already fixed to Tuesdays 10am PST?
        - Not a good time for EU participants
        - Ask for adding the weekly calls to the calendar
        - Who’s chair? Not clear.
        -
- Sandbox https://github.com/ossf/wg-best-practices-os-developers/issues/631
    - There’s interest, but who will work to start making it happen?
    - Mickaël Salaün (l0kod)? Anyone?
    - Stefan Bavendiek is working on a paper to provide a guide to sandboxing
        - PhD is on attack surface measurement
        - Wants to write paper, then create user-friendly guide
        - Could start with a markdown document
- FYI on W3C Ethical Web Principles: https://www.w3.org/blog/2024/w3c-statement-on-ethical-web-principles-guides-the-community-to-build-a-better-web/
    - One of the principles is : “The web is secure and respects people's privacy.”
    - First W3C Statement meaning it’s not a standards document but it has been officially “endorsed” by W3C.

    - Underpins other more actionable guidance such as the Web Platform Design Principles and the Privacy Principles docs.

Backlog Review

- 523 and 524: Add request for contributions to regex guide
    - I assume this is always the case
    - https://github.com/ossf/wg-best-practices-os-developers/pull/523
        - Dan: I updated based on David's proposed wording - I think this can be merged.
    - https://github.com/ossf/wg-best-practices-os-developers/pull/524
        - Dan: I updated based on David's proposed wording - I think this can be merged.
- Ok to close
    - https://github.com/ossf/wg-best-practices-os-developers/issues/535
- Rendering style of guides
    - https://github.com/ossf/wg-best-practices-os-developers/issues/160
- Feedback appreciated
    - https://github.com/ossf/wg-best-practices-os-developers/issues/628

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Mass updates of software/infrastructure
    - Updated database - Postgres 14->16
    - Updated Ruby, Containers, dependencies, etc.
- Plan to add database-based backend for jobs to eliminate a race condition (between the app and CDN) that in rare cases causes badge images to not update for many hours https://github.com/coreinfrastructure/best-practices-badge/issues/2193
    - Internet packets aren't necessarily received in the order sent. Order is recreated within one TCP stream, but not between TCP streams.
    - Badge images are cached. We can control event sequences within the app, but not between the app and our CDN (Internet packets). As a result, it's possible for the app to send an old image and then a cache invalidation, but the CDN may receive the invalidation first, then an old image - and it will cache the old image. The CDN then keeps serving the old image.

    - Solution: Send a cache invalidation later after there’s been time for all already-sent old images to be received by the CDN. This requires a database to ensure cache invalidations are always sent, even if the system is restarted.
    - Remember, there are 2 hard problems in computer science: cache invalidation, naming things, and off-by-one errors.

Education (Security Fundamentals etc.) (David A. Wheeler)

- LFD121
    - 2024 Enrollment 9,054 so far (far beyond 7,990 goal) as of 2024-12-17
    - Made various small improvements: Define OSS, added some story times, etc.
- Management course - CRob reviewed, we have 2 issues with proposed resolutions, then we’re ready to record.

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob & Dave R)

- FULL SIG Notes
- Developer Manager course script review in progress, recordings are scheduled to commence shortly

Memory Safety SIG (Nell)

- FULL SIG Notes
- Working on new stream, interoperability esp. Rust/C++
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
- See retrospective further down for a good summary of this year

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
- Discussed need to clarify scope. It is NOT trying to describe how to use various Python libraries (there are too many), so it focuses only on built-ins. That wasn’t clear to some new readers, need to tweak.

- Structured by CWE (currently). Needs to be easier to read/use. It's a pain to navigate right now.

WebDev Security Guide (Daniel)

- BEST Issue 367
- We held a brief call this week. I've also socialized our with with the OpenJS Foundation security coord call. We're going to start up again in new year working on the "Security Guidelines for Library Developers" doc. We also had a few presentations from Google on their tooling that they have developed for CSP and Trusted Types. Will circulate as soon as those are published. We've also been inputting into some PRs on MDN about a new XSS guide: https://github.com/mdn/content/pull/36412

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
-

2024-12-16 Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Helge Wehder	Helge.wehder@ericsson.com	Ericsson		myteron
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation		david-a-wheeler
x	Bartlomiej Karas	Bartlomiej.karas@ericsson.com	Ericsson		Bartyboi1128
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson		gkunz
x	Noah Spahn	noah.spahn@open.ac.uk	Open University		noah-de

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

-
  - Welcome new friends
  - Is someone willing to scribe for the meeting?
  - Call for opens (list new items below)

Opens

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Review of 680 pySCG: Missing rules on CWE Top 25
  The issue contains a quick, potentially inaccurate, assembly of CWEs we are potentially missing and requires review.

  David: Scope is not clear in the main pySCG readme.md
  https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Secure-Coding-Guide-for-Python

  @david-a-wheeler: Missing "only" including the modules listed in ..... could be even more clear by mentioning what is excluded.

  Helge suggests adding: ”Specific encodings around YAML, JSON, XML and web languages such as JavaScript currently not covered.”. Created a PR to address this:
  710 *pySCG: updated to scope addressing Davids feedback, fixed formatting*

  eval() check if there is something for CWE-94

- Review of NEW open PRs
  - 698 CWE-330: Use of Insufficiently Random Values Documentation / wo 2nd review
  - 697 CWE 1339: wo on 2nd review, Noa going to cover 2nd reviewer.
  - 519 Issue avoid having C&P code to MD,
    PR using Jekyll, :528 Code examples with Jekyll /
    alternative options: RMarkdown, Jypiter
    missing decision.

- Open issues waiting for volunteers to pick them up:
  - 652 pySCG typo or error in CWE-703/CWE-392/compliant03.py
  - 632 pySCG: Python Hardening Guide: we should mention and explain audit hooks, sys.audit and sys.addaudithook
    - Pending. A volunteer may pick this up

    - 708 pySCG: CWE-89 image formatting wonky, need correct license quote for XKCD using CC-BY-2.5

- Old Open issues
    - 657
        - It is a valid question. Maybe we can include the comment by Mitre in the Readme.
          No answer from @openrefactorymunawar,/ close issue?
    - 646
        - More discussions needed. Collaboration with the C/C++ compiler guide and the memory safety WG and the Python security team.
        - Such a requirement can be tricky because it may create a push towards closed source implementation to hide well-known bad functions or - even worse - towards re-implementations.
        - Issue was brought up with Full WG, general agreement by the group. NCSC is generally not open to comments at the same level as NIST. Might Need to move this to main WG?

    - 635 / needs 2nd CWE-681 and 1339 to move from Confluence to GitHub.
        - Bart is working on CWE 1339 up for PR.
        - The suggested way forward is not to bring in more CWEs and then discuss how to handle this weakness generally in the guide.
    - .

2024-12-12 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler

x	Gabriel Dos Reis	gdr@microsoft.com	Microsoft		GabrielDosReis

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

- Holiday schedule: Thomas is proposing to cancel call on Thursday, December, 26
    - This was decided unanimously. Next call will be on January 9.

- Retrospective from year two of the guide:
    - What did we do well?
        - Got word out. Multiple presentations, multiple mentions in media.
        - Good job of maintaining high quality of mature product. We've added material, judiciously. E.g., information on compiling compilers, control flow protections, etc.
        - Overall it's been successful!
    - What have we learned?
    - What should we do differently?
        - Find a way to occasionally (quarterly?) get status checks from Linux distros, various users of the guide (CPython, Wireshark, Erlang VM)
        - Apple is proposing a hardened version of C++ language to standards body. It would include bounds-checking and other stuff. "Safe C++" and profiles were also discussed.
            - We'll probably see more convergence
            - Proposal for hardened C++ Standard Library: https://isocpp.org/files/papers/P3471R1.html
            - Gabriel is involved in C++ standards community
            - There are various C++ conferences that we could present to, could submit talk:
                - Meeting C++ <https://meetingcpp.com/> (Berlin) - 14th - 16th November, deadline for proposal ?
                - ACCU in UK https://accu.org/conf-main/main/
                - CPPCon https://cppcon.org/
        - Linux kernel is increasingly using C variants/extensions to counter security issues (attributes / annotations, etc.). See self-protection project, style guide, etc.
        - Could broaden to enhanced annotations / coding styles specifically to counter security issues? Earlier wasn't considered ready for prime time, but maybe we can now.
    - What do we not understand?

        - How do we test these features? LLVM is doing static analysis. That is, how ensure it works correctly across many real-world programs and across CPUs. Thomas has talked with some folks, e.g., using Juliet test suite (not really intended for its purpose).
        - Some just reject any static analysis of *any* kind. This is odd. Static anlysis (like anything) can be done badly, but that doesn't mean it never applies. We do already discuss greenfield vs. brownfield.

- New/Updated Issues/PRs:
    - New/Updated Issues/PRs:
        - Clarify compiler versions for __fallthrough__ attribute and feature testing via __has_attribute (#688)
            - Merged
        - Improve -fno-strict-overflow description (#694)
            - C++ 20 and later define two's complement representation. The PR should be adjusted accordingly: References:
              for C++26:
              https://open-std.org/JTC1/SC22/WG21/docs/papers/2024/p3477r0.html
            - for C++20 and up: https://eel.is/c++draft/basic.fundamental#1
        - Clarify compiler options hardening limitations when linking to pre-built artifacts (#705, #706)

Guide Notes

-

2024-12-03 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Georg Kunz* Co-chair	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Sean McGinn	Sean.McGinn@amd.com	AMD		

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)

New Friends

-

Opens

-

Backlog Review

- Open PRs (low handling fruits)
  - 523 and 524: Add request for contributions to regex guide
    - I assume this is always the case
    - https://github.com/ossf/wg-best-practices-os-developers/pull/523
    - https://github.com/ossf/wg-best-practices-os-developers/pull/524
  - 560: recommendation to counter xz
    - Discussions have converged. One comment left
    - https://github.com/ossf/wg-best-practices-os-developers/pull/560
      - The group agrees to finalize this PR
- Open Issues
  - [SOSS TASK FORCE] issues
    - https://github.com/ossf/wg-best-practices-os-developers/issues/255
    - https://github.com/ossf/wg-best-practices-os-developers/issues/256
    - https://github.com/ossf/wg-best-practices-os-developers/issues/257
  - Concise Guide for Evaluating OSS: Questions 9.i. and 10.v. seem redundant
    - https://github.com/ossf/wg-best-practices-os-developers/issues/678
  - Sandboxing
    - https://github.com/ossf/wg-best-practices-os-developers/issues/631

    - Ok to close
        - https://github.com/ossf/wg-best-practices-os-developers/issues/545
        - https://github.com/ossf/wg-best-practices-os-developers/issues/535
    - Blocked
        - https://github.com/ossf/wg-best-practices-os-developers/issues/160
    - Unlabeled
        - https://github.com/ossf/wg-best-practices-os-developers/issues/628

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- We now have user search
    - Only for admin purposes, primarily to handle GDPR requests. It can search for emails & names, so privacy issues.
- Working to eliminate dependency on component with known vuln
    - The vuln is believed to be not exploitable, but it's not a good sign
    - The vulnerability has actually been fixed upstream, but a vulnerable version remains mid-stream
    - It's a polyfill for Safari that is no longer needed - best to remove.

Education Courses (Security Fundamentals etc.) (David A. Wheeler)

- LFD121 continues to climb in enrollment
- Management course: added more about reusing software (including defining OSS), waiting for CRob to review script before re-record

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- See David's updates above regarding the courses
- LF Education working on global skills matrix (w/Clyde)
    - CRob has talked with NIST on how to potentially align this with NIST NICE; might be other alignment opportunities as well

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
    - Chainguard is using these flags in their “guarded images”
    - https://www.linkedin.com/feed/update/urn:li:activity:7265344458316034048/?origin=NETW[…]YzA0NzMzMjcwZjNmNTcxMTgxYWEzNTczYWVkOGI2OWJkMDkwLDEsMQ%3D%3D
    - https://www.chainguard.dev/unchained/enhanced-compiler-flags-for-building-chainguards-guarded-images
    - Enhanced Compiler Flags for Building Chainguard’s Guarded Images
    - Chainguard Images are now built using enhanced compiler flags for C/C++ projects. See how this strengthens the security posture of Chainguard's build systems.
    - E.g.: thomas stromberg said, "The OpenSSF flags list is surprisingly well done. Kudos to them and to Chainguard for getting hardened binaries into customers' hands!"
-

Python Hardening Guide SIG (Helge & Georg)

- BEST
- Issue 481
- We are contemplating creating a blog post to raise awareness.

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
-

2024-12-02 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Helge Wehder	helge.wehder@ericsson.com	Ericsson	he/him	
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Bart Karas	bartlomiej.karas@ericsson.com	Ericsson	he/him	

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

Opens

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Review of open issues
    - 657
        - It is a valid question. Maybe we can include the comment by Mitre in the Readme.
    - 652
        - Pending. A volunteer may pick this up.
    - 646
        - More discussions needed. Collaboration with the C/C++ compiler guide and the memory safety WG and the Python security team.
        - Such kind of requirement can be tricky because it may create a push towards closed source implementation to hide well-known bad functions or - even worse - towards re-implementations.
            - We should bring this topic to the Full WG call
    - 635 / needs 2nd CWE-681 and 1339 to move from Confluence to GitHub.
        - Bart is working on CWE 1339

        - The suggested way forward is not to bring in more CWEs and then discuss how to handle this weakness generally in the guide.
    - 632
        - Pending. A volunteer may pick this up.

- Review of open PRs
    - 696 Doc2GitHub CWE-89 / Reviewers: Georg and Bart
    - 692 CVE for CWE-78 / Reviewers: Georg Bart
    - 519 Issue avoid having C&P code to MD,
      PR using Jekyll, :528 Code examples with Jekyll /
      alternative options: RMarkdown, Jypiter
      missing decision.

Guide Notes

- Discuss content of Missing rules on CWE Top 25 #680 in the next meeting.

2024-11-19 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Georg Kunz* Co-chair	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Jack Kelly	Jack at control-plane.io	ControlPlane/ ITSC		06kellyjac
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Kevin Dix	kevinrdix@gmail.com	Boeing	he/him	

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- Issues:
    - Update on https://github.com/ossf/wg-best-practices-os-developers/issues/646
    - [SOSS TASK FORCE] issues
        - https://github.com/ossf/wg-best-practices-os-developers/issues/255
        - https://github.com/ossf/wg-best-practices-os-developers/issues/256
        - https://github.com/ossf/wg-best-practices-os-developers/issues/257
    - Concise Guide for Evaluating OSS: Questions 9.i. and 10.v. seem redundant
        - https://github.com/ossf/wg-best-practices-os-developers/issues/678
    - Sandboxing
        - https://github.com/ossf/wg-best-practices-os-developers/issues/631
    - Ok to close
        - https://github.com/ossf/wg-best-practices-os-developers/issues/545
        - https://github.com/ossf/wg-best-practices-os-developers/issues/535
    - Blocked
        - https://github.com/ossf/wg-best-practices-os-developers/issues/160
    - Unlabeled
        - https://github.com/ossf/wg-best-practices-os-developers/issues/628
-

New Friends

- Prince Oforh Asiedu - not strictly new, but it’s been a while

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- I keep processing GDPR requests. I've started to add a simple admin interface for searching names/emails to make it easier to process GDPR requests.

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- I've been watching the LFD121 course enrollments carefully, but the data pipeline to my dashboard has temporarily stopped working over the weekend. It's being fixed, but in the meantime I went to find out what our LFD121 enrollments are now. We've been monitoring 2024 enrollments of LFD121, excluding email addresses with @linuxfoundation.org OR @linux.thoughtindustries.com, so we had to re-filter at the origin. Drum roll please...
- **HOORAY**! Our 2024 goal for LFD121 enrollment was 7990, and we have 8080 as of 2024-11-19 (this morning). THANK YOU SO MUCH EVERYONE!
- Once the dashboard works again I'll report other figures/information.
- What about completions?
    - Our current data claims 1,492 have a completed status, but we believe that number is NOT correct. There are issues with Thought Industries (TI) in how they calculate the % complete of courses and as a result, the completion statuses are sometimes inconsistent. This has been a long standing issue with TI, however, they updated us last week to say the fix will be released soon. We can update further once we get more updates from TI but any completion numbers are subject to change following the release and application to historical data by TI.
    - Background: We noticed the issue about a year ago when user course progress % was showing as above 100% (for example, 543% complete). As we investigated further, we noticed in some of our panoramas that new clients, who had not completed any learning yet, had completed statuses. We escalated and TI confirmed the issue to be related. It's been in development with them for a while. We have been provided with assurances that the fix is coming soon.
- Management course: We now have a written script. CRob to review.

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- See above
-

Memory Safety SIG (Nell)

- FULL SIG 2024 Notes 2023 notes Old notes
- Currently - completed another iteration of the continuum when developing software. E.g., using Rust, but making everything unsafe, is a problem.
- The group is transitioning to collect best practices for interfacing between memory safe and not memory safe languages
    -

C/C++ BP Guide SIG (Thomas)

- We are continuously improving the guide
- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
- Need to talk to Seth about applying it to CPython
    - There was a Google summer of code project targeting the application of the guide to CPython. It would be great for the team to look into the learnings of this work to identify potential improvement and additions to the guide.

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
- **Call for participation!**
- The team is continuing to add more guidelines based on CWEs

WebDev Security Guide (Daniel)

- BEST Issue 367
- We had a special call of the SWAG group this week to hear from Google about tooling they are developing to help developers with CSP and Trusted Types. The minutes are here: https://github.com/w3c-cg/swag/blob/main/meetings/2024-11-18-minutes.md and a video & slides will be published soon.
- We need help on a number of issues : https://github.com/w3c-cg/swag/issues
    - Specifically, thinking about security criteria for software packages (from a web developer perspective).

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
-

2024-11-18 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Noah Spahn	noah.spahn@open.ac.uk	Open University		noah-de
x	Bart Karas	bartlomiej.karas@ericsson.com	Ericsson		
x	Helge Wehder	helge.wehder@ericsson.com	Ericsson		

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
-

Opens

-

Guide Notes

-

2024-11-14 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Canceling call due to low attendance/calendar mishap. The upcoming C/C++ Compiler BP Guide call on 2024-11-28 is canceled as well due to Thanksgiving! Next scheduled call is on 2024-12-12

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
  - Clarify compiler versions for __fallthrough__ attribute and feature testing via __has_attribute (#688)
  - Improve -fno-strict-overflow description (#694)

Opens

-

Guide Notes

-

2024-11-05- Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	CRob	christopher.robinson@linuxfoundation.org	Linux Foundation	he/him	SecurityCRob
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Kevin Dix	kevinrdix@gmail.com	Boeing	he/him	
x	Venu Vardhan Reddy Tekula	vt2182@nyu.edu	NYU	he/him	vchrombie

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
-

New Friends

- Kevin Dix (Boeing) - software assurance focal point. Have been at Scorecard. Hawaii.
- Venu - Not really new here, but let’s introduce. Student at NYU.

Opens

- Mention of last week’s discussion about NCSC Vendor Security Assessment (https://github.com/ossf/wg-best-practices-os-developers/issues/646)

        - Action Items [Avishay]:
            - Write to CRob about TAC & TSC visibility to this
            - VulnCon proposal for discussion around this document
- Review PRs
    - https://github.com/ossf/wg-best-practices-os-developers/pull/489
    - https://github.com/ossf/wg-best-practices-os-developers/pull/503
    - https://github.com/ossf/wg-best-practices-os-developers/pull/560
    - Action Item: Avishay: Reach out to SIG leads to review open issues and PRs
-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- No big changes. Continue to process GDPR, new projects, etc.

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- Developing Secure Software (LFD121)
    - We have all tier 0 and tier 1 labs.
        - Quoted in OpenSSF updates its Developing Secure Software course with new interactive labs by Jenna Barron (there's also an OpenSSF press release).
        - We'd love to have more, but we're currently more focused on increasing enrollment.
    - LFD121 enrollment in 2024 as of end of October 2024 is 7,325.
        - In 83% (10/12) of the year we've achieved 92% of our aggressive 2024 goal (7,990). That's no guarantee of success (e.g., we can't keep spamming email), but clearly we're making progress.
    - Continue reaching out & spreading word.
        - Plan to have emails about the labs this month, to those who'd expresed interest in LF things.
    - ***Please help us*** - let others know about LFD121, encourage them to try it out!
- Security for Software Development Managers (LFD125)

    - Have final draft, addressing LF Education feedback, plan to re-record soon
    - https://docs.google.com/presentation/d/19IolYrumwUa7qHV65OW0IJ-oTpLV0I2KqEVGzjf0FSI/edit#slide=id.g3042855f76d_0_59

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-

Memory Safety SIG (Nell)

- FULL SIG Notes
- Draft 2 of the Continuum - https://github.com/ossf/Memory-Safety/blob/main/docs/memory-safety-continuum/memory-safety-continuum-draft2.md

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
-

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
- Seeking to release 1.1 version of baseline in the next few weeks…comments welcome
- Once baseline items are agreed upon, we'll be working with BP Badges, Scorecard, Sec Insights, & Minder to integrate

2024-11-04 - Python Hardening Guide

11:00 Eastern Time / 0800 Pacific / 1600 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Helge Wehder		Ericsson		
X	Bart Karas		Ericsson		
X	Georg Kunz		Ericsson		

Agenda

- Welcome new friends
    - Victor, interested in PyTorch
        - https://www.youtube.com/watch?si=4uVAoYgvB1J_jUf2&v=rgP_LBtaUEc&feature=youtu.be
        - https://github.com/pytorch/executorch
    - This guide can be interesting to the PyTorch community
        - Apply the general recommendations of the guide to PyTorch or users of PyTorch
        - Incorporate PyTorch / AI / ML specific best practices
- Is someone willing to scribe for the meeting?
- Call for **Opens, general or new discussions** (Please add)
- PRs and issues

Opens, general or new discussions

- GitHub permissions

PRs and issues

Pull Requests Open or in Review

- #690 pySCG adding missing CVEs for 755 and 532 by myteron · Pull Request
  Author: myteron, reviewers: gkunz

merged

- #689 pySCG adding CWE-78 code and doc by myteron · Pull Request
  Author: mtyeron, reviewers: gkunz
  Gkunz promised to review

- #687 Adding documentation to CWE-175 as part of #531 by s19110 · Pull Request
  Author: s19110, reviewers: myteron
  Reviewers wanted!

- #676 Changed wording to quote OpenSSF as main contributor by myteron · Pull Request
  Author: myteron reviewers: gkunz, 06kellyjac
  Merged. At some point in time, we should have a thank you section for the contributors just like https://best.openssf.org/Compiler-Hardening-Guides/Compiler-Options-Hardening-Guide-for-C-and-C++#contributors

- #528 Fixes #519: code examples use Jekyll by tommcd · Pull Request
  Author: tommcd reviewers:

Issues waiting for a volunteer to pick up:

- 652 pySCG typo or error in CWE-703/CWE-392/compliant03.py
- 632 pySCG: Python Hardening Guide: we should mention and explain audit hooks, sys.audit and sys.addaudithook
- #680 pySCG: Missing rules on CWE Top 25 · Issue
  - Label as help-wanted / good first
  - This is a great way to prioritize our work

Issues in discussion:

- #657 pySCG: Replacing CWE-400 with something that describes the resource exhaustion case better · Issue
  It is a valid question. Maybe we can include the comment by Mitre in the Readme.
  - gkunz will get back to this issue.

- #646 NCSC Vendor Security Assessment V.B.5 Unsafe functions - not used in vendor's released code · Issue
  - This was presented to the main SIG
  - More discussions needed. Collaboration with the C/C++ compiler guide and the memory safety WG and the Python security team.

    - Such kind of requirement can be tricky because it may create a push towards closed source implementation to hide well-known bad functions or - even worse - towards re-implementations.
    - We should bring this topic to the Full WG call

- #635 pySCG: Modifying the description of CWE-197 so that it captures the CWE better · Issue
    - Bart is working on CWE 1339
    - The suggested way forward is not bring in more CWEs and then discuss how to handle this weakness generally in the guide.
        -

2024-10-31 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
x	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac
x	Jon Williams	jrwil20@uwe.nsa.gov	NSA/ESF	he/him	

Agenda

- Welcome new friends
    - Jon Williams - working on memory-safe languages.
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    - Add to background more on *why* C and C++ will keep existing (PR #675)
        - Merged after brief discussion.
    - Fix fallthrough example macro to work with very old gcc versions (PR #681)
        - David noted we should add the specific version number in GCC that need the additional check, but that's not an objection not to include the proposed change. Thomas will open and issue for the addition.
    - Modernise Clang guidance (#624, PR #683)
        - David noted it would be great to point to more detailed information as a reference.
    - Compiler flags notes/comments (#330)
        - Consider -Wdangling-gsl and -Wreturn-stack-address for C and C++ Compiler Hardening Guide (#684)
            - On by default in clang, so ok to use
            - See if it's C++ only or also C; Note it's clang only (at this time). Note it's on by default.
        - Consider -ftrapv for C and C++ Compiler Hardening Guide (#685)
            - Based on a discussion, it was though the best option would be develop the 3.21 Integer overflow section to list all the relevant options (-fwarv, -trapv, -fno-strict-overflow, and `-fsanitize=signed-integer-overflow`.Thomas will make a proposal for text, and update the issue with the conclusions from the call.
        - Is #330 ok to close?
            - It was decided #330 is ok to close.
    - Safe++ concept
        - Article about it: https://www.infoq.com/news/2024/10/safe-cpp-proposal/
        - Proposal itself: https://safecpp.org/P3390R0.html#implementation-guidance
        - There's interest in safer C++, including this proposal.
        - This proposal isn't complete yet, nor is it implemented in gcc or clang.
        - Bjarne Stroustrup (creator of C++) "Delivering Safe C++" CPPCon 2023 presentation - https://www.youtube.com/watch?v=I8UvQKvOSSw
            - Being careful doesn't scale
            - US Government emphasizing memory safety, governments can coerce
        - ONCD report https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf

Opens

-

Guide Notes

- David’s slides on Improving Memory safety without a trillion dollars: https://docs.google.com/presentation/d/1EDQL-6MUKrqbILBtYjpiF96uW5LXcnIuE-HxzyClr68/edit#slide=id.g2ddb8e6973c_0_115
- Document available here: https://best.openssf.org/Compiler-Hardening-Guides/Compiler-Options-Hardening-Guide-for-C-and-C++
-

2024-10-22 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Georg Kunz* Co-chair	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Eddie Knight* [Baseline]		Sonatype		
x	Helge Wehder	helge dot wehder at ericsson.com	Ericsson	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Sean McGinn	sean.mcginn@amd.com	AMD	he/him	
x	Venu Vardhan Reddy Tekula	vt2182@nyu.edu	NYU	he/him	vchrombie

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Parris Lucas	ParrisLFX@linux.com	Open Studio Labs	he/him	groovecs
x	John Mertic	jmertic@linuxfoundation.org	LF	he/him	

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)

New Friends

-

Opens

Backlog Review

-

Meeting Notes

- NCSC Vendor Security Assessment V.B.5 Unsafe functions
  - Uplifted from discussion in the Python Secure Coding SIG (issue 646)
  - UK government has released a document with requirements for software vendors
    - this
    - One requirement is requesting to avoid "unsafe functions"
    - This is a very broad statement, not defining what an unsafe function actually is
  - Such kind of requirement could be tricky because it may create a push towards closed source implementation to hide well-known bad functions or - even worse - towards re-implementations.
  - For discussion:
    - What is the perspective of the group on this?
    - Can / should it be supplemented by more detail, e.g., technology (e.g., programming languages)

        - Can the OpenSSF create and publish a statement on this topic
        - Previous response by the OpenSSF
            - https://openssf.org/blog/2024/02/26/openssf-supports-efforts-to-build-more-secure-and-measurable-software/
    - Avishay
        - Memory Safety WG
            - It is nearly impossible to avoid unsafe functions entirely, for instance in drivers.
            - WG is advocating to avoid binary safe / unsafe classification
            - Memory safety is a continuum
                - https://github.com/ossf/Memory-Safety/blob/main/docs/memory-safety-continuum.md
                - Work in progress - to be published soon
    - Definition of "unsafe" is very broad / unclear
        - "There are no unsafe functions used within the vendor’s released code. Unsafe functions are those commonly associated with security vulnerabilities or those considered unsafe by industry best practise."
        - Is this only focussing on memory safety or vulnerabilities in general?
            - Example: is Python pickle unsafe?

- Potential future actions
    - Maybe an OpenSSF blog on this topic could be interesting

- Avishay did some housekeeping, assigning labels to open issues

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes

Memory Safety SIG (Nell)

- FULL SIG Notes
- The SIG is working on defining Scorecard probes
  - https://github.com/ossf/scorecard/issues/3736
  - Ecosystem / programming language specific probes checking for language specific memory issues
  - Based on
    - https://github.com/ossf/Memory-Safety/blob/main/docs/best-practice-non-memory-safe-by-default-languages.md and
    - https://github.com/ossf/Memory-Safety/blob/main/docs/best-practice-memory-safe-by-default-languages.md

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
- We ran SAST tools on the non-compliant code examples which are part of the guide
  - The tools didn't find many issues, which means that they have a hard time identifying real issues
  - https://github.com/ossf/wg-best-practices-os-developers/pull/653
  - Potential future work: integrate Python-specific SAST tools and run them on the code examples which are part of the guide

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
- Security Baseline
  - Request for feedback
  - https://github.com/ossf/security-baseline/blob/main/baseline.md
  - https://openssf.slack.com/archives/C07DC6TT2QY
- Development of Scorecard probes to check criteria

2024-10-21- Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Helge Wehder	helge.wehder@ericsson.com	Ericsson		myteron
X	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
X	David Mather	david.mather@ericsson.com	Ericsson		davidmather
X	Bart Karas	bartlomiej.karas@ericsson.com	Ericsson		

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Review of open issues
  - 657
    - It is a valid question. Maybe we can include the comment by Mitre in the Readme.
  - 652
    - Pending. A volunteer may pick this up.
  - 646
    - More discussions needed. Collaboration with the C/C++ compiler guide and the memory safety WG and the Python security team.
    - Such kind of requirement can be tricky because it may create a push towards closed source implementation to hide well-known bad functions or - even worse - towards re-implementations.
      - We should bring this topic to the Full WG call
  - 635
    - Bart is working on CWE 1339
    - The suggested way forward is not bring in more CWEs and then discuss how to handle this weakness generally in the guide.

    - 632
        - Pending. A volunteer may pick this up.
- Review of open PRs
    - 647
        - Georg will review. Hubert, too.
        - We should determine how to add more contributors to the team.
    - 669
        - This is great for new contributors
        - We should eventually mentioned this on the landing page / or better: in the contribution guide
            - Related to https://github.com/ossf/wg-best-practices-os-developers/issues/520
- The TAC election is upcoming
    - https://github.com/ossf/tac/blob/main/elections/tac-and-scir-election-process.md
- CCC
    - Helge has submitted a proposal covering the guide.

2024-10-17 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
X	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
X	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
X	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends

- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    - _FORTIFY_SOURCE recommendation is a timebomb (#659)
        - Jack noted that NIX OS injects build flags at the end using a wrapper. That might be a better way to build in-general as it does not assume projects adhere to a particular set of flag:
            - https://github.com/NixOS/nixpkgs/blob/9f589ea3a088fd2cdca91a14c0f59fb2331f972f/pkgs/build-support/cc-wrapper/cc-wrapper.sh#L177-L179
            - https://github.com/NixOS/nixpkgs/blob/9f589ea3a088fd2cdca91a14c0f59fb2331f972f/pkgs/build-support/cc-wrapper/add-hardening.sh
            - https://github.com/NixOS/nixpkgs/blob/9f589ea3a088fd2cdca91a14c0f59fb2331f972f/pkgs/build-support/bintools-wrapper/default.nix#L37-L63
        - David suggested we should also cover ways to set flags which allow them to be sanely overridden, e.g., AM_CFLAGS in Automake, possibly in a separate section covering different build systems.
        - We cannot tell Linux distributions what do do, but we can describe how the major ones set default flags, and suggest approaches to be compatible as many as possible.
    - _FORTIFY_SOURCE guidance confuses people, should suggest undefining with more care (as order matters) (#658)
    - Optimization option recommendations should have caveats (#660)
        - David thinks -fno-delete-null-pointer-checks has a strong justification, but we should revisit -fno-strict-aliasing, at least to ensure the description of the options covers the caveats pointed out in #660
    - Sanitizers need a bigger caveat with suid binaries at least (#661, PR #670)

Opens

-

Guide Notes

-

2024-10-08- Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob	christopher.robinson@linuxfoundation.org	Linux Foundation	he/him	SecurityCRob
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Parris Lucas	parrislfx@linux.com	Open Studio Labs	he/him	GrooveCS
x	Daniel Appelquist	dan@torgo.com	Samsung	he/him	Torgo

Agenda

- Is someone willing to scribe for the meeting today?
  - David A. Wheeler will help!
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- Baseline update
- EDU courses/accreditation update
- Memory Safety SIG updates
  - Safety Continuum
  - Scorecard Memory Safe checks
- Seeking new WG Lead/co-lead

    - There's no rule that CRob can't chair, but would like leadership be from community. Seeking lead or co-lead.
    - What are their roles, etc?
        - Generally, make sure the meetings work (which reviews existing work, starts new work, occasional collaboration), & report status up to TAC & report down from TAC to WG.
        - There's no formal term limit, but TAC elections occur annually in late fall, & we typically review chairs then. In this case, CRob would prefer to retire early.
    - BEST Issue 630
        - @balteravishay and @gkunz volunteered
            - Avishay Balter @balteravishay
            - Georg Kunz @gkunz
        - Both are long-term members, there was general consensus that they'll be our new co-chairs
    - WG chairs must periodically report WG status up to TAC
        - This was the last TAC update that can be used to start from going-forward - https://github.com/ossf/tac/blob/main/TI-reports/2024/2024-Q3-BEST-WG.md
- We encourage everyone to join in Tech Talk, Oct 10, 1:00PM EDT, Jumpstart Your Journey: Mastering OSS Security Development with the Linux Foundation Education
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Added ability for web admins to change project owners. Ownership changes don't happen often, but they happen, and now that we have many more participating projects they happen ~2/month. In the past we've had to run SQL commands to do this. This addition makes it easier & less error-prone.
- Updated dependencies due to a vulnerability in a dependency (puma). It's not clear this was exploitable, but our policy is to apply security updates as long as the functionality continues to work (as shown by our thorough tests).

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- ■ LFD121 enrollment - numbers update - David
  - All: While enrollment numbers for our free course "Developing Secure Software" (LFD121) have impressively grown, I must sadly report we have NOT yet met our 2024 annual goal as of 2024-10-04. I had reported earlier that we'd met our goal, but those numbers I reported appear to have been mistaken. Either the intermediate system had errors, OR David made multiple errors when calculating the summaries. To address the problem, I coordinated with LF Education. They have flushed & resynced the system that provides data to us ("Informer") and have performed various checks to verify that the data is now correct. We have also put steps in place to detect any related problems and created automated various summaries to reduce manual steps.
  - Our August 2024 LFD121 enrollments were 2,026 (not 2,292), and the enrollments of Jan-Sep 2024 where 6,296. The goal for this year is 7,990 (6658*1.2), a number I've been informally rounding up to 8K. To meet our official goal we need 1,694 (7990-6296) more enrollments over the next 3 months. We'll still try to reach our annual goal and we have plans in place to grow our enrollment numbers.
- LFD121 labs
  - ○ We have some labs, but some assignees haven't completed their assignments.
  - ○ David will probably jump in to make a few labs to complete the "most important" ones ("tier 1")
  - ○ We now have enough labs integrated into the course that it's worth telling the world. We're developing materials to announce that, e.g., as part of a new email campaign.
- Management course - reviewed by LF Education, David & CRob are incorporating feedback
-

Scorecard project (Laurent - Spencer)

- ■

EDU.SIG (CRob + SIG)

- FULL SIG Notes

-

Memory Safety SIG (Nell)

- Note: Memory Safety SIG notes have moved, will update.
- FULL SIG Notes (note: this is a corrected URL, which has also been corrected in the BEST WG repo)
- Safety continuum (Nell leading)
    - Memory safe isn't really a binary, there's a range. We're working to complete a description of these ranges.
- Scorecard (Avishay leading)
    - Memory checks, specific to specific programming languages
    - Have proposed it to Scorecard, using probes. Plan to start with 1 ecosystem (either Rust or Golang, probably start with golang).

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
-

WebDev Security Guide (Daniel Appelquist)

- BEST Issue 367
- I gave a talk at SOSS community day about this
- I also organized a session at W3C TPAC about it: https://www.w3.org/2024/09/25-mdn-security-minutes.html
- Focusing on information that is specific to web applications. Encourage people to get involved.
- Update on SWAG group - we've started a very early draft of web dev best practices doc. Patches and issues welcome.
- Minutes from our last call (yesterday) here: https://github.com/w3c-cg/swag/blob/main/meetings/2024-10-07-minutes.md

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
- Baseline criteria 1.1 ready for comment!
-

2024-10-07 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Helge Wehder	helge.wehder@ericsson.com	Ericsson		myteron
X	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
X	David Mather	david.mather@ericsson.com	Ericsson		davidmather
X	Noah Spahn	noah.de@gmail.com	Open University		noah-de

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

Guide Notes

- Meeting time
  - **Georg**: Create a new Doodle to find a new meeting time.
- Issue #635 Modifying the description of CWE-197 so that it captures the CWE better
  - We got feedback from a contributor we met in Vienna
  - Helge will comment on the issue
- Issue #632 Python Hardening Guide: we should mention and explain audit hooks, sys.audit and sys.addaudithook

- CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
  - **Question**: in case of running processes with shell commands: is it more secure to use the shell commands as part of a command (string) or use dedicated libraries (such as pathlib, fsutils).

    - What is the position of the CPython developers?
        - **Helge**: describe the question in a GitHub issue & reach out out to Seth Larsson on Slack
        - Created issue: https://github.com/ossf/wg-best-practices-os-developers/issues/654
- Unsafe functions
    - https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf
    - "V.B.5: There are no unsafe functions used within the vendor's released code."
        - What is an unsafe function?
        - How does this map to Python?
            - One example: eval function
            - Are there other examples?
        - Sources of information
            - PEPs
            - CWEs
        - **Helge**: create an dedicated GitHub issue to collect input and examples of potentially unsafe functions in Python
        - Done: https://github.com/ossf/wg-best-practices-os-developers/issues/646

    - Corresponding CWE: https://cwe.mitre.org/data/definitions/94.html

- Valuable additions to the current material - contributions welcome
    - Identifying actual CVEs for the CWEs
    - Tool automation: create GitHub actions to run static code analyzers on our code examples
        - Example: Bandit

2024-10-03 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
X	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler

X	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
  - Describe linker configuration options (#623, PR #626)
    - The group is happy with this additional kind of material. There are some comments that need to be addressed. Let's work it on GitHub PRs, if they work out, we plan to accept before next meeting.
  - Add note on PT_GNU_STACK on 32-bit x86 (PR #622)
    - This is a minor clarification. Group agreed, merged.
  - Add note on enabling RELRO for library dependencies (PR #640)
    - Group reviewed, proposed some minor improvements to the text to make it clearer and simpler. Group agreed to add it (as tweaked).
- More generally, Thomas plans to add binary checkers, lets you record options. Haven't had time to do it yet.
  - David: Also: in CI/CD check to ensure that some options like RELRO will actually work (it will be quietly disabled if one new library being added doesn't have it enabled). This is easier to check for embedded systems (because you control everything). Obviously, if the compiled application is later loaded into a different environment, that other environment might have a different result. Another solution is initialization-time checking ("only run if option X is working") - not sure how difficult that is in this case (might not be portable). Probably need to investigate.
  - Ideally, the first draft will be ready next meeting. This will be a bigger chunk of work.

Opens

- Thomas gave a talk on the Compiler Options Hardening Guide at NSSS'24. Slides available at conference site: https://nsss.se/y2024/talks/compiler-options-hardening-for-c-and-c/
  - We need to help people learn about the guide (if they might want to use it). Let's keep our eyes open for this, Thomas is open to presenting it again.
  - Would Thomas be open to recording the talk & posting on Youtube? FOSDEM version already has a recording. NSS is longer, it had more info. We might be able to re-post FOSDEM version.
  - How can we help more people learn about the guide? In late 2023 we did an OpenSSF blog about the compiler options guide, but should we do more? What about those outside OpenSSF?
  - It'd be good to the word out to those outside OpenSSF. Maybe the compiler communities more directly?

-

Guide Notes

-

2024-09-24 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Mickaël Salaün	mic@digikod.net	Microsoft	he/him	l0kod
x	Venu Vardhan Reddy Tekula	vt2182@nyu.edu	NYU	he/him	vchrombie

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
    - Seeking new WG Leads - https://github.com/ossf/wg-best-practices-os-developers/issues/630

- Sub-project updates (as needed)
- [DavidW] A few fixes proposed for “Correctly using Regex” table https://github.com/ossf/wg-best-practices-os-developers/pull/629 - merged.
- [Avishay] .Net support in Scorecard
    - https://github.com/ossf/scorecard/issues/1578
- [Mickaël] What about Landlock sandboxing at OpenSSF?
    - Landlock: unprivileged access control — The Linux Kernel documentation
    - landlock-lsm/rust-landlock: A Rust library for the Linux Landlock sandboxing feature (github.com)
    - landlock-lsm/go-landlock: A Go library for the Linux Landlock sandboxing feature (github.com)
    - Last week talk’s at OSS: Open Source Summit Europe 2024: Linux Sandboxing with Landlock - Mickaël... (sched.com). E.g., 3 tools that build on top of Landlock are:
        - setpriv
        - Firejail
        - Minijail
    - David: There are many things we could do. We could develop guidance documents
      “How to do x?”. What about bubblewrap, etc., what are the differentiators?
    - Suggested he open an issue to get the word out to the larger group to see if anyone has feedback; possibly look at putting this info into a “concise guide”
        - Project idea: Security sandboxing guidelines · Issue #631 · ossf/wg-best-practices-os-developers (github.com)

New Friends

- Mickaël Salaün
    - GitHub - l0kod
    - Email - mic@digikod.net
    - About me - I’m the kernel maintainer of Landlock, the Linux unprivileged access control system designed for sandboxing: https://landlock.io

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

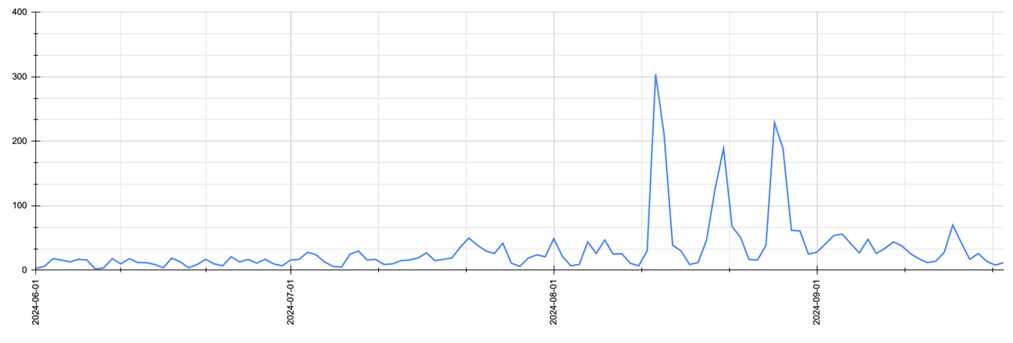
(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Our TLS certificates didn't update automatically on 2024-09-09, it was fixed hours later. That said, we always try to create a post-mortem to learn from. Now available: "final" draft of "Post-mortem Report for OpenSSF Best Practices Badge TLS Renewal Failure on 2024-09-09" https://docs.google.com/document/d/1DhJ582xZoW7BvhsPqhvSi1XfYy-l-aF5duqewO8Kbt4/edit#heading - comments welcome!

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- Security for Managers - making progress. Divided into small video sections (per request from LF Education), created quizzes & first draft final exam
- LFD121 course
  - Distributed flyers at Open Source Summit EU, many interested!
  - LFD121 enrollments have been great, see chart below of last few months.
    - In particular, we did an email campaign of 3 emails to people who had expressed an interest in LF materials, and on those days there was a fantastic response.
    - There was a recent spike on 2024-09-17; we need to track down & verify its cause, but that was during Open Source Summit Europe & we suspect it was caused by our outreach there.



LFD121 daily enrollments (recent)

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- Academic Accreditation program continues to work with legal and hopes to announce program at Kubecon this fall
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
-

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
- Working on compliance crosswalk & rephrasing of requirements
-

2024-09-23 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

X	Bartlomiej Karas	Bartlomiej.Karas @ericsson.com	Ericsson		BartyBoi1128
x	Helge Wehder	helge.wehder@ericsson.com	Ericsson		myteron

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Discuss a potential public kanban board?
- Recap of presentation at SOSS Community Day EU
    - We got a pitch from a vendor of a static code analysis tool
    - Another question asked for Python-specific weaknesses which would not be valid in other languages. Pickle is a good example.
    - We had a good few conversations at the OpenSSF
- Community growth activities
    - Blog post
    - Reach out to Seth / PSF to determine how to achieve a regular exchange between PSF security work and this guide
    - Potential additional / new rules:
        - based on CVEs
        - Based on CWEs + CVE + applicable to Python
    - List of existing content available here: https://github.com/ossf/wg-best-practices-os-developers/issues/531
- [Potential] Improvements
    - Make content more consumable: add description to directory name
        - Improve rendering of content to a web page for those who want to consume the guide on the web
    - Collaboration with GitHub gamification project
        - https://skills.github.com/
    - Host the guide in a separate repository
        - Check OpenSSF governance wrt to whether or not we could get a separate repository

Opens

-

Guide Notes

-

2024-09-19 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
x	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    - Compiler flags notes/comments (#330)
        - Clarify the interaction between trampolines and -Wl,-z,noexecstack (PR #611)
            - David noted that GNU GNAT has to handle nested functions, and at least used to handle this through GCC-generated trampolines Other languages also must handle nested functions, and if trampolines are used there is a conflict. We believe the new wording better handles and explains this case.
            - Modern 64-bit systems generally support this. Probably not correct to say every every 32 bit system supports this. Thomas will add a note in a separate PR to address this.
            - This is a large change, let's merge as it is, if we want to clarify further we'll do that separately. GCC supports a lot of processors, it's hard to make claims across all processors. Maybe at the top

        we should note that some options are only supposed by certain processors and/or chipsets.

        - Clarify -D_FORTIFY_SOURCE interaction with optimization levels (PR #620)
            - William noted that the addition is valuable as the is in general confusion around the optimizations and -D_FORTIFY_SOURCE is quite common
            - Some binary checkers cause false positives with -D_FORTIFY_SOURCE
            - Let's merge this one as-is, it's a big improvement, we can separately create a sentence or two in the same section to warn about binary checkers producing false reports about problems (this can happen if the option is enabled but there's no case where the more detailed call is generated). William volunteered to add an additional note on binary hardening.
    - There's a new LLVM release, we need to see if they've finally added the C++ options for hardening. If so, then we'll add that.

Opens

-

Guide Notes

2024-09-10 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Cristian Urlea	cristian.urlea@glasgow.ac.uk	University of Glasgow		cristianurlea
x	Laura Voinea	laura.voinea@glasgow.ac.uk	University of Glasgow		LauraVoinea
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Reden Martinez	rmartinez@linuxfoundation.org	LF	he/him	
x	Prince Oforh Asiedu	prince14asiedu@gmail.com			princeasiedu

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)

New Friends

- Cristian Urlea
  - Slack - @Cristian Urlea
  - Github - cristianurlea
  - Email - cristian.urlea@glasgow.ac.uk
  - About Me - Postdoctoral researcher at the University of Glasgow. Advocating for the use of Formal Methods, Programming Language Theory, Type System Theory and Runtime Verification to strengthen security in Software Development, Build Systems and Supply Chain Integrity.
- Laura Voinea
  - Slack - @Laura Voinea

    - Github - LauraVoinea
    - Email - laura.voinea@glasgow.ac.uk
    - About Me - Postdoctoral researcher at the University of Glasgow. Advocating for the use of Formal Methods, Programming Language Theory, Type System Theory and Runtime Verification to strengthen security in Software Development, Build Systems and Supply Chain Integrity.

Opens

- Cristian - coming from a direction of seeing how many best practices can be automated - e.g. evidence of that having happened. Is there any appetite for that level of automation here?
    - Crob: that's what our scorecard project does a lot of…
        - Cristian: scorecard produces human readable evidence
    - Crob: then "allstar" project can try to fix things that Scorecard notes… e.g. by filing PRs…
        - Mention of Scorecard/Allstar bi-weekly meeting next Monday
    - Cristian: i want to get to : a build platform … not relying / trusting the build platform - but audit trails for the entire build process to see if that has happened…
        - Mention of SLSA Specification meeting also next Monday
- David: we need people to help with labs. Please contact me - we have a list of labs we need to create.

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Yes, the TLS cert expired last Monday. We fixed it soon afterwards. We have automation, but there was an authentication failure that led to failure of the automation. We're investigating.
    - Georg notes this broke an internal build process in his organization.
- May want to add some improvements for security baseline

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- One of the OpenSSF staff's objectives has been met, regarding LFD121 enrollment!! We had wanted at least 8K enrollments this year. LFD121 enrollment has seen a dramatic increase in the last two months. The month of August had 2,292, far surpassing July (our previous record setter). By the end of August we had 8,966 enrollments in LFD121, exceeding our goal of 8,000 enrollments for the year. This is remarkable, since earlier we were concerned that we might not meet our goal this year. My thanks to everyone who spread the word, and especially to Sally & Angelah (marketing), who have worked tirelessly with me to find ways to get the word out.
- We're working on marketing project.
- Management course. Slides here: https://docs.google.com/presentation/d/19IolYrumwUa7qHV65OW0IJ-oTpLV0I2KqEVGzjf0FSI/edit - Crob says almost mission accomplished. Crob & David will be asking for feedback.

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- Security for dev mgrs course ready for broader review; look for forthcoming email & slack for details to provide feedback!
-

Memory Safety SIG (Nell)

- FULL SIG Notes
- Still making progress. Working on putting together a workshop. It's not JUST "convert to Rust".

C/C++ BP Guide SIG (Thomas)

- GeorgIssue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler-Hardening-Guides
- Continuing, new content continues to come in.
- This guide is very mature, so the discussions are often "complex & geeky".
- There'd been discussion about CPython using the guide.

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
- Still early work. Working on growing the group.

-

WebDev Security Guide (Daniel)

- BEST Issue 367
- SWAG group met this week https://github.com/w3c-cg/swag/blob/main/meetings/2024-09-09-minutes.md we talked about CSP and federated identity.
- We're planning a session at TPAC 2024: Overview (w3.org) - 23-27 September in Anaheim, CA. Session will be on the 25th (timing tbd).
- Dan will be speaking at SOSS Community Day Europe
- SWAG issues here: Issues · w3c-cg/swag (github.com)

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
- Working on compliance framework crosswalk to help levelset the baseline
- Thinking through ways to streamline things and perhaps update BP Badges
- Originally "security baseline" was focused only OpenSSF & what project should do beyond current requirements (like best practices badge). Now it's being devised so it could be applied further, at least to other LF foundations, and perhaps others.
- In that process, we noted that security-insights doesn't cover many best practices badge items. After discussion, worked out a way to completely resolve this: https://github.com/ossf/security-insights-spec/issues/93 - if you have thoughts about this approach, please comment there!
    - Cristian: looking for alignment with the work we're doing …
    - Crob: the "crosswalk" does that …
    - David: this has focused on "why don't we do this for other LF projects and create a spec that others can re-use if they choose to do so…"

2024-09-09 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Bartlomiej Karas	Bartlomiej.karas @ericsson.com	Ericsson	He/him	BartyBoi1128

x	Helge Wehder	Helge dot Wehder at ericsson dot com	Ericsson		myteron
x	Noah Spahn	noah.spahn@open.ac.uk	Open University		noah-de

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
-

Opens

- CVSS EPSS CWE vulnerability patterns

Guide Notes

-

2024-09-05 - C/C++ Compiler BP Guide - 0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
x	Prince Asiedu	prince14asiedu@gmail.com			princeasiedu

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
  - New/Updated Issues/PRs:
    - Update compiler guide contributors (#587)
      - Merged by Thomas before the call
    - Runtime enable info for Intel CET shadow stack (PR #563)
      - William noted that different programming languages have consideradions around support across OSs, e.g., golang issue https://github.com/golang/go/issues/66054
      - Should ask Red Hat / Gentoo representatives about userspace support in distros
      - Merged
    - Improve description of control-flow protection (PR #586)
      - Thomas will merge after fixing conflicts
    - Compiler flags notes/comments (#330)
      - Discourage use of -mmitigate-rop (#589, PR #608)
        - Merged
      - Clarify the interaction between trampolines and -Wl,-z,noexecstack (PR #611)
        - Leaving open on Github for further review

Opens

- Nate Ohlsson's CPython Compiler Hardening Summer Retrospective http://nohlson.com/blog/CPython-Compiler-Hardening-Summer-Retrospective/
- Wireshark hardening compiler options https://gitlab.com/wireshark/wireshark/-/issues/19995

Guide Notes

2024-08-27- Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Daniel Appelquist* [TAC]	daniel.appelquist@partner.samsung.c	Samsung	he/him	Torgo

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
		om			
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Eddie Knight* [Baseline]		Sonatype		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Prince Asiedu	prince14asiedu@gmail.com			princeasiedu

Agenda

- Is someone willing to scribe for the meeting today? Dan & David
- Welcome new friends
    - Prince - Python developer Ghana
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)

New Friends

- Prince Oforh Asiedu
  Slack - @__bm6
  GitHub - princeasiedu
  email - prince14asiedu@gmail.com
  About Me - I am a newbie seeking to learn, grow and contribute to the open source landscape. [software developer from Ghana]

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Officially switched licenses for data as of 2024-08-23 to **CDLA-Permissive-2.0** license updated data. The Linux Foundation legal team has asked us to use the CDLA-Permissive-2.0 license for newer data. This is an *extremely* permissive license, we've noted this change with lots of warning, and it's a requirement for our legal formation.
    - https://spdx.org/licenses/CDLA-Permissive-2.0.html
- GDPR impact: person has asked to have account deleted, but project badge entries must have an owner. Have contracted project & trying to transfer to someone else, since otherwise would have to delete the badge entry (not desirable!).

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- EDU SIG notes
- LFD121 - tell more people! More enrollment! - https://training.linuxfoundation.org/training/developing-secure-software-lfd121/ Need word spread on this free course
    - Accepted by “Tradewinds AI” -US Gov program related to AI - and this course has an AI section - we hope this will give awareness of course to many who otherwise wouldn’t have heard about it.
- Labs
    - Wrapped up a shall injection LAB…
    - A SQL injection lab is stalled…
    - Some volunteers haven’t delivered…
    - https://best.openssf.org/labs/ - esp. “PLANNED-1 UNASSIGNED”
    - Q: What are the most pressing labs? A: wh
        - Daniel - will contact someone to see if can help, for XSS.
- Manager course
    - Reorg - Bottom Line Up Front (BLUF)
- Security architecture
    - Labs are a challenge for this abstract a topic - suggestions welcome

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
- Group of contributors is still growing (join us and be part of the group!)
  - https://github.com/ossf/wg-best-practices-os-developers/pull/587/files
- Presentation as Nordic Software Security Summit upcoming
  - https://nsss.se/y2024/talks/compiler-options-hardening-for-c-and-c/

Python Hardening Guide SIG (Helge & Georg)

- Tracking of content in issue 531

WebDev Security Guide (Daniel)

- BEST Issue 367
- Work has been continuing in the issues Issues · w3c-cg/swag (github.com)
  - Work item: come up with a set of security criteria for packages · Issue #1 · w3c-cg/swag (github.com)
  - Security Features List · Issue #2 · w3c-cg/swag (github.com)
  - How can we help CSP gain more adoption with Web Developers · Issue #3 · w3c-cg/swag (github.com)
  - David: a whole section on CSP in the 121 course… Though nothing on TurstedTypes yet…
    - Here's a link to the LFD121 text about Countering Cross-Site Scripting (XSS) https://github.com/ossf/secure-sw-dev-fundamentals/blob/main/secure_software_development_fundamentals.md#content-security-policy-csp
    - LFD121 doesn't discuss Trusted Types, since we want something that's widely supported by many browsers (Firefox & Safari don't support them yet)

        - https://developer.mozilla.org/en-US/docs/Web/API/Trusted_Types_API
        - Dan believes this is a matter of developer time, there’s general agreement in adding it.
-

Security Baseline SIG (Eddie & Michael)

- Meeting Minutes
- Eddie: presents timeline board… We did a survey in places like CNCF and Finos… Was suggested that we look at work in OpenJS Foundation… They have a baseline definition. We’re refining this list of suggestions including the list from OpenJS… Compiling into a master list. *presents spreadsheet* Please attend the SIG calls and trying to get agreement… Sandbox definition by next week…

2024-08-26 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson		gkunz
x	Bartlomiej Karas	bartlomiej.karas@ericsson.com	Ericsson		ebakrra

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
-

Opens

-

Guide Notes

- Currently there no open PRs
- Two more rules are currently under review and will be pushed shortly
- Upcoming presentation at SOSS Community Day EU
    - For reference: Thomas Nyman on the C/C++ guide
        - https://fosdem.org/2024/schedule/event/fosdem-2024-3468-compiler-options-hardening-for-c-and-c-/
    - We should start thinking about creating a presentation soon
    -

2024-08-22- C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    - Runtime enable info for Intel CET shadow stack (PR #563)
        - William will give an update on state of Glibc tunables in next meeting
    - Improve description of control-flow protection (#586)
        - No objections, Thomas leaves PR up for review on Github
    - Add Wl,--as-needed and -Wl,--no-copy-dt-needed-entries (#510, PR #571)
        - Merged
    - Update compiler guide contributors (#587)

- Leaving up on Github for new contributors to acknowledge and any additions.
- Compiler flags notes/comments (#330)
  - Consider -Wl,-z,separate-code (#588)
    - Check for potential contra-indicators for resource constrained systems as the option may impact the program image layout / padding etc.
    - Check whether already enabled by default in any distributions
  - Discourage use of -mmitigate-rop (#589)
    - William noted that the 2018 deprecation notice should be linked in the description for the rationale and why the option is “security theater” -like
    - William volunteered to write-up PR on #589
  - Refer to 'RIP-relative addressing' in position-independent code description (#590)
    - William noted that PIC does not necessarily require RIP-relative addressing, but in practice it’s the most common way to realize (on x86_64)
    - Merged

Opens

-

Guide Notes

-

2024-08-13 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [SCM]	dan@torgo.com	Samsung	he/him	Torgo
x	David A. Wheeler*	dwheeler@linuxfou	Linux		

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
	[Badges + courses]	ndation.org	Foundation		
x	Eddie Knight* [Baseline]		Sonotype		
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	

Agenda

- Is someone willing to scribe for the meeting today? - Dan
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- TAC PR 359 - BEST WG read-out
- Baseline WG Latest

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

- Crob: next TAC meeting we will be doing an update from the Best wg. See TAC PR 359 - please leave updates in that PR if you would like something added to this…

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- “Developing Secure Software” (LFD121) fundamentals course
    - We’re taking many steps to make people more aware of it.
        - DEF CON flyers, emails to OpenSSF participants, emails to those who are not necessarily OpenSSF participants, etc.
        - Please help! Let others know about LFD121!
    - About to add the first set of labs to LFD121
        - We want more labs. Several volunteers didn’t actually make labs, still need help. Please contact David A. Wheeler dwheeler <AT> linuxfoundation.org
- Still working on security architecture

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
- Many documents need to be worked on so they can be published… We also have a slot in SOSS community day…
- Gegorg: we are wondering about time slot… [for call] … not a lot of external participation…
- Crob: let’s get this on the TAC call for next week.

- Helge: We have the one issue - https://github.com/ossf/wg-best-practices-os-developers/issues/531 - working through things to add…
- Crob: let's do a community **office hour** about this. Staff should be able to help set this up.
- Crob: other ideas: blog post, SOSS community day breakout session (community meeting) …

WebDev Security Guide (SWAG) (Daniel)

- BEST Issue 367
- Minutes from this week's call: https://github.com/w3c-cg/swag/blob/main/meetings/2024-08-12-minutes.md
- Update on discussion regarding use of Scorecard to score packages….
- https://github.com/w3c-cg/swag/issues/1
- Also doing a (short) session at SOSS community day

Security Baseline SIG (Eddie & Michael)

- Meeting Minutes
- Support required for this SIG - as the OpenSSF person assigned to this is no longer at OpenSSF. Dana designed the baseline for OpenSSF… she pushed it through with TAC and got approval. She was working with a list of projects to roll it out to. Looking for thoughts and input.
- Dan: I think *we* should ask OpenSSF management to help fill this gap. TAC supported this. As a TAC member I would support the call for additional resources…
- Crob: I will help fill the gap - and see what Dana had committed to and then line up a conversation with OpenSSF management next week.
- Eddie: So what is the direction TAC would like to see for Baseline?
- Crob: from my PoV it will be nice to have a set of criteria - requirements - pushed out and then see that certain projects have gone through these and hit a certain standard. From that we can show that either it was a moderate amount of work, or it was a lot. Us showing off that OpenSSF projects have done this can show other projects (such as finos) to do the same.
- Dan: One criticism is "too much work" - need to show this is the bare bones, not too much work, really important, etc.
- Chris: this intersects with an effort within OpenJS foundation **security group…** OpenJSF has developed security guidelines for OpenJS Foundation projects… ranging from SCM practices to other things… Some OpenSSF guides were cross-referenced for these … almost ready to socialize that more broadly. Would like this group to review these items. That could be a resource for Baseline. Painstaking iteration … "our target audience is open source maintainers" - so sensitive to demands on their time and also prioritizing…
- Eddie: we're trying to categorize these based on project maturity level - sandbox, incubating, graduated…

- OpenSSF/CNCF list of levels (not including “archived”):
    - Sandbox
    - Incubating
    - Graduated
- Chris: that is there - OpenJSF foundation projects are at levels : incubating, at-large and impact. There are some deltas… we didn’t distinguish between at-large and impact. Also OpenJSF meets on Mondays at 10:30 AM central time…
- Dan: please share with SWAG group as well…
- David: We should use numbers for the tiers, and then show common mappings – of allow a group to NOT use their levels
- Best practices badge - can have a minimal requirement & foundations can add higher requirements
- Eddie: … not mapping to a level allows e.g. OpenJS to map as appropriate…

2024-08-12 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Bartlomiej Karas	bartlomiej.karas @ericsson.com	Ericsson	he/him	BartyBoi1128
X	Thomas McDermott	thomas.mcdermott@ericsson.com	Ericsson	he/him	tommcd
X	Paulus Gandung	paulus.gandung @efishery.com	eFishery	he/him	plvhx
X	Helge Wehder	Helge . wehder at ericsson	Ericsson		

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Reviews
    - PR 573

- Presentation at SOSS Community Day EU
  19 September 15:00 Schedule | LF Events (linuxfoundation.org)

Opens

-

Guide Notes

- Time slot
  - This times lot works for the core contributors from Ericsson, but we'd like to grow the community. It seems we need to run a new Doodle poll. Helge and Georg are planning to join the Full WG call tomorrow to socialize this idea.
- Presentation at SOSS Community Day EU
  - This is meant to advertise and socialize the activity with the larger community
  - Discussions about who will present are still ongoing
- Review of PR 573
  - Condensed the text to make it more concise
  - Ready for review

2024-08-08 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
X	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
X	Gabriel Dos Reis	gdr@microsoft.com	Microsoft		GabrielDosReis
X	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani
X	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
X	Paulus Gandung	paulus.gandung@efishery.com	eFishery	he/him	plvhx

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting? William H.
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    - Create guidance on using buffer overflow attributes in C ([#551](#551))
        - New attribute that contains real time size of buffer to allow for additional bounds check in real time
        - Being added by the Linux kernel
        - Is not a compiler switch per se (so not strictly related to this group), but is a related language feature
        - Gabriel: probably too early to recommend, it's still under active development and is subject to change, the C and C++ committee are also discussing this separately from compiler communities
        - Thomas: more properly belongs in the C/C++ Annotations Guide (https://github.com/ossf/wg-best-practices-os-developers/blob/main/docs/Compiler-Hardening-Guides/Compiler-Annotations-for-C-and-C%2B%2B.md)
        - Decision was to not add to compiler flags or annotation guide, but to keep the issue open for monitoring, possibly add a label for scenarios like this?
    - Runtime enable info for Intel CET shadow stack (PR #563)
        - Extension of control flow integrity checks section
        - Documents that the feature requires Linux kernel 6.6+, glibc 2.39+, and setting of the GLIC_TUNABLES environment variable
        - Linux distributions do not currently enable this by default
        - Will: Intel (i.e. Will) will look into this to figure out the proper guidance for gcc vs clang
        - Will: Will look into IBT glibc tunables as well
        - Decision was to defer while Will looks into it
    - Contribute scraper script for compiler options hardening guide (#549)
        - Thomas: tried it and it works, but current merge conflict
        - Decision was for Georg to look at it offline, Mayank fix the merge conflict, then merge it
    - Add Wl,--as-needed and -Wl,--no-copy-dt-needed-entries (#510, PR #571)
        - -Wl,--as-needed:
            - Affects linker's behavior for what libraries are included during linking
            - Reduces attack surfaces via less code, omits static initializers when not needed
            - Could possibly affect applications that depend on static initializers, but this is expected to be an edge case
            - Default behavior in GNU linker since 2.22
        - -Wl,--no-copy-dt-needed-entries

        - Requires user to list transitive dependencies explicitly when linking
        - Better informs users what exactly they're linking in
        - Default for many Linux distributions
      - Decision was to leave online for a bit for community to have more time to look at, then merge

Opens

- Thomas will deliver talk on the Compiler Options Hardening guide at the Nordic Software Security Summit in Stockholm, September 23-24
- Just for info: Guide has been made part of the Security Baseline for OpenSSF projects
  - The security baseline recommends for OpenSSFprojects in Sandbox state to reduce the risks of memory-based vulnerabilities by evaluating and adopting the C/C++ Compiler Option Hardening Guide, if the project is written in C/C++
  - https://github.com/ossf/tac/blob/main/process/security_baseline.md#security-baseline---once-sandbox
- Just for info: For the SOSS Community Days in Vienna, it is planned to run a Table Top Exercise (TTX). It is planned to use a memory-based vulnerability in the scenario and the guide will be mentioned as one means to minimize the risk of future memory-based vulnerabilities.

Guide Notes

2024-07-30 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	daniel.appelquist@samsung.com	Samsung	he/him	Torgo
x	Eddie Knight	eknight@sonatype.com	Sonatype		
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Justin Gosses		Microsoft		
x	Adrianne Marcum	amarcum@linuxfoundation.org	OpenSSF	she/her	afmarcum
x	Reden Martenez		LF		

Agenda

- Is someone willing to scribe for the meeting today? - Dan A.
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- LFD121 course (“Developing Secure Software”) - please let everyone know about it, we want more to enroll!
    - Please encourage people to sign up for this
    - https://openssf.org/blog/2024/07/08/learn-how-to-develop-secure-software/
    - https://training.linuxfoundation.org/training/developing-secure-software-lfd121/
    - Planning to drop edX support for LFD121, edX charges for cert of completion
- LFD121 labs - many who said they’d contribute a lab by July 19 have not. Anyone willing to contribute a lab? Takes < day!
    - Need some volunteer help to make labs.
    - Crob: some potential volunteers from the education SIG - see slack.
    - Eddie Knight: we are getting ready to launch integration between CNCF and Finos with baseline effort. Do we want to tap into those same channels to extend a request to content creators?
    - Crob: yes.
- Welcome Security Baseline SIG! - Eddie Knight
    - https://forms.gle/Cr2iSBUDK3nbEtSy6 <- gathering feedback on the baseline OpenSSF has adopted… what changes would we need to see? Survey is intended to be wider than the openSSF. Also Dana will be collaborating with several projects in OpenSSF that have agreed to pilot the baseline… once that wraps, we are going to in and see how we refine and adapt to be “the open source project security” baseline. Goal: by end of the year ~50 projects will be covered.

    - This is not intended to be a survey to post on social media. Instead, want people to take it if their opinion would be valuable. OSS project maintainers, etc.
- Update on W3C SWAG community group: [Security Web Application Guidelines Community Group (w3.org)]() - Daniel App
    - Live group, meeting weekly for past 3 weeks. Mozilla, W3C appsec WG, Google, OWASP, OpenJS, etc.
    - Working on Threat model doc..
    - Members
- https://github.com/ossf/wg-best-practices-os-developers/issues/557 - Justin Gosses
    - This is regarding cross linking between OSSF guidance on source code configuration (SCM) and InnerSource Commons guidance on SCM.
    - Both orgs are non-profits. Some of the same company involved.
    - Basically just proposing a link that says something like "for another perspective on SCM for internal only code platforms see...". This style of link always exists on InnerSource Commons content.

New Friends

- Eddie Knight - leading security baseline SIG
- Justin Hosses - Microsoft

Opens

-

Backlog Review

-

Meeting Notes

- Justin Gosses presents: [Complete crosslink between OSSF and **InnerSource Commons** SCM guidance · Issue #557 · ossf/wg-best-practices-os-developers (github.com)]()
- Similar to the documentation that you currently have … it's for an internal platform… a lot of overlap there - innersource commons - already links out to the best practices guide… We're supporting a cross-link back. I understand a reluctance to endorse… so maybe "OpenSSF doesn't endorse this guide but … it's available to look at as it's coming from a slightly different perspective."
- David: there's no policies against links - our only challenge is that if we link to a product then we endorse one commercial product over another - so as long as it helps our readers then cross-linking sounds wonderful. You've raised the general issue… do you want to come back and propose some specifics?

- Justin: in the github issue there is a link to the innersource commons: https://innersourcecommons.gitbook.io/managing-innersource-projects/innersource-tooling one way … a guidance page.
- Dan: any commonalities between this and SCM guide? Also any differences in recommendations?
- Justin: your guide is written with the assumption of public repositories - whereas ours is written from the perspective that it's a platform just for internal code. So some of the guidance around new repositories and forks will be different.
- David: since it's a different circumstance I don't think we need to say they're identical. We could say "for additional guidance for inner sourcing, consider… : <link>". I'd suggest a pull request with suggested text.
- Justin: OK - I can do that.

- LF T&C - **Scorecard course**, etc.? Should they be labeled as "OpenSSF Course"?
- David: we put an openssf logo on the course and cert of completion… and then raised the followup question: which courses would this apply to? We do want to put logos on the right courses. We no LFE is in that list… we presume scorecard is on that list…
    - Scorecard? I know the Scorecard course is a year out of date, it needs to be updated. Should we update it before we put an "OpenSSF" logo on it?
        - David: Changes weren't radical
        - Eddie: True, but it doesn't mention GitLab (it was released before that)
    - LF Express 1006/7/8 - 45 min course. Not sure they're OpenSSF related.
    - David: focusing on the scorecard - we should update it… whether or not it has the logo …
        - Doesn't note that we now have gitlab support. That should be added.
    - https://training.linuxfoundation.org/express-learning/automating-supply-chain-security-sboms-and-signatures-lfel1007/ - middle, sort-of OpenSSF, wasn't requested by OpenSSF, splits difference
    - https://training.linuxfoundation.org/express-learning/securing-projects-with-openssf-scorecard-lfel1006/ - definitely OpenSSF
    - https://training.linuxfoundation.org/express-learning/security-self-assessments-for-open-source-projects-lfel1005/ - wasn't originally created by OpenSSF at all, it's a CNCF internal thing from CNCF TAG. "One day threat model".
    - David: No need to delay Scorecard logo to update note about GitLab. We should at least note it, but those could be in parallel
    - David: Let's start with the obvious & focus on that.
    - Eddie: It's not clear to me how to maintain it.
    - [discussion on how to edit course material] - Eddit will email David with request, David will forward & get the right people connected.
    - *General agreement that Scorecard course should be labeled as an OpenSSF course.*

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

    -

Scorecard project (Laurent - Spencer)

    -

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
-

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & Dana)

- Meeting Minutes

2024-07-29 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Georg Kunz	georg.kunz@ericsson.com	Ericsson		gkunz
X	Bartlomiej Karas	bartlomiej.karas@ericsson.com	Ericsson		ebakrra
X	Thomas McDermott	thomas.mcdermott@ericsson.com	Ericsson	he/him	tommcd

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

Opens

-

Guide Notes

- Review of open PRs
  - https://github.com/ossf/wg-best-practices-os-developers/pull/566
    - Currently in draft state, Thomas will further update this
- Presentation of the Python Guide has been accepted at OpenSSF Community Day EU
  - https://events.linuxfoundation.org/soss-community-day-europe/program/schedule/
- AOB
  - Georg to arrange (again) for merge permission for Helge

2024-07-16 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Dana Wang	dwang@linuxfoundation.org	OpenSSF	She/Her	danajoyluck
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- [DanaW + Eddie] new SIG proposal - OpenSSF Baseline
  - In-flight PR with initial load for OpenSSF Baseline - https://github.com/ossf/tac/pull/353/files
  - LF-wide effort, from LF Summit
  - Proposed SIG leader - Eddie Knight
  - CRob agreed to be sponsor for the OSSF Baseline SIG
  - List of things to be done, organized by levels (sandbox, etc.)
  - Intent is to make it useful for multiple foundations
  - Capturing adoption in addition to what to implement, effectiveness. Looking to add "use-cases" to white paper.
  - Targeting different foundations as potential adopters.
  - "Smoke-testing" before pushing for wider adoption.

    - Already talked to FINOS and CNCF, some buy-in from CNCF TOC already.
    - OpenSSF Best Practices WG is a good place for this, as we focus on identifying best practices (for security). Identifying best practices in general is a good thing. This suggests a good synergy.
    - Vote. Unanimously accepted! Baseline SIG has been added to this Best Practices WG. Do you want a Slack? Email? Work through ops group. The SIG creates updates, then the canonical version goes into the OpenSSF TAC repo.
    - “We want as many project maintainers as possible”
    - CRob sent a note to ossf-ops to get git, slack, and mailing list setup on 16july
- [DavidW] it’d be good to create guidance to counter attacks like the polyfill.io subversion
    - More information on attack: https://blog.qualys.com/vulnerabilities-threat-research/2024/06/28/polyfill-io-supply-chain-attack
    - Proposed addition to Concise-Guide-for-Developing-More-Secure-Software.md to address this: https://github.com/ossf/wg-best-practices-os-developers/pull/559
    - “The lessons are not getting learned”. It’s become common to link to other sites that you don’t control for dependencies.
    - Subresource integrity: opens yourself up to denial of service, setting yourself up for problems.
    - Dan Applequist starting Web Security SIG here in OSSF working with the W3C. Point them towards this idea to propagate this.
- [DavidW] it’d be good add guidance to counter xz utils like attack
    - Proposed text: https://github.com/ossf/wg-best-practices-os-developers/pull/560
    - In many cases when folks get source packages, it’s not always a tarball generated from source. Sometimes generated, like autotools.
    - Ensure your source packages only have version-controlled source. If you use autotools, don’t use the autotools generated source… need to ensxu
    - Could build provenance (SLSA) also cover this attack? SLSA 1.0 for builds, not necessarily. But maybe? Follow along for source track. Need to ensure that they get version controlled source.
    - [Seth] Should we recommend users grab the source code instead of the “artifact”? Users these days don’t do the source code clone and recompile.
    - Redistributors might be interested, should we make a recommendation towards them, and not end-users? Maybe not in this current guide, if we add one for repackagers.
    - [Chris] Upstream is Debian for OS, not aware of any way that this could have been prevented. What processes and procedures could be added? Trust in upstream, can only lock down the bytes.
    - [David] Once it’s been compiled, checking the bytes stay the same doesn’t help. The gap is “what was reviewed” is not what was being used. Source code was different from built artifact, but there are historical reasons that this is the case.
    - [Avishay] Maps to the S2C2F rebuild it practice which is “Level 4” (aspirational)
    - [Chris] We rebuild everything from source.

    - [David] Version controlled software was safe, the artifact with autoconf-generated artifact had the trigger for the vulnerability included.
    - [CRob] Redistributions add “time” to the stability/risk mitigation process. Not pulling latest, latest only happens in the unstable release stream.
- [DavidW] Trying to increase LFD121 enrollments this year!
    - Any more ideas?
    - Can anyone help/volunteer, esp. sign-ups by their organization?
    - Please help us increase LFD121 enrollments! https://openssf.org/training/
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- Working on: (1) developer manager training (slides) & (2) security architecture training (course outline). Two meetings, general EDU SIG meeting & workshop meeting

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
- SIG hosted a gr8 discussion with the .Net security folks at the last SIG call about memory safety in “managed languages” and proposed several changes to the “memory safety continuum guide” based on this discussion, as reflected in the following issues
    - https://github.com/ossf/Memory-Safety/issues/26
    - How does unsafe code fit in? · Issue #28 · ossf/Memory-Safety (github.com)
    - What's the definition of "use after free"? · Issue #29 · ossf/Memory-Safety (github.com)
- The .Net team will work internally to produce the .Net best practices for the Best Practices - Memory-Safe By Default Languages Guide
-

C/C++ BP Guide SIG (Thomas)

- Cancelled meetings in July 2024 due to summer, will restart in August
- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
- Google Summer of Code contributor Nate Ohlson:
    - Adopting the guide for CPython
    - Creating a tool for incremental adoption of warnings

Python Hardening Guide SIG (Georg & Helge)

- BEST Issue 481
-

WebDev Security Guide (Daniel)

- BEST Issue 367
-

2024-07-15 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
-

Opens

-

Guide Notes

2024-07-02 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Fotis Georgatos	fotis@cern.ch	CERN		
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Hasan Yasar	hyasar@cmu.edu	Carnegie Mellon University		
x	Reden Martinez	rmartinez@linuxfoundation.org	LF	he/him	redenmartinez

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- [DavidW] Guide on regular expressions (regex) & corresponding blog is out!
  - Guide: https://best.openssf.org/Correctly-Using-Regular-Expressions
  - Have proposed modification of LFD121 to match https://github.com/ossf/secure-sw-dev-fundamentals/pull/155
- [DavidW] Trying to increase LFD121 enrollments this year!
  - Any ideas?
  - Can anyone help, esp. sign-ups by their organization?

    - DaveR: LMS integration. Will people be counted? Will let DavidW know when this goes live in my org.
        - David: My understanding is that the answer is “yes”
        - Dave: We’re working on it in RH!
        - 2 reasons for LMS integration: (1) visibility, and (2) tracking
    - Fotis G: What about the OSPOs? Are they being informed?
        - If OSPOs encourage, many will do
        - David: I’ll add that to my list - David will contact the TODO Group & maybe others, cc: Georg Kunz
        - Hasan: I”ll get my students to take course! hyasar@cmu.edu
    - Chris A: Looking at IBM - search for it, I find the credential but NOT the learning activity. When I try to add it, it’s already there. Something is preventing it from being revealed. Will email David A. Wheeler
- [Dan from Slack] Update from Dan Appelquist (Via Chris de A):
    - we have started the SWAG community group up and held 2 initial calls so far. The minutes are here: https://github.com/w3c-cg/swag/tree/main/meetings. Mozilla, OpenJS Foundation and Open Web Docs have been early active members. We have started creating a skeleton for an initial deliverable for web application security best practices. We’ve decided on a weekly call schedule of 16:00 (UK time) on Mondays to try to accommodate a wide range of time zones. Please have a look at the charter here https://w3c.github.io/charter-drafts/2024/swag-cg.html and join the group here https://www.w3.org/community/swag/. Let me know if you have any questions.
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- Updating fundamentals course for regex
- Working on: (1) developer manager training (slides) & (2) security architecture training (course outline). Two meetings, general EDU SIG meeting & workshop meeting

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Georg & Helge)

- BEST Issue 481
- Continue to meet, attendance is a little low, adding material to guide. May want to discuss in this group how to rendering
- Simplest possible approach publication so far.
- It'd be good to have a sidebar system - may want to have something more specialized
- Georg Kunz is still maintainer - it'd be good if others could be added. **@Georg** to e-mail CRob to send to Operations / or send it directly to Operations (cc to CRob for his affirmation)

    - Provide names, e-,mail and github IDs

WebDev Security Guide (Daniel)

- BEST Issue 367
-

2024-07-01 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson		gkunz
x	Bartlomiej Karas	bartlomiej.karas@ericsson.com	Ericsson		BartyBoi1128
x	Helge wehder	Helge dot wehder at ericsson.com	Ericsson		
x	Fotis Gerogatos	fotis@cern.ch	CERN		fgeorgatos

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Review of open PRs
    - CWE-191 / PR547
        - All good, merged
    - Code snippets for CWE-197 / PR555
        - Helge will push a fix, then we review again.
- Review of open issues
    - Overview of all CWEs to be moved / issue 531
        - How to best track individual items?
        - Shall we try to create a project for our guide?

        - We will go for the simple strike through method for now
        - Reach out to CRob on Slack
    - Update landing page / issue 520
        - Split into separate issues?
            - Georg will create a separate item for the contributor guide

Opens

-

Guide Notes

-

2024-06-27 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Siddhesh Poyarekar	siddhesh@gotplt.org	Red Hat	he/him	siddhesh
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani
x	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Meetings in July?

  - Thomas is unavailable for the two calls scheduled in July (July 11 and July 25).
  - Are there volunteers to run those calls or is it preferable to cancel?
    - No volunteers. Thomas will ask OpenSSf operations to cancel July calls.
- Issues ok to close? init
  - Compiler Hardening Guide should include -ftrivial-auto-var-init (#245)
    - No objections to close.
  - Options -Wtrampolines and -fstack-clash-protection not universal (#277)
    - Georg: value in tooling around validating the options, but no concrete plans as of now
    - Mayank's scraper script is a better starting point for validation compared to current Makefile, but there's currently no plans for option validation
    - Issue seems to be about the placement of the options primarily. In that sense, it is ok to close.
  - Clarify why -O2 (#331)
    - Some restructuring of the optimization options happened as a result of #490.
- New/Updated Issues/PRs:
  - Consider Annobin -grecord-gcc-switches (#509)
    - Siddhesh noted that Nick Clifton is author and maintainer of Annobin and annocheck for both GCC and Clang. It's heavily used in the Fedora ecosystem.
    - Annobin / annocheck adds ELF notes on the object file level which typically survive binary stripping that removes DWARF.
  - Consider Wl,--as-needed and -Wl,--no-copy-dt-needed-entries (#510)
    - Siddhesh noted that libraries added to DT_NEEDED may, in addition to reduce the attack surface also preclude the execution of constructors in libraries that as excluded as a result of –as-needed.
    - Thomas will write initial PR. Siddhesh eager to contribute.
    - Siddhesh noted new option -W,-z,separate-code which puts executable segments in different pages from non-executable pages to avoid overlap at the cost of increased binary size. Siddhesh opened a new issue with enhancement suggestion.
  - Add GCC option for checking virtual table pointers (341, ~~PR #440~~, PR #485)
    - Recap of the discussion on the Github PR. Will wait for response of original contributor.
  - Contribution of python scraper script (PR #549)
    - Question around licensing: Mayank initially released the script under MIT. In that case the script should have license information included explicitly. If the script is licensed under Apache 2 the license statement in the README is sufficient.
    - Mayank decided to re-license the script under Apache 2.
    - Would be good to add a mention of the scraper script to the guide itself as an appendix and in the README

Opens

-

Guide Notes

-

2024-06-18 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Fotis Georgatos	fotis@cern.ch	CERN		fgeorgatos
x	Mohammed Anghabo	moh.anghabo@gmail.com	SariaTech		mohanghabo
x	Dick Hardt	dick.hardt@hello.coop	Hello		dickhardt
x	Rohan Harikumar	rohanharikumar80@gmail.com			rohanharikr
x	Reden Martinez	rmartinez@linuxfoundation.org	Linux Foundation		redenmartinez

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- Regular expression guidance document - vote for release as new guidance
  - On 2024-05-04 the WG voted to accept the guidance on regular expressions. You can see the guidance here: https://best.openssf.org/Correctly-Using-Regular-Expressions and the supporting rationale here: https://best.openssf.org/Correctly-Using-Regular-Expressions-Rationale per issue https://github.com/ossf/wg-best-practices-os-developers/issues/518
  - Let's add the guidance to our list of guidance & not wait for the blog post - David will ask
  - Draft blog post (please comment): https://docs.google.com/document/d/1nvlk-eAGdApbmDpKZDdBKYLvFEzBwLvs0wC2EjljAcQ/edit
    - Looking for feedback - please give feedback soon.

New Friends

- Dick Hardt - startup focused on securing identity for developers.
- Rohan Harikumar - startup focused on securing identity for developers.

Opens

- [David A. Wheeler] Key item for this meeting (as agreed at last meeting) - review of draft "Security Architecture Course Outline" here: https://docs.google.com/document/d/1D_IVQZ3P52vNnCreQF4D1r7rPp78C3xQIw2Nvo5Ss8s/edi
  - Anything important missing? Anything there that shouldn't be?
  - Would like agreement on scope by end of meeting. We still need to create the detailed content, and we can make changes as we go, but it's best to agree on basic scope first.
  - Crob: this is designed to be a “201” type - intermediate level - course.
  - Dana has commented to shorten this down… Also wanted to get feedback from community. Not opposed to dropping things.
  - David: The plan will be to **charge** for this course and use the proceeds to help fund the OpenSSF.
  - The course content starts with a definition of “security architecture” - This starts with a discussion of Saltzer & Schroeder's security design principles. This isn't a literature review.
  - Crob: “guiding” vs. “applied principles”... typically it's important to showcase a few kep principles for a particular project…

- Dan: suggest more “plain language” around the principles … e.g. “Minimal Trusted Elements” - does it also include “data minimization”
- David: many of these are written in an overly complex way.
- Crob: as a for example domain .. falls into the umbrella of “least privilege” (zero trust).
- Security Domains / Security Patterns …
- Crob: security architecture similar to enterprise architecture… you need a holistic approach. Different level of granularity. I’d avocate talking about network security … but maybe not endpoint security. This Is a good start.
- David: “the who is this for” section… at first i was thinking enterprise architects but could also be useful for software developers…
- Crob: developers would benefit from this. Directionally I’m fine with this as an outline. Network and data considerations absolutely need to be talked about.
- Enterprise architecture frameworks… e.g. TOGAF…
- Crob: depending on what the learner’s intention is we can send them to those but not spend time on it… the O-ESA is how to structure your security program within an enterprise architecture programm.
- David: Threat modeling - this should belong as its own corpus - but noting what they are seems important. We can point them to a separate course on threat modeling.
- Crob: I feel we should do an overview of threat modeling tehniques … e.g. 4-step model starting with “what can go wrong” - then tell them this is a whole discipline into itself.
- Dan: agree this is important - to have a baseline.
- Crob: we should talk about data flow diagrams here… Attack tree is another technique. As you’re moving “security boundaries”...
- David: we’ve planned “labs” - people surveyed were interested in the security architecture topic - but labs are challenging… What I’m thinking of is a case study where you review materials and answer questions… A threat modeling excercise.
- Crob: ISC2 would show you a diagram and ask “where would you apply a control” - i don’t think this should be a coding exercise but should be some interactivity.
- Crob: 3 main skill areas: Threat modeling / threat assessments / reference architecture diagram / powerpoint & communication skills.
- DickH: reflecting on security best practices in IETF and identity organizations - in IETF we’re struggling with terminology - it might be useful to add a terminology section… Also: I also often tell people to not build stuff themselves… use something that’s already built as opposed to building it yourself… That’s a pragmatic principle…
- Crob: agree - TOGAF would call it “use standards based security solutions” - within Open Source people are already making that choice by reusing…
- David: *adds some notes into the doc on these points*

    - Crob: some of the terms are discussed in the security manager class - we decided there that we will create some kind of artifact for terminologies…
    - DickH: at the beginning maybe provide some guidance on common attacks / common vulnerabilities - to give people … guidance on where to spend their time…
    - DichH: in IETF we take the approach to not define things but to use existing definitions… point to existing definitions… helps people understand that the term may be used differently in different contexts…
    - Crob: next steps?
    - David: I will take all these comments and update …
- W3C swag group (see below).

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- New admin: John Mertic, Director of Program Management - Linux Foundation, Academy Software Foundation, LF Energy, and Open Mainframe Project. Has been involved in badges for years

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- We have some people creating labs - but we need more! Please contact David to learn more.
        - https://github.com/ossf/wg-best-practices-os-developers/issues/483
        - https://docs.google.com/document/d/1wNoNjLpdkgoXkRDvDBI32tm62rbASIfF6gxwyEkyTYs/edit
        - https://best.openssf.org/labs/
-

Scorecard project (Laurent - Spencer)

- Changes in the project - scorecard has adopted Allstar…
-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Georg & Helge)

- BEST Issue 481
- Participation is a little low, probably due to bad timing (public holiday overlaps)
- All content from ericsson repos now part of the best practices working group repos…
- wg-best-practices-os-developers/docs/Secure-Coding-Guide-for-Python at main · ossf/wg-best-practices-os-developers (github.com)
- They are looking for additional contributors… Looking to add someone to appropriate github team

WebDev Security Guide (Daniel)

- BEST Issue 367
- The SWAG group has launched as a proposed community group- see https://www.w3.org/community/groups/proposed/#swag - please register your support and we can get this going.
- https://w3c.github.io/charter-drafts/2024/swag-cg.html ← draft charter
- Noting that this is a “community group” because CGs are lightweight and have a lighter weight IPR policy as well.

2024-06-17 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Helge Wehder	Helge dot wehder at Ericsson.com	Ericsson		myteron
x	Bartlomiej Karas	Bartlomiej.karas@ericsson.com	Ericsson	he/him	BartyBoi1128
x	Thomas McDermott	thomas.mcdermott@ericsson.com	Ericsson	he/him	tommcd

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- SOSS Community Day EU
    - A proposal for a 10 min presentation was submitted
- Adding Thomas to the repo
    - Georg will reach out to OpenSSF staff to get Thomas added as maintainer to the repo
- Review of open PRs
    - 534 - CWE-1095
        - There is a commit in the PR which does not belong there
        - Georg and Helge will fix this
        - More reviews welcome
    - 532 - Multithreading
        - The content is fine
    - 530 - add SPDX license headers
        -
    - 528 - include code example via Jekyll
        - No strong opinion in the team
        - Better rendering would be needed anyway (e.g., a navigation bar)
        - We put this on hold for now and focus on the other content
    - Review of issues
        - Issue 531 now lists all outstanding CWEs to be moved to the OpenSSF repo

Opens

-

Guide Notes

-

2024-06-13- C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
x	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)

- Continue discussion on machine readable format and guide versioning - should we transition to more structured versioning of the guide?

    - We often update (every 2 weeks), so we have been simply showing the updated date
    - Some may want a more stable guide that doesn't change every 2 weeks
    - We could occasionally copy the source file to an "archive" directory, with filenames of form filename-YYYY-MM-DD.md (or maybe filename-MAJOR.MINOR.PATCH) so people can have a fixed unchanging version.
    - Discussion on whether versioning of the machine readable version of the guide is sufficient.
    - What about the tool for generating JSON from the HTML? That can continue to be an advance use people can use if they want.
    - Are there real teams where this is a problem? Currently hypothetical, but potential concern.
    - If there's a user, we can enable. Don't want to do it until we know there's a user of it.
    - **Decision**: We won't make any archive copies yet, since we don't know of anyone who we're sure needs it. We'll probably start creating archives once we know there is a user of it, we can make that decision then.
    - Mayank is willing to contribute tool to generate JSON from guide. Thank you! MIT - no license problem.
        - Probably need to bring to Best Practices WG.
        - There's no trademark issue, no patent issue. It's just a ~150 line program.
        - Would this be a new repo, or just embedded in our existing section as a contribution? Let's discuss via Slack.
- New/Updated Issues/PRs:
    - Add Guide Conventions section in README, Fix FORTIFY_SOURCE for improved machine readability (#537)
        - Yes. There's a minor merge conflict, please rebase, & we'll merge.
        - Is this the last one necessary for machine readability?
        - Should we also create a link to the tool that extracts from HTML to JSON, or incorporate?
            - Reasonable, that'd be a separate PR
            - Also the possibility to include the script as part of the OpenSSF Github organization. Procedurally it would be better to discuss that in the general BEST WG call.
    - Corrected/Missing GCC and Clang version for -fstack-protector and -fstack-protector-all options (#512, #513)
        - Thomas reviewed and found the proposed version is incorrect
    - Add -fhardened to Compiler Options Hardening Guide (#240, PR #492)
        - Passed-in options override; this is now more clearly documented in this PR.
        - All happy.

  - Add GCC option for checking virtual table pointers (341, ~~PR #440~~, PR #485)
    - Comments from 2024-05-16 call communicated to PR with some additional feedback.
    - Sam James (Gentoo) communicated some concerns whether the feature has any users any longer?
    - David noted on Github that the significant performance impacts on a relatively narrowly focused countermeasure suggests we should not recommend this outright, but we should still document the option.
    - “This option can have significant performance impact, while only countering a narrow type of vulnerability. Thus, we have not included this option as a recommended option in the current version of this guide.”
    - Maybe add a new table “specialized options”? Or just not mention it in any table?
    - Let’s just not create another table - that way the information is available, but people don’t have to wade through another table.
  - Consider Annobin -grecord-gcc-switches for C and C++ Compiler Hardening Guide (#509)
  - Consider Wl,--as-needed and -Wl,--no-copy-dt-needed-entries for C and C++ Compiler Hardening Guide (#510)
- Issues ok to close?
  - Merge early work on "Recommended compiler option flags for C/C++ programs" into latest draft (#97)
    - We’ve merged the relevant ones in, so we can close this!
    - Some people had started to work on a new document (cited here), then Ericsson contributed its work & we switched to that as the baseline. This was just a PR to ensure we didn’t lose any good ideas - but we’ve incorporated them all.
    - We all agree that this effort has been a huge success story. The resulting document has information that we wouldn’t have had separately. Ericsson uses this internally, for example. Thank you everyone!
  - Out of time, we can discuss these separately:
  - Compiler Hardening Guide should include -ftrivial-auto-var-init (#245)
  - Options -Wtrampolines and -fstack-clash-protection not universal (#277)
  - Clarify why -O2 (#331)

Opens

- FYI: Nate Ohlson’s weeknotes for week 2 of Google Summer Code adoption of the compiler options guide for CPython with detailed benchmark results: https://s3.amazonaws.com/nohlson.com/week2ntoes.pdf

Guide Notes

2024-06-04 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Fotis Georgatos	fotis@cern.ch	CERN		fgeorgatos

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- Regular expression guidance document - vote for release as new guidance
    - The guidance on correctly using regexes is now in markdown on the best practices site. You can see the guidance here: https://best.openssf.org/Correctly-Using-Regular-Expressions and the supporting rationale here: https://best.openssf.org/Correctly-Using-Regular-Expressions-Rationale

- The last Best Practices WG agreed to move the Google doc into markdown (which David A. Wheeler has done).
- Please take a look at it & be ready to vote on whether or not it should be released as guidance from the WG, as requested in issue https://github.com/ossf/wg-best-practices-os-developers/issues/518
- No negatives. Would like blog post.
- +6 yes, no nos. Majority.
- It will go into the OpenSSF guidance documents list, we'll craft a blog post to go out at the same time.
- Draft blog post (please comment): https://docs.google.com/document/d/1nvlk-eAGdApbmDpKZDdBKYLvFEzBwLvs0wC2EjljAcQ/edit

-

New Friends

- Fotios Georgatos - European Org for Nuclear Research (CERN)

Opens

- David: For next best practices call - can we go through the course… ? [general agreement on that]

Backlog Review

-

Meeting Notes

- TAC closing off second quarter of funding requests - please let us know if you're looking for funding so we can put it on the agenda for the next TAC call. Deadline is next week. Deadline for Q3 will be September.
- Regexp projects: we've been developing guidance on regular expressions… partly because regexps are widely used for input validation… Now 2 documents - a short guidance document and a larger rationale document…
    - Crob: i endorse. I'm good moving forward…
    - Dan: looks good to me
    - David: final technical content 2 weeks ago - I think it's technically all correct.
    - Dave Russo: looks good to me
    - Crob: it's in github - so people can file issues if they find any.
    - Dan: I suggest a special line just inviting comments and pointing to the issues list - I will leave a PR. Also suggest a blog post.
    - Chris: I support. I would suggest a test suite - e.g. a monorepo
    - David: there are snippets of source code in the rationale.

- ***Group resolves to publish***
- Crob: let's do a blog post - we'll start a google doc soon.

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- We had some annoying attackers on the badge application that I believe I've addressed.
    - They were sending a large number of activation emails to specific email addresses, which I'm sure annoyed the recipients *AND* threatened to take away our ability to send emails (due to spam rate limits).
    - I did some investigations & found that they were exploiting activation emails - they were sending lots of activation emails. They couldn't control the content of the emails, but doing that is annoying.
    - I think I've addressed it. I've added a new rate limit: activation emails require a timeout for a specific account before they can be resent (default is 24 hours). I also made another rate limit more stringent (for a given IP address, the number of new accounts in a given time period).

Education SIG / Courses (Security Fundamentals etc.) (David A. Wheeler)

- We have some people creating labs - but we need more! Please contact David to learn more.
    - https://github.com/ossf/wg-best-practices-os-developers/issues/483
    - https://docs.google.com/document/d/1wNoNjLpdkgoXkRDvDBI32tm62rbASlfF6gxwyEkyTYs/edit
    - https://best.openssf.org/labs/
- Academic Accreditation project - joint project between us an CNCF - certifying university courses… - there is a gap in current academic curricula - this is a step forward on improving that… we'll test it with [a few] universities … we can expand this after.
- Course Content Collaboration project - 2 projects lined up - meeting weekly on getting content hammered into shape - and plugged into lf training platform and lf events; **fundamentals** class and **manager** class. Person who created the original class (from Intel) joined as well… manager class: teaching a manager basic security concepts - rather than how to plug these things into a developer workflow. The class could be split into two offerings - a "security concepts" offering with basic stuff - then another manager class on how to integrate these ideas into a development project - e.g. prioritization of security issues in a backlog…
    - Dan: suggest concepts training be free
    - David: if the manager material depends on the earlier stuff we need to make sure they got the earlier material… - the concepts could be embedded in the manager course.

- Possible crypto class - looking at a contribution soon….
    - Sounds good. It’s an “applied” class, so probably focused on developers.
- David A. Wheeler will present on the outline for Security Architecture class at next best practices WG meeting, June 18.

Scorecard project (Laurent - Spencer)

- Changes in the project - scorecard has adopted Allstar…
-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Georg & Helge)

- BEST Issue 481
- Participation is a little low, probably due to bad timing (public holiday overlaps)
- All content from ericsson repos now part of the best practices working group repos…
- wg-best-practices-os-developers/docs/Secure-Coding-Guide-for-Python at main · ossf/wg-best-practices-os-developers (github.com)

WebDev Security Guide (Daniel)

- BEST Issue 367
-

2024-06-03 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Thomas McDermott	thomas.mcdermott@ericsson.com	Ericsson	he/him	tommcd

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Review of migrated content
- Review of issues
    - 519
        - The current best WG rendering using Jekyll is a minimal viable solution to the problem
        - In contrast to the other guides, this guide is spread out across plenty of pages which makes navigating through the guide challenging without a navigation bar. That might be an improvement for future version of the rendering.
        - Thomas has a proof of concept using mkdocs.
            - To be discussed if we just want to / can render this guide using mkdocs or the entire Best WG documentation.
            - Thomas will investigate if mkdocs can be limited to the Python guide only, i.e., not impacting the other guides
        - We anyway want to move ahead with using includes instead of copy-and-pasting the code snippets

    - 520
        - This is about fixing broken links on the landing page, adding additional documentation and description on how to use the guide
    - 521
        - For future reference
- Review of PRs
    - None right now
- AOB
    - Nothing

Opens

-

Guide Notes

-

2024-05-30 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
X	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
X	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
X	Gabriel Dos Reis	gdr@microsoft.com	Microsoft		GabrielDosReis
X	Siddhesh Poyarekar	siddhesh@gotplt.org	Red Hat	he/him	siddhesh
X	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnan

					i
X	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
X	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
    - Status of `_LIBCPP_ENABLE_HARDENED_MODE` in guide
        - Inconsistency in the document.
        - William will make a PR to fix this
        - See: https://libcxx.llvm.org/Hardening.html
        - Jack raised the question whether we should cover version ranges for recommendations for the guide when a recommendation is dropped or tweaked.
        - TL;DR; options should target the latest compiler versions. The detailed descriptions can contain special considerations for older compiler versions and older variants of flags
- New/Updated Issues/PRs:
    - Conversion of compiler option guide to machine readable format (#490, PR #507)
        - Siddhesh noted that up GCC 5 had point releases that added flags in minor releases. After GCC 5 maintenance releases do not introduce new flags. Specific to GCC x.x.0 is generally not a stable release, x.x.1 is a stable release.
        - David noted that GCC versioning does not follow semversion, we should be consistent with the upstream version label and always follow the ACTUAL version numbering system of upstream.
        - The homepage says only 2 numbers, but the tarballs use 3 numbers. Since the tarballs use 3 numbers, we can justifiably also use 3 numbers. So we'll accept the proposed chang as-is.
        - William noted that for machine readability for the guide, the guide itself should also be clearly versioned. This is likely leads to a more broader conversation around ways of working. Thomas will add an agenda item to the next call.
    - Add -fhardened to Compiler Options Hardening Guide (#240, PR #492)
        - Siddhesh, William and David noted that we should not enumerate the implied options, linking to the GCC manual page should be sufficient.

        - David noted the example should be changed to show that the precedence rules are not order dependent.
    - Review "C style" ideas from mcinglis (#498)
        - Thomas left comments on the Github issue and re-iterated those points during the call.

Opens

- FYI, David A. Wheeler created presentation “Improving Memory Safety without a Trillion Dollars (FINOS)”, proposed presentation for later this year https://docs.google.com/presentation/d/1EDQL-6MUKrqbILBtYjpiF96uW5LXcnIuE-HxzyCIr68/edit - it highlights this guidance material, trying to get the word out

Agenda items beyond this points were postponed to the next call.

    - Consider Annobin -grecord-gcc-switches for C and C++ Compiler Hardening Guide (#509)
    - Consider Wl,--as-needed and -Wl,--no-copy-dt-needed-entries for C and C++ Compiler Hardening Guide (#510)
    - Add GCC option for checking virtual table pointers (341, ~~PR #440~~, PR #485)
        - Comments from 2024-05-16 call communicated to PR with some additional feedback.
        - Sam James (Gentoo) communicated some concerns whether the feature has any users any longer?
- Issues ok to close?
    - Merge early work on "Recommended compiler option flags for C/C++ programs" into latest draft (#97)
    - Compiler Hardening Guide should include -ftrivial-auto-var-init (#245)
    - Options -Wtrampolines and -fstack-clash-protection not universal (#277)
    - Clarify why -O2 (#331)

Guide Notes

-

2024-05-21 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Reden Martinez	rmartinez@linuxfoundation.org	Linux Foundation	he/him	redenmartinez
x	Aditya Mukherjee				
x	Neal McBurnett	nealmcb@gmail.com	independent	he/him	nealmcb

Agenda

- Is someone willing to scribe for the meeting today? - Dan
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
  - Memory Safe workshop: Memory-Safety/workshop/proposal.md at main · ossf/Memory-Safety (github.com)
    - Planned for November
    - Next steps: Committee members
- BEST issue 461: New guidance document: Correctly using Regular Expressions for Secure Input Validation. We'd like to approve it as guidance from the group!
  - Draft in Google docs format is here: https://docs.google.com/document/d/1Ors5T04Pgh3dcBfelbBrEBrvY3OKB7IoUBUJPYBmmZw/edit
  - The big question was Java, as different documents disagreed on what Java actually did. We've run tests on various versions of Java on

Windows & Linux, and determined that Java's "$" is *never* permissive. A big thanks to Nikita Koselev for writing & running tests on many systems!
  - Proposal: let's convert the Google document to 2 markdown documents, a short "guidance" and a long "rationale". The first 2 sections become guidance, the rest become rationale. It was convenient to have as 1 document while we were doing researchers, but most readers will want the short guidance.
  - Vote request: Approval for conversion to 2 markdown documents & then release them as new guidance on the WG site?
  - Discussion Should we have a blog post about this (to be posted after it's released)? - CRob - YES!
  - We'll convert & come back to group async via Slack and mailing list
- BEST issue 489: Add secret scanning to SCM guide
  - Inspired by vulnerabilities reports against best practices badge project
  - Adds it for both GitHub & GitLab. GitLab's "main" approach only warns about problems via CI/CD (it can't prevent them), but that's still an improvement. GitLab does have an experimental enforcement mechanism, but it's not available to all, so this simply notes its existence.
  - We tried to avoid adding tools to the SCM guide
  - Also, how do we generate this? Need to work with Legitify.
  - Agreement that we need this kind of guidance SOMEWHERE - maybe not SCM guide?
  - Dan & David to chat with Legitify on what to do next, Dan will kick that off.
- FYI: Python Google Summer of Code (gsoc) https://python-gsoc.org/ideas.html list includes "Adopting Hardened Compiler Options for C/C++ in CPython" - working to integrate the OpenSSF C/C++ compiler options list into Python when it compiles C/C++ code. Seth isn't here today, unfortunately.
- FYI - EDU.SIG new Course Content Creation stream - we'll be meeting weekly Mondays at 1pm et to collab on new course materials in hopes of delivering two new classes this year
  - Developer Manager Training - EDU Issue 48
  - Security Architecture - EDU Issue 79
- FYI - EDU Issue 78 - EDU.SIG - Curriculum Certifications effort. Working with Dana, Justin Capos & folks from CNCF to develop a certification program for collegiate programs

New Friends

- No new friends :(
  - Well, Neal McBurnett joined briefly, but had to run before introducing himself….

Opens

- Memory safety SIG - looking to put together a workshop. (Avishay) Been iterating on this - a link to the document : Memory-Safety/workshop/proposal.md at main ·

ossf/Memory-Safety (github.com) - “Improving Memory-Safety in an Imperfect World” - we are aiming for November. Our next stage is to assemble committee members. Committee members will help us to assess the submitted papers - and to reach out to the community. Please reach out if you want to be on the committee. Outcomes (final report) will be published as well as papers and videos - aligned with how the workshop with W3C happened.. Leverage the existing platforms provided by LF.

  - **Biggest ask is for committee members.**
  - Aditya - would like to be in the committee.
- Best issue 461 : (David Wheeler) - been working on input validators… there’s common misinformation e.g. that regexp is the same across all programming languages … has led to a lot of problems. Google doc is collecting some of this information. I propose compose it into 2 markdown documents - one “basic guidance” and another longer “rationale.” Can we have a vote on this to release these as new guidance?
  - Dan: what’s the confidence level?
  - David: we’ve drilled down into specific languages… I’m fairly confident in it. For .NET everything is quite consistent… but not easy to find - so very useful to have a guidance document. Java as the annoying one because of some disagreeing docs…
  - David: asking for a vote to publish this to our github.
  - Crob: we’ve talked about this several times now - we can publish the files into git and then make a broader call to circulate it - before we do a blog post or anything.
  - Dan: 👍
  - David: I don’t have examples of specific vulnerabilities that have resulted from this yet…
  - **Recording consensus of the group that we’re good to publish this as output of the group.**
  - Question on white papers… and what we publish.
  - David: this will be a short guidance doc and a larger rationale doc. I’ve also proposed this as a blackhat topic.
- BEST issue 489: David: this was triggered by a vulnerability - there was a secret in an OpenSSF repo … I’m also proposing a new working group 489… adding secret scanning to the SCM guide.
  - Different between github and gitlab…
  - Avishay: SCM guidelines tries to differentiate between SCM itself and tooling / code… this is one of many tools you can apply… e.g. dependabot … we tried to make this differentiation…
  - Dan: should probably go in the general
  - Agreement that we need this kind of guidance somewhere…
  - Avishay: code scanning tool is something that is on the code - not currently the kind of thing
  - David: it’s one of the things you can enable
  - Avishay: for public repositories…
  - Dan: I can help…

    - *some discussion on what level of detail*
    - David: for github - enable secret scanning (no separate tooling to install). For gitlab it's a little more. You enable "autodevops" and it's automatic. Otherwise there's a template.
    - Crob: it sounds appropriate.
    - Dan / David / Noam to organize a chat.
- Education SIG is working on with Justin, security community member in residence + David Wheeler + CNCF people - to create a **certification program** for academic curricula. LF would certify the the quality of the content of the course. Working in bi-weekly calls.
    - David: We have a good one-page summary - we need to yank that out
    - Crob: i have one issue with the 10 point list…
    - *discussion ensues*
- Changes to scorecard - incorporating allstar into that project + some other tools that will be donated…
- c/c++ guide - majority of open PRs
- Dan: still working on w3c swag group - will update soon with a launch date
- Backlog Review

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Had vulnerability reports in Feb 2024, not a vulnerability but led us to look for similar problems & found one, no evidence it was exploited, fixed. Details: https://docs.google.com/document/d/1MWBTqpO8XofvN9EITX5tPB8a7N1N0Wp9JgEQ9ff4Qvo/edit

Security Fundamentals Course SIG (David A. Wheeler)

- Development of labs for class (lab makers welcome!)

Scorecard project (Laurent - Spencer)

- Allstar & Scorecard will be officially joining forces
- Several other projects will be joining "the Scorecard Universe"
-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- Academic Accreditation group continues on
- Developer Manager course under review (reviewers needed!)
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

Python Hardening Guide SIG (Georg & Helge)

-

WebDev Security Guide (Daniel)

- BEST Issue 367
- Still working it, call w/ W3C this week.
-

2024-05-20 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Venu Vardhan Reddy Tekula	vt2182@nyu.edu	NYU	he/him	vchrombie

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Proposed next steps for working on our content
- Review of PRs

Opens

-

Guide Notes

- Proposed next steps for working on our content
    - Review pending PRs in old repository
        - https://github.com/Ericsson/secure_coding_one_stop_shop_for_python/pulls
        - Get feedback from the group about the general structure of the content
        - Once agreed on structure, move ahead with updating + merging pending PRs in old repository
        - Then transfer content to https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Secure-Coding-Guide-for-Python
- Recommendations for how to manage executable code examples and markdown files
    - Include vs. copy vs. ???
- Review of PRs
    - CWE-134
    - CWE-400
    - CWE-410
    - CWE-501
    - CWE-502
    - CWE-1335
    - CWE-392
- Any other content
    - Nice landing page is needed to describe the purpose of the guide and how it it can be used
    - Any other suggestions for valuable content are highly appreciated
- **Suggestion:** create a tool which checks the rules described in the guide to give developers something simple to use and not having to rely on reading the whole guide.
    - Some of the rules already list some tools and those could be leveraged for specific rules.

2024-05-16 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	Siddhesh Poyarekar	siddhesh@gotplt.org	Red Hat	he/him	siddhesh
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani
x	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
  - Removed duplicated text and added commas after conditional clauses (#482)
    - Reviewed the changes, viewed them as appropriate
  - Extend clang-tidy notes related to trojan source lints (#484)
    - Reviewed the changes, short discussion around the existing clang-tidy commentary being limited to lints covered by GCC options. New content outlines extra lints related to trojan source that would not suit compiler flags but are still useful for security. No objections and merged.
  - Mention that implicit function declarations harm _FORTIFY_SOURCE (#486)
    - Reviewed and merged.
  - C fallthrough: Which version of the Linux kernel? (#480)
  - Add GCC option for checking virtual table pointers (341, ~~PR #440~~, PR #485)

      - Siddhesh noted that performance implications section reads very differently than text elsewhere in the guide, should be reworded to be more consistent with other sections
      - Performance numbers should be attributed to specific benchmarks, 5% impact in Chrome may be acceptable, but 5% impact on SPEC benchmark would generally be undesirable
      - Thomas will look into whether UBSAN -fsanitize=vptr is similar
      - Siddhesh noted that usage of UBSAN of production has traditionally been discouraged but there has been cases where UBSAN has still been used in production
      - Siddhesh noted that minimal-runtime is only present in Sanitizer project mirror https://github.com/llvm/llvm-project/blob/main/clang/docs/UndefinedBehaviorSanitizer.rst#minimal-runtime
    - Conversion of compiler option guide to machine readable format (#490)
      - Some edgecases that the scraper doesn't handle yet. Discussed approaches to deal with this
      - Discussed some version requirements are mentioned as major version only. GCC since 5 has not added flags within patch versions so do not need to include the patch. Maybe standardize on 5.0.0 vs 5 or 5.0
      - Could use hidden html to be used in options like FORTIFY_SOURCE where prerequisites are needed (-O2)
    - Add -fhardened to Compiler Options Hardening Guide (#240, PR #492)
  - Discuss general ticket grooming

Opens

- Require comments/feedback on issue regarding modifying compiler options guide to be more machine readable: https://github.com/ossf/wg-best-practices-os-developers/issues/490

Guide Notes

-

2024-05-07 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [SCM]	daniel.appelquist@samsung.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
x	Marta Rybczynska	rybczynska@gmail.com	Syslinbit	she/her	
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson
x	Helge Wehder	Helge.wehder@ericsson.com	Ericsson	he/him	myteron
x	Tapas Jena	Tapas Jena	Red Hat	he/him	tjena-ansible
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	

Agenda

- Is someone willing to scribe for the meeting today?

- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- BEST Issue 481 - Python Hardening Guide SIG - every other Monday at 11a et
    - Georg & Helge will be leading
    - Ericsson has some material, but their internal material included material from others & couldn't relicense that, so instead extracted the parts they could share (CVE list & code examples). https://github.com/Ericsson/secure_coding_one_stop_shop_for_python
    - Voted on whether or not to form the SIG. No objections, many approvals. The "Python Hardening Guide SIG" is now an official SIG of the OpenSSF Best Practices WG to create Python Hardening guidance.
- BEST issue 367 Brief update on W3C SWAG group (no big news this week)
    - Security Web Application Guidelines (SWAG) Community Group Charter (w3c.github.io)
    - Met with Google group working on securing Google properties, they want to share more.
- "Please help us create labs (for the fundamentals course)!" https://docs.google.com/document/d/1wNoNjLpdkgoXkRDvDBI32tm62rbASlfF6gxwyEkyTYs/edit
    - We need several people/organizations to help! If 7 people write 5 labs we'd be done. Each lab takes ~6 hours to research & id correct answer (+2 hours to create automated hints & evaluation).
    - Please contact David A. Wheeler for more information if you have any interest or might be able to help.
    - This is BEST issue 483.
    - Could we apply funding this way?
        - We could, but we're trying to do it first just by asking organizations.
    - Will add request to GB material.
- David: Teaser: Best Practices badge had a pair of vulnerability reports in Feb 2024. They weren't actually vulnerabilities, but searching for anything similar did find one vulnerability which is already fixed. We believe this was never exploited (its impact would have been fairly limited). We've also made changes to reduce the likelihood of this in the future. We plan to post more details at the end of this week.

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

- TAC formalized TI funding process - so of there are projects we want to kick off we now have the ability to request funding from the TAC and the GB…
    - https://github.com/ossf/tac/blob/main/process/TI%20Funding%20Request%20Process.md
- Memory safety SIG will request funding fot a workshop…
- Issue 481 - Python hardening … Will be constructing a new artifact that will have best practices + tooling / code examples…
    - Georg/Helge: we had a first call yesterday - a couple of folks interested - the group decided that it's a reasonable idea to provide educational material for python developers… We're asking for friends and volunteers in OpenSFF community to help drive it from here.
    - Initial seed repo is here: Ericsson/secure_coding_one_stop_shop_for_python: Secure Coding in Python (github.com) - this may soon be moved to OpenSSF
    - Material will be moved to a creative commons license…
    - CROB: this is the same pattern we used for the C/C++ compiler hardening guide.
    - Main page of the current repo - provides an education baseline for coders… Regulations require you have training but current state of training is not good. So this is based on the std module library… We stop at 3.9…
    - 24 rules online – 40-50 we need to get online…
    - [call for participation / objections / alterations]
    - (Lots of support and no dissenters)
    - David: **we'll call this an official work item of this group in that case.**
    - Crob: agred.
- David on secure software fundamentals course - and labs. After some discussion I have implement a "lab" framework with some sample labs. But we'd like a lab for every unit in the education section… at least 35… If 7 people write 5 labs than we'd be done. Each one would take 6 hours of research…
    - https://docs.google.com/document/d/1wNoNjLpdkgoXkRDvDBI32tm62rbASIfF6gxwyEkyTYs/edit
    - Dan: could we use the funding to fund a tech writer?
    - David: a tech writer wouldn't be the right person… but we could use external funding
    - Crob: as chairperson of the TAC - I have a periodic update to the GB - I could add this request to the TAC update. That might help this initiative alone…

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Security Fundamentals Course SIG (David A. Wheeler)

- Development of labs for class (lab makers welcome!)

Scorecard project (Laurent - Spencer)

- Allstar & Scorecard will be officially joining forces
- Several other projects will be joining “the Scorecard Universe”
-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- Academic Accreditation group continues on
- Developer Manager course under review (reviewers needed!)
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-05-06 - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

x	CRob	crob_at_intel_dot_com	Intel/TAC	he/him	SecurityCRob
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson
x	Helge Wehder	helge.wehder at ericsson.com	Ericsson	he/him	myteron
x	Nisha Kumar	nisha@ctlfsh.tech	Oracle	she	nishakm
x	David A. Wheeler	dwheler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Robert C. Seacord	rcseacord@gmail.com	Woven by Toyota	he/him	rcseacord
x	Tapas Jena	tjena@redhat.com	Red Hat	he/him	tjena-ansible

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Nominations for chair/co-chair to help lead this effort
- Describe the project so it can be captured into an issue in gh
-

Opens

-

Guide Notes

- Helge has started a guide inspired by the Java group: https://github.com/Ericsson/secure_coding_one_stop_shop_for_python
- Georg provides us context
    - Ericsson has started a python guide inspired by the Python SEI Cert guide (https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java)
    - Based on the CWE framework with coding examples, linking to docs/guides

    - It may also be useful to look at the static code analysis landscape around python; may be useful to compile into the guide to add value to new developers/raise awareness with current devs
    - What else may be useful for the group to work on for the larger python community
    - Original document in Ericsson had complicated licensing situation. Solution: Just list the CWEs which are relevant; CWEs are public.
    - Helge - we switched to MIT for licensing and format. We want to to always be available for the community
        - Core idea is to have a learning resource for python developers
        - Need to clear up examples and get them entered into the doc
        - Guidance should stay within/close to the IDE to be useful for devs (so GH makes a great location for this content)
        - There are some additional devs from Ericsson that also can contribute.
        - Using two people reviewing the code (yay), but some mistakes have slipped through
- Tapas - what is our scope? Do we cover frameworks like Flask as part of this guide?
    - Helge - no plans at this time, try to remain close to core python as possible. Doesn't mean we could eventually get into that, but not intended at this point
- Issue: "What? Another guide?!" Do we want people to read more, vs. create a tool.
    - Can't put everything in a tool.
    - Have a way to execute the code (like the Java tool) - makes it easy to verify, remedy, etc. That proves that what you're discussing makes sense.
    - Need to review multiple times.
    - David: Need both docs and tools. Tools have false+ and false-, people need material to help them understand the tool results.
- Nisha (from Chat) - As a python dev who doesn't know anything about CWE, my feedback is that navigating this doc (the repo) is a little confusing. Maybe a "how to use this document" guide would be helpful?
    - Georg - agrees. The repo is a seed to start out joint collaboration together. We're seeking to see if there are like-minded people that are interested in working together on trying to solve this problem
- David: tools vs. documentation: both is needed
- David: Here are some suggestions for specifics to capture:
    - Be careful with pickling (only from trusted sources)
    - Regex - $ is permissive, and \z doesn't have its usual meaning; use \Z for "match end of string"
    - XSS: Use templates
    - SQL injection: Use parameterized statements
    - f-strings are simple string concatenations - be careful if untrusted users can influence any of those values
- Seth - anything related to "security" is baked into the python docs. Currently there is no stand-alone document for security / secure coding

- Helge reviews the page, talking through the sections that discuss CWEs and sample code
- David: Need front matter, middle matter.
- Georg - we can start off with the existing repo and migrate to an openssf repo
- Helge - desire to use MIT & CC-BY licenses (CWE is already under CC)
- Is there a plan to make this a PEP?
  - No plan. It can reference PEPs of course
- Scope: Writing secure Python code. Maybe expand to packaging later, but that's a challenge in Python & might be better as a separate document.

2024-05-02 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated PRs:
  - Update Compiler-Options-Hardening-Guide-for-C-and-C++: make the fallthrough macro look like a function call (PR #469)
    - David noted accompanying text should be updated to reflect the fact that the changed code example no longer matches the definition in the Linux kernel

  - Add -fexceptions to recommended options and -fasynchronous-unwind-tables to list of considered compiler options (342, PR #379)
    - Special case consideration for security, David noted some typos but no objections to merging. Thomas will fix nits offline.
    - Mayank noted that “When not to use?” section here is particularly useful.
  - Add -Werror=format-security to list of recommended options (342, PR #473)
    - David wondered whether or not gettext is affected by the heuristic.
    - Thomas noted that even if gettext is affected, the heuristic only triggers in cases where fetched format strings are used without additional format arguments, so the use of gettext falls under the same pattern of fixes as in the provided example.
    - Thomas will fix typos offline and then merge the PR.
  - Add GCC option for checking virtual table pointers (341, PR #440)
    - Another round of discussion around the performance penalties but no objections to merge the material as long as is is not positioned as a direct recommendation.
    - Thomas will make a PR to fix linter errors in origin submission and a suggestion for a reworded description of Table 2 to make it clear that not all options in that table should be considered as strong recommendations.
  - Make 'What should you do when compiling compilers?' a top-level section (PR #467, minor)
    - No objections, merged.
  - Use consistent wording for options treating obsolete C constructs as errors (#474, minor)
    - No objections, merged.

Opens

- Is there a need for having the compiler option guide in a machine readable format?
  - Discussion on whether the machine-readable description should be merged to the BEST WG repository.
  - Mayank has developed a Python script for extracting options directly from the Markdown version of the guide but it currently requires manual fixup of some options. Changes would be needed to the guide to facilitate completely automated extraction.
  - Both Mayank and David were in favor of aiming towards extraction options from guide rather than maintaining separate, machine-readable descriptions.
  - Mayank will open a separate issue to describe the changes to the guide needed to support his extraction script.

Guide Notes

-

2024-04-24 - C/C++ Compiler BP Guide

0800 Eastern Time/ 0500 Pacific / 1200 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Gabriel Dos Reis	gdr@microsoft.com	Microsoft		GabrielDosReis
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Results from Doodle poll for new time for fortnightly call:
    - Most people indicated availability for Thursday 9am EDT / 3 pm CEST starting on May 2 (5 yes, 2 if need be)
    - Most popular time based on Doodle poll chosen as new meeting time.
    - ~~Runner up: Friday 10am EDT / 4 pm CEST starting May 2 (4 yes / 3 if need be)~~
    - Thomas necessary adjustments to calendar and Github page
- New/Updated PRs:
    - Add GCC option for checking virtual table pointers (341, PR #440)
        - The information that this check needs to be compiled into GCC should be moved to the "compiling compilers" section.
        - The performance impact is high, so that we agreed not to add this option to the TL;DR tables. Additionally, the performance impact should be pointed out more strongly than "can impact performance".

    - We agree to include this option in the set of recommended options, though. The reasoning being that the TL;DR is a stronger recommendation than the "recommended options".
    - We want to tone down the term "recommended options" a bit to separate it more clearly from the TL;DR
    - Should look into whether `std`or `preinit` is preferable. Thomas or Gabriel will look into this.
- Add -fexceptions to recommended options and -fasynchronous-unwind-tables to list of considered compiler options (342, PR #379)
    - Thomas updated the PR with additional information and links, with the intention of making this easier to understand.
    - No objections on content so far but Thomas will leave up the PR for comments on Github until the next meeting.

Opens

-

Guide Notes

-

2024-04-23 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericss	Ericsson	he/him	

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
		on.com			
x	Marta Rybczynska	rybczynska@gmail.com	Syslinbit	she/her	mrybczyn
x	Salve J. Nilsen	sjn@cpan.org	CPANSec		sjn
x	Venu Vardhan Reddy Tekula	vt2182@nyu.edu	NYU	he/him	vchrombie
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Reden Martinez	rmartinez@linuxfoundation.org	Linux Foundation	he/him	redenmartinez

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- C/C++ Compiler hardening meeting time doodle poll - https://doodle.com/meeting/participate/id/b6z8NDLb
    - Seeking new meeting time…
- Python Secure Coding Guidelines [Georg and friends]
    - Ericsson has developed a set of code examples
    - This work was originally inspired by SEI Cert's secure coding material, with the intention of translating those to Python
    - https://github.com/Ericsson/secure_coding_one_stop_shop_for_python
    - Can’t release documentation, but could derive documentation from the code examples
    - Doodle poll will be set up to discuss creating a Python guide
- Daniel still seeking collaborators for Issue 367 - Sec BP for WebDevs
    - Would be a collabortive effort with W3C - https://w3c.github.io/charter-drafts/2024/swag-cg.html
- Regex guide - Draft by David A. Wheeler here: https://docs.google.com/document/d/1Ors5T04Pgh3dcBfelbBrEBrvY3OKB7IoUBUJPYBmmZw/edit with issue https://github.com/ossf/wg-best-practices-os-developers/issues/461
    - On 2024-04-09 group agreed to work on developing this narrowly-focused guide.

        - Hacker News discussion yesterday once again showed it’s needed! People confidently incorrectly claimed “$ always means end of string” - once again.
        - Request: Java & C#/.NET - need someone to write a short test program in each. E.g., “^ab$”, will this match both “ab” and “ab\n”? David thinks it does, but we want to verify. Nikita will do Java & C#
        - Please comment on Google doc!
        - FYI: David’s proposed this as a Black Hat topic (don’t know if it’ll be accepted). If you know of vulnerabilities caused by this, let David know.
        - Getting close to a version for final review (once Java & C# added).
    -

New Friends

- Helge Wehder, Ericsson
- Venu, nyu & open source contributor
- Nikita Koselev, working on AI & security intersection
- Salve J. Nilsen, CPAN Security Group

Opens

- [Venu] - lincc (license inconsistency checker)
    - https://github.com/vchrombie/lincc - Apache 2.0
    - David A. Wheeler can contact the licensing world, should do that whether or not we pick this up. Kate Stewart / Venu Tekula. David: Please send me email at dwheeler @ linuxfoundation.org
- Still need volunteers for creating labs! Talk to David! It only takes <day for a lab, need help. https://best.openssf.org/labs/create_checker on how, https://best.openssf.org/labs/ shows context. Contact me dwheeler @ linuxfoundation . org if interested.

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- http(s)?://bestpractices.dev now redirects to https://www.bestpractices.dev, per a GitHub request

Security Fundamentals Course SIG (David A. Wheeler)

-

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
- Academic Certification project
- Developer Manager Security Training course review
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-04-10 - C/C++ Compiler BP Guide

0800 Eastern Time/ 0500 Pacific / 1200 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Sy Tran Dung	sytrancsvn@gmail.com		he/him	sytranvn
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Doodle with poll for new time for fortnightly call: https://doodle.com/meeting/participate/id/b6z8NDLb
  - Starting with the first call in May we will switch to a new time / day which has not yet been determined. You can influence the new time for call by participating in the Doodle poll which is open between now and Wednesday, April 24.
  - Please note that the poll has an option for changing the bi-weekly cycle on which the call alternates, so if you prefer to k**eep the call on the odd weeks** you can vote on times between May 6 - 10. If you would prefer to have the call **moved to even weeks**, you can vote on times between April 29 - May 3.
  - Thomas will also send this same information to the BEST WG mailing list later today.
  - The new time, based on the poll, will be announced in the call on April 24 and disseminated in the usual channels
- New/Updated PRs:
  - Add -Wbidi-chars=any (#283, PR #438). All concerns addressed. Merged!
  - Add GCC option for checking virtual table pointers (341, PR #440)

    - Fix miscellaneous footnote issues (PR #439, minor). Merged!

Opens

- Guide Notes
- Mayank Ramnani: Mini-demo of Temper - Tool based on the OpenSSF compiler hardening guide to check and recommend compiler options
    - Source code available at: https://github.com/mayank-ramnani/temper
    - Discussion about GNU make vs POSIX make. GNU make is especially common so it might be better to use the spec instead of directly parsing the Makefile using regex. There were many specific comments.
    - Discussion about work on extraction of compiler options in a machine readable format from the Markdown file.
- Our Slack is at: https://join.slack.com/t/openssf/shared_invite/zt-2gv026obk-iIIGW4l9h1L6oywfl~QcvA

2024-04-09 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	
x	Maximilian Huber	maximilian.huber@tngtech.com	TNG Technology Consulting	he/him	maxhbr
x	Greg Kroah-Hartman	Greg Kroah Ha…	Linux Foundation		gregkh

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Salve J. Nilsen	sjn@cpan.org	CPANSec		sjn
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Reden Martinez	rmartinez@linuxfoundation.org	Linux Foundation	he/him	redenmartinez

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
    - @CRob ask the Security Toolbelt and Scorecard teams to come by and give updates
- OSS-NA next week - numerous folks from across the working groups will be presenting.
    - CRob will be presenting “Developing a secure, open future” based on a lot of this group’s work focused on helping DEVs.
    -
- xz conversation - is there anything BEST WG can assist with?
    - Vuln WG Issue 142 - Resources to help protect developers (humans) from attacks similar to the xz backdoor compromise
    - Vuln WG Discussion 143 - From a technical perspective, are there any options available to projects & maintainers to detect or avoid situations like the recent xz compromise?
    - Use “Second party” term for OSS that a business USES
        - Business that uses OSS makes the OSS developer in some sense is a second party, accepting the license could be considered a second party (there’s a closer relationship)
        - Issue: “I am not a supplier” - many will not be happy with that terminology, they don’t view themselves as supplier/vendor
        - Businesses won’t focus on software they don’t use
        - sjn's blogpost on "Second Party" and similar words: https://code.foo.no/2024/04/05/open-source-components-you-depend-on-are-not-third-party-components/
        - The dependencies include transitive dependencies. If “A depends on B depends on C” and you bring in A, then A & B & C are “second parties” under this terminologies, though they may or may not be considered important.

    - sjn's related blog post proposing some new vocabulary to be used in Open Source: https://code.foo.no/2024/04/03/a-vocabulary-for-a-new-open-source-age/ (also linked from the above post)
- Differentiate between what's important & what isn't
- Autotools made complexity easy to hide generation of tarball. Need to make it easy to generate the source code that's distributed.
- Need to separate build from test process. Test process shouldn't change build
- Hard to contribute money - how make that easier? Foundations could create their own programs so money can be sent to them.
- How do we influence how to send money? Tech Sovereign Fund as an example. OpenSSF/Alpha-Omega engaged with some governments. A "tech sovereign fund" has been hard to work out. NATO isn't an organization we've been contacting, that's an interesting idea.
- Note: Daniel Stenberg from curl - (Easy) ways to help struggling open source projects:
    - step in and help review a few PRs
    - help the project triage/reproduce bugs
    - if code in the PR looks complicated or is hard to understand, ask for an explanation
    - express your gratitude to the maintainers
    - make your company sponsor projects they depend on (which could be allowing an employee to spend time to do upstream work)"

- Proposal from David A. Wheeler
    - Secure programs must validate untrusted inputs. A widely-used mechanism for input validation is regular expressions.
    - Seth Larsen's *Regex character "$" doesn't mean "end-of-string"* made it clear that many people misunderstand regular expressions. In particular "$" means "end of string" in POSIX and JavaScript, but *not* in Perl, Python, Ruby.
    - Need to have stand-alone guidance making it clear how to use regular expressions for input validation, as well as modifying the fundamentals course to make this clear. The fundamentals course has some of this, but it's not as obvious.
    - Proposal: New guidance document "Correctly using Regular Expressions for Secure Input Validation"
    - Draft by David A. Wheeler here: https://docs.google.com/document/d/1Ors5T04Pgh3dcBfelbBrEBrvY3OKB7IoUBUJPYBmmZw/edit
    - Needs review & it'd be good to add new platforms
    - It's narrowly focused, but that's not a bad thing.
    - +1 CRob, +1 Seth L. & willing to review

    - +1 Max H
    - Max may have Java/.NET devs who can do this
    - Finding Java & C#/.NET
    - Don’t mind focused topic.
    - David will create GitHub issue: https://github.com/ossf/wg-best-practices-os-developers/issues/461
- Need to create labs for the fundamentals course!
    - Looking for someone willing to volunteer to develop labs, or at least a small example of “how to do X properly” where “X” is a topic in the fundamentals course.
    - List is here: https://best.openssf.org/labs
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Security Fundamentals Course SIG (David A. Wheeler)

-

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-03-27 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	George Wilson	gcwilson@us.ibm.com	IBM	he/him	gcwilson
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
x	Fotis Georgatos	fgeorgatos@gmail.com	HPE	he/him	fgeorgatos

Agenda

- Welcome new friends
  - Fotis Georgatos
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated PRs:
  - Add -Wbidi-chars=any (#283, PR #438)
    - Detailed comments were left on the PR on Github.
  - Add options from Weimer2018 especially errors for format-security and implicit-function-declaration(#342, PR #379)
    - Thomas has commented on #342 with some new information on -fexceptions in relation to Glibc's pthread implementation and thread cancellation
    - -Werror=format-security only impacts `printf` and `scanf` functions where the format string is not a string literal and there are no format arguments, as in `printf (foo);`
  - Fix incorrect reference to Weimer23 (PR #439, minor)

Opens

- Suggestion to revisit the time of the call.
  - Support for opening a Doodle poll for possible times. Announce on Best Practices Working Group Mailing list, BEST WG call, and Slack. Announce on this group's Slack. Thomas takes action point to organize.
  - Contact previous reviewers on GitHub
- We're generally very happy with the current document. There's still work to be done, but it's already quite helpful. It'd be good to have more voices heard.

- We also need to help make people aware of it. Many who should be using it don’t know about it. Let’s make sure people keep pointing to it. Should aso point people to it at events. etc.
-

Guide Notes

2024-03-26 - Full WG

Attendees:

NOTE

This meeting time conflicts with VulnCon. CRob can’t make it, David A. Wheeler had to be late. No one volunteered to lead the meeting. We’ll continue next meeting.

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Note: David A. Wheeler has a conflicting meeting, sadly, & plans to join ~20-30 minutes into the meeting. He *does* have things to share!
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
-
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- TSC approved legal documents. We're now waiting on LF Legal to create a Series (a mechanism that provides added legal protections)
- Per Dana Wang's request, added a mechanism so you can jump to specific sections of a project entry (in addition to jumping to a specific criterion). Use "section_NAME" where name is lowercased and space becomes underscore. E.g., <https://www.bestpractices.dev/en/projects/34#section_static_code_analysis>
- Various housekeeping tasks done
    - Made a large number of ownership/editor changes for LF ONAP. This changed the access rights for 42 project badge entries, due to changes within ONAP. Specifically whenever David McBride's ID 4469 and Jim Baker ID 3607 were editors, the project owner got "additional rights", the new owner become Sandra Jackson, and those two editors were removed from those with additional rights.
    - Fixed badge entry: https://www.bestpractices.dev/en/projects/8575 for project "Integration-Project" <https://github.com/XxBMRPxX/Integration-Project> that was making many false claims. This appears to be a student project, which is fine but making false claims is not. I gave them a second chance, as it appears they didn't understand what they were doing.
    - Deleted Best Practices badge project 8593, this was clearly a fraudulent effort
    - Hand-activated an account that for some reason wasn't activating & wasn't getting email <https://github.com/coreinfrastructure/best-practices-badge/issues/2119>. I've left a ticket with LF IT to see if there's a systemic issue with email.

Security Fundamentals Course SIG (David A. Wheeler)

- Enrolment continues to grow:

    - Developing Secure Software (LFD121) - 13,049 enrollments
    - Secure Software Development: Requirements, Design, and Reuse (LFD104x) - 6,135 enrollments
    - Secure Software Development: Implementation (LFD105x) - 3,147 enrollments
    - Secure Software Development: Verification and More Specialized Topics (LFD106x) - 2,923 enrollments
- We have a draft framework for creating optional labs for the fundamentals course *AND* several sample draft labs
- REQUEST 1: Please try out the new labs out & provide feedback/pull requests:
    - https://best.openssf.org/labs/hello.html
    - https://best.openssf.org/labs/input1.html
    - https://best.openssf.org/labs/input2.html
    - https://best.openssf.org/labs/csp1.html
    - Please provide feedback as issues or ideally pull requests. Note that the labs are maintained in the Best Practices WG's docs/labs/ directory.
    - It won't take long to try them out!
- REQUEST 2: Please help us create labs! Two steps: (1) create an example of "how to implement this fundamentals concept", (2) explain how to do it, (3) encode into a lab
    - List of labs we need to create & instructions here: https://best.openssf.org/labs/
    - Currently want to create 37 more labs, each relatively small. See "NEED" at https://best.openssf.org/labs/
    - If a few people would do just a few, it'd be a huge step forward. David would be delighted to work with you.
    - Demo (from EDU SIG presentation): https://zoom.us/rec/play/xBZRAb3m-bypXk3BfKHutUy4Co9NePbLIwXg2m_fGF4vRivXAwMTeTbkNawQsLyCajTP07TRvBSfVG0r.zYX71FXfm3eNsm0J?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fzoom.us%2Frec%2Fshare%2FF-tVKS7BZ-RXZKbksgqJh-5sDb7rIyDG7nh5qJiv2E1vFkeGj_T_0k8vjy4-fcKc.Bu9-LqHSA0KAhTG4

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG OpenSSF EDU.SIG Meeting Notes - 2024
- Education plan released! See: OpenSSF Releases Plan for Improving Software Developer Security Education

- If you're involved in software development, please take our secure development education survey: https://www.research.net/r/9TGV738 - for more details see https://openssf.org/blog/2024/03/11/participate-in-our-survey-on-secure-software-development-education/
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-
-

2024-03-13 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	CRob	crob@intel.com	Intel	he/him	SecurityCRob
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler

x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani

Agenda

- Welcome new friends
  - Mayank Ramnani - grad student at New York University (NYU)
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Talk at SOSS Community Day NA, April 15, 2024 (Georg will present).
  - Accepted as lightning talk
  - Probably should post on Slack channel so others will know.
  - Are there key points we should note?
  - Note connection to government recommendations. The US government has big press on memory safe languages, but there’s an admission that you can't rewrite everything, note this when you don’t rewrite. Might mention EU CRA. Also Secure by Design (MANY governments backing).
  - Maybe look at Thomas’ FOSDEM material: https://fosdem.org/2024/events/attachments/fosdem-2024-3468-compiler-options-hardening-for-c-and-c-/slides/22562/Slides_3vYNJqd.pdf
  - WG Google drive: https://drive.google.com/drive/folders/11CsDjMe5OeKg5cwIbdKGRnui529N8CPY
- New/Updated PRs:
  - Require use of Modern C, addendum (#339, PR #378)
  - Add -fasynchronous-unwind-tables and -fexceptions options from Weimer2018 to list of considered options (#342, PR #379)
  - Both #378 and #379 agreed on with some typo fixes. Plan to leave up for a few day
- Issue #342. Still need to cover -Werror=format-security. Need to investigate if it’s reasonable to add it to the very top. Maybe ask the distros?
  - See https://fedoraproject.org/wiki/Format-Security-FAQ
  - Need more research
  -

Opens

- Utility of tool/python script based on the guide that recommends/checks compiler best practices for a project, and creates a new project with secure compiler options.
-

Guide Notes

-

2024-03-12 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Jared Miller	jared.miller@sap.com	SAP		
x	Mohit Singh	mohit.singh@sap.com	SAP	he/him	

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- **New group meeting**: EDU SIG will have a group of folks focused on academic certification and content modularization for broader academic use of our content. (Every other Weds 9am ET - see OSSF Community Calendar)
- **New SIG** focused on BP for Web Devs - contact Daniel and Randall if you are interested in collabing. Meetings/calendar entry forthcoming
- Mem Safety SIG working on creating a workshop to further M.S. practices across the ecosystem. Reach out to M.S. SIG if you’re interested to learn more or to participate

- OSS-EU - CFP now open! Vienna - Sept 16-18 -
    - https://events.linuxfoundation.org/open-source-summit-europe/
- SOSS*Fusion - CFP open now! - ATL -Oct 22-23 -
    - https://events.linuxfoundation.org/soss-fusion/
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

- A new group is formed under the education SIG. It includes members of academia and are named the Certification Education SIG.
- David A. Wheeler will create some labs.
- Daniel and Randall from the BEST WG are leading a new SIG for Web Security. Look for further updates about that
- The Memory Safety SIG that rewrote the mobilization plan's section on Memory Safety and are collaborating with the C/C++ hardening guide group. The SIG is forming a workshop that will try to increase the usage of memory safe by default languages and improve upon the continuum of memory safety within the ecosystem and hopefully provide insights and tools to the community on how to make memory safe decisions in software development. Reach out to the SIG on their repo or through Avishay Balter or Nell Shamrell-Harrigton.
- Open Source Europe conf is still open for talks. CRob will present best practice guides and tools for developers to use seamlessly that were developed under the OpenSSF
- The US SOSS fusion conference is still open for talks. It should be open for maintainers and contributors and hopefully will have a larger crowd to present the work we've been doing.
- David A. Wheeler is sharing an update about the labs for the fundamentals course. We're hoping to have three courses under development which are planned.
- The fundamentals course should have labs soon and is now under construction to be able to run fully on the client side, without any server-side components.
- David: I'm looking at a minor change in approach.
    - The first labs were meant to be based on JavaScript, where people write JavaScript code that is executed client-side. The original idea is that we'd

        emulate parts of a framework (Express) and validator (express-validator). However, there are some technical difficulties and missing documentation that are making this approach take a long time to develop.
    - Instead, the solution that is proposed is to only check the answer. A question is asked about the experience for the trainee. The goal is that the trainee presses a button that redirects them to the "problem" that they have to solve. The problem is described as text and the answer is given as text, and there is no emulation taking place. The good news is that this approach will be MUCH faster to implement, and it'll be much easier for others to contribute labs.
    - If later on we decide to create a more complete emulation, that isn't wasted effort, because this way we'll focus first on creating the right questions.
-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Security Fundamentals Course SIG (David A. Wheeler)

-

SKF project (Glenn)

-

OpenSSF Scorecard project (Laurent - Spencer)

- OpenSSF Scorecard New Contributor Workshop co-located at OSS NA <link> April 15
    - Goal is to attract long-term contributors with a hands-on onboarding experience
    - Participants will need to register for OSS NA and add workshop as an add-on
    - Community drafting elements of MVSR, conducting backlog refinement, improving docs in preparation for workshop
- OpenSSF Scorecard Tech Talk scheduled for tomorrow (March 13) - register here
- OpenSSF Scorecard Blog Post mentions upcoming events:
    - "Finally, the OpenSSF Scorecard website, including documentation and API is changing from securityscorecards.dev to scorecard.dev. The new site is up and running. **We'll continue to host api.securityscorecards.dev for 12 months,**

    afterwhich the API will redirect to api.scorecard.dev. Migrate your applications, or ensure you follow redirects.”
    - Structured Results feature release coming in April
    - User survey open until after OSS NA to help steer project strategy <link>

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-02-28 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	balteravishay
x	Andrew Fryer	andrewtfryer@gmail.com		he/him	Andrew-Fryer

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Discussion on related activities:
    - FYI: US White House - Memory-Safety. OpenSSF post notes the C/C++ options guide.
        - https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf
        - https://openssf.org/blog/2024/02/26/openssf-supports-efforts-to-build-more-secure-and-measurable-software/
    - This options guide was also mentioned in the OpenSSF response to CISA
    - CISA OSS roadmap: https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c.pdf
- Updated PRs:
    - Require use of Modern C (#339, PR #357)
        - David: There's a minor verb form to fix, recommend fix that & merge it later today
        - David: Thanks everyone for the back-and-forth to work this out!
        - All agreed to merge after fixing the verb form.
        - Thomas: I'll fix that & merge it later today.
    - Should there be a "what should you do when compiling compilers" section at all? (#335, PR #363)
        - This is still relevant especially in the embedded space.
        - Thomas: Instead of removing this material, move it to the end of the document.
        - David: I like this solution!

            - (Some technical discussions on the options ensued to ensure they were fine.)
            - No objections, let’s merge.
        - Compiler attributes for improved security (#201, PR #268)
            - David: If we add this, we should add cross-links between the options guide and this new compiler attributes guide, once it’s mature enough that we’re ready for that.
            - David: We probably need more examples. Don’t need examples for everything, but more examples would clarify things.
            - Thomas: Needs a little refining.
            - Let’s work with Siddesh, merge as incubating, then add examples.
        - Recommend use of -Wformat and -Wformat=2 together (#334, PR #368)
            - Clang’s behavior is really strange & unexpected. Asking for both flags resolves it & gives the same results for GCC and Clang.
            - Godbolt output shown, shows that this solution really works.
            - Thomas will file an issue on LLVM: https://github.com/llvm/llvm-project/issues/83271
            - David: This is a bizarre situation, and a good solution. Supportive!
            - Agreed to merge.
- Open questions from the Memory SIG workshop (Andrew Fryer & Avishay)
    - Looking for early feedback. In-person or online? Date? Focus?
    - Idea: “OS support for memory-safe languages in drivers (Linux, Windows)”
    - Idea: Memory-safety nuances
    - Idea: If working with Rust & have to use unsafe Rust, guidance on how to write unsafe Rust
    - Idea: How to rewrite PARTS of a system from memory-unsafe to memory-safe
    - Not a conference of lectures, but a workshop for discussion of gaps/issues.
    - Maybe consider having the workshop create a document/material
- Open Issues
    - Vtable verification during compiling C++ code (#341)
        - Need more information
    - Add options from Weimer2018 especially errors for format-security and implicit-function-declaration (#342)
- Notes:
    - There is a lively issue on Scorecard that tries to address some of that gap with great responses from the likes of Art Manion and more: Adding memory safety related checks · Issue #3736 · ossf/scorecard (github.com)
    - Avishay Balter to Everyone (Feb 28, 2024, 8:50 AM)
        - Memory-Safety/docs/best-practice-memory-safe-by-default-languages.md at main · ossf/Memory-Safety (github.com)
        - Memory-Safety/docs/best-practice-non-memory-safe-by-default-languages.md at main · ossf/Memory-Safety (github.com)
- Thank you everyone! We got a number of PRs accepted & we welcome our memory-safety SIG friends!

Opens

-

Guide Notes

-

2024-02-27 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [SCM]	d.appelquist@samsung.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	Randall T. Vasquez [LF]	randall@linux.com	The Linux Foundation	he/him	ran-dall
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
x	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip
x	Sean McGinn	Sean.McGinn@amd.com	AMD	he/him	
x	Cheuk Ho	cheuk@openssf.org	OpenSSF	she/her	Cheukting

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Mohit Singh	mohit.singh@sap.com	SAP	he/him	
x	Jared Miller	jared.miller@sap.com	SAP		

Agenda

- Is someone willing to scribe for the meeting today?
    - David & Daniel
- Welcome new friends
    - Sean McGinn (AMD)
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
- BEST Issue 364 - Create TAC PR to document BEST WG in TI Lifecycle levels - BEST = Graduated
    - WG's & TIs are being asked to complete assessment of the level they are operating at & file a PR to discuss with TAC.
    - We have a few small gaps that if we closed, BEST would be at the highest level - Graduated
    - Can we work on a few pieces of documentation and get this finished?
- Education (from education SIG, EDU.SIG)
    - Proposed education plan complete, QUICKLY provide last-minute comments: https://docs.google.com/document/d/1SrFkV4JRpqTSonp7VTKhyLYVpzOzSzgW4eOKIfCYwO8/edit#heading=h.qzrjscev9ut3 ; David will write a blog post
    - Draft education survey instrument (SRM) complete, comments due tomorrow. https://docs.google.com/spreadsheets/d/1IHsHM4BU2jkF7arGTat1dN915MJ4mc8Go83q3zmRiUY/edit
    - EDU.SIG is working on reviewing Developer Manager donated content & working up proposal for modularized curriculum for academics' consideration
        - https://docs.google.com/presentation/d/1W0NpN28kSw0BxmHF2L63LsKdy0OT5jb342zQo30AS30/edit#slide=id.p1
- Best Practices badge: LLC & TSC
    - FYI: The Linux Foundation plans to move this project into its own LLC (this provides various legal protections). This requires us to do some paperwork & set up process formalities that we should do anyway.

Starting to work on that. Details here: https://github.com/coreinfrastructure/best-practices-badge/pull/2107

- Update on W3C Community Group / Web Security Joint Work… (Dan)
    - https://github.com/w3c/secure-the-web-forward-workshop/issues/42
    - W3C has a new security lead, Simone Onfri
    - They are looking for co-chairs of a potential working group
    - Create a tracking issue in our repo? [agreed yes, and https://github.com/ossf/wg-best-practices-os-developers/issues/367 was created]
- Open questions from the Memory SIG workshop.
- FYI: US White House released "PRESS RELEASE: Future Software Should Be Memory Safe" on 2024-02-26, https://www.whitehouse.goif yov/oncd/briefing-room/2024/02/26/press-release-technical-report/
    - Full report "BACK TO THE BUILDING BLOCKS: A PATH TOWARD SECURE AND MEASURABLE SOFTWARE" at https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf
- Please interact via mailing list & Slack channel, please participate in our work!
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Security Fundamentals Course SIG (David A. Wheeler)

-

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-02-14 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	Siddhesh Poyarekar	siddhesh@gotplt.org	Red Hat	he/him	siddhesh

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Updated PRs
    - Require use of Modern C (#339, PR #357)
        - Siddhesh noted that it would be useful for add references to GCC 14 and Clang 17 to the detailed description
    - Should there be a "what should you do when compiling compilers" section at all? (#335, PR #363)
        - Siddhesh was supportive of the proposed change and pointed to an ongoing, orthogonal discussion around possibilities to sandbox the compiler when dealing with untrusted code being built. There are some connection points to other OpenSSF guidance, e.g., the Go guidelines being developed at the Memory Safety SIG. Thomas will look into if there are relevant material this section could refer
- Open Issues
    - Consider documenting additional sanitizers (#336)
        - Siddhesh noted that software CFI is a requested feature for also for GCC (but not yet supported).
        - Thomas will look into adding some text for Clang -fsanitize-cfi and -fsanitize-shadow-stack.
        - -fsanitize-safe-stack has been discussed earlier but not added in the main guide due to compatibility issues
    - split-stack feature on GCC and clang compiler (#340)
        - Discussion around the intended use of the split-stack feature: originally added to support Go coroutines and possible other user-level, co-operatively, scheduled thread implementations, such as Boost fibers. May have limited applicability (x86 only) and there were some questions w.r.t. how split-stacks interacts with the

        kernel guard pages and contiguous stack resizing. Thomas will look into the concrete implementation.
        - Siddhesh noted that the blog post referred to in the issue was intended to cover the relevant options for stack control available in GCC, and not necessarily imply a recommendation to use split-stack.
    - Vtable verification during compiling C++ code (#341)
    - Add options from Weimer2018 especially errors for format-security and implicit-function-declaration (#342)

Opens

- https://github.com/ossf/wg-best-practices-os-developers/issues/201
    - Thomas and Siddhesh agreed to change the “Supported by” column to state “Supported since” to be consistent with the main guide and indicate GCC 2.95.3 as the version number for annotations that “have been around for ever”
    - It was agreed to merge the initial draft after addressing the nitpicks, and then work towards adding more detailed descriptions for the annotations going forward

Guide Notes

2024-02-13 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	d.appelquist@samsung.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	Randall T. Vasquez [The Linux Foundation]*	randall@linux.com	The Linux Foundation	he/him	ran-dall
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
x	Cheuk Ting Ho	cheuk@openssf.org	OpenSSF	she/her	Cheukting
x	Mohit Singh	mohit.singh@sap.com	SAP	he/him	
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson
x	Jared Miller	jared.miller@sap.com	SAP		jdmcyber

Agenda

- Is someone willing to scribe for the meeting today?
    - Dan! (yay!)
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
    - CRob must leave at the bottom of the hour
- Sub-project updates (as needed)
    - Memory Safety - Progress on workshop and new content
- Thoughts on Best Practices for Web Developer project
    - We'll get an issue filed to track this after today
    -
- [drusso] Question about Best Practices badge access requirements: "This badge asks for read-level access to certain elements of a Github repository and organization. The Best Practices badge is an open source project and there are no public docs on what it needs access to/uses the access for, which is why we need the official evaluation."
    - Believe it is to verify certain files, e-mail David W for information
- SOSS*FUSION conference Oct22-23 near ATL. CFP opens today-ish
    - https://events.linuxfoundation.org/soss-fusion/

New Friends

- No new friends.

Opens

-

Backlog Review

-

Meeting Notes

- **Memory safety** - Avishay - working on some new content … defining new aspects … talking to rust, python. Go, communities… not a “binary” but a continuum… drafting that doc. 2nd initiative we’re trying to promote - a workshop … want to organize such a workshop - maybe along side of SOSS conference (https://events.linuxfoundation.org/soss-fusion/) ? Want to speak to Daniel… One topic is how memory safe languages are being natively handled by operating systems…
- What kinds of communities? Looking to W3C / OSSF workshop as a template. The Audience would relate to the topics… Microsoft could share some info on the OS side… maybe other OS vendors could do the same…
- Crob: Rust foundation as well…
- [dan: suggest Mozilla…]
- Cheuk: suggest Steve Dower? … active in python.
- CROB - brand new conference - **SOSS fusion -** dream is to unite security communities - premier security event -will be held near Atlanta, GA, USA… Oct 22-23 2024.
- Dave Russo**: Question about best practice badge**: need some info. Will chase David.
- **Creating some kind of artifact compiling best practices for web developers** - 2 or 3 folks have expressed interest.
- Dan: thinking of collaboration with the w3c … they have a new security person….
- Dan: was thinking same magnitude as the SCM guide…
- Crob to ask staff to create a channel… and will send a doodle to find a time…
- Dan: I can play a coordination role - would be great to have another person as well…

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Security Fundamentals Course SIG (David A. Wheeler)

-

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-01-31 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler

x	Mark Esler	mark.esler@canonical.com	Canonical	they/them	eslerm

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New PRs
    - Require use of Modern C (#339, PR #357)
        - These are based on [^Weimer2023] Weimer, Florian, "Porting to Modern C", <https://fedoraproject.org/wiki/Changes/PortingToModernC>
        - Discussed if we should recommend this for everyone or only to projects already using modern C.
    - tl;dr section suggests options that it maybe shouldn't (#333, PR #358)
        - Ack'd #358, has implications to #277
- Open issues
    - Clarify why -O2 (#331)
        - Discussed pros and cons of adding -O2 as a separate option vs. -O0 as a discouraged options since it interferes with _FORTIFY_*SOURCE*
    - -Wformat=2 vs -Wformat (#334)
        - GCC Documentation
        - Clang Documentation https://clang.llvm.org/docs/DiagnosticsReference.html#wformat
        - See gcc: https://gcc.gnu.org/onlinedocs/gcc/Warning-Options.html
        - Unfortunately this appears to be an unintentional divergence between gcc and clang.
        - Possible solution: “-Wformat -Wformat=2”. Adding the second option would make the first option a no-op in gcc, but might add the options desired in clang. We need to test this.
    - Should there be a "what should you do when compiling compilers" section at all? (#335)
    - Consider documenting additional sanitizers (#336)
    - Require use of Modern C (#339)
    - split-stack feature on GCC and clang compiler (#340)
    - Vtable verification during compiling C++ code (#341)
    - Add options from Weimer2018 especially errors for format-security and implicit-function-declaration (#342)

Opens

Guide Notes

- Action point from 2023-01-17: Evaluate -fsanitize-minimal-runtime for possible hardening (#326)
    - Thomas still looking into this.
    - Some relevant discussion on uses of -fsanitize-minimal-runtime on GCC Bugzilla: https://gcc.gnu.org/bugzilla/show_bug.cgi?id=94307

2024-01-30 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	CRob [WG]	crob@intel.com	Intel	he/him	SecurityCRob
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	Randall T. Vasquez [SKF]	randall@linux.com	Gentoo/Homebrew	he/him	ran-dall
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
x	Cheuk Ho	cheuk@openssf.org	OpensSF	she/her	Cheukting
x	Seth Larson	seth@python.org	PSF	he/him	sethmlarson
x	Mohit Singh	mohit.singh@sap.com	SAP	he/him	
x	Lucas Gonze	lucas@gonze.com	Independent	he/him	lucasgonze

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
  - Benilda (staying up late!)
- Randall T. Vasquez has agreed to be our WG Co-lead! (Issue 220)
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
  - EDU.SIG training update
- SOSS Task Force Issues 255, 256, 257
  - Any group interest to help move these forward?
  - David: I've done some research on automatically identifying if someone knows how to develop secure software.
- Issue 232 - archive Great MFA
- Any interest from the group in colabing on any of these items we put onto our WG roadmap:
- https://github.com/ossf/wg-best-practices-os-developers?tab=readme-ov-file#roadmap
  - Evangelize OpenSSF "best practices" and tooling through blogs, podcasts, conference presentations, and the like. -- Create a "Secure from the (open) source" expert podcast to showcase the work across the foundation. -- As new guides/best practices are launched, we will create blogs and a conference presentation to raise awareness about it. -- Amplify talks and artifacts created by other groups within the foundation -- Create 3 EvilTux artifacts each quarter
  - Create express learning classes for our body of work: working group explainer, SCM BP Guide, C/C++ Guide, Scorecard/Badges, Concise Guides
  - Create a "Best Practices Member Badge" for member organizations
  - Support and promote our sub-projects with contributions and feedback - Scorecard, BP Badges, OpenSSF - SkillFoundry, Classes, and Guides, Secure Software Guiding Principles (SSGP)
  - Create a Memory Safety W3C-style workshop to assemble development leaders to talk about how to integrate memory safe languages and techniques more deeply into the oss ecosystem.
  - Expand DEI AMA Office Hours to more broadly engage new-to-oss individuals and provide a forum for mentorship and guidance as they launch into and grow within their careers.
  - Identify, curate, produce, and deliver new secure development education such as Developer Manager Training, Implementing/Integrating OSSF tools such as Scorecard, Badges, OSV, OpenVEX, etc), advanced secure development techniques, and more.
  - Evangelize and embed all of our guides across OpenSSF Technical Initiatives and understand what makes sense to integrate into Scorecard

    - Evangelize OpenSSF “best practices” and tooling through blogs, podcasts, conference presentations, and the like. -- Create a “Secure from the (open) source” expert podcast to showcase the work across the foundation. -- As new guides/best practices are launched, we will create blogs and a conference presentation to raise awareness about it. -- Amplify talks and artifacts created by other groups within the foundation -- Create 3 EvilTux artifacts each quarter
    - If want to go higher, use the Concise Guide
    - Create express learning classes for our body of work: working group explainer, SCM BP Guide, C/C++ Guide, Scorecard/Badges, Concise Guides
    - Create a “Best Practices Member Badge” for member organizations
    - Support and promote our sub-projects with contributions and feedback - Scorecard, BP Badges, OpenSSF - SkillFoundry, Classes, and Guides, Secure Software Guiding Principles (SSGP)
    - Create a Memory Safety W3C-style workshop to assemble development leaders to talk about how to integrate memory safe languages and techniques more deeply into the oss ecosystem.
    - Expand DEI AMA Office Hours to more broadly engage new-to-oss individuals and provide a forum for mentorship and guidance as they launch into and grow within their careers.
    - Identify, curate, produce, and deliver new secure development education such as Developer Manager Training, Implementing/Integrating OSSF tools such as Scorecard, Badges, OSV, OpenVEX, etc), advanced secure development techniques, and more.
    - Evangelize and embed all of our guides across OpenSSF Technical Initiatives and understand what makes sense to integrate into Scorecard
    - Best practices for web development - possibly in coordination with w3c. <- Dan, David, Randall expressed interest. Possibly a concise guide, possibly more like the SCM guide in scope.. Needs to be scoped out. Riffing on the output of the W3C workshop run last year: Workshop overview - W3C Workshop Secure the Web Forward
    - Many React developers think security doesn’t apply, then end up with bad cryptography, etc. Also, single-maintainer projects don’t have a lot of time.
    - Last yera’s W3C Workshop Secure the Web Forward: Driving developer awareness and adoption of Web security standards & practices https://www.w3.org/2023/03/secure-the-web-forward/
    - Some blind spots for client-side JavaScript:
        - Builders. Vipe was broken into
        - CORS allows client-side to contact untrusted sites, yet developers haven’t adjusted.
- [lucas] Markdown for Badges

New Friends

-

Opens

- Translations?

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

- Modified badge entry form to make it more obvious how to show "what's left to do" - increased color contrast of button, changed its text, moved it closer to the panels. https://github.com/coreinfrastructure/best-practices-badge/pull/2098

Security Fundamentals Course SIG (David A. Wheeler)

- "Improving Software Developer Security Education" - draft by David A. Wheeler - https://docs.google.com/document/d/1SrFkV4JRpqTSonp7VTKhyLYVpzOzSzgW4eOKIfCYwO8/edit - comments welcome!

SKF project (Glenn)

-

Scorecard project (Laurent - Spencer)

-

EDU.SIG (CRob + SIG)

- FULL SIG Notes

- Developer Manager training donated to the OpenSSF from Intel! Review & revision process begins now. CONGRATS to Intel!
    - David & CRob will look through, then share probably by converting to Google slide.

Memory Safety SIG (Nell)

- FULL SIG Notes
-

SCM BP Guide SIG (Dan + Christine) [In hibernation after guide release]

- Issue 102
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/SCM-BestPractices
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides

2024-01-17 - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1400 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
x	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
x	CRob	crob@intel.com	Intel	he/him	SecurityCRob
x	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
x	Siddharth Sharma	siddharth@redhat.com	Red Hat	he/him	sidhax

x	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
x	Siddhesh Poyarekar	siddhesh@gotplt.org	Red Hat	he/him	siddhesh
x	George Wilson	gcwilson@us.ibmoh.com	IBM	he/him	gcwilson
x	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- FOSDEM’24 talk proposal by Thomas accepted to lightning talks track: https://fosdem.org/2024/schedule/track/lightning_talks/
    - It’d be great to see a proposal on 2024 SOSS day NA - proposals due Feb 9. Thomas Nyman will look at it, if not going, Georg Kunz might be around. Wheeler will be around, will consider. More info: https://openssf.org/blog/2024/01/11/submit-to-speak-at-soss-community-day-north-america-2024/
    - Other SOSS days too.
    - Will continue discussion on Slack

Opens

- David A. Wheeler created a number of pull requests, can we merge them?
    - You can see Wheeler’s PRs here: https://github.com/ossf/wg-best-practices-os-developers/pulls?q=is%3Apr+is%3Aopen+label%3A%22Product%3A+Compiler+Hardening+Guide%22
    - More clearly distinguish -Werror with and without selectors (#345) - accepted
    - Discuss further how to apply the guide (#328) - accepted
    - Add threat model, goals, objectives (#317) - accepted
        - Siddhesh noted that we should be careful with the actual flag recommendations to be inclusive of languages and encodings particularly (right-to-left languages) which may be impacted by the option recommendations. The threat model text itself is not a concern.
            - David: Agreed!
        - Accepted
    - Add -fno-delete-null-pointer-checks and friends (#323)
        - Long discussion:

    - Change this paragraph about trivial-auto-var-init:
      - The setting `-ftrivial-auto-var-init=pattern` is sometimes useful when generating instrumented test code. However, the `pattern` value can interfere with *other* tools that are being used to monitor instrumented test code. For example, the `pattern` value interferes with `-fsanitize=memory` in clang 17.0.1. Due to these conflicts, the `pattern` value is not universally recommended for generating instrumented test code.
      - Into: “This setting can sometimes conflict with other tools that are being used to monitor instrumented test code, since it is expressly setting a value that was not set by the source code.”
      - David: After the meeting I made 2 tiny last-minute changes: conflict -> interfere; instrumented test code -> executable code
      - David Wheeler will change after meeting today.
      - Thomas Nyman will update date once it’s added
    - This had some notes from the previous meeting (marked in yellow):
    - Have discussed this several times in the past (somewhat controversial). Options don't make sense for using in production use cases as it could hide some bugs - Now addressed in the latest iteration
    - Guide now has made distinction between release and instrumented test code, that could allow us to add these items
    - Siddhesh - perhaps add the note it could mask bugs
    - Siddhesh - the mitigation is good, but might interfere with actually finding the bugs. This should be disabled in test
    - Thomas - perhaps move these options to their own table, removing them from he more straight-forward ones
- New(ish) issues:
  - Evaluate -fsanitize-minimal-runtime for possible hardening (#326)
    - This is feedback on Hacker News from the release of our guide!
    - Thomas will look into this.
  - Compiler flags notes/comments by Dominik Czarnota (#330)
  - Clarify why -O2 (#331)
  - tl;dr section suggests options that it maybe shouldn't (#333)
  - -Wformat=2 vs -Wformat (#334)
  - Should there be a "what should you do when compiling compilers" section at all? (#335)
  - Consider documenting additional sanitizers (#336)
  - Require use of Modern C (#339)
  - split-stack feature on GCC and clang compiler (#340)
  - Vtable verification during compiling C++ code (#341)
  - Add options from Weimer2018 especially errors for format-security and implicit-function-declaration (#342)

Guide Notes

-

2024-01-16 - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
x	Daniel Appelquist* [TAC]	dan@torgo.com	Samsung	he/him	Torgo
x	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
x	Randall T. Vasquez [LF]	randall@linux.com	LF/Gentoo/Homebrew	he/him	ran-dall
x	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
x	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	
x	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
x	Jessica Marz	jessica.marz@intel.com	Intel	she/her	jkmarz

Regrets: CRob will be late.

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review

- Sub-project updates (as needed)

New Friends

- Lucas Gonze - interested in workflow views of scorecard
- Aristide Bouix - a user of scorecard and allstar in their company

Opens

- “Improving Software Developer Security Education” - draft by David A. Wheeler - https://docs.google.com/document/d/1SrFkV4JRpqTSonp7VTKhyLYVpzOzSzgW4eOKIfCYwO8/edit - comments welcome!
    - Have been writing a draft paper on improving security education - with education SIG. 2 years ago we developed materials after log4shell, etc… expectation of funding to improve funding - funding didn’t happen. So what do we do instead? Step 1 - look more at what’s already out there. I’ve briefly summarized what’s out there in this doc. Please send me comments. Plan after this is to work with others…
    - Randall: agree with the ideas developed in the education plan…
    -
- Workflow views of the Scorecard - note, Lucas Gonze is in a noisy place
    - https://github.com/ossf/wg-best-practices-os-developers/issues/344
    - Lucas : a thread - a non-regular OpenSSF contributor critiqued … Scorecard sees itself as a metric but maintainers might use it to guide their workflows. But as a metric it’s a little less clear. We discussed this… I proposed… (in the linked issue) a couple of ideas to implement this…
    - David: original discussion covered both scorecard and best practices badge… We’re moving one element of best practices badge to help make it more findable. Another option is generating markdown… after some discussions … since there isn’t a standardized kanban format we generate some markdown - for a checklist… Might make sense for scorecard…
    - Lucas : a markdown export… makes sense. A kanban export seemed to be out of scope for OpenSSF. For Best Practices badge UI - might be productive to consult with usability specialists - how to communicate info that is being lost right now. Also how about a CSV output (for the to-do).
    - *JSON can already be generated*
    - As next steps: write a feature request for both scorecard and best practices to generate the markdown… other followup, write a ticket on usability in best practices…
        - Usability review of "hide completed" toggle in Best Practice UI (Change top button colors to increase contrast coreinfrastructure/best-practices-badge#2093)

        - Auto-generate markdown to copy/paste. (Add ability to generate Markdown "todo" list for GitHub/GitLab issues, Kanban boards, etc. coreinfrastructure/best-practices-badge#2094)
    - Lucas: one way to think about it is that workflow is a primary output of OpenSSF - helping Open Source maintainers deal with security issues is a general mandate.
    - David: different people have different workflow approaches - so we need to integrate into others' work-flows.

Backlog Review

Issues · ossf/wg-best-practices-os-developers (github.com)

- Lots of compiler hardening issues.. Should be dealt with in that SIG.
- Proposal to Archive - Great MFA distribution SIG · Issue #232 · ossf/wg-best-practices-os-developers (github.com)
    - Dw: i think info from that group is important - but we are not active so we should declare this as archived… I think we can archive…
    - Randall: 2nded.
    - David: 2nd
    - *no objections*
    - WG agrees that MFA is archived. We accomplished a lot, 2FA is now more common, we're moving on.
    - Randall to add it to the issue.
    - This is not a failure, this is a success. We got tokens distributed to many important OSS projects.
- (1) Proposal: workflow view of scorecard and badge output · Issue #344 · ossf/wg-best-practices-os-developers (github.com)
    - Dan: should this be transferred over to Scorecard repo?
    - Dw: I think it's fine to open
    - Dw: I think this actually makes sense to keep here - as it straddles 2 project - but yeah someone needs to open an issue in scorecard. We can then close it here.
- Link to short presentation on developing secure software (EDU) · Issue #243 · ossf/wg-best-practices-os-developers (github.com)
    - Dw: i created it but didn't create the link yet… Brief intro on how to develop secure software…
    - Randall: looks good.
    - Dw: I will create a PR for this (adding the link to the presentation) and then we can close this.
    - Presentation is here: https://docs.google.com/presentation/d/1GzLX4CYr4HtXrNF6wyO11hzz9EgwriKhnbvVZ9-LG2E/edit
- Modify CSS of generated pages · Issue #160 · ossf/wg-best-practices-os-developers (github.com)
    - Dan: is this done?

    - DW: i think there is a broader issue - main OpenSSF site is a wordpress site… some discussion on moving to github… significant modification to css will wait on that…
    - So it’s “on hold” for now… *added **blocked** label and added that label here*

Meeting Notes

-

< TEMPLATE > - Full WG

Attendees:

(please **Mark your attendance if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present?	Name	Email	Affiliation	Pronouns	GitHub ID
	Avishay Balter* Co-chair	avbalter@microsoft.com	Microsoft	he/him	balteravishay
	Georg Kunz* Co-chair	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
	CRob	christopher.robinson@linuxfoundation.org	Linux Foundation	he/him	SecurityCRob
	Christine Abernathy * [SCM]	c.abernathy@f5.com	F5	she/her	caabernathy
	Daniel Appelquist* [SCM]	daniel.appelquist@snyk.io	Snyk	he/him	Torgo
	Dave Russo* [EDU]	drusso@redhat.com	Red Hat		drusso-rh
	Thomas Nyman* [C/C++]	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
	Nell Shamrell-Harringt	nells@microsoft.com	Microsoft	she/they	nellshamrell

Present ?	Name	Email	Affiliation	Pronouns	GitHub ID
	on* [Mem Safe]				
	Laurent Simon* [Scorecard]		Google		
	David A. Wheeler* [Badges + courses]	dwheeler@linuxfoundation.org	Linux Foundation		
	Eddie Knight* [Baseline]		Sonotype		
	Michael Lieberman* [Baseline]		Kusari		
	Jeff Borek		IBM		
	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
	Yotam Perkal		Rezilion		
	Matt Rutkowski	mrutkows@us.ibm.com	IBM	he/him	
	Marta Rybczynska	rybczynska@gmail.com	Syslinbit	she/her	
	Ixchel Ruiz	ixchelruiz@yahoo.com	jfrog		
	Eric Tice	eric.tice@wipro.com	Wipro		erictice
	Chris de Almeida	SoftwareChris@us.ibm.com	IBM	he/him	ctcpip

Agenda

- Is someone willing to scribe for the meeting today?
- Welcome new friends
- Call for opens (list new items below)
- WG Administrivia/bookkeeping/backlog review
- Sub-project updates (as needed)
-
-

New Friends

-

Opens

-

Backlog Review

-

Meeting Notes

-

Project Updates

(please enter and speak to anything interesting)

OpenSSF Best Practices Badge project (David A. Wheeler)

-

Education (Security Fundamentals etc.) (David A. Wheeler)

- ▪

Scorecard project (Laurent - Spencer)

- ▪

EDU.SIG (CRob & Dave R)

- FULL SIG Notes
-
-

Memory Safety SIG (Nell)

- FULL SIG Notes
-

C/C++ BP Guide SIG (Thomas)

- Issue 97
- https://github.com/ossf/wg-best-practices-os-developers/tree/main/docs/Compiler_Hardening_Guides
-

Python Hardening Guide SIG (Helge & Georg)

- BEST Issue 481
-

WebDev Security Guide (Daniel)

- BEST Issue 367
-

Security Baseline SIG (Eddie & Michael & CRob)

- Meeting Minutes
-

<TEMPLATE > - SCM BP Guide [In hibernation after guide release]

Attendees:

(please **Mark your name in black if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
	Christine Abernathy * [DEI & SCM]	c.abernathy@f5.com	F5	she/her	caabernathy
	Daniel Appelquist* [SCM]	daniel.appelquist@snyk.io	Snyk	he/him	Torgo
	Noam Dotan	noam@legitsecurity.com	Legit Security		
	Arnaud J Le Hors	lehors@us.ibm.com	IBM	he/him	lehors
	Crob	crob@crob.crob	crobtel	he/crob	crob

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- Is anyone interested in co-leading this project?
- Review existing guide
- Next steps

Opens

-

Guide Notes

-

<TEMPLATE > - C/C++ Compiler BP Guide

0900 Eastern Time/ 0600 Pacific / 1300 UTC

Attendees:

(please **Mark an "X" next to your name if you are here,** or add-row name/email/affiliation if joining)"*" denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID
	Thomas Nyman*	thomas.nyman@ericsson.com	Ericsson	he/him	thomasnyman
	CRob	Christopher R…	OpenSSF	he/him	SecurityCRob
	David A. Wheeler	dwheeler@linuxfoundation.org	Linux Foundation	he/him	david-a-wheeler
	Siddharth Sharma	siddharth@redhat.com	Red Hat	he/him/his	sidhax
	Georg Kunz	georg.kunz@ericsson.com	Ericsson	he/him	gkunz
	Randall T. Vasquez	randall@linux.com	LF/SKF/Gentoo	he/him	ran-dall
	Gabriel Dos Reis	gdr@microsoft.com	Microsoft		GabrielDosReis
	Siddhesh	siddhesh@gotplt.	Red Hat	he/him	siddhesh

	Poyarekar	org			
	Avishay Balter	avbalter@microsoft.com	Microsoft	he/him	balteravishay
	George Wilson	gcwilson@us.ibmoh.com	IBM	he/him	gcwilson
	Mayank Ramnani	mr7172@nyu.edu	NYU	he/him	mayank-ramnani
	William Huhn	william.huhn@intel.com	Intel	he/him	wphuhn-intel
	Jack Kelly	jack@control-plane.io	ControlPlane/ITSC		06kellyjac
	Jon Williams	jrwil20@uwe.nsa.gov	NSA/ESF	he/him	

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
- New/Updated Issues/PRs:
    -

Opens

-

Guide Notes

-

<TEMPLATE > - Python Hardening Guide

1100 Eastern Time/ 0800 Pacific / 1500 UTC

Attendees:

(please **Mark an “X” next to your name if you are here,** or add-row name/email/affiliation if joining)“*” denotes sub-project/initiative lead

Present	Name	Email	Affiliation	Pronouns	GitHub ID

Agenda

- Welcome new friends
- Is someone willing to scribe for the meeting?
- Call for opens (list new items below)
-

Opens

-

Guide Notes

-