Uploaded on Github

2023 OpenSSF Security Tooling Working Group Meetings Notes

Links

- https://github.com/ossf/wg-security-tooling/discussions
- https://slack.openssf.org/ #wg_security_tooling channel
- Old tracking doc (no access?)
- Current LFX Zoom

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.

Please use the 2024 Meeting Notes

2023-Dec-15

- Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Seth Larson (PSF)	he/him	sethmlarson
X	Jerod Heck (Lockheed Martin)		jhlmco

X	Victor Lu (Independent)	he/him	victorjunlu
X	Keith Ganger (Lockheed Martin)	he/him	kgangerlm

Agenda:

- Intros
- Opens
- SBOM Manipulation Tooling Issue
- Notes:
    - Lots of piecemeal tools that address specific portions of the problem but want to collaborate with them for a holistic solution.
    - Should we add OAuth authentication?
    - Will look at it.
    - Merge command: Many projects have just wanted a single SBOM for everything in a project instead of just one.
    - Patch: License update or changed ownership or tools. Around SBOM metadata
    - Diff: Find symmetrical difference
        - Does it also cover the metadata?
        - Potentially with licensing
    - Visualize:
        - How would this work? Command line? Web document? Could be either.
        - Utilize VEX
    - Task: What should it be named
    - Task: How do we bring in as a sandbox
    -

2023-Dec-01

- Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Terri Oda (Intel)	she/her	terriko

X	Jonathan Howard (Lockheed Martin)	he/him	jhoward-lm
X	Nisha Kumar (Oracle)	she/they	nishakm
X	Adolfo Garcia Veytia (ChainGuard)	he/him	puerco
X	Seth Larson (PSF)	he/him	sethmlarson
X	Chan Voong (Comcast)	she/her	voongc

Agenda:

- Intros
- Opens
- Overview of cve-bin-tool from Terri Oda
- SBOM Naming Document Review - @Josh Bressers
- protobom overview - @puerco

Notes:
Nisha asks for a summary of what the wg's goals are. Goals: OSS devs can understand what security tooling exists. Help people writing code.

Terri: cve-bin-tool or CVE Binary Tool. Goal is to make vuln scanning for free. Imports and exports triage data. Known patches are included for debian and rh(?). Not many people publish this kind of data. Risk data is from EPSS. Does binary scanning and component list parsing. Challenges: naming, version ranges and semantics. SBOM parser understands CycloneDX, SPDX. Creates VEX files. Would be nice to track them in source control.

- Cve-bin-tool github repo: https://github.com/intel/cve-bin-tool
- Cve-bin-tool Github Action: https://github.com/intel/cve-bin-tool-action
- NVD mirror for json/xml files: https://cveb.in/
- Pre-release with all the new features to test: https://pypi.org/project/cve-bin-tool/3.3a0/

Josh: SBOM everywhere naming:
https://github.com/ossf/sbom-everywhere/blob/main/reference/sbom_naming.md
Create an issue if you have comments/concerns

Adolfo: protobom came out of DHS SBOM initiative. Software identifier translator and SBOM format translation tool. Format neutral representation using protobuf. Can read SPDX and CycloneDX SBOMs and can write SPDX and CycloneDX SBOMs. Project would like to find a home in OpenSSF. It uses a graph model which some properties in the two formats breaks. Features that exist in one and not in the other are documented; will issue a formal document soon.

No meeting on Dec 29.

2023-Nov-17

- Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Dennis Zhang (New York University)	he/him	yzhang0701
X	Adrianne Marcum (OpenSSF)	she/her	amarcum
X	Jared Miller (SAP)		jdmcyber

Agenda:

- Intros
- Opens
- Opening Thoughts
- SBOMit Overview
- MVSR Thoughts

2023-Oct-13

- Attendance ((please **mark an "X" if you are here,** or add-row name/email/affiliation if joining)

	Name/Affiliation	**Pronouns**	**GH ID**
X	Ryan Ware (Intel)	he/him	ware
X	Josh Bressers (Anchore)	he/him	joshbressers
X	Ian Dunbar-Hall (Lockheed Martin)	he/him	idunbarh
X	Georg Kunz (Ericsson)	he/him	gkunz

X	Matt Rutkowski (IBM)	he/him	mrutkows
X	Dana Wang (OpenSSF)	She/Her	danajoyluck
X	Mike Lieberman (Kusari)	he/him	mlieberman85
X	Kirby Linvill (CU Boulder)	he/him	klinvill
X	David Kirichen (Intel)	he/him	Kirich

Agenda:

- Intros
- Opens
- Opening Thoughts
- Feedback on reimaged WG
    - Security Tools Standardization & Consensus
        - Drive consensus for open source when tooling standards and implementations are fuzzy and conflict
        - SBOM Everywhere SIG perfect example
    - Developer Resource Security Tool
        - Open source developers need to know easy ways to enable security tooling
        - Create a solution to give developers all they need based upon dev environment, language, etc
        - Developer able to see:
            - What security tool categories they should be using
            - A selection of tools in each category they can use
                - **Not** picking winners and losers
                - Just ensuring tools listed meet a minimum set of criteria
                - Pull requests meeting criteria accepted
            - For each tool, the easiest way to incorporate into their development process
    - Security Tool Development
        - Not all projects in OpenSSF have people to develop tools
            - A number of groups focusing on specs and not implementations
        - Where possible, this group should drive development based on:
            - Volunteer developers
            - Contractors?
        - Only where WGs/SIGs aren't able to do this development
- Proposals
    - Proposal to Archive - False-Positive Suppression Spec SIG
    - Proposal to Archive - Guide to Security Tools SIG

    - Proposal to Archive - cve-benchmark SIG
    - Proposal to Archive - DAST scanning & web app
- Additional Topics?
    - SBOMit - Ian
    - Proto-bom
    - Standardizing low-level sbom tooling
    - Operationalizing

2023-09-26

Attendees:

- Josh Bressers (Anchore)
- Marius Biebel (hm.edu)
- Dennis Zhang (NYU)
- Ian Dunbar-Hall (Lockheed Martin)
- Maximilian Huber (TNG)
- Rob Guinness (Snyk)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.
- SBOM Tooling Item for Security Tooling WG
    - Secure Open Source Software Summit Task Force
    - Specifically on SBOM tooling was an output of this meeting
    - A lot of tooling is very ecosystem dependant today
    - Put together a requirements on document on what basic SBOM tooling should look like
    - Survey existing companies and projects out there to see what exists
    - Consolidate the list and encourage others to open source the tools
    - How do we build very low level tools for manipulating SBOMs?
    - Example: https://github.com/opensbom-generator/
    - Example: https://github.com/bom-squad

2023-09-12

Attendees:

- Josh Bressers (Anchore)
- Nisha Kumar (Oracle)
- Allan Friedman (CISA)
- Gary O'Neall (SPDX)
- Ian Dunbar-Hall (Lockheed Martin)

- Andres Orbe

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-08-29

Attendees:
- Josh Bressers (Anchore)
- Maximilian Huber (TNG)
- Simon Bennetts (ZAP/SSP)
- Ian Dunbar-Hall (Lockheed Martin)
- Seth Larson (PSF)
- Dennis Zhang (NYU, SBOMit)
- Anthony Harrison (APH10)
- Marius Biebel (hm.edu)
- Georg Kunz (Ericsson)
- Will Woodworth (CISA)
- Ixchel Ruiz (JFrog)
- Kate Stewart (LF)

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-08-15

Attendees:
- Josh Bressers (Anchore)
- Dennis Zhang (NYU)
- Georg Kunz (Ericsson)
- Sarah Evans (Dell Technologies)
- Cole Kenendy (TestifySec, in-toto, SBOMit)
- Marius Biebel (hm.edu)
- Arnaud Le Hors (IBM)
- Ian Dunbar-Hall (Lockheed Martin, SBOMit)
- Allan Friedman (CISA)
- Gary O'Neall (Source Auditor, SPDX)
- Nisha Kumar (Oracle)
- John Kjell (TestifySec)
- Max Combüchen (Snyk)

- Anthony Harrison (APH10)
- Matt Rutkowski (IBM)
- Josh Buker (Cloud Security Alliance)

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.
- SBOMit - Sandbox Support
    - https://docs.google.com/presentation/d/1l3dPqw67uf9VQ4yJEbhZkjhHhhhEYpjGdrWclmdTJFg/edit?usp=sharing

2023-08-01

Attendees:
- Josh Bressers (Anchore)
- Dennis Zhang (NYU)
- Dan Appelquist (Snyk)
- Kate Stewart (LF)
- Ian Dunbar-Hall (Lockheed Martin)
- Rob Guinness (Snyk)
- Georg Kunz (Ericsson)
- Karen Bennet (IEEE)
- Marius Biebel (hm.edu)
- George-Andrei Iosif (Canonical)
- Sarah Evans (Dell Technologies)
- Chris de Almeida (IBM)

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-07-18

Attendees:
- Kate Stewart (LF)
- Marius Biebel (hm.edu [DPMA])
- Dennis Zhang (NYU)
- Allan Friedman (CISA)
- Dan Appelquist (Snyk)
- David A. Wheeler (Linux Foundation)
- Jeff Borek (IBM)

- George-Andrei Iosif (Canonical)
- Matt Rutkowski (IBM)
- Sarah Evans (Dell)
- Chris de Almeida (IBM)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-06-20

Attendees:

- Josh Bressers (Anchore)
- Matt Rutkowski (IBM)
- Marius Biebel (hm.edu [DPMA])
- Georg Kunz (Ericsson)
- Max Combüchen (Snyk)
- Behan Webster (LF, Yocto Project)
- Emily Ratliff (IBM, OASIS Open CTI STIX)
- Mark Symons (Fujitsu)
- Ryan Ware (Intel)
- David A. Wheeler (Linux Foundation)
- Sarah Evans (Dell Technologies)
- Brian Behlendorf (LF/OpenSSF)
- Faseela K (Ericsson)
- Csaba Zoltani
- Rob Guinness (Snyk)
- Yotam Perkal (Rezilion)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-06-06

Attendees:

- Kate Stewart (LF)
- Matt Rutkowski (IBM)
- Jeff Borek (IBM)
- Joshua Watt (Garmin/Yocto Project)
- Avi Deitcher (independent consultant, involved with lfedge/eve-os) avi@atomicinc.com

- Dan Appelquist (Snyk)
- Sarah Evans (Dell)
- Marius Biebel (hm.edu [DPMA])
- Allan Friedman (CISA)
- Brian Behlendorf (OpenSSF)
- Jonathan Leitschuh (Alpha Omega)
- Tim Pepper
- Georg Kunz (Ericsson)
- Josh Clements
- David A. Wheeler (LF)
- Aditi Sharma
- Emily Ratliff (IBM)
- Daniel Bardenstein (Manifest)
- Josh Burker

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-05-23

Attendees:

- Josh Bressers (Anchore)
- Dan Appelquist (Snyk)
- Tim Pepper (VMware)
- Eric Allard (SOOS)
- Chris de Almeida (IBM)
- Georg Kunz (Ericsson)
- Marius Biebel (hm.edu [DPMA])
- Sarah Evans (Dell Technologies)
- David A. Wheeler (Linux Foundation)
- Kate Stewart (Linux Foundation)
- Arnaud Le Hors (IBM)
- Sanket Naik (Palosade)
- Yotam Perkal (Rezilion)
- Jeff Borek (IBM)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-05-09

Attendees:

- Ixchel Ruiz (JFrog)
- Allan Friedman (CISA)
- Csaba Zoltani (Nokia)
- Ixchel Ruiz (JFrog)
- Ryan Searle (Snyk)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

Notes:

- Updates from your friends in the US gubmint
    - Executive Order 14028 update
        - A draft self-attestation form was circulated for comment
            - https://www.cisa.gov/secure-software-attestation-form (Draft)
            - Comments due June 26
        - SBOM relevant language *"The software producer maintains provenance data for internal and third-party code incorporated into the software;"*

2023-04-25

Attendees:

- Josh Bressers (Anchore)
- Chris de Almeida (IBM)
- Dan Appelquist (Snyk)
- Csaba Zoltani (Nokia)
- Josh Buker (CSA)
- Ixchel Ruiz (JFrog)
- David A. Wheeler (Linux Foundation)
- Rob Guinness (Snyk)
- Matt Rutkowski (IBM)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2023-04-11

Attendees:

- Josh Bressers (Anchore)
- Dan Appelquist (Snyk)
- Emily Ratliff (IBM)
- Kate Stewart (The Linux Foundation)
- Sarah Evans (Dell Technologies)
- David A. Wheeler (Linux Foundation)
- Georg Kunz (Ericsson)
- Csaba Zoltani (Nokia)
- Allan Friedman (CISA)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- Related: “Open Source is Bigger Than You Can Imagine” By: Josh Bressers, MAR 27, 2023
    - https://anchore.com/blog/open-source-is-bigger-than-you-imagine/
- SBOM everywhere - go there.

2023-03-28

Attendees:

- Josh Bressers (Anchore)
- Justin Murphy (CISA)
- Tim Pepper (VMware)
- Ixchel Ruiz (JFrog)
- Kate Stewart
- David Wheeler
- Adrian Diglio
- Justin Murphy
- Danial Bardenstein
- Matt Rutkowski (IBM)
- Allan Friedman (CISA)
- Daniel Appelquist (Snyk)
- Max Combüchen (Snyk)
- Rob Guinness (Snyk)
- Sarah Evans (Dell Technologies)
- Emily Ratliff (IBM)
- Jeff Borek (IBM)
- Josh Buker (CSA)
- Csaba Zoltani (Nokia)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- S2C2F topic
    - Adrian Diglio: Summary: add a new section to the Guide to Security Tools about tools that help improve OSS patching speed (i.e. Mean Time To Remediate (MTTR))
    - https://openssf.slack.com/archives/C019Q1VEA87/p1674671096846249
    - E.g., dependabot (warn), dependency-review (review pull requests)
    - Proposal to add these to wg-security-tooling/guide.md
    - Recommendation: Create PRs here: https://github.com/ossf/wg-security-tooling/blob/main/guide.md
- Other new topics?
    - (Matt Rutkowski) OpenSSF Diagrammers Society - Review diagram/obtain feedback
        - https://docs.google.com/presentation/d/1ZQ7WjNH5fQL7qvpFN3jTFt-iQHqPpUc5of_azQc8iic/edit#slide=id.g21f97cb2aa1_1_503
        - i.e., entries listed at onset are:
            - **Q. .SBOM Everywhere SIG**
            - R. False-Positive Supporession Spec SIG
            - S. Guide to Security Tools SIG
            - T. cve-benchmark SIG
            - U. **OSS Fuzzing SIG**
            - V. DAST scanning & web app definitions SIG
        - David Wheeler: we're maneuvering toward "close to or primarily code == project" and "otherwise == SIG" per TAC decision, but that was a later change so not everyone's consistent
        - Matt will submit a PR to update the WG README to follow the SIG terminology and qualify past SIGs from current SIGs
- SBOM everywhere - go there.
    - action plan: https://github.com/ossf/sbom-everywhere/tree/main/action-plan
    - SBOM landscape: conceptually similar to the CNCF's landscape documents to give a sense of the many projects and domains around SBOM creation and management

2023-03-14

Attendees:

- Josh Bressers (Anchore)
- Ryan Ware (Intel)
- Emily Ratliff (IBM)

- Matt Rutkowski (IBM)
- David A. Wheeler
- Dan Appelquist (Snyk)
- Rob Guinness (Snyk)
- Justin Murphy (CISA)
- Arnaud Le Hors (IBM)
- Georg Kunz (Ericsson)
- Eric Tice (Wipro)
- Jeff Borek (IBM)
- Sanket Naik (Palosade)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- Other new topics?
    - FYI: OpenSSF Governing Board wants to see “sterling toolchains” & SBOM everywhere is expected to part of this.
- SBOM everywhere - go there.

2023-02-28

Attendees:

- Josh Bressers (Anchore)
- Dan Appelquist (Snyk)
- Xujia Zhou (Snyk)
- Ixchel Ruiz (JFrog)
- Max Combüchen (Snyk)
- David A. Wheeler (LF)
- Kate Stewart
- Emily Ratliff (IBM)
- Justin Murphy (CISA)
- Csaba Zoltani (Nokia)
- Georg Kunz (Ericsson)
- Thomas Steenbergen (EPAM)
- Sarah Evans (Dell Technologies)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people

- SBOM everywhere - go there.
- Renode Zephyr dashboard demo (Kate) - shows SBOM generation, already working in embedded side. https://zephyr-dashboard.renode.io/

- SBOM generation tooling mini summit at open source summit in May [KateS]

2023-02-14

Attendees:

- Josh Bressers (Anchore)
- Daniel Gutson (Eclypsium)
- Franco Lombroni (Eclypsium)
- Matt Rutkowski (IBM)
- Ixchel Ruiz (JFrog)
- Justin Murphy (CISA)
- Max Combüchen (Snyk)
- Anthony Harrison (Independent)
- Dan Appelquist (Snyk)
- David A. Wheeler (Linux Foundation)
- Rob Guinness (Snyk)
- Eclypsium (IBM)
- Emily Ratliff (IBM)
- Sarah Evans (Dell Technologies)
- Eric Tice (Wipro)
- Csaba Zoltani (Nokia)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- Tools topics
    - "You Shall Not Parse" library – an extensible static-checkers output parser and converter library, to help to adopt SARIF, develop linter aggregators, and secure debt/tech debt research. It can convert other static analysis output formats into SARIF.
    - Currently waiting for publication clearance - expect release next week, by end of the month for sure, will release on GitHub on a permissive free license. At that point we'll ask for help for more parser.
- SBOM everywhere - go there.
- SBOM landscape is huge. Need to split it into separate sections e.g. look at SBOM generators to support license compliance, SBOM generators to support vulnerability management, etc.... One SBOM generator won't cover everything. We also need to look at where in the SBOM lifecycle the generators fit (design, build, runtime etc). The CycloneDX tool center is a great start (and resource). We need a single format agnostic resource.
- FOSDEM showed that very little use of SBOMs was happening. Some movement in generation but no traction on consumption of SBOMs.

2023-01-31

Attendees:

- Josh Bressers (Anchore)
- Eric Tice (Wipro)
- Dan Lorenc (Chainguard)
- Adolfo García Veytia (Chainguard)
- Dan Luhring (Chainguard)
- David A. Wheeler (Linux Foundation)
- Justin Murphy (CISA)
- Georg Kunz (Ericsson)
- Csaba Zoltani (Nokia)
- Dan Appelquist (Snyk)
- Bradford Bartlett (Sonos, representing myself)
- Rob Guinness (Snyk)
- Max Combüchen (Snyk)
- Charles Timko (Red Hat)
- Mattia Rizzolo (Reproducible Builds)
- Sarah Evans (Dell)
- Rosaria Carr (Indeed)
- Anthony Harrison (independent)
- Arnaud Le Hors (IBM)
- Thomas Steenbergen (EPAM)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.
- Demo of OpenVX http://github.com/openvex by Dan Luhring and Adolfo Veytia
- Idea (Sarah Evans) Model the proposal for Security Tooling WG →SBOM everywhere (OSS Mob Plan stream 9) off the proposal created by CRob http://github.com/ossf/tac/issues/134 for the Education SIG →Education (OSS Mob Plan stream 1). Group thought it made sense to model the “bones” for consistently bubbling up to the TAC, GB and OpenSSF community
- What projects and activities should we begin to support?

2023-01-17

Attendees:

- Josh Bressers (Anchore)
- Eric Tice (Wipro)
- Arnaud Le Hors (IBM)

- Justin Murphy (CISA)
- Allan Friedman (CISA)
- Sarah Evans (Dell Technology)

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2022-12-20

Attendees:
- Josh Bressers (Anchore)
- Charles Timko (Red Hat)
- Daniel Marcano (VMware)
- Yotam Perkal (Rezilion)
- David A. Wheeler (Linux Foundation)
- Kate Stewart (Linux Foundation)

Agenda:
- Please introduce yourself in the chat
    - Everyone, not just new people
- SBOM everywhere - go there.

2022-12-06

Attendees:
- Josh Bressers (Anchore)
- Georg Kunz (Ericsson)
- Sean Goggins (CHAOSS Project/University of Missouri)
- Allan Friedman (CISA)
- Rosaria Carr (Indeed)
- Thanassis Avgerinos (ForAllSecure / Oasis SARIF)
- Rodrick Blanton (Microsoft)
- Ixchel Ruiz (JFrog)
- Jamie Magee (Microsoft)
- Sarah Evans (Dell Technologies)
- Tracy Ragan (DeployHub / Ortelius)
- Ivana Atanasova (VMware)

Agenda:

- Please introduce yourself in the chat
    - Everyone, not just new people
- Expanding the tools group [GKunz]
    - Has co-workers interested in the tooling working group
    - Is there interest in expanding the group scope?
        - More than just SBOMs
    - What about connecting to Alpha/Omega?
    - There are a lot of tools
    - George will mail the list and see if there is interest in this
- SBOM everywhere
- SBOM Everywhere Goals and Purpose
    - Alan F.: How do we get metadata for consumption? What is needed (e.g. 8 lines of comments in a project? Funding? Well defined package data model) Outcome of SBOM everywhere is a public good.
    - Tracy R: Ortelius.io is working on a project leveraging blockchain related to SBOM [LINK]
    - Chris B: Sharing channels will evolve over time. Where is synergy? (e.g. DBOM consortium)
    - Alan F: Side point: while it's not consensus, many SBOM folks are reluctant to advocate putting SBOM data and Vuln data in the same data structure: SBOM is static wrt code, but Vuln data changes over time.
    - Tracy R: Should evaluate LF umbrella tools pre-OpenSSF that may already be addressing security issues, metrics and risks that are adjacent to security. Could this evaluation be a 2023 goal? Bring in and categorize.
    - Josh B: Please read before the next meeting, to lay out the "approach".
    - Sarah E: Dell is interested to perform/contribute SBOM consumption research to build on LF research in parallel with the approach to develop SBOM goals. This will allow SBOM goals to have visibility into consumption gaps and OSS SBOMs could evolve over time with consumption needs. The home of Dell research is TBD (e.g CISA working group vs SBOM everywhere), but would want visibility research in SBOM everywhere landscape.
- The tl;dr for the LF CHAOSS Project: sean@chaoss.community / goggins@missouri.edu
    - CHAOSS Slack: https://join.slack.com/t/chaoss-workspace/shared_invite/zt-1kve0jo4k-5JFYQKTOerSUPxekGPc02Q
    - The working group focused on risk concerns has repo is here: https://github.com/chaoss/wg-risk
    - Our meeting notes are here: https://docs.google.com/document/d/1iqIMpLBwuKSnE0BbQTgbsb9Im87IoN7IUzukochClCw/edit?pli=1#
    - **The community website** has a lot of information about released metrics, and metrics models: https://chaoss.community

    - We leverage several OSSF Tools, and an SBOM/License scanner developed with my collaborator at the University of Nebraska-Omaha about a decade ago:
        - Augur: https://github.com/chaoss/augur
        - augur-license: https://github.com/chaoss/augur-license(This will build an SBOM using an older standard of SPDX)

2022-11-22

Attendees:

- Josh Bressers (Anchore)
- David A. Wheeler (Linux Foundation)
- John Scott (Ion Channel)
- Prateek Mishra (ADP)
- Arnaud Le Hors (IBM)
- Georg Kunz (Ericsson)
- Daniel Marcano (VMware)
- Katherine Druckman (Intel)
- Chris Blask (Cybeats)
- Mehdi Entezari (Unisys/DBoM Project)
- Justin Murphy (CISA)
- Ivana Atanasova (VMware)
- Kate Stewart (Linux Foundation)
- Ixchel Ruiz (JFrog)
- Jomcy Pappachen(Google)
- Anthony Harrison (Independent)

Agenda:

- SBOM everywhere
- SBOM-Know-How

2022-11-08

Attendees:

- Josh Bressers (Anchore)
- Rosaria Carr (Indeed)
- Chris Blask (Cybeats)
- Anthony Harrison (Independent)
- Sebastien Awwad (Anaconda)
- Daniel Marcano (VMware)
- Katherine Druckman (Intel)
- Brandon Lum (Google)
- Avishay Balter (Microsoft)

Agenda:

- SBOM everywhere

2022-10-25

Attendees:

- Josh Bressers (Anchore)
- Alex Goodman (Anchore)
- Prateek MIshra (ADP)
- Katherine Druckman (Intel)
- Justin Murphy (CISA)
- Georg Kunz (Ericsson)
- Daniel Marcano (VMware)
- Matt Rutkowski (IBM)
- Chris Blask (Cybeats)
- Anthony Harrison (independent)
- Brian Fox (Sonatype)
- David A. Wheeler (Linux Foundation)
- Mehdi Entezari (Unisys, DBoM Project)
- Avishay Balter (Microsoft)
- Tracy Ragan (DeployHub)

Agenda:

- SBOM everywhere - see that for more
    - Work ongoing to improve the SPDX library in Python

2022-09-27

Attendees:

- Josh Bressers (Anchore)
- VM Brasseur (Wipro)
- John-Luc Bakker (BlackBerry)
- Justin Murphy (CISA)
- Will Woodworth (CISA)
- Jeff Williams (Contrast)
- Cameron Banowsky (SHE BASH)
- Bunny Hernández (SHE BASH)
- Katherine Druckman (Intel)
- Csaba Zoltani (Nokia)
- Brandon Lum (Google)
- David A. Wheeler (Linux Foundation)

- Kate Stewart (Linux Foundation)
- Saundra Monroe (Anaconda)
- Mehdi Entezari (DBoM Open Source Project & Unisys)
- Dan Appelquist (Snyk)
- Randall T. Vasquez (Gentoo)
- Thanassis Avgerinos (ForAllSecure)
- Brian Fox (Sonatype)

Agenda:
- SBOM everywhere

2022-09-13

Attendees:
- Josh Bressers (Anchore)
- VM Brasseur (Wipro)
- Cameron Banowsky (SHE BASH)
- Bunny Hernandez (SHE BASH)
- Sebastien Awwad (Anaconda)
- Csaba Zoltani (Nokia)
- Prateek Mishra (ADP)
- Daniel Marcano (VMware)
- Mark Sturdevant (IBM)
- Katherine Druckman (Intel)
- Tracy Ragan (DeployHub)
- Eric Tice (Wipro)
- Jay White (Microsoft)

Agenda:
- SBOM everywhere

2022-08-30

Attendees:
- Randall T. Vasquez (Gentoo)
- **Josh Bressers (Anchore, WG Chair)**
- Matt Rutkowski (IBM)
- Kathleen Goeschel (Red Hat)
- Prateek Mishra (ADP)
- Aeva Black (MSFT, OpenSSF TAC, OSI)

- Daniel Marcano (VMware)
- Steve Taylor (DeployHub)
- Mark Sturdevant (IBM)
- Chapman Pendery (Bloomberg)
- Jamie Magee (Microsoft)
- Mehdi Entezari (Unisys, DBoM)
- Cameron Banowsky (SHE BASH)
- Bunny Hernandez (SHE BASH)
- Tracy Ragan (DeployHub)
- Allan Friedman (CISA)
- Justin Murphy (CISA)
- Will Woodworth (CISA)
- Rahul Gupta (Microsoft)
- David A. Wheeler (Linux Foundation)
- Kate Stewart (Linux Foundation)
- Sarah Evans (Dell)
- VM Brasseur (Wipro)
- Avishay Balter (Microsoft)
- Eric Tice (Wipro)
- Muuhh Ikeda (Cybertrust Japan)
- Alex Goodman (Anchore)
- Vinod Anandan (Citi)
- Adoolfo García Veytia (Chainguard)

Agenda:

- SBOM everywhere
- Allan Friedman gave overview. US Government Executive Order has a number of requirements, including SBOMs
- SBOM team at CISA: SBOM@cisa.dhs.gov
- CISA is convening the 5 workstreams. Allan: “I try very hard to not put my thumb on the scales” - goal is to enable collaboration to solve the problems.
- Aeva: “Are any of the workstreams focused on the CONSUMPTION of signal (information)?”
    - Allan: Yes. There’s a necessary lag, until we have SBOMs can’t focus on consuming them. Cloud side does cloud things. VEX integrates SBOM + VEX.
- Python library funding: Contract SOW reviewed, expect to start Sep 1
- [Matt] In terms of SBOM completeness (maturity) relative to formulation against complete SDLC is being looked at… initially a taxonomy (links here), but I have also seen an event model against the formulation (but do not have that link handy)...
    - The mindmap of the taxonomy currently in development is located:
    - https://drive.google.com/file/d/1Uot5Ntm0NB3kJgHAc7fDtZTleJIhZS2P/view?usp=sharing

    - Use XMind to view the draft: https://drive.google.com/file/d/1_GIyIG4K3mT_TPeGJIIUj4HtouNRgtPQ/view?usp=sharing
-

2022-08-16

Attendees:

- Josh Bressers (Anchore)
- Alex Goodman (Anchore)
- Randall T. Vasquez (Gentoo/Homebrew)
- Eric Tice (Wipro)
- Cameron Banowsky (SHE BASH)
- Bunny Hernandez (SHE BASH)
- Matt Rutkowski (IBM)
- Prateek Mishra (ADP)
- VM Brasseur (Wipro)
- Jeff Borek (IBM)
- David A. Wheeler (Linux Foundation)
- Brandon Lum (Google)
- Daniel Marcano (VMware)
- Csaba Zoltani (Nokia)
- Steve Taylor (DeployHub)
- Yehuda Gelb (Checkmarx)
- Ixchel Ruiz (JFrog)
- Brain Fox (Sonatype)
- Georg Kunz (Ericsson)
- Sarah Evans (Dell)
- Daniel Appelquist (Snyk)
- Tracy Ragan (DeployHub/ Ortelius)
- Peter Singh (Fuzzy, AstroTech)
- Rodrick Blanton (Microsoft)
- Jamie Magee (Microsoft)
- Álvaro Figueroa (Microsoft)
- Munawar Hafiz (OpenRefactory)

Agenda:

- SBOM everywhere
- Request for future project volunteers

2022-08-02

Attendees:

- Josh Bressers (Anchore)
- Eric Tice (Wipro)
- Charles Timko (Red Hat)
- Cameron Banowsky (SHE BASH)
- Bunny Hernandez (SHE BASH)
- Munawar Hafiz (OpenRefactory)
- Prateek Mishra (ADP)
- David A. Wheeler (Linux Foundation)
- Randall T. Vasquez (Gentoo/Homebrew)
- Csaba Zoltani (Nokia)
- Daniel Marcano (VMware)
- Kathleen Goeschel (Red Hat)
- Kate Steawrt (Linux Foundation)
- Aeva Black (Microsoft, TAC)
- Georg Kunz (Ericsson)
- Matt Rutkowski (IBM)
- Brian Behlendorf (OpenSSF/LF)
- Gary O'Neall (Source Auditor)
- Alexios Zavras (Intel)
- VM Brasseur (Wipro)
- Jamie Magee (Microsoft)
- Avishay Balter (Microsoft)

Agenda:

- SBOM everywhere
    -

2022-07-19

Attendees:

- Matthew Neal Miller (Red Hat)
- VM (Vicky) Brasseur (Wipro)
- Kathleen Goeschel (Red Hat)
- Josh Bressers (Anchore)
- Prateek Mishra (ADP)
- Yehuda Gelb (Checkmarx)
- Altaz Valani (Security Compass)
- Patricia Tarro (Dell)
- Daniel Marcano (VMware)
- Avishay Balter (Microsoft)
- Brian Behlendorf (LF/OpenSSF)
- Kate Stewart (LF)
- Yotam Perkal (Rezilion)
- Randall T. Vasquez (Gentoo)

- Daniel Gutson (Eclypsium)
- Eric Tice (Wipro)

Agenda:

- Red Hat's Component Registry is now open source: [Kathy / Matt]
    - (https://github.com/RedHatProductSecurity/component-registry)
    - Our Component Registry is under development and much work still needs to be done. It is an internally-focused application for our manifests and not some "magical SBOM generator".
    - It can be viewed as a recipe on how to build your own registry in your own company. It is dependent on your own products/services and you need your own manifest data to implement your solution.
    - As Red Hat is further along with development, we will inform the open source community.
- How do the workstreams affect this working group?
    - Is there anything we believe should fall under our umbrella?
    - Stream 9 seems to become part of this group, what does that mean? [Josh]
        - I would like Brian or David to address this
    - There is a mobilization plan
        - https://openssf.org/oss-security-mobilization-plan/
    - SBOMs everywhere is Stream 9
    - How do we evolve the 5 page plan and turn it into fundable work
    - A proposal is in front of the TAC (waiting for their approval)
    - One SIG per stream
    - SIG would take ownership of the plan
    - What's the next chunk of work to do? Paying someone to do a thing
    - Proposals submitted to 1 of 2 places
        - Proposal can go in front of an org that made a pledge to the mobilization plan
        - Can also go in front of the TAC (they have some budget for this)
    - We can informally start the SIG work before TAC approval
    - Is this the right place for SBOM everywhere?
        - The goal is to get generation and consumption built into the tooling
        - Very little friction is a goal
        - Make SBOM generation a commodity
    - Would guidance be in scope?
        - Kate and Josh think yes
    - Interested in being involved: Kathleen Goeschel Brian Fox
- Prioritization of contributions (Scorecard, ORT, …) [Daniel]
    - Should this group prioritize the projects that need contributions?
        - This would let us invite people to help
    - Daniel is creating a list of tools that need contributions
- Is there an inventory of standard tools someplace? I am specifically interested in BOM generators for a range of languages and artifacts.[Prateek]

- Let's start to track lists of tooling here
    - https://github.com/ossf/wg-security-tooling/blob/main/guide.md
- ACTION: Get someone from the CNCF tool landscaping to connect with us?

2022-06-07

Attendees:

- Josh Bressers (Anchore)
- Eric Tice (Wipro)
- Daniel Marcano (VMware)
- David A. Wheeler (Linux Foundation)
- Yotam Perkal (Rezilion)
- Altaz Valani (Security Compass)
- Georg Kunz (Ericsson)
- Arnaud J Le Hors (IBM)
- Charles Timko (Red Hat)

Agenda:

- How do the workstreams affect this working group?
    - Is there anything we believe should fall under our umbrella?
    - We discussed some of this at a high level, it belongs in a future meeting, whoever added it can add some commentary
- False Positives Suppression Specification
    - David: Distracted but do intend to return to it!
    - We have many tools now documented (Thank you everyone!!)
    - Should we include linters (non-security) in scope?
        - If a project wants to be part of it, great! If not, great!
    - We need critical players involved or it's a waste of time. Not sure the toolmakers have a big incentive to implement this.
    - Also: Get Community license on specification.
- Josh's working on: https://github.com/joshbressers/SBOMeasure (personal time) - awareness. Originally was trying to figure out what analysis they were good/bad at. However, "it's shocking how hard it is to run these tools". I can't even get many of the SPDX tools to run. (Relates to stream on "SBOM everywhere"). Need to do some work to identify pain points.
    - Tried to get them to run
        - Fossology: At least there was an install instructions, but it ran for a while & then crashed without an error message
    - David: I know of some SBOM generators, there may be others:
        - The spdx-sbom-generator (https://github.com/opensbom-generator/spdx-sbom-generator).
        - The Kubernetes alternative https://github.com/kubernetes-sigs/bom.
        - Anchore's Syft (OSS, in golang): https://github.com/anchore/syft
        - Tern https://github.com/tern-tools/tern

        - See also: https://spdx.dev/spdx-tools/
        - https://github.com/fossology/fossology
    - David: I used spdx-sbom-generator. It ran fine. In my case I was scanning a Ruby *applicatioh* - but it's only designed currently to handle Ruby *libraries*. I did file a bug report.
    - "If haven't been updated in 2 years it's probably dead"

2022-05-24

Attendees:

- Eric Tice (Wipro)
- Yehuda Gelb (Checkmarx)
- Josh Bressers (Anchore)
- Kathleen Goeschel (Red Hat)
- David A. Wheeler (Linux Foundation)
- Navid Emamdoost (Google)
- Arnaud J Le Hors (IBM)
- David Sastre (Red Hat)
- Jeffrey Borek (IBM)
- Daniel Gutson (Eclypsium)
- Daniel Marcano (VMware)

Agenda:

- OSSF Fuzz Introspector presentation (Navid Emamdoost) - status update (this project is part of this WG)
    - Look at fuzzer internals, help then understand how it works and how to improve
    - In particular, helps you understand where the fuzzer is "stuck" (e.g., so authors of fuzzing tools can figure out how to improve their tools)
    - Identifies coverage blockers (places that are hard to get past for a fuzzer)
    - Identifies performance blockers
        - Like OOM and crashes
    - Almost finished with Integration with OSS-Fuzz - already seeing proof of effectiveness
    - Gave an example of xpdf where an exploit used by NSO wasn't getting hit, introspector showed that the path wasn't getting hit at all. They then created added code to fuzz those new areas.
    - Currently have statement & branch coverage, though the presentation only shows statement coverage (statement is easier to show)
    - Jsonnet: fuzz introspector showed many statements weren't covered, so they then wrote new fuzz targets to greatly improve coverage.
    - Daniel Gutson: What about supporting binary fuzzers?
        - Generally we have the source code. Fuzz introspector uses source for coverage information & also for call graph. If that information can be provided another way then it'd work.

        - Ghidra can provide call graph, we can get coverage info too - maybe we can get students to work that out!
    - David: Are you getting ready for a blog post?
        - Yes.
        - David: If it's via OpenSSF, make sure the TAC knows, & make sure the documentation is ready for potential new users.
        - Agreed. We created some specific examples here: https://github.com/ossf/fuzz-introspector/blob/main/doc/CaseStudies.md
    - How to solve?
        - Add fuzz target to call it directly
        - Look at code to see why it's not getting called (find root cause) & fix that
    - Currently only supports C/C++. Why?
        - Have a compiler plug-in for extracting call tree, it's an LLVM plug-in.
        - To add a new language must modify the static analysis part to support new languages.
        - We're focused on memory safety, so this made sense as a first step.
    - When will this be integrated into OSS-fuzz?
        - That's what's we're working on now & intend to have a blog post on.
- Measuring the tools
    - Josh's document
    - https://www.rezilion.com/blog/log4j-blindspots-what-your-scanner-is-still-missing/ - "Log4j Blindspots: What Your Scanner Is Still Missing"
- False Positives Suppression Specification – progress & status (David & Daniel)
    - David: I was overwhelmed by the Washington, DC meeting (and am still catching up) so haven't had time to work on it yet.
    - Don't think we need to limit it to SAST - including linters is fine, there's often a blurry line.
    - Just need to make sure you suppress the related line, not an unrelated line many lines down.

2022-Apr-26

Attendees:

- Josh Bressers (Anchore)
- VM Brasseur (Wipro)
- Yehuda Gelb (Checkmarx)
- David A. Wheeler (Linux Foundation)
- Harimohan Rajamohanan (Wipro)
- Marta Rybczynska (OSTC)
- Jory Burson (Linux Foundation)
- Yotam Perkal (Rezilion)
- Jonathan Leitschuh (Dan Kaminsky Fellowship @ Human Security)
- Thomas Steenbergen
- Vinod Anandan (Citi)

- Eric Tice (Wipro)

Agenda:

- False Positive Suppression Specification
    - https://docs.google.com/document/d/1811qanC8h9egv3Iszn_rrXGtAoSCz0YJGzp9vACjjH8/edit#
    - How to collaborate
        - Google docs are an easy first step
        - Move this over to markdown in a github repo eventually
        - There are some tools to convert google docs to markdown, we will document them when they are found
        -
    - What now?
        - David: I think we need more research on what tools do
        - How do we want to “projectize” this
- Hot off the press - OpenSSF Day Virtual info
    - AccelEvents virtual platform. Attendees will be able to access all talks via the platform, and we will also be showing "virtual" talks in the actual room
    - Talks available online ~2 weeks after the event
- Next meeting (May 10)
    - Josh is gone
    - Cancel, or does someone else want to run the call?
    - We will cancel it
- OpenSSF staff are out next week at an all hands

2022-Apr-12

Attendees:

- Josh Bressers (Anchore)
- David Sastre (Red Hat)
- Eric Smalling (Snyk - new attendee)
- Patricia Tarro (Dell)
- Arnaud J Le Hors (IBM)
- Yotam Perkal (Rezilion)
- Jeff Borek (IBM)
- Matt Rutkowski (IBM)

Agenda:

- Review David A. Wheeler: Okay, I started working on “False Positive Suppression Specification”, link here: (DRAFT) False Positive Suppression Specification
    - Do we want to support this project?
    - It falls under the “improve” objective of the group
    - There are other ways to log supressions such as an external file

        - These files have long term maintainability issues
    - **DECIDED:** There was general consensus by the WG to add this project as a WG item
    - Josh will email to TAC that we plan to add this as a project, for coordination
    - Next steps: reach out to some tool makers to find out their preferences and/or what they do
        - David: Will talk with RATS, Flawfinder
    - ONAP uses SonarQube now SonarCloud
        - AT&T has some connections, maybe can contact
    - David Sastre suggested to consider the challenges disabling comments pose in the context of static analysis tools
- Current list of proposed ideas
    - https://github.com/ossf/wg-security-tooling/issues/38
- How do we start moving projects and ideas forward?
    - Dead vs completed
    - Dead: Clearly mark the project as archived
    - Suggested process
        - Discuss in a public forum (e.g., this WG)
        - Do people think this makes sense?
            - Look for duplicate efforts, related efforts - ask WG & do some web searches
            - Find interested people
        - Periodic static from a project (housekeeping)
            - If nothing is happening, we can archive these projects
        - Basic requirements
            - How many people are interested (minimum number)
    - Josh will write this up and mail the list
- Get rid of the github discussion group
    - Josh will mail the list, the mailing list is the best place for discussions
- Josh B: **Where possible, do things on the mailing list**. There are many more on the mailing list than can show up at a synchronous meeting (we have 13 today at our meeting, there are many more on the mailing list).
- OpenSSF Day, June 20, Austin, TX

2022-Mar-29

Attendees:

- Josh Bressers (Anchore)
- Jon Zeolla (Seiso)
- VM Brasseur (Wipro)
- Eric Tice (Wipro)
- Marta Rybczynska (OSTC)
- Jory Burson (Linux Foundation)
- Daniel Gutson (Eclypsium)

- Tracy Ragan (DeployHub / Ortelius)
- Jack Kelly (ControlPlane)
- David A. Wheeler (Linux Foundation)
- Harimohan Rajamohanan (Wipro)
- Yotam Perkal (Rezilion)
- Anton
- David Sastre (Red Hat)

Agenda

- Josh Bressers: WG reboot
    - Goals and expectations
        -
    - Charter review (we need to gut this thing)
        - https://github.com/ossf/wg-security-tooling/blob/main/CHARTER.md
    - The README also needs review
        - https://github.com/ossf/wg-security-tooling

Notes

- Reboot!
    - Josh has ideas, but this will be a team effort
    - Will probably take a few weeks to sort this out
    - What inspired Josh for this group
        - https://www.rezilion.com/blog/log4j-blindspots-what-your-scanner-is-still-missing/
        - Vendors decided to check more boxes after log4j
        - Would like to see us do this but for open source
    - VM: ORT: LF, works with OpenChain. https://github.com/oss-review-toolkit/ort - focuses on license compliance & noting known vulnerabilities
- Daniel Gutson: Proposal: Standard format for comments to say “ignore the next report” so that people can easily eliminate false positives when using many different tools. We want to use multiple tools, but they all do it differently.
    - David A. Wheeler: I like it. That’s very small, concrete, solves a real problem. SARIF standardizes static analysis outputs, this would help standardize inputs
        - If you handle your allowing/denying by feeding the combined SARIF -> a policy engine (e.g. OPA) you can ignore false positives across separate tools in one place
- Marta: Proposal: document tools that exist, interchange formats, find out what the gaps are, share knowledge and make it easy to access to developers
- Fuzzing working group is a subgroup of this
    - Meets once a month
    - Developing a tool that helps see where the fuzzers are failing to reach, to either improve the fuzzing of tools & using the tools
- More broadly: Improving tools, improving use of tools, etc.
- What’s up with the CVE benchmarking suite

    - https://github.com/ossf-cve-benchmark/ossf-cve-benchmark
- Be careful about publishing benchmarks of proprietary tools - DeWitt clause issue. Avoid it, or be prepared for legal problems:
    - https://dwheeler.com/essays/dewitt-clause.html
- Just SAST? Also SBOM?
    - Josh B: Anything security is a go. SBOM creation & ingestion are things I care about!!
        - Jack: Looking forward to working on nix drv -> SBOM - Nix thesis drv section 2.4 page 40
- Jon Zeolla interested in tooling to help with controls
    - The CNCF TAG WG is doing some of this
- David Sastre: threat modeler - interested in aggregating information. Too many formats
    - There's no way to aggregate data from all the sources that exist today (CVE, NVD, …)
- David A. Wheeler: Okay, I started working on “False Positive Suppression Specification”, link here: (DRAFT) False Positive Suppression Specification

2022-Feb-7

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Josh Bressers (Anchore)
- David Sastre (Red Hat)
- David A. Wheeler (Linux Foundation)
- Eric Tice (Wipro)

Agenda

- WG Lead
    - Paul Duplys is willing to lead the WG
- There seems to be some confusion about the date/time of the meeting
    - It was discussed.
    - Was changed to Monday, some didn’t seem to expect it.
- Which day? :)

2022-Jan-25

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Tom Bedford (Bloomberg LP)
- Paul Duplys (Bosch)
- Aeva Black [they/them] (Microsoft, OSI)
- David A. Wheeler (Linux Foundation)
- Yotam Perkal (Rezilion)
- Azeem Shaikh (Google)

- Jeffrey Borek (IBM)

Agenda:

- Web Application Definition Reboot
    - A simple file to say “how can I get this up & running (e.g., for fuzzing)
    - https://github.com/ossf/wg-security-tooling/wiki/WebAppDefn
- Aeva Black: Summary: https://github.com/AevaOnline/supply-chain-synthesis
-
- : I’d like to have a WG on security tooling - e.g., how to apply tooling to your projects
    - https://github.com/ossf/wg-security-tooling/blob/main/guide.md - has helpful information, does not specify specific tools (by intent)
    - Wheeler: Picking specific tools is really hard. It’s hard to get data about them, especially with DeWitt clauses: https://dwheeler.com/essays/dewitt-clause.html
    - Aeva: Blessing specific security tools probably something OpenSSF shouldn’t do - “no kingmaking” - ends up with inappropriate pressures to pick one tool
    - Aeva: CNCF TAG-Security has published recommendations in a WP: tag-security/security-whitepaper at main · cncf/tag-security (github.com)
    - Can create a list of all OSS tools” or “all tools” in this category”
    - https://github.com/psiinon/open-source-web-scanners
- Simon: https://github.com/psiinon/open-source-web-scanners
- David: https://dwheeler.com/essays/static-analysis-tools.html (a little old but perhaps a useful starting point)
- Simon: OWASP has a list of DAST & SAST tools
- Aeva: Question: is this the right working group to “own” the generation and maintenance of lists like these? Maybe publish a paper / some recommendations?
- Simon: Issue is, who wants to actually do some work? :-). If people aren’t willing to pick up work, won’t get done, needs to be driven.
- Paul: Advantages of a problem driven approach
- Simon: no one’s really been looking at what this group should be doing overall. Depends on who shows up to meetings. Interesting to know what folks want to get out of it now.
- Round table - what do people want from this group?
    - Paul - learning about security tools, automation, getting help making decisions about what to use
    - David: help folks make OSS more secure
    - Aeva: Would like to see work done - list of open source tools important, help make people aware of what tools exist & how to pick them
        - We don’t need meetings to talk about things we’re not going to do :-)
    - Simon: No silver bullets, DAST doesn’t do everything, want to make sure DAST isn’t misrepresented, looking to learn
    - Tom: here to see how company can contribute to OSSF, but haven’t been able to figure out what this WG’s purpose is. Here to help but unsure how. Building list of tools seems like a useful objective.
    - Yotam: came here to see how company could contribute to OSSF

    - Azeem Shaikh: Leads Scorecard work, wants to know what to check for re: tools, etc.
    - Simon: https://github.com/ossf/scorecard/issues/581
- WebAppDefn PoC ideas
    - GitHub Action to check whether WebApplicationDefn was present
    - If present, start the web app in Docker and try to access it
    - If access is successful, then checkmark, if not then return an error or something
    - We can add such a check to Scorecards directly (if you find a certain file, assert certain things)
    - Let's start a discussion on Scorecard Slack channel or in a GitHub issue and define the specific next steps
- Several will look at the guide: https://github.com/ossf/wg-security-tooling/blob/main/guide.md

2022-Jan-11

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Jenn Bonner (PM, Linux Foundation, OpenSSF)
- Arlen Baker (Wind River)
- Tom Bedford (Bloomberg LP)
- Paul Duplys (Bosch)
- Georg Kunz (Ericsson)

Agenda:

- Web Application Definition Reboot
    - https://owasp.org/www-project-vulnerable-web-applications-directory/
    - https://github.com/psiinon/bodgeit
    - https://owasp-juice.shop/
    - https://github.com/marketplace/actions/owasp-zap-baseline-scan

2021-Dec-14

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Brian Behlendorf (LF)
- Azeem Shaikh (Google)
- Carter Gawron (D2iQ)

Agenda:

- https://twitter.com/psiinon/status/1470699473349316611

2021-Nov-30

Attendees:

- David A. Wheeler (Linux Foundation)
- Matt Rutkowski (IBM), he/him, CST
- Simon Bennetts (ZAP, StackHawk)
- Arnaud J Le Hors (IBM)
- Joshua Gay (IEEE), he/him
- Arlen Baker (Wind River)

Agenda:

- Small number of participants today!
- What results does this WG want to achieve? Brainstorm
    - Getting back to mission - list of tools to use, ways to evaluate tools
    - Could classify tools, but edX course, SOAR, etc. already do this
    - Could evaluate tools, e.g., score them
        - Our cve test suite can help, at least for certain kinds of tools
        - You generally need an evaluation tool suite for a specific kind of tools (e.g., source code static analysis different from web application scanners)
        - E.g., add categories like extensibility, integratibility
    - Could encourage use of SARIF
    - One SBOM tool vendor can generate SPDX & CycloneDX, but if you want “all the data” you have to use their proprietary data format
    - Work to help ensure OSS tools meet security requirements, e.g., Scorecard, CII Best Practices, generate SBOM, etc. A few OSS tools we could analyze include:
        - OWASP ZAP
        - Flawfinder
    - Would like the tools being provided for my communities (IEEE OSS platforms, focused on standards development) - want them to be able to set up & verify their environments. Want it to be OSS, e.g., setup scripts, etc. E.g., what should be in the CI/CD yaml file?
    - Suggested CI/CD settings for common situations (!)
        - E.g., projects on GitHub, GitLab, etc.
        - How to implement SLSA (e.g., hermetic builds), static analysis tools, web application tools, SBOM generation, sigstore (signing), etc.
        - Include issues “must be built in <location>”
            - Verified reproducible builds could help deal with that
        - Also need to assess/test/score: Scorecards, etc.
        - Approach: Start with SLSA 3, see how well we can achieve it with tooling etc. Pick a few specific projects, try to generalize
            - If I have a container, I can drop it in - how do I get a normative report from a SAST scanner? At least DAST should be doable

2021-Nov-16

Attendees:

- Abhishek Arya (Google)
- Navid Emamdoost (Google)
- Michael Winser (Google)
- Matt Rutkowski (IBM)
- David A. Wheeler (Linux Foundation)
- Carter Gawron (D2iQ)
- Josh Bressers (Anchore)
- Azeem Shaikh (Google)

Agenda:

- Abhishek: Discuss fuzzing collaborations in a fuzzing bi-weekly as part of OpenSSF
    - There's an existing group named "Fuzzing collaboration" that discusses fuzzing: Google, Mozilla, Facebook, AFL++ developers, libfuzzer developers, meets every month, they have a Google groups mailing list (fuzzing-collaboration@googlegroups.com, 37 members)
    - Propose: A focused sub-WG meeting specifically focused on fuzzing
    - Currently they're working on improving fuzzers as measured by fuzzbench - https://github.com/google/fuzzbench - benchmarks fuzzers
    - Abhishek has asked the group if they're fine doing this, they're fine with it
    - **Approved - will need to inform TAC**
- Incubate some fuzzing projects inside OpenSSF
    - Abhishek: E.g. FuzzWatch - tool to find coverage blockers (when fuzzing stops being productive).
- No opposes, several in favor (David, Abhishek). David to check & raise to TAC if appropriate & also to try to get more involved.
    - Abhishek will Jory to create an OpenSSF repo for "fuzzwatch"
    - David: Worried about the name, there's a Python tool with that name.
- Broader question: do we just accept projects as they request & approve, or do we want to be more deliberate?
    - Michael: Fuzzers, probably let many flowers bloom, different approaches make sense. For SBOM generators, perhaps we should be more deliberate.
    - David:
- Do need a clear path to becoming an official project
    - Michael: I worked on CDF, didn't want to become a dumping ground and wanted to have projects with legitimate communities rather than single-vendor projects. This may not be scalable for where we are right now.
    - Before accepting a project:
        - If pre-existing: Willing (if pre-existing) & health-chcek
        - WIlling to release as OSS & follow other OpenSSF rules/policies

        - Check for existing work - if there is, what's different that justifies creating it? Could they be merged/combined? Especially try to avoid duplication of work within OpenSSF
        - Want to allow incubation of many projects, but focus $ on a smaller set
        - Don't want everything at the whim of a single developer / organization if we can reasonably avoid it
    - Need to be careful about making something be viewed as "this is officially blessed by OpenSSF" when it's just a work in progress that may never get anywhere
    - David: Will talk with Brian Behlendorf about project acceptance - now that OpenSSF is on a stronger footing, what should be required? Possibly bring up something for TAC.
- Proposed blog post about fuzzing (basic explanation about fuzzing)
    - Should this be a blog post (point in time) or a long-term-maintained blog post?
- Michael: I don't care about what tool people use, I want secure software, fuzzing can help us get there.
- We are an "august body" it appears
- What results does this WG want to achieve?
    - Identify the mission, vision, strategy (goals), roadmap
- SBOM tools from Anchore? Syft?

2021-Nov-02

Attendees:

-

Agenda:

- Meeting Cancelled → Moving to Nov. 9th @ 8AM PST/4PM GMT (see slack thread, or e-mail in mailing list)

2021-Oct-10

Attendees:

- Ryan Ware (Intel)
- Jeffrey Borek (IBM)
- Pierre Tempel (GitHub)
- Simon Bennetts (ZAP, StackHawk)
- Azeem Shaikh (Google)
- David A. Wheeler (Linux Foundation)
- Bas van Schaik (GitHub)

Agenda:

- NOTE: Fixed tracking doc in meeting notice?

- Opens:
    - Bas: GitHub builds CodeQL and code scanning
        - CodeQL has a constant stream of libraries and frameworks that it needs to keep up to date with
        - Needs to understand tainted user data
        - A lot of maintenance work
        - Standard to annotate source code to ease maintenance
        - Has anyone done any work in this area?
        - Concern is how many people will use it (Simon)

- Tools Listing
    - Temporarily here
    - Long Term Format:
        - Sheets?
        - CSV?
        - JSON?
        - MD?
    - Here's David A. Wheeler's list of OSS static analysis tools, which in turn points to other lists: https://dwheeler.com/essays/static-analysis-tools.html
    - DeWitt clauses generally make it illegal to benchmark closed-source tools. More about the problem: https://dwheeler.com/essays/dewitt-clause.html
    - Could try to measure popularity, but that's not necessarily the same as "good"
    - NOTE: Don't say "commercial" if you mean "closed source" or "proprietary". By definition, OSS available to the public is commercial (at least under US law, & probably in others).
    - Rating tools can involve legal issues, we're recommending something
    - Perhaps require proposers to provide evidence of "significant use"
        - This is a good example of the contribution process to the kind of tool lists the GitHub community maintains, and here is an index of all lists maintained by the community.

2021-Sep-07

Attendees:
- Ryan Ware (Intel)
- Marc Greisen (Microsoft)

Agenda:
- Opens:

2021-Aug-24

Attendees:
- Ryan Ware (Intel)

- David A. Wheeler (Linux Foundation)
- Grey Baker (GitHub)
- CRob [Intel]
- Joe Ranweiler (Microsoft)
- Pierre Tempel (GitHub)
- Bas van Schaik (GitHub)
- Jon Zeolla (Seiso)

Agenda:

- Opens:
    -
- Collaboration with Best Practices:
    - Start putting together content, best practices on using tools…
- How can we get people to learn about this?
    - This is a very hard problem! There's no single "send information here & everyone who should know it will know it" forum. This is fundamentally marketing & it takes time. David A. Wheeler spends a SIGNIFICANT amount of time trying to get the word out about open source software / security / supply chain. You can see some of the presentations & papers he's done here: https://dwheeler.com/presentations.html

2021-Aug-10

Attendees:

- Ryan Ware (Intel)
- Vijay Sarvepalli (CERT)
- Joe Ranweiler (Microsoft)
- CRob [Intel]
- AlonaHlobina [GitHub, CodeQL]
- Vinod Anandan [Citi]
- Matt Rutkowski (IBM)

Agenda:

- Opens
    -
- CRob - Developer Best Practices WG
    - List of industry tools developers should be utilizing
    - TAC proposal for project for whole foundation
    - 1-stop shop
    - Request to write/curate section of project
    - Joint meeting in 2 weeks

2021-Jul-13

Attendees:

- Ryan Ware (Intel)
- Matt Rutkowski (IBM)
- Daniel Silverstone (Codethink)
- Marc Greisen (Microsoft)
- Grey Baker (GitHub)
- John Speed Meyers (IQT Labs)
- Muuhh Ikeda (Cybertrust Japan)

Agenda:

- Opens
    -
- IQT “Secure Code Reuse” Survey

2021-Jun-29

- Meeting Canceled.

2021-Jun-15

Attendees:

- Ryan Ware (Intel)
- Simon Bennetts (StackHawk)
- Grey Baker (GitHub)
- Marc Greisen (Microsoft)
- David A. Wheeler (Linux Foundation)
- Bas van Schaik (GitHub)
- John Speed Meyers (IQT Labs)
- Azeem Shaikh (Google)
- Vinod Anandan (Citi)
- Matt Rutkowski (IBM)
- Vijay Sarvepalli (CERT)
- Alexis Challande (Quarkslab)
- Bentz Tozer (IQT)
- Laurent Simon

Agenda:

- New people
- Opens
- Scorecard: Azeem S.

    - Working to scale up to many more projects. Currently have 30K projects of data, soon will move up to 50K (metrics.openssf.org brings the scorecard data in & displays it)
    - It'd be great to detect more static analysis tools (e.g., Coverity, Fortify, etc.)
- US Executive Order Cybersecurity: David W.
- David W: New release of Flawfinder (simple security-focused source code static analyzer of C/C++ code)
    - Now supports OASIS SARIF as an output format & has better cross-platform execution
    - David is looking for volunteers to help get Flawfinder integrated into GitHub code scanning (through the SARIF integration) - see https://github.com/david-a-wheeler/flawfinder/issues/49
- IQT Survey Results: Next meeting

2021-Jun-01

Attendees:

- Ryan Ware (Intel)
- Simon Bennetts (StackHawk)
- John Speed Meyers (IQT Labs)
- Jon Zeolla (Seiso)
- Vinod Anandan (Citi)
- Vijay Sarvepalli (CERT)
- Matt Rutkowski (IBM)
- Bas van Schaik (GitHub)

Agenda:

- Opens
    - About a month; possibly John Meyers' team may have a report out.
- Whitepaper
    -

Notes:

- Matt suggests:
    - Take secure criteria (e.g.,, govern, build, sign, encrypt) language from "Securing Crit. Projects WG" and adopt them as a basis for evaluating the secure tooling presented (thus far and will be) to this group.
        - Evolve this guidance into a profile that could be used by a scoring system
        - Work with the SCP WG collaboratively to add additional criteria for CI/CD stages
        - Record and agree upon principles of governance (as we discussed today) around scoring/recommendations statements (such as "not picking

winners", "configurations of tooling are important" and "hope to provide assessment relative to secure prescriptions from the group to improve the ecosystem of tools", etc.)
- "Run" the tooling this group has already been disclosed/reviewed against said scoring system and see what it produces.
- Assure the granularity of scoring is such that pros/cons of one tool against another, in any class (SAST, DAST, etc.) can be highlighted
- Assure we focus on the most common build/packaging/deps. Mechanisms (and most popular languages) in providing such guidance and breakdown of scoring granularity (and agree that protecting the "app stack" as built/coded within OCI/Docker containers/packaging deserves special tooling consideration as recognized by the SLSA discussions at the SCP WG)
    - Recognize dockerfile, K8s resource/config YAMLs, etc. as key documents for (targeted) analysis and automation.
- See if we could create a profile to be used/imported by Scorecard (?) or other projects (longer term)
- Provide Service descriptors for hosted tooling (inclusive of OpenAPI, etc.) as well as self-hosted containerized OSS versions of same/similar
    - (longer term) provide descriptors of output/export descriptors of tooling that could be used by artifactory/aggregation services for other analysis tools and dashboards.

2021-May-18

Attendees:

- Ryan Ware (Intel)
- Matt Rutkowski (IBM)
- Fabien Buisson (self)
- Genwei Jiang(Tencent)
- Vinod Anandan (Citi)
- Simon Bennetts (StackHawk)
- John Speed Meyers (IQT Labs)
- Mona Gogia (IQT Labs)
- Daniel Silverstone (Codethink)
- David A. Wheeler (Linux Foundation)
- Vijay Sarvepalli (CERT/CC)

Recap of WG goals for Fabien :
What are the tools dev should use to provide secure code
Integration in git contributions
Make sure the code is secure

End goal : Improve our code security and give means to developers means to advertise about their code security (through badges ?)

Agenda

- Opens
- David: I think it'd be great for this group to pick specific things to develop, e.g., tools / services / documents (guidance, standards) - if you want some funding now is the time to request it. In general, not a good idea to rebuild something already built or being build
    - Proposal: Bring dependency-check from OWASP to OpenSSF. Note: its lead not here. (Note there's also dependency-track, that's different, more focused on SBOMs)
    - CERTCC SBOM project - https://github.com/CERTCC/SBOM/ generates SBOMs in SPDX, CycloneDX and SWID formats.
    - Some ideas are here: "OpenSSF Technical Initiative Wishlist" https://docs.google.com/document/d/1yLo713am8_hvU90Lw0YdYBvXhfTjh7Shn4ATXPNX9ic/edit
    - Idea: Creating specific tool guidance for specific stacks (e.g., some plausible tools, how to configure them over time, etc. Deal with greenfield & brownfield)
    - Problem: Package manager/IDEs do not automatically generate SBOM formats (e.g., SPDX) - there's work ongoing with SDPX, CycloneDX. Maybe we can identify plugin gaps. Maybe the real problem is that people don't know about it - need marketing awareness campaign (blog posts, etc.) - Could have those groups present. (David: I know Kate Stewart, she can tell about about SPDX)
      https://github.com/CycloneDX
      https://github.com/CycloneDX/cyclonedx-maven-plugin
      https://github.com/spdx/spdx-maven-plugin
      https://github.com/swidtags/rpm2swidtag
    - Modify IDEs (Eclipse, etc.) so they generate SBOM.. David: I think they just need to connect to the other tools that do it, not reimplement it all. Default plug-in.
        - Maybe start with OpenSSF and/or LF projects. Scorecard. Kubernetes, Linux kernel. Also other projects like Docker (?) - https://www.cncf.io/projects/
    - Could have a catalog of tools. E.g., SAST tools, etc. Could id properties ("free for OSS", etc.). David; I have a list of OSS static analysis tools; https://dwheeler.com/essays/static-analysis-tools.html OWASP has some: https://owasp.org/www-community/Source_Code_Analysis_Tools
    - https://owasp.org/www-community/Vulnerability_Scanning_Tools
        - Could have list of OSS vs. proprietary (if proprietary, can they be used for free by OSS?) (careful: "commercial" software includes open source

software, since OSS available to the public is by definition commercial software at least in the US).

- Firmware analysis: Sure. Firmware is a kind of software.
- We could benchmark tools - what are the “best” tools? (perhaps just OSS tools).
    - Issue: Benchmarks are hard
    - OSS-only would avoid DeWitt clause issues
- CERT ideas (to be added after the meeting here): These are some big software security tools concern areas that CERT/CC’s Vijay Sarvepalli is tracking
    - SBOM - make tools to create SBOM (native, easy) and improve software traceability.
    - CVD - Automate Coordination of Vulnerability Disclosure. Reach vendors, developers and other stakeholders in a timely fashion with clear and crisp vulnerability information
    - Automate patching of software vulnerabilities - Automate distribution of patches under platforms like GitHub to reach widely used projects and close time for a developed patch to reach all “downstream” forks, copies and includes.
- http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.503.6262
    - ^ Bad link
- This is an interesting code security benchmarking paper from ten years ago http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.503.6262

We can continue next week.

2021-May-04

Attendees:

- Ryan Ware (Intel)
- Simon Bennetts (StackHawk)
- Marc Greisen (Microsoft)
- Jonathan Leitschuh (Gradle)
- Kinga Dobolyi (IQTLabs)
- Raymond LeClair (IQTLabs)
- Genwei Jiang (Tencent)
- John Speed Meyers (IQT Labs)
- Martin Carnogursky (self)
- Mona Gogia (IQT Labs)

- Bentz Tozer (IQT)
- Jon Zeolla (Seiso)
- Vinod Anandan (Citi)
- Matt Rutkowski (IBM)
- Jonathan Schneider (Moderne) - new to group!
- David A. Wheeler (Linux Foundation)
- Daniel Silverstone (Codethink)

Agenda

- OpenSSF Town Hall happened yesterday
- Opens
    - Tools from Jonathan Leitschuh for mass PR requests:
        - Created mass PRs to switch many repos http->https, fix a random number generator use caused by a bad code generator
        - https://github.com/eclipse/repairnator
        - https://github.com/JLLeitschuh/bulk-security-pr-generator
        - Jonathan Schneider's "Rewrite"
        - https://github.com/openrewrite/rewrite
        - http://moderne.io/
            - Uses type-attributed Abstract Syntax Trees (ASTs)
            - Has an AST for Maven, YAML, XML, etc.
            - All recipes are OSS
            - "We'd like to see a world where vulnerabilities aren't just reported, but a remediation is released"
    - Bulk PR generation - Jonathan L has a lot of lessons learned (e.g., rate limits, etc.)
        - How test? Can create unit tests for the transformation
        - Could do a small percentage (say 2%, preferring orgs that have CI), see if they accept & passes their test. Then do more/the rest
        - Can't really do lots of private generation, just don't have the time
    - Currently working on automated disclosure software
    - Concerned about GitHub integration with CodeQL
    - LGTM stores a version of the data on their site, but all is moving to GitHub.com
    - Some things still unclear how it'll be transitioned to GitHub

- Aura: ← The plan is to pick this up at the next meeting (we ran out of time)
    - SAST Analysis on a large scale.
    - Analyze entire Python packaging ecosystem
        - Presentation: https://drive.google.com/file/d/19Hw-GkzKxmmW5kRshSQuFT-clvD7giMb/view?usp=sharing
        - Github: h
        - ttps://github.com/SourceCode-AI/auraHomepage: https://aura.sourcecode.ai/

    - The AuraBorealis repo: https://github.com/IQTLabs/AuraBorealisApp

2021/03/23

Attendees:

- Ryan Ware (Intel)
- David A. Wheeler (Linux Foundation)
- John Speed Meyers (IQT Labs)
- Genwei Jiang(Tencent)
- Vinod Anandan (Citi)
- Bentz Tozer (IQT)
- Simon Bennetts (StackHawk)
- Matt Rutkowski (IBM)

Agenda

- Opens
    - https://www.fuzzcon.eu/
    - Web app defn (reprise)
- Mission Statement: *Identify, Build, Evaluate, Improve & Ease Deployment of universally-accessible, developer focused tooling to help the open source community secure their code*
- Agenda for 2 weeks:
    - Aura - tool for large-scale python stack analysis. E.g., PyPI. Use case: You want to proactively search for suspicious/malicious packages, and have MANY to analyze. https://aura.sourcecode.ai. This is an OSS program. Aura Borealis is the front-end to it.
    - David W: The Critical projects WG has “package-feeds” that could tell you when something was added to PyPI - it’d be great to integrate Aura with that.
- TAC would like WG to:
    - Have received TAC approval of the readme.md per Incubating requirements above
    - Have met at least 4 times over a period of at least 2 months since becoming Incubating
    - Have at least 5 regular members from at least 3 different organizations attending regularly as recorded in meeting minutes.
    - Request TAC approval. TAC will vote to approve or provide constructive guidance
- Per TAC lifecycle: https://github.com/ossf/tac/blob/main/working-group-lifecycle.md
- README template: https://github.com/ossf/project-template/blob/main/README.md
    - Clearly we need the updated mission statement in the README
    - Ryan Ware will create a draft update of README, we’ll review electronically before next TAC meeting

- This WG will start working on identifying tool category names/definitions (as much as possible reusing existing names/definitions) - one problem is that some category names (like DAST) have different definitions & are confusing
    - We'll reuse where we can, with credit
    - OWASP guides
        - E.g. https://owasp.org/www-community/Source_Code_Analysis_Tools
    - edX course about secure software development - identifies some key types & some naming problems - https://docs.google.com/document/d/1oN6juqVR7KXuvclHvoY0pr_XQmC6t6uXMLcYphPsUsA/edit
    - SOAR (Wheeler) https://www.ida.org/research-and-publications/publications/all/s/st/stateoftheart-resources-soar-for-software-vulnerability-detection-test-and-evaluation-2016
    - Simon: I think the WG's resulting document should be markdown, so it can be more easily a living document
    - Ryan: Markdown
    - Wheeler: If the intended result is Markdown, then we should start there. Please cite your sources!
-

2021/03/09

No meeting

2021/02/23

Attendees:

- Ryan Ware (Intel)
- Simon Bennetts (StackHawk)
- Mona Gogia (IQT Labs)
- Vinod Anandan (Citi)
- David A. Wheeler (Linux Foundation)
- Jon Zeolla (Seiso)
- Marc Greisen (Microsoft)
- Nick Ozmore (Veracode)
- Michael Scovetta (Microsoft)
- John Speed Meyers (IQT Labs)

Agenda

- Opens
    - ?
- OSS Gadget - typosquatting detection
    - Problem trying to solve is OSS security things; same common things.
        - Find the source of the package, does it use crypto

    - Swiss army knife for detecting metadata
    - It's really chatty (tries lots of possibilities); on CDNs that's not too bad, but those without CDNs need throttling
    - Heuristic: If the code seems similar, & name is similar, probably typosquatting
    - Supports these ecosystems:
        - Cargo - pkg:cargo/...
        - Cocoapods - pkg:cocoapods/...
        - Composer - pkg:composer/...
        - CPAN - pkg:cpan/...
        - CRAN - pkg:cran/...
        - GitHub - pkg:github/...
        - Hackage - pkg:hackage/...
        - Maven - pkg:maven/...
        - NPM - pkg:npm/...
        - NuGet - pkg:nuget/...
        - RubyGems - pkg:gem/...
        - PyPI - pkg:pypi/…
        - (Go isn't there, working on that)
    - A similar Python-specific tool is pypi-scan: https://github.com/IQTLabs/pypi-scan
    - Also https://aura.sourcecode.ai/
    - Perhaps ecosystems should prevent allowing the creation of packages within certain edit distances of especially common packages
        - PyPI already gets an alert with edit distance of 2, but that makes too many alerts. It'd be better if it was automated.
    - It's a tool, don't plan to build a service. Could be within the package ecosystem (might generate too much noise). Could also be part of the metric dashboard.
- ZAPCon - Simon Bennetts. ZAP Conference. March 9. https://zapcon.io/. Half a day, starting 8am PT.
- Flawfinder is working on supporting the SARIF data format for static tool data interchange https://github.com/david-a-wheeler/flawfinder/issues/33

2021/02/09

Attendees:

- Ryan Ware (Intel)
- David A. Wheeler (Linux Foundation)
- Jon Zeolla (Seiso)
- Everett Maus (Google)
- John Speed Meyers (IQT Labs)
- Marc Greisen (Microsoft)
- George Sieniawski (IQT Labs)
- Mona Gogia (IQT Labs)
- Kinga Dobolyi

- Matt Rutkowski
- Miltos Grammatikakis
- Stanislav Tishkin

Agenda

- Opens
- We hope to see you at our next OpenSSF Town Hall Meeting on Monday, February 22, 1:00-2:00p ET (1800-1900 UTC). It's open to the public; please tell others so that they can join us!
    - PLEASE REGISTER HERE if you're able to join us: <https://zoom.us/webinar/register/WN_5iCAH2-ETaGpiI7UQNSMXw>
    - Please let others know!
- Flawfinder - considering adding support for an OASIS standard for exchanging static analysis tool results (SARIF). Currently planning to say "yes". Comments?
    - https://github.com/david-a-wheeler/flawfinder/issues/33
    - Ev: Positive. It's a little verbose but useful.
    - Johnspeed Meyers: Bart Miller worked on a different spec but now says SARIF is a good format
    - David A. Wheeler: Thanks! We'll plan to add SARIF then.
- Demo from Marc Greisen about platform "REST API Fuzz Testing" (RAFT) - OSS, platform so can launch service, then can run fuzz testing against them (it's not really limited to API fuzz testing). From Microsoft.
    - https://github.com/microsoft/rest-api-fuzz-testing
- David A. Wheeler: Comparison with oss-fuzz?: https://github.com/google/oss-fuzz
    - Ev: OSS fuzz handles the infrastructure for you, but doesn't do service/REST API fuzzing (instead it's focused on code coverage+mutation based fuzzing, i.e. with libfuzz/afl/etc.)
        - One Fuzz is really the comparable solution to OSS Fuzz
- Python malware datasets
    - To see how you can detect the undetectable.
    - https://www.microsoft.com/en-us/research/project/project-freta/
- Need some standard conventions
    - Maybe use: https://github.com/github/scripts-to-rule-them-all
    - There are also GNU conventions, but they don't do what RAFT needs (./configure, make, make install … with DESTDIR)

2021/01/26

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Grey Baker (GitHub)
- Bas van Schaik (GitHub)
- David A. Wheeler (Linux Foundation)

- Stas Tishkin (Microsoft)
- Marc Greisen (Microsoft)
- Ryan Ware (Intel)
- Mona Gogia (IQT Labs)
- Matt Rutkowski (IBM)
- John Speed Meyers (IQT Labs)

Agenda

- New WG Lead: Ryan Ware
- Web app definition
    - https://github.com/microsoft/rest-api-fuzz-testing - “REST API Fuzz Testing (RAFT) A self hosted REST API Fuzzing-As-A-Service platform. RAFT enables painless fuzzing of REST API's using multiple fuzzers in parallel. Using a single command line baked into your CI/CD pipeline developers can launch fuzz jobs against their services.” It supports RESTler, OWASP ZAP, Dredd, Schemathesis
    - Marc and Stas will do a show and tell next meeting.
    - https://github.com/microsoft/restler-fuzzer
      RESTler is the first stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services. For a given cloud service with an OpenAPI/Swagger specification, RESTler analyzes its entire specification, and then generates and executes tests that exercise the service through its REST API.
- CII Best Practices badge - passing criteria are at https://bestpractices.coreinfrastructure.org/en/criteria/0 - we discussed the static & dynamic tool requirements
    - https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/api.md
    - David A. Wheeler did an analysis of the popularity of various static analysis tools a few years ago, he’s having trouble finding that presentation. It was at a Linux Foundation conference.
- IQT Labs Software Supply Chain Security Project: https://the-broken-links-project.netlify.app/ - Thank you! We’d be glad for any and all help and feedback. We’re early!

Here’s the list from the edX course “Secure Software Development Fundamentals” about how to select reusable software (including OSS):

Selecting Reusable Software

There are many important things to consider when selecting reusable software. For security here are a few things to consider:

1. Is it *easy to use securely*? If something is hard to use *securely* the result is far more likely to be insecure.

    a. Look at the defaults of its interface and configuration. Is its API secure by default, or are “simple examples” using the defaults also insecure?
    b. If it has a discussion about how to use it securely, that is generally a good sign, especially if it is clear that its warnings recommend that you keep its defaults.

   This is a reason to avoid using C and C++ to implement new software when there is no significant reason to use them; C and C++ have many insecure defaults (as we will discuss later).
2. Is there evidence that its developers *work to make it secure*?
    a. If it is OSS, has the project earned a Core Infrastructure Initiative (CII) Best Practices badge (or at least are they well on their way to that)? An OSS project that has earned a CII Best Practices badge implements a number of best practices for sustainably developing secure software. We will discuss this in more detail later in the section on verification. You can learn more about the CII Best Practices badge online.
    b. Is there evidence that the developers use tools to detect defects and vulnerabilities as early as possible?
    c. Is there documentation explaining why its developers believe it is secure (aka an “assurance case”)?
    d. Is there evidence of a security audit, and that any problems found were fixed? Security audits are relatively uncommon, but they are a great sign when they exist. An audit that finds a large number of vulnerabilities could have found them because the software is just full of vulnerabilities, or because the audit was thorough, but no matter what, if the problems were found and fixed, those problems no longer exist in the version you plan to use.
    e. Consider using SAFECode’s guide *Principles for Software Assurance Assessment* (2019), which has a multi-tiered approach for examining the security characteristics of software.

   This entire course discusses how to develop secure software; the more of these actions you see in the software you are considering, the better!
3. Is it *maintained*? Unmaintained software is a risk. If the software is not maintained, it is more likely to have serious unaddressed security vulnerabilities, and it is more likely that its developers will fail to quickly fix vulnerabilities when they are reported. In theory, software can be “completed” and not need future changes, but usually software that is not being changed is not being maintained.
    a. If the software is OSS, you can generally look at its repository and see its commit history. If it continues to have active commits, especially by multiple people, that is a good sign. An OSS component with no changes in the last year is generally much riskier.
    b. Are there recent releases or announcements from its developer?
4. Does it have *significant use*? Just because there are many users, or a large company (like Google or Facebook) uses it, does not mean it is appropriate for you. If you only choose the latest fad, you will sometimes make horrific mistakes! However, knowing that software is widely used can be useful information. If software has many users or large (corporate) users, then there’s more likely to be useful information on how to use it

securely, and more people who will care about its security. Also, if it has a small number of users, see if something else with a similar name is more popular - that could indicate a typosquatting attack. We will discuss typosquatting in the next unit.

5. What is the software's *license*? Licenses are technically not security, but licenses can have a big impact on security.
    a. Some software is released without a license at all; this can be legally dangerous, especially if it is more than a line or two of code, because in most countries and situations the law does not permit its use. Sometimes this can be fixed by contacting the original developer and proposing a license. A developer who puts users at legal risk is probably not worried about preventing security risks either.
    b. If the software has a license, make sure that its license is consistent with what you are trying to do. **Beware**: the costs of failing to abide by a license can be extremely steep. Be especially careful if the software is not released with an OSS license, since by definition you will have fewer rights, and in practice there will only be one supplier who will decide what information you can have and how it will change. Make sure you follow the license requirements. If you won't follow the license requirements, you are not only at legal risk for using it, but you will generally not have the right to use its security updates either.
6. If it is important, what is *your own evaluation* of it? If the software is important to you, and especially if it is OSS, you can download and examine it yourself. Some people are scared of doing this, but there is no reason to be afraid. Even a brief review of software source code, and its changes over time, can give you some insight into the software you are thinking about using. This can be time-consuming, so many will not do this. But if the software you are developing is very important, this is a step worth seriously considering. Doing a thorough evaluation of such software is outside the scope of this course. There are many organizations with expertise in doing code-level security audits for a fee; you may want to engage their services if you want an in-depth review. However, if you decide that you want to do just a brief review, here are things to consider:
    a. When you review the more detailed artifacts (e.g., the source code), is there evidence that the developers were trying to develop secure software (such as rigorous input validation of untrusted input and the use of prepared statements)?
    b. Is there evidence of insecure or woefully incomplete software (such as a forest of TODO statements)?
    c. What are the "top" problems reported when running it through static analysis tools (that examine the code to look for problems)?
    d. Is there evidence that the software is malicious? The authors of *Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks* (2020) article notes traits that are especially common in malicious packages: most malicious packages perform malicious actions during installation (so check the installation routines), most aim at data exfiltration (so check for extraction and sending of data like `~/.ssh` or environment variables), and about half use some sort of obfuscation (so look for encoded values that end up being executed). You could also run the software in a sandbox with an environment intended to trigger likely issues, and see if the software attempts to do something malicious. Some

malicious software detects that it is being examined and behaves well when examined, so running code in a sandbox does not guarantee detection… but it may reduce risk.

Also, from the edX course:
If you are starting a new project, it is important to turn on as many of these tools (including compiler warnings) as soon as you can. If you turn them on early, you will see a few reports recommending a different approach and just use that instead. If you try to add them to an *existing* project, you will often see far too many issues to fix, even though the odds of any one being a serious problem is small. So if you have an existing project, you typically need to add these tools slowly, configuring them to only report a subset (such as only reports triggered by a change) and then slowly expanding what they report.

2021/01/12

Attendees:

- Simon Bennetts (ZAP, StackHawk)
- Bas van Schaik (GitHub)
- Alona Hlobina (GitHub)
- Mona Gogia (IQT Labs)
- Björn Kimminich (OWASP Juice Shop)
- John Speed Meyers (IQT Labs)
- Everett Maus (Google)
- Maciej Mensfeld (Castle)

Notes:

- MITRE developed Heimdall Data Format (HDF) for exchanging data between vulnerability tools: https://github.com/mitre/heimdall_tools
- It'd be good to create a list of these exchange formats
    - SARIF was developed by some folks at Microsoft in collaboration with Semmle (pre-acquisition) and a number of other static analysis vendors: https://sarifweb.azurewebsites.net/
- David A. Wheeler just released a new version of flawfinder
- https://codeql.github.com/publications/
- https://github.com/ossf-cve-benchmark/ossf-cve-benchmark
- https://github.com/google/fuzzbench
- Juice Shop now has a WebAppDefn spec at https://github.com/bkimminich/juice-shop/blob/develop/.config/webapp.yml
- https://lgtm.com/query
- https://codeql.github.com/docs/

Template - 2021-Mmm-XX

Attendees:

-

Agenda:

-