LFN Security Forum

Meeting RecordingThe Security Forum is where LFN community members can discuss anything security related. That may include threat analysis, industry trends, best practices, tools, etc.

- Threats and industry trends analysis
- Security Best Practices
- Security tools
- Securing EMCO
- 2022 LFN Security whitepaper
- Security tools adoption survey
- Peraton Labs Project Development Meeting

Interested parties:

Name	Affiliations	Interests
Ranny Haiby	LF, ONAP TSC, LFN TAC, LFN MAC	Cross-community collaboration
Tony Hansen	AT&T, ONAP SECCOM	best practices, tools, cross-community collaboration, CII badging
David McBride	LFN, ONAP, Anuket, US-GOV-OPS	best practices, considerations for software release
Brandon Wick	LFN, LFN MAC	Messaging, communications, content
Robert Heinemann	MITRE Corp, ONAP SECCOM	Adversarial threat, Threat Informed Defense
Muddassar Ahmed	MITRE Corp, ONAP SECCOM	Adversarial threat, Threat Informed Defense
Byung-Woo Jun	Ericsson, ONAP Architecture Subcommittee, SECCOM	security architecture, best practices, industry trends
Amy Zwarico	AT&T, ONAP SECCOM	Security architecture, software composition analysis, static application security testing, software bill of materials, PKI, cross community collaboration
Pawel Pawlak	F5 Networks, ONAP SECCOM	Best practices sharing accross LFN projects, security architecture, automation, software composition analysis, static application security testing, software bill of materials, security in the containers scanning, adoption of tools to increase software security.
Karine Sevilla	Orange, Anuket	Cross-community collaboration, tools, open source software security, software bill of materials, zero trust architecture
Ruben Merz	Swisscom	Security architecture, cross-community collaboration, security automation, zero-trust architecture, PKI, telco security topics, supply-chain security, secure CI/CD
Ragashree M C	Nokia, CNCF, Anuket, OWASP	Security architecture, best practices, industry trends, cross-community collaboration, security automation,
Samuli Kuusela	Ericsson, ONAP SECCOM, Anuket	Cross-community collaboration, best practices, security architecture

Mailing list:

https://lists.lfnetworking.org/g/lfn-securitywg

Meeting minutes:

- April-21-2022 Meeting with David Wheeler
  - Slides: https://docs.google.com/presentation/d/1VrLTfSV4K75XZCG7Mtb00RXQcGJFKk6Y0QQ91BVflCw/edit
  - Recording:video1793455011.mp4

- August-18-2021 Forum kick-off meeting
- November-18-2021 SBOM Discussion
- December-12-2021 DDoS mitigation Discussion
- March-21-2022 DDoS mitigation Discussion (follow up to Dec 12 discussion)

April-21-2022 Meeting with David Wheeler

- OpenSSF badging:
  - https://bestpractices.coreinfrastructure.org/en/criteria/0
- Applicability to "non-code" projects
  - David invites review of the best-practices, and then providing feedback to him
- Re-starting badging effort
  - Should be possible
- Training
  - There is a LF certificate that is good for two year
  - Recommend to have one maintainer take at least one course
- Automatic scorecards
  - Automatically scan the repos
  - SLSA
- Sigstore
  - Verify public key used
  - detect malicious signing, revocation
  - Facilitates easy signing of artifacts
  - There are several integrations ready, e.g. Maven
- Recommendations:
  - Learn to develop secure code
  - OpenSSF badging
  - Use vulnerability tools
  - Monitor for vulnerabilities
  - Enable rapid updates
- LFX SECURITY DASHBOARDS
  - Already have several of the automated tools integrated
- Muddasar Ahmed - https://saf.mitre.org/#/ - Security Automation Framework for DevOps pipelines
- Muddasar Ahmed - Any best practices for people and processes (in addition to the code itself)?
  - The training course is people oriented
  - Some of the badging are process oriented
  - New initiative "Secure Software Factory" - aimed at recommending a pipeline for secure software production
- Follow-up
  - The OpenSSF is open to everyone
  - If you can't find what you were looking for, contact David Wheeler - dwheeler@linuxfoundatioh.org

Slides: https://docs.google.com/presentation/d/1VrLTfSV4K75XZCG7Mtb00RXQcGJFKk6Y0QQ91BVflCw/edit

Recording:video1793455011.mp4

August-18-2021 Forum kick-off meeting

Attendees:

Agenda/Minutes:

- Focus areas
  - Best practices could be further broken down to 'developer best-practices' and 'end-user best practices'
  - How can we collaborate with the OpenSSF - https://github.com/ossf , https://openssf.org
  - Are there other initiatives, in addition to the OpenSSF, that we should be aware of? Suggestion to add a reference in our wiki.
  - What might be unique to the LFN (e.g. CI/CD) that would require a separate security work? At least we need synchronization.
  - Reach out to David Wheeler and organize an introduction call - help define the boundaries between OpenSSF and LFN security. Recent Blog By David Wheeler: https://www.linuxfoundation.org/blog/how-lf-communities-enable-security-measures-required-by-the-us-executive-order-on-cybersecurity/
  - Amy's presentation to the LFN board could be a good starting point for defining the unique security aspects of networking projects. An opportunity to be though leaders on security practices.
  - Please upload any material or links to our existing wiki space - treat it as a sandbox. We can discuss it on the mailing list.
  - We should focus on understanding what projects are doing, not be too prescriptive.
  - Our main objective for now should be knowledge sharing. Later we can decide to broaden the scope, producing white papers, consolidating best-practices, etc.
  - How to test security? How to detect vulnerabilities in dependencies (added to best-practices wiki page)
- Preferred mode of operation
  - Uploading relevant material to the wiki pages
  - ~Monthly meeting, where authors of the uploaded material can walk us through it.
  - Additionally, a newsletter or meeting notes to highlight the new topics.

Action items:

- Reach out to David Wheeler an organize an introduction to the OpenSSF Ranny Haiby

- Upload material to the wiki space - @all

Recording:

LFN_Security_Forum_August_18_2021.mp4

November-18-2021 SBOM Discussion

Agenda/Minutes:

- ONAP SBOM status - https://wiki.onap.org/display/DW/Software+Bill+of+Materials – Pawel/Amy
  - Still WIP. Expecting to generate SBOM soon
  - Started with existing set of NTIA requirements
  - Focusing on SPDX format provides ~85% of the minimum required BOM. Might require some manual work to complete.
  - Working on making the SPDX task part of the CI chain.
  - Q: What are the disadvantages of CycloneDX? A: Failed to extract information in some cases. SPDX seems to be more successful. Also, some operators may required SPDX format for the BOM.
  - There are tools that can generate different formats of SBOM and translate between formats. Different customers may require different formats.
  - Q: Are there CI plugins (specifically for Maven) that can trigger generating the SBOM? Jessica Wagantall may have some such configurations available. Robert Vargawill reach out.
  - Q: How is signature related to SBOM? A: There is a standard methodology in the LF. ONAP is following that. It is mandated by mavenCentral.
- Anuket SBOM work - https://github.com/cntt-n/CNTT/blob/master/doc/ref_model/chapters/chapter07.md#77-open-source-software-security - Karine
  - Started with the NTIA document. analyzed SPDX as well. SWID Tags came up in the analysis as well.
  - At this point planning to come up with recommendation only, no requirement yet.
  - Muddasar Ahmed - Generating the SBOM should become transparent to developers and project leaders.
  - The document linked above is planned to be a living document reflecting recent evolution of SBOM specifications. May include more prescriptive requirements for tools and process.
  - Muddasar Ahmed - SPDX 3.0 specifications will most likely be accompanied by a 3.0 version of the SPDX tool.
- Using Scancode.io for Docker image license and vulnerability scanning -https://static.sched.com/hosted_files/onesummit2021/78/one2021.pdf - Ranny
- recent NTIA recommendations for SBOM. They are quickly becoming de facto standards -https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom - Amy
  - Minimum requirements are already out - 10 fields - name, URL, etc.
  - More fields are in the works. There seem to be alignment between NTIA specification and SPDX.
  - There are external details in the NTIA specifications, some are ambiguous.
  - US entities may be required (by a US executive order from may 2021) to be aware of their software composition. SBOM may soon become part of RFCs issued by such companies.
- Q&A
- Next steps
  - Add links to ONAP page and presentation.
  - Robert Varga - Add information received from Jessica regarding automation scripts
  - Muddasar Ahmed , Pawel Pawlak - Will add a session to the Jan-2022 developer forum

Recording:

Security_Forum_11_18_2021.mp4

December-12-2021 DDoS mitigation Discussion

Agenda/Minutes:

- Mon Dec 13, 2021 10am – 11:30am Pacific Time zoom.us/j/95225604398
- Peraton Labs DDOS Mitigation Technology Overview
  - Slide decks are not available for distribution yet - This is an introduction meeting. Follow-up meeting will be scheduled when slides are available if necessary
  - Peraton's project is focused on protecting edge2edge of a network operator's network. Focusing on OPS-5G DDoS attacks carried out by bots. The project delivers predominantly software, with some interfaces to hardware (switches). In OPS-5G network programmability is used as a measure for mitigating attacks (while not letting the programmability compromise security).
  - Discussion about where the project fits in the LFN landscape.
  - Next steps - Have a slide deck with technical material to share and have a follow-up meeting.

Next steps:

Action Items

March-21-2022 DDoS mitigation Discussion (follow up to Dec 12 discussion)

Agenda/Minutes:

- This is a follow-up to the December meeting, including technical slides that were not previously available

Next steps:

Action Items

Recording: video1184668288.mp4

Slides: ProD3 overview for LF 20220321.pdf