

2022-03-25 Meeting Minutes

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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.



Hyperledger is committed to creating a safe and secure community for all. For more information please visit the [Hyperledger Code of Conduct](#).

Welcome and Introductions

Who you are, which project you represent, your role in the project and what your interest is in the Hyperledger security process effort.

Attendees

[Arun S M](#)

[Ry Jones](#)

[Danno Ferrin](#)

[Hart Montgomery](#)

[Kamlesh Nagware](#)

[Artem Barger](#)

[Peter Somogyvari](#)

Announcements

Agenda

- Welcome
- Cover the threats
- Open Agenda

Next Meeting

Future Topics

Notes

1. Document all the threats first, it helps in creating the categories later. This will also help in prioritising what is important.
2. Define the assets or properties that are to be protected before adding in threats.
3. Infrastructure
 - a. Supply delivery of the open source software.
 - b. Continuous delivery, continuous integration.
 - c. Binaries and outcome authenticated/signed. The end binary user can verify the source and integrity of the software.
 - d. Include physical break into the data center or cloud going down.
 - e. Operational threats.
 - f. Insufficient test bed setup, recommend ways for reproducibility.
4. Architecture
 - a. Data confidentiality.
 - b. Excessive backward compatibility.

- 5. Implementation
 - a. Deployment issues

Action items

- ☐ Checklist for members to follow while reporting vulnerabilities.
- ☒ Questionnaire to report vulnerability ~ calculate CVE score. Danno Ferrin
- ☐ Define scoring guidelines for blockchain & non-blockchain projects in Hyperledger Foundation. [Hart Montgomery](#)
- ☐ Propose to break the task force activities into multiple work streams. [Hart Montgomery](#) [Mic Bowman](#)
- ☐ Define threats in each of the defined category, bring it up for discussion. **Action:** Everyone

Recordings

File	Modified
Multimedia File GMT20220325-145910_Recording.m4a	Mar 25, 2022 by Ry Jones
File GMT20220325-145910_Recording.transcript.vtt	Mar 25, 2022 by Ry Jones
Multimedia File GMT20220325-145910_Recording_1724x1176.mp4	Mar 25, 2022 by Ry Jones
Text File GMT20220325-145910_Recording.txt	Mar 25, 2022 by Ry Jones

[Download All](#)