Meeting information

Every **Friday** from **15:00 - 16:00 ET** at https://nyu.zoom.us/j/93302778069

Governance Committee Meeting

General Notes

- ★ **Please add yourself to the attendance list (below) if you plan to attend, or have just joined the meeting.**
- ★ If you're a new member or if you have an update, please just provide your name. The facilitator will invite you to speak during the check-in phase of the meeting.
    - E.g. Jane Doe.
- ★ Follow the Code of Conduct
    - Let others talk (don't interrupt)
        - Be polite when you disagree
    - Be respectful of others' time (e.g., no rambling and limit piggybacking in agreement)
    - We'll tend to defer things that start to dominate to a future meeting and put a fixed slot up for it.

Jun 18, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Rick McGeer (Berkeley / EngageLively)
- Marcela Melara (Intel Labs)
- Yaxuan(Alice) Wen (NYU)
- Alexios Voulimeneas (TU Delft)
- Hugo Lefeuvre (UBC)
- Glenn Ricart (University of Utah)
- Lluis Vilanova (Imperial College London)
- Anjo Oberwagner (Intel Labs)

Facilitator(s):

- Marcela Melara

Scribe(s):

- Yaxuan(Alice) Wen

Recording

- 2025-06-18.mp4

Agenda & Meeting Notes

- Welcome new members joining the meeting!
- Finalize our vision and mission.
    - Marcela introduced the current status of the vision, the mission, and strategy. Robust on both usability and security perspective
    - Marcela and Rick talked about why we need robust compartmentalization. Lluis suggested explaining what compartmentalization is and why it matters. Hugo, Rick, and Marcela discussed what we are going to submit to LF. Marcela thought “why we are pursuing…” slide should be on a website or repo, not submit to LF.
    - People discussed the vision. Glenn suggested replacing “robust” by “securely” to make the statement more clear. Marcela agreed that we need more explanation about what “robust” means. Lluis suggested describing things like computing stack to make the vision more abstract. Glenn thought the current version (securely, efficiently, and usably) can be applied to network stack as well. Rick suggested thinking from why people use docker (efficient) and applying to why we need robust compartmentalization today.
    - Marcela asked if we should include “flexibly and efficiently” in both the mission and vision or just keep it in one. People suggested adding composability on the vision.
    - After discussion, composability should also be added to the strategy. Marcela thought we can mention the gaps between composability and usability. Hugo suggested also adding security as gaps. Marcela and Hugo discussed whether we should describe “4 pillars” more precisely. Hugo suggested explaining composition more to be more precise.
    - Lluis, Hugo, Rick, and Marcela discussed that we not only “serve” the knowledge but also “advocate”. We not only advocate knowledge but also adoptions. After discussion, we came up with three points to summarize: advocate, serve, and facilitate. Lluis suggested to add “robust compartmentalization" on the strategy to fallback our purpose.
- The next step would be the governance structure of the community. Talk about things like how we want to structure the governance community in the future, transparency, how companies participate (what they need to pay, employ time / etc.), how to host, etc..
- We’re hoping to submit documentations to LF by the end of June. Marcela will send out after finalizing.

May 30, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Hugo Lefeuvre (UBC)
- Alexios Voulimeneas (TU Delft)
- Yaxuan(Alice) Wen (NYU)
- Yuchen(Dennis) Zhang (NYU)
- Rick McGeer (Berkeley / EngageLively)
- Marcela Melara (Intel Labs)
- Glenn Ricart (University of Utah)

Facilitator(s):

- Marcela Melara

Scribe(s):

- Yaxuan(Alice) Wen

Recording

- 2025-05-30.mp4

Agenda & Meeting Notes

- Welcome new members joining the meeting!
- Our candidate name: Open Resilient Compartmentalization Alliance (ORCA)
    - Hugo asked if using “resilient” and “compartmentalization” would be redundant. Marcela answered that using “Resilient” to emphasize security is the top thing we care about, but we’re open to other candidate names.
    - Marcela wanted to mention that we are not focusing on adoption.
    - **Finalized our name after discussion: Open Robust Compartmentalization Alliance (ORCA)**
    - Robust means working together in different ways, and compartmentalization means different components.
    - It’s about good interoperation between different abstractions, mechanisms, and policies.
    - Bringing together research proof of concepts in a way that is robust and industry can adopt widely.
    - Alex suggested that the logo should include LF to ensure the association is clear.

- Finalize the mission and vision
    - Alex, Hugo, Marcela, Rick, and Glenn discussed what's the most concrete way to describe the high cost during adoption, performance, engineering time, etc..
    - Glenn mentioned that we should also include isolating HW bugs, not only software.
    - The team discussed and refined the sentence structure and word choices in the vision and the mission statement, including whether specific terms accurately captured the intended meaning, such as whether bugs encompass 'vulnerabilities'.
    - Rick mentioned that we can mention "Build trustworthy systems from untrustworthy components" in our mission.
- Talk about what should happen after we submit the application to LF.
    - Rules for people joins the community
    - Should we have more industry engagement?

May 16, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU, Lind)
- Justin Cappos (NYU, Lind)
- Yuchen(Dennis) Zhang (NYU, Lind)
- Marcela Melara (Intel Labs)
- Hugo Lefeuvre (UBC)

Facilitator(s):

- Marcela Melara

Scribe(s):

- Yaxuan(Alice) Wen

Recording

- 2025-05-16.mp4

Agenda & Meeting Notes

- Nathan and Marcela are working on the mission and the vision.
- End of notes today and paste to a more official document.
- Differences between the mission, the vision, and strategy:
    - Mission (the What): end goal we're trying to achieve.
    - Vision (the Why): why that goal matters (how the world would change if we achieve the goal) & to what end.
    - Strategy (How): how we accomplish our mission. Better to form this documentation after we are confident about the mission and the vision.
- Marcela shared drafted the mission and the vision:
    - Mission (the What): Advance fine-grained compartmentalization towards a general, efficient, and secure compute paradigm.
    - Vision (the Why): Inter-scale adoption of fine-grained compartments in a broad set of application domains.
- Justin mentioned motivation should be independent of strategy.
- Marcela mentioned that we need official documentation like the vision when joining LF.
- Hugo suggested we can mention that we're trying to fill the gap between academia and industry. Hugo and Marcela discussed the specific content we should mention in the mission and the vision. Marcela shared the mission and the vision of OpenSSF (a larger community) last year, to give a clearer view of the differences between the mission and the vision.
- Marcela thought finishing the vision first would be more natural.
- Marcela, Hugo, and Justin discussed the vision details. Hugo asked if we wanted to mention "fine-grained". Hugo mentioned the definition of compartmentalization in SoK: isolation of components within a program. (...working on the mission and vision together…) Justin asked should we be longer or shorter? Marcela's opinion is that we are smaller than OpenSSF, so we may need a longer vision than OpenSSF (more specific).
- Hugo and Marcela discussed what we should write in strategy. Marcela shared OpenSSF's strategy, which has corresponding approaches to each goal OpenSSF mentioned in its mission. (...working on the strategy together…)
- https://www.cybok.org/supplementaryguides/
- Marcela mentioned the reason why naming matters: it's really difficult to change after we join the LF.
    - Candidate: Consortium for Privilege Separation (CoPr, pronounced "copper")
    - Marcela, Justin, and Marcela had a discussion about terminology of "Privilege Separation" and "Compartmentalization". Hugo mentioned privilege definition: application and processes, but privilege means more in practice. Compartmentalization is more general.

May 2, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan Alice Wen (NYU, Lind)
- Justin Cappos (NYU, Lind)
- Yuchen (Dennis) Zhang (NYU, Lind)
- Marcela Melara (Intel Labs)
- Nathan Dautenhahn (Serenitix)
- Rick McGeer (Berkeley / EngageLively)

Facilitator(s):

- Marcela Melara

Scribe(s):

- Yaxuan Alice Wen

Recording:

- 2025-05-02.mp4

Agenda & Meeting Notes

- Naming the community
    - Top names we got from our previous discussions:
        - Alliance for secure compartmentalization
        - Protection Alliance
        - Information Protection Alliance
        - Alliance for Resilient Compartmentalization (ARC)
        - Secure Performance Compartmentalization Consortium (SPCC)
        - Userspace Isolation Alliance
        - Scalable Isolation Alliance
        - Trusted User Space Alliance
        - Alliance for Privilege Separation in Computing (APSC)
        - League of Privilege Separation Enthusiasts
    - Justin suggested that fundamentals may better focus on compartmentalization. We should consider what the names mean in practice besides the definition.
    - Nathan suggested that name should have more connection with what we're doing. Separation privilege is not same with

    - Justin and Nathan had a discussion about whether it makes sense to name a community now or after we decide what specific techniques we are going to focus on. Justin mentioned that we need a name to form the entity. Nathan mentioned that we want to create our mission asap. Marcela joined the discussion and preferred to have a broader name now, which may attract more people to join, and create the mission at the same time. Justin suggested that we can get the mission with a wider discussion group.
    - Nathan mentioned that separation privilege focuses more on computer domains and not in a narrow way.
    - We proposed our names and will send out next week.
- Work on the charter we received from the Linux Foundation
    - Marcela shared the doc and listed future todos
        - Justin mentioned that we are naming a legal entity, so we'd better be careful about the name of the alliance. Justin also suggested asking LF staff because the example GOVERNANCE.md looks a bit weird.
        - We need to email corresponding people (maybe mick) for more information / clarification, since we are not only doing a spec community.
        - Justin preferred that we can first look at use cases and then form our spec, and Justin would love to hear more thoughts on this matter.
        - Rick suggested that we can follow the paper.
- Mission Vision
    - Marcela mentioned that, normally in the open source projects, there'll be a technical vision in the github repo under the spec section of the umbrella community.
    - Nathan suggested that should we start collecting all mini-thoughts in a shared GDrive doc to form several proposals
    - Nathan will start forming a draft vision while trying to pick everyone's thoughts and then we can discuss from the initial draft. Marcela shared the agreement doc / mission vision / LF file format to Nathan through email.
    - Mission docs are not due today.
- Marcela won't be able to attend the next meeting, but she will send out the reminder and naming poll early next week.
- Nathan suggested having this meeting biweekly (every other week). Marcela and Justin are fine with this and we can have conversations through email.
    - We will probably meet on 5/16, and we will decide the following meeting times offline
- LF documentation should be better to be finished asap.

Apr 25, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU, Lind project, no update)
- Yuchen (Dennis) Zhang (NYU, Lind project, no update)
- Justin Cappos (NYU, Lind project, no update)
- Rick McGeer (Berkeley / EngageLively)

Facilitator(s):

- Justin Cappos (NYU)

Scribe(s):

- Yaxuan(Alice) Wen (NYU)

Recording

- 2025-04-25.mp4

Agenda & Meeting Notes

- We had a nice conversation with LF this week.
- One challenge is to find a name. Try to avoid being too big (e.g.: compartmentalization is not only isolation). The thinking was making decision within a smaller group.
    - Rick mentioned that the name is better to be attractive. “Caging” is not popular among others.

Apr 18, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU, Lind project, no update)
- Yuchen (Dennis) Zhang (NYU, Lind project, no update)

- Justin Cappos (NYU, Lind project, no update)
- Marcela Melara (Intel Labs)
- Nathan Dautenhahn (Serenitix)

Facilitator(s):
- Justin Cappos

Scribe(s):
- Yaxuan(Alice) Wen

Recording

- 2025-04-18.mp4

Agenda & Meeting Notes

- We should invite people from Hyperlight and Oracle (https://blogs.oracle.com/java/post/introducing-graalos)
- We've reached out to LF and are waiting for their response
- Discuss the Code of Conduct
- Marcela suggested that we can do "Community Project + Funding"
    - "Community Project" is more like a base level (basic system). "Community Project + Funding" has additional tech support (CI systems / testing / events / etc.). "Umbrella Community + Funding" has bigger infrastructure to handle bigger scope.
    - We want extra help from LF so "Community Project + Funding" is a good choice.
    - We want at least 2 or 3 co-founders
- People are more interested in techniques of Caging instead of governance now.
    - Nathan mentioned we can provide the value back (maybe we can provide a platform for people?) to attract more people to involve. Roadmap (technical and governance might be different), but a technical roadmap (use cases / concrete roadmap / architecture / etc.) can help.
    - Marcela mentioned that open source maybe seem overwhelming so less people attended following meetings even though we had ~50 people in the first meeting
        - Justin thought people from academia maybe don't understand "what open source means"
        - Nathan said people maybe cannot see benefits from doing open source. Purposed a way to move forward: students purpose a potential solution and attract more attention to optimize because the challenge in academia is engineering. (Bidirectional flow)
        - Marcela said papers play a more important role in academia but the developing path is slow in this field.

        - Having use cases (impact) – academia can mention this in their paper.
    - We need a community with credibility + sth that can work (prototype) => make people treat us more seriously.
        - Maybe we can draft a vision-level document to show people. (ELF has a template). Set an agenda (concrete roadmap for a group) to ensure we have sth to show when people show interest.
        - Maybe either single prototype or parallel projects could attract more people.
- Next steps
    - Parallel: academia + inviting other orgs (2-3 more people before we define what governance means).
    - Maybe a new github repo that looks tight to at least one of us. (LF should have a place to do this).
    - Where do we start doing our paperwork? Shared google doc because there is lots of stuff already? Should be easy to integrate once all paperwork of LF finishes.
    - Nathan can set up a new github to help us start.
    - Naming

Apr 11, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU, Lind project, no update)
- Justin Cappos (NYU, Lind project, no update)
- Yuchen (Dennis) Zhang (NYU, Lind project, no update)
- Marcela Melara (Intel Labs)
- Rick McGeer (Berkeley / EngageLively)

Facilitator(s):

- Justin Cappos

Scribe(s):

- Yaxuan(Alice) Wen

Recording

2025-04-11.mp4

Agenda & Meeting Notes

- OpenInfra merged into LF, maybe the next home for our community. LF seems to have more foundation over time.
- Marcela mentioned joining LF(?)
- Justin mentioned OpenInfra fit better with us. We could engage with them, but joining
- Rick mentioned which works best for additional contributors. Justin thought LF is better at marketing.
- Top level LF. Otherwise: downside: lose lots of control.
- Marcela mentioned that we might be limited to OpenInfro's boarding (foundation / etc.).
- Justin thought we can make our own destiny.
- Final decision: Work directly with LF.
    - Justin and Marcela will work on the following paper works (~1 month) and reach out for candidate funders.
    - Question: what is the best way for others (e.g.: companies / etc.) to be involved? For example: in the governing board or not? Levels? Maybe we could talk with people at Intel / Google / University / Mozilla.
    - We want to be inclusive now. Architecture will be different if companies put in extra money.
    - Quiet quickly to form a foundation.
    - Point relevant people to recording to see if they are interested. We care about the outcome. Rick mentioned people may be interested in use cases. Initial sale and then upgrade?

Apr 4, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU)
- Dennis Zhang (NYU)
- Rick McGeer (Berkeley / EngageLively)

Facilitator(s):

-

Scribe(s):

- Yaxuan (Alice) Wen

Recording

Agenda & Meeting Notes

- Standalone foundation:
    - Need to have our own rules. (License / etc.)
    - Problem: getting attach
- Be part of other foundation:
    - Would be better
    - How compatible are we similar to other projects? Apache focuses on data projects (Spark / etc.). LF is more system orientated – virtualization projects. Maybe LF would be a good choice but Justin or Marcela would have more ideas. Maybe we can be parallel to OpenSSF (one level below LF but one level higher than SBOMit). Need to discuss the decision with Justin and Marcela next week.
- Outreach is important. We need a release to give shape to others.

Mar 28, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Yaxuan(Alice) Wen (NYU)
- Justin Cappos (NYU)

Facilitator(s):

-

Scribe(s):

- Yaxuan(Alice) Wen

Recording

-

Agenda & Meeting Notes

- Discuss further about Linux Foundation pros and cons in more detail
- Agree on initial code of conduct

    - LF code of conduct makes more sense, so this will be code of conduct of this foundation

Mar 21, 2025 | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
- Justin Cappos (NYU)
- Marcela Melara (Intel)
- Alice (Yaxuan) Wen (NYU)
- Dennis Zhang (NYU)
- Nathan Dautenhahn (Serenitix)
- Rick McGeer (Berkeley / EngageLively)

Facilitator(s):

- Justin Cappos

Scribe(s):

- Alice(Yaxuan) Wen

Recording

https://nyu.zoom.us/rec/share/TDgkuUz_y-xCIjtTAH2XnHZUB_5tQKZ_GhGQMe0HtDCziEZ2i0kM-pLU-jCqgno5.mzl94gG8XS2K_JIC

Agenda & Meeting Notes

- Introductions
- A foundation has a technical committee(board), in general deciding “are these projects we want to put efforts for”. Efforts means marketing resources / etc. → benefits. (Depends on how foundation wants to run things)
- Normally organizations put money, and we want to decide the role of the governance committee in the Caging foundation / general structure of the foundation.
- We want to move to maturity level. Different projects (technical specific things) would compete with each other, while foundation is more like an umbrella infrastructure that judges the projects.
- Nathan mentioned: the governance committee should be a set of representative people.
- Justin mentioned: the composition of the governance committee members (academia / target users and adoptions / etc.)

- Marcela mentioned: Projects can play around with each other very well. They can observe / combine each other's strength.
- We will try to invite LF staff to give a talk
- Which open source foundation format should we choose?
    - Under linux foundation:
        - We want to interface with linux / llvm / containerd / etc
        - Easier to motivate participants
    - Goal: review the project and choose the project that is coming. Standardized bar.
- Potential preferred software licenses
    - Apache 2.0 (recommend)
    - Community Specification License 1.0
    - CC-BY 4.0 INTL
    - Need to handle cases for older code
- Code of Conduct
    - Example from the LF: https://events.linuxfoundation.org/about/code-of-conduct/

<Template, copy below and put date here> | Type: Working Session

Attendance

Include role if you have one (in this group, other group or relevant security-related org)

- J. Smith (Big U, SuperFI Tool Maintainer, no update) ← example
-

Facilitator(s):

-

Scribe(s):

-
-

Recording

Agenda & Meeting Notes

-