

01-05-2022 TSC Meeting Minutes

TSC Meeting [Zoom link](#)

[Meeting Recording](#)

[Meeting Chat File](#)

Attendees & Representation. Please add your name to the attendance table below.

Attendees	
Name	Company
Daniel Havey	Microsoft
Eric Tice	Wipro
VM (Vicky) Brasseur	Wipro
Brian Merrell	Walmart
Karan Dalal	Walmart
Balachandra Kamat	Wipro
Dave Thaler	Microsoft
Divya Reddy	Walmart
Jason Niesz	Walmart
Satya Pradhan	
Kanthi P	

LF Staff: [LJ Illuzzi](#)

Agenda

- [LF Antitrust Policy](#)
- Meeting note taker
- Welcome to new attendees
- Cross-platform signing
- [Draft of KF Marketplace](#)
- Private Enterprise Number (PEN) Request for L3AF- Application submitted 12/27
- [Developer and Testing Forum in January 2022](#) (virtual event)
 - Topic submission- [L3AF: eBPF for Windows and Cross Platform eBPF programs](#)
 - Tuesday Jan 11, 08:15am to 08:45am noon ET
- LFN Induction
- General Topics (cover as needed)
 - Use Cases
 - Roadmap
 - Project structure
 - Governance
 - Technical Steering Committee

Minutes/Updates

Cross-platform signing proposal:

- [Listen to the call](#)
- [Review the patch](#)
- Discuss on this list (if needed)
- Discuss [on the patch](#) (required)

Details:

Matteo Croce from Microsoft joined today's TSC call ([excellent notes here](#), thanks to Daniel's speedy fingers) to introduce and discuss [his BPF patch](#) to support cross-platform signing. Unfortunately, several key people were unable to make it to today's call (that's the holidays for you), so Matteo was able to introduce his patch but we weren't able to get into a deep conversation about it.

A summary of today's discussion: Matteo's patch is cross-platform and will allow for signed BPF programs to be distributed remotely. Soon after Matteo's patch, Alexei (maintainer of BPF) sent over a separate patch for signing BPF programs. It relies on an approve-list(*) as well as on Linux's fs verity (meaning it's not cross-platform).

The full discussion is in the [recording of today's call](#). Please give it a listen.

We were going to have an in-depth discussion of this be the topic of the next TSC call, but it seems Matteo's patch is time-sensitive. Since the next call is January 5th, we'll need people to have a look at the patch, the conversation in response to it, and then come up with an opinion based upon L3AF and its needs. That opinion should be expressed in the conversation on the patch.

- Cross platform signing
 - DaveT: Was anybody able to review the patch.
 - Brian: Went through the conversation
 - DaveT: Topic will be discussed in the eBPF foundation BSC meeting. 1 Week from today L3AF will be presenting. Next meeting - design of signing needs to be cross-platform.
 - Two proposals:
 - Matteo's - cross-platform, very well aligned with L3AFd.
 - Would be helpful if the L3AF community supported this proposal
 - Other - approved list of binaries (Linux centric)
 - Can load anything that is on the authorized list.
 - Does not meet L3AF or eBPF for Windows needs.
 - Would be fine if both were merged
 - DaveT: Cisco's (Chris) opinion would be very helpful
 - Weigh in on the Linux discussion group and on the BSC call.
 - Karan could add a bullet point to presentation - collective opinion of the L3AF community.
 - Brian: Add a point in your document about this?
 - Matteo's original patch was a config option to add only signed programs.
 - Alexi's other patch is moving forward
 - John Fastabend (on Linux discussion) and Luca agreed that the features needed by MSFT could be implemented inside of libBPF and as an eBPF program
 - This conversation ended on Dec. 9th (Before Matteo presented at L3AF)
 - DaveT: Meeting with Matteo after this call
 - Brian: L3AF could include the signing eBPF program as part of its eBPF program chain. (According to discussion on Linux group)
 - Vicky: Invite Matteo to next weeks meeting.
 - Have L3AF call next week to discuss signing before BSC meeting.
 - Louis: Will not be at the L3AF call next week but will give the keys to an appropriate host.
 - Brian: L3AF Kernel Marketplace
 - <https://github.com/l3af-project/l3af-arch/discussions/9>
 - DaveT suggests adding this as a PR for line-level comments (Brian will do)
 - DaveT: Kernel functions only disallows eBPF programs that can be uploaded to NICs. Suggest a name change.
 - Vicky: Suggest package manager as a concept for the name. Define broadly. Names have power.
 - DaveT: The name implies scope.
 - Brian: What should we name it?
 - eBPF is difficult to say and will probably need an acronym.
 - Vicky: eBPF Package Manager == EPM
 - Karan: EPM / eBPF package manager does make a lot of sense, in terms of scope
 - Brian: is the Kernel Function Marketplace part of the L3AF project?
 - May make sense to migrate to its own project.
 - In the future a platform agnostic place may be apropos for the EPM
 - Vicky: L3AF could be its initial client. This could really help L3AF. Define it as something standardized that a package manager can use.
 - This way the EPM would be a force to increase L3AF adoption and help us push towards standardization for both EPM and L3AF.
 - DaveT: Benefits to both ways of doing this:
 - Inside L3AF then it is closely located with all the other parts of L3AF. This could help widen the scope of L3AF.
 - Outside L3AF then it can include things that do not work with the current version of L3AF.
 - There isn't a BSC opinion yet. It is forming now.
 - Distinguish between L3AFd and eBPF.
 - Answer: What is the L3AF project?
 - Today it is the L3AFd, but in the future we will expand scope.
 - Vicky: EPM should be outside L3AF because there will be others working on it.
 - DaveT: Is it part of one of these or both?
 - Thing that LF sanctions - L3AFP (legal entity)

- L3AFp - Github repo
- DaveT: eBPF code signing portion in additional bullet point in the lifecycle management section.
 - Brian: 2 different layers of signing
 - Package contribs of compiled source code (signed). This is app layer packaging.
 - Signing of eBPF programs.
 - Doc only currently talks about package signing
 - DaveT: Please put that in proposal.
 - Some cases where signing should be done by author, others signed by the repository.
- Brian: Initial version Github repo may be sufficient
 - Assumes that everyone will be okay pushing their code to a L3AF Project repo
 - Revisions could be tested and reviewed by L3AF team
- DaveT: Requiring manual review? Good/Bad?
 - Brian: Short term - no manual vetting
 - We currently do not have automatic review
 - DaveT: Requirement to have automated review.
 - Vicky: Marketplace needs manual review for safety.
 - DaveT: Manual review could be optional.
 - Vicky: Is part of the review going to be for security.
 - Automatic review - definitely. Manual reviews - maybe. (at the start)
 - DaveT: Notion of private repo
 - Jason: For startup we need manual review
- Brian: Hosting source code or packages
 - Source code - versioning etc.
 - Package or archive - what is needed to run the program along with docs
 - Signed by repo
- Karan: Please review doc. We will discuss in next meeting.
 - This is the area where we need support from the community.
- Brian: Will put up the pull request today.
 - Please discuss on PR.
- Louis: LEAF session is 8:15 ET will this work?
 - Daniel: Will check with Poorna
 - Need email for presenters.
- LFN induction - Need a separate meeting to discuss this
 - Needs a lot of community input.
 - General agreement.

*** Minutes from 12/15/2021 ***

- PEN request
 - Raga: Schedule call after this meeting
 - Dave: What layer of the org is the PEN assigned to?
 - L3AFD project, LF, L3AFP?
 - Louis: Just put it under LFN. Ramnifications?
 - Dave: Next PEN would probably have a sub-delegation under the original PEN
 - This is how MSFT does this so that there is a single management point.
 - Lous: Difference between L3AFd and L3AFP?
 - Dave: Github organization with different GitHub repos under it.
 - Louis: PEN that covers L3AF as a project and all current and future repos?
 - Dave: Common use of PENS is for OID and PEN is inserted into the OID with arbitrary number of layers underneath.
 - OIDs are used in x.509 certificates, etc.
 - Lous: How are we going to use the PEN for L3AF? Want a PEN that covers all of L3AF, but not all of LF or LFN,
 - Raga: As part of flow exporter we will add custom field support identified with PEN number.
 - Dave: Inventing a new slot that fields are going to go in, can it be just an array of fields of integers?
 - Raga: Will dig more and find out?
 - Dave: It matters to how we will fill out the application.
 - Raga: This is a requirement for the flow_exporter. We will not need another PEN number for L3AF.
 - Lous: Will reconsult with legal and set up call with Raga. Review by email with rest of L3AF team (if this is doable).
 - Dave: It's just a simple web form and cannot be pending
 - <https://pen.iana.org/pen/PenApplication.page>
 - Dave: Do we use LF, L3AFP or L3AFd for the name?
 - Lous: Will discuss with legal.
 - Dev testing forum
 - Set date and time for MSFT presentation
- Cross platform signing
- Matteo: No way to do cross platform signing with eBPF programs
 - Implementation that allows loading eBPF programs to kernel that takes care of relocation
 - Created patch that does this. Creates eBPF prog and adds sig to it.
 - <https://lore.kernel.org/bpf/20211203191844.69709-1-mcroce@linux.microsoft.com/>
 - Dave: talked about 3 peices in kernel function marketplace
 - Orchestrator pulls stuff from marketplace
 - Can you put signed programs in the marketplace
 - We are discussing an option that allows remote distribution and is compatible with L3AF.
 - The other approach does not play well with the L3AF vision that we have discussed.

- Vicky: Do we have representation as the L3AF at the kernel level where these decisions will be made?
 - Dave: Need Karan, Chris, ect. If we had a collective decision it would carry more weight.
 - This could be a call to create new contacts.
- Dave: This discussion is happening on the Linux kernel list
 - MSFT would like cross-platform
 - Move to the eBPF foundation (which is cross-platform)?
- Dave: Next BPF steering committee meeting would like L3AF to present.
 - Invited Karan.
- Dave: BSC does not officially have an answer if the meeting is open.
 - Still have time to ask. Should be a yes answer (at least for this meeting)
- Matteo: Proposed to BPF ML & then another solution appeared from the BPF maintainer
 - Very different solution: create an approve-list of programs that can load BPF programs
 - Only allow programs loaded from progs on this approve-list
 - Suspects this solution won't be cross-platform: verification requires Linux fs verity method
 - Also allows L3AFd to install anything it wants if L3AFd is in the allow list, Could be a security flaw
 - Matteo's approach allows individual signing and allows individual verification, reputation, etc.
 - Raga: Where is the signature exactly? Do you still have the verification step on signed programs? Use case please.
 - Matteo: XDP. Some BPF programs take actions on packets. These can be loaded and attached to network drivers.
 - Malicious programs can mangle packet traffic (very dangerous). Must make sure that program is safe.
 - Dave: Big value add: signing instead of verification step.
 - Verification step can be CPU intensive. Signature check is cheap.
 - Verification and signing together does not give this benefit. This is what the patch does.
 - Raga: Does this work for UM progs also? Yes.
 - Dave: Other approach with white list? How is this different from cap BPF?
 - Matteo: Whitelist enforces Cap BPF.
 - Dave: L3AFd pushes out both kernel function as well as a program that can use the kernel function.
 - Matteo: Whitelist is a list programs that can be loaded
 - Matteo: Sig verification is before verification check.
 - Dave: Also reduces DOS style attacks.
 - If sig check fails then verification does not run and waste cycles.
 - Santhosh: Verifier runs only once at load time.
 - Dave: Yes, but you can spin the loader.
- Dave: That is the intro.
 - If we can get several orgs to support this then we can approach the BSC.
- Vicky: Once the video for the call is available we can take this to the mailing list.
- Lous: Cancelling next weeks call on the 22nd?
- Dave: Nope, on vacation.
- Vicky: Probably most people have made plans so Jan 5th would be better.
- Matteo: PR is urgent for MSFT because we want a signature system.
 - It's too dangerous to load untrusted BPF programs
- Dave: Please post opinions on Linux Kernel mailing list sooner rather than later.
- Dave: Include signing into the BSC meeting on Jan 12th at 1PM PST.
- Lous: Please register for Dev and Test Forum

Action Items

- ☒ Schedule Dev & Testing Forum L3AF session (LJ/Daniel/Poorna)
- ☒ Schedule call with Raga to fill out the PEN application. (LJ/Raga)
- ☐ Ask BSC if the meeting can be open to the public (Dave)
- ☐ Vicky: Will post to mailing list so that people can discuss signing on list after watching video.

Future Agenda Items

***** Minutes from previous call *****

- Abhi Patil: Where is the L3AF project at currently? (high level overview)
 - Orchestration across any eBPF platform in order to solve business problems
 - L3AFd which runs on any host.
 - Many eBPF programs - see wiki
 - Create marketplace/repo of eBPF programs
 - Simplify chaining of eBPF programs
 - extend eBPF programs to Kubernetes
- Abhi P:
 - Targeting DDOS programs
 - Lead for DDOS initiative
 - Peraton Labs and Georgia tech working on their project
- Karan: More details on the and use case yo move forward
- General Topics (cover as needed)
 - Use Cases
 - eBPF program (soon to be open sourced)
 - export records in IBPF format

- Enterprise number will be needed for this
- Dave T: eBPF programs that will be put into marketplace
 - L3AF could include signed programs
 - samples
 - Include other programs that are not signed by L3AF
- Is L3AF a framework for marketplace?
- Vicky B: Peel off marketplace from L3AF?
 - Handled by different team that works with L3AF so it can support different project such as Polycube
- Dave T: Is the PEN for L3AF
- Karan: L3AF team is contributing programs and that is what the PEN is for.
- Jason: Agree with Dave, be careful with diluting L3AF
 - Walmart added programs should not be natively part of L3AF itself, but rather the Walmart contribution to L3AF
- Dave T: Could you use a Walmart PEN and contribute that to L3AF?
- Karan: Once the eBPF program is OSSed then we should use the Walmart PEN and it should be under the LF after OSSing
 - What kind of signing are we looking for?
 - Verification that the eBPF programs are compatible with the L3AF platform
 - For instance chaining.
 - Need deeper dive.
- Dave T: Whose PEN do you use. Whoever the signer is going to be?
 - Karan: For now we don't have a clear bifurcation. It's just one L3AF.
 - We should consider how to do this.
 - Louis: IPfix program, is this a one time sign off or every time it is used?
 - Dave T: Whenever there is a change to the program it must be resigned. Not a one time thing.
 - PEN is a one time number. The signature changes with updates and revs.
 - Karan: If someone wants to use IPfix and change the PEN they can do this. Not tying anyone to the existing PEN.
 - Dave T: Then it would be a different program. Stars and other marketplace artifact would be invalidated.
 - Christopher L: Maintainer of the code should sign the code. The org that controls the commit bit.
 - Raga P: planning to use PEN on IPfix to define custom fields. If there is no PEN then it would be an unknown field.
 - Karan: Anyone could pass a PEN into these fields and change things. If you don't change things then you get the predefined custom fields.
 - Term L3AF has been overloaded. L3AF team, platform, project, marketplace
 - Dave T: L3AF is the foundation. The more we put programs into it the more it becomes the L3A instead of L3AF.
 - Karan: If L3AF is the platform (L3AFd) how do we want to structure the remaining components?
 - Keep L3AF marketplace as a separate project? Should we drop the L3AF branding on it?
 - Vicky: Makes sense to have the marketplace be a separate thing with separate branding that is closely tied into L3AF.
 - L3AF becomes the initial consumer of this, but we plan for other consumers.
 - Louis: Consider breaking off separate projects under L3AF to ensure that the output of these is compatible with L3AF.
 - Common in OSS world for Project Tech Leads to spin off other projects in this manner.
 - Vicky: Makes a lot of sense to have things under L3AF initially. Perhaps move them later (eBPF Foundation).
 - Jason: Small set of programs provided by L3AF itself and make sure they are compatible to help get things started in the beginning.
 - Vicky: This will help to get L3AF off the ground with a small set of programs that are useful and work.
 - Jason: Yeah, these could be examples and building blocks that others can use.
 - Karan: Definitely a good thing.
 - Dave T: 3 categories of stuff: core daemon, marketplace, programs
 - Which one should be in different projects?
 - Are they all under the L3AF?
 - Where do the programs go?
 - Is the marketplace part of the L3AF repo?
 - Multiple marketplaces (Google, Apple, etc.). Is the marketplace part of the foundation?
 - Does L3AF just contain samples? Leaning towards this one?
 - Vicky: If marketplace is separate this is incredibly valuable because orgs can run their own marketplace. Should be a separate project.
 - LJ: are any programs in the marketplace paid for items?
 - DaveT: Yes, Vicky: leave door open
 - LJ: Not sure it should be OSS?
 - DaveT: Marketplace is not the programs. Paid programs can be distributed by on open source marketplace.
 - Vicky: cannot confuse monetization strategy with the licensing strategy. For pay programs should not be excluded from an OSS project. It's the licensing.
 - Brian M: This is good. Will take all these thoughts and work them into paper. Available this month(?), when we reconvene.
 - Karan: Better to leave it open so that it is an attractive proposition for folks to contribute. We need to iterate on this a little more.
 - Vicky: Brian's paper will help us to create a parallel working group to address this.
 - Jason: Start them in the base and then move when available.
- Housekeeping: Next meeting is the 15th. Dec 22 and 29th are cancelled, reconvene on January 5th for Dev and testing forum prep