06-08-2022 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
Jason Niesz	Walmart
Dave Thaler	Microsoft

LF Staff: LJ Illuzzi

Agenda

- LF Antitrust Policy
- Meeting note taker
- Welcome to new attendees
- Issues/pull requests
    - Reposupport by Atul-source · Pull Request #69 · l3af-project/l3afd (github.com)
        - Where is the JSON config documented? I couldn't find it.
    - when should PR's be merged: How many approvals needed? Is a meeting needed? E.g., should Added some tests by Atul-source · Pull Request #66 · l3af-project/l3afd (github.com) have been merged last week when I approved? Or yesterday when Santhosh approved? Or this morning when Satya approved? Or during this meeting?
    - Add OpenSSF scorecard workflow by dthaler · Pull Request #71 · l3af-project/l3afd (github.com)
- Roadmap planning
- Release Management
- LJ Illuzzi will not be on the 06/15 (DTF) and 06/22 (Vacation) TSC calls.
- General Topics (cover as needed)
    - Use Cases
    - Roadmap
    - Project structure
        - Governance

        - Technical Steering Committee

Minutes/Updates

- RepoSupport #69
    - Create document (see below)
    - Changes look great. Need a test or a doc page.
- OpenSSF scorecard
    - Best practices badge now merged
    - Some GitHub actions
        - Someone with Admin in the L3AFd permissions needs to set up PAT.
    - Create read only token and add it under the security tab.
    - Generates score between 0-10.
    - Jason Niesz to do this.
- Added some tests #66
    - Dave has permissions.
    - When should Merge be done?
        - 2-3 code owners sign off
        - Second person merge or third person merge?
        - 2 approvers besides the submitter to merge.
- Reposupport #69
    - Guidelines for PR
        - 100% code coverage
        - full documentation
        - There is no documentation change here.
        - Couldn't find a doc that needs to be updated. Is there one?
        - The code changes look good, but should there be a doc page? Should we add tests?
        - We need to create a document. Santhosh Fernandes
    - l3af.io needs refreshed
        - Add Cloud Native eBPF presentation
        - Lj: PAge was set up through the LF creative services group.
            - Can we put this in a GitHub repo where we can maintain it?
            - Dynamically generated from GhPages feature
                - Doxyfile - generates HTML from Markdown.
                - GitHub workflows: UpdateDocs - creates site from DoxyGen file
                - Switch branch to GhPages and check in there.
            - eBPF.io website generated by netlify
                - Runs in CI/CD and generates a preview.
                - We just want to be able to manage the website without having to ask an outside entity.
            - Is ebpf.io going to be community managed or is there going to be a contractor?
                - Who will set this up in GitHub? LFIT or community?
                - Can we take over WebMaster for l3af.io? Lj
                    - https://www.netlify.com/
                - Does eBPF.io use the free version? Dave Thaler to find out.
- Roadmap planning
    - LFN board meeting in May
        - Challenges: Roadmap, release management, contib diversity, community growth.
        - What is our Roadmap and Release cycle?
            - We can get media attention with this.
                - LFN blog, linked in pages, our company linked in and blog posts
            - This will help us build our community.
        - 1-2 people to take on Release Manager role
            - Training and consulting is available for release management is available
        - We should define release management cycle
            - We will get some more resources soon We should assign the release manager roles then.
        - In the interim we can define the roadmap. Put some dates on it.
            - LFN board and at the end of June the LF board. Project updates.
            - They can help with guidance and resources
    - Lj: back in 2 weeks (29th of June) Vacation and Dev end test forum.
- Security for the localhost
    - Don't have a database to store tokens in the l3afd environment
    - Need to auth with username/pass, get a token back and validate based on token
        - Two types: Normal and Admin user
    - Some kind of script that will generate token
    - Hostname and role will be passed
        - Token will be stored in l3afd.cfg file as a part of deployment
    - First we pass the token and check for validity
        - Should we validate on host that the roles are matching?
        - "If the software produced by the project causes the storing of passwords for authentication of external users, the passwords MUST be stored as iterated hashes with a per-user salt by using a key stretching (iterated) algorithm (e.g., Argon2id, Bcrypt, Scrypt, or PBKDF2). See also OWASP Password Storage Cheat Sheet). [crypto_password_storage] This criterion applies only when the software is enforcing authentication of users using passwords for external users (aka inbound authentication), such as server-side web applications. It does not apply in cases where the software stores passwords for authenticating into other systems (aka outbound authentication, e.g., the software implements a client for some other system), since at least parts of that software must have often access to the unhashed password."
            - Should we be storing the password in a file?
            - This is probably not best practice. How do ensure that the file cannot be read by the world?
            - Today we do not encrypt the file.

- Storing secrets in a file is probably not best practice.
  - Can we store a hash of the key?
    - ..."Iterated hashes using a per user salt"...
  - We could look at public key to connect on localhost
    - Use cert signed by CA
  - We could create a CA in mTLS which has a private key. It could issue a client cert and then we only allow TLS.
  - Token Base or tcert public key or something like this
- Atul: if we try ssh type authentication private and public keys
- Dave: Can we do this with mutual TLS and put the client cert as the TLS cert?
  - Doesn't work in browser land.
  - Could be done with a fancy rest api
- Make l3afd a group and members will be validated to the password in the system?
  - Different code for Linux and Windows
  - TLS will have the same code for Linux and Windows.
  - We should, if possible, optimize for user experience.
- Only ever store public info in files. Never store secret keys anyplace in the file system.
- Unless we make a dynamic key like a hostname or a some combination then the client cannot generate the token again.
- pub/private key is probably the easiest or we have to have a hash value stored in the file.
  - Store the hash value as a key, but...
  - We need a way for the client to generate the hash file.

- Satya will be pursuing other opportunities. Will be here next week.
  - New resources coming in July.

Action Items

Future Agenda Items