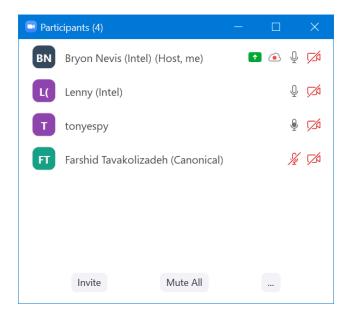
EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

November 17, 2021

Attendees



Agenda

- Opens
 - o Snap secret store disable issue is resolved.
- SPIFFE ADR status
 - TODO: Note that the unix:// connection via sock-dir is over GRPC!
 - Explored https://github.com/lixiangyun/grpc-c
 - Single-person project; project age is ~3 years; would not pass dependency vetting
 - Doesn't compile in newer Linuxes due to header changes
 - Has blocking bug that doesn't pass per-request metadata tags
 - Could be made to work with effort, but for how long?
 - Explored https://github.com/Juniper/grpc-c
 - More popular, but older -- 4+ years, unmaintained
 - Works over domain sockets, but socket path is hard-coded in code; despite manual inspection suggesting that metadata tags might work
 - Has lots of build issues as well

Called the experiment off before proving that it could talk to the real SPIRE agent.

Options?

- [] Explore alternatives. Use ____ instead. (Suggestion?)
 - [] Create a utility to create one-off secret store tokens
 - Distributed file system e.g. gluster instead to share tokens
- [TE(no)] Move on. Deprecate existing C device services.
- [LG(+/-)] Hybrid. Convert existing C device services to Go, deprecate the C SDK; and use native C interface to call required C APIs.
- [no] Adopt. Fork one of the grpc-c libraries and make it work.
- [TE(yes)] Bridge. Create a C to C++ bridge library using the official GRPC C++ library; create hooks in Device-SDK-C to enable SPIFFE/SPIRE mode. (e.g. build a shared library, dynamically load and use it based on a flag).
- [TE(yes)/LG(yes)] Modernize. Rewrite/rearchitecture Device SDK in C++, provide legacy API bridge. All device services would be mixed C/C++ from now on. (Aligns with Eaton initiative.) Need to fix handling of main().
 - Why does lan want to keep it in C?
- [] Double-down. Adopt SPIFFE/SPIRE as the primary means to obtain secret store tokens, and build on it for other uses e.g. microservice authentication. For snap compatibility, make upstream contributions to SPIRE to allow Unix workload attester to take command line arguments into consideration or develop a systemd workload attester. Ignore the legacy problem for now and kick the can down the road to reassess at a later date.
- Other things going on
 - Functional device services using gRPC
- o Discussion
 - Today, this only impacts delayed start device services in secure mode (C device services can't be distributed in secure mode). Unless had one-off-tokens, or distributed filesystem.
- Next steps
 - Take recommendation into device-services WG on 11/29 (8am pst) or into 12/7 app services meeting
 - Bring "modernize" (seems huge)
 - Bring "bridge" (lowest friction) ← expect support for this
 - Bring "hybrid" (almost as much work as modernize)
 - Bring "fork grpc-c"
- Reviewed pending CVE and made updates to mention snaps

Standing Agenda

- Review Security Board
- Securing Consul Board (skip)
- <u>Review CIS docker scan</u> (will skip unless something changes) (click latest run, go to classic, view console output).
 - Last checked: Tue Nov 16 05:36:01 UTC 2021
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
 - o ! Sys-mgmt-agent base image perpetually out-of-date
 - Everything else looks OK (some false positives, or not exploitable)
- Review action items from previous week

Action Items

• 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.