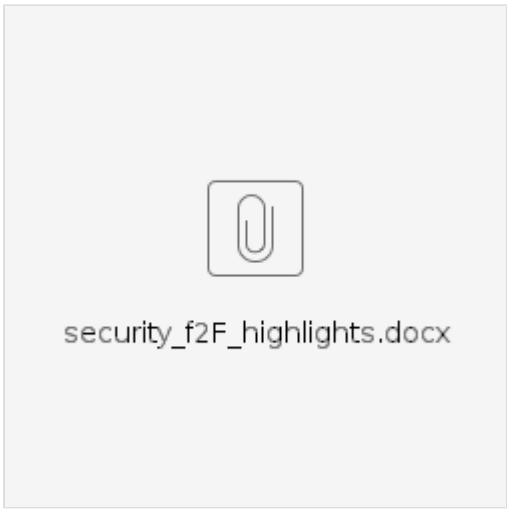
Hardware Security F2F August 1, 2019

cation: SC-12/Intel, 3600 Juliette Ln, Santa Clara, CA 95054

Planned Attendees: Jim Wang, Bryon Nevis, Jim White, Doug Gardner (remote) Tingyu Zeng, and Malini Bhandaru.

Host: Jim Wang yutsung.jim.wang@intel.com

Meeting Recording: https://zoom.us/recording/share/R9lPtU2l3ILhnPEqYClIOqUVQPH8cProuLmXCKKqbm2wIumekTziMw

Highlights: 

Lo

Agenda:

1) PKI Initialization - Status, Code Review, Testing - Jim Wang

2) Hardware Security - Bryon Nevis + Jim Wang (slides)

1. High level design,
2. Architecture
3. development status, items still needing completion
4. Testing methodology and how-to (hardware requirements or TPM SW emulator ..)

3) Threat Modeling - Tingyu

4) Opens - Security Vulnerability Handling, Linters in CI pipeline

Time Permitting: Any other topics, please specify.

Meeting Minutes

Thank you to Jim Wang and Bryon Nevis and Intel for hosting the event!!

Attendees (in room): Intel: Eno Udoko, Jim Wang, Dryon Nevis, Dell: Jim White, Tingyu Zeng, HP: Henry Lau/Retail, VMware: Malini Bhandaru

(remote): Canonical: Ian Johnson, Tony Esp, Dell: Trevor Conn, IOTech: Rodney Hess

The chief outcomes were:

1) PKI set-up design shared by Jim Wang. We did not get into details of testing. The discussion however prompted discussion around container start-up dependencies and the need to ensure

predictable success or application launch given we are at a 1.0 release. Arbitrary sleep times just do not work across different hardware platforms with different compute/RAM etc resources.

a) **Agreement that EdgeX containers have finer grain inter-dependencies beyond just container "was start" that Docker compose offers.**

Plan is to support this using Consul scripts to ensure predictable successful launch of the EdgeX sequence of containers.

Ian Johnson will share his expertise here, he developed such scripts for Snap.

b) **A second decision here was to move the PKI setup code in smaller chunks directly into EdgeX-go**, to make code review easier in addition to landing the tests, which are thorough into the main repository.

The tests cover common functionality thus they will serve to increase test coverage across the project as opposed to a PKI only sub-project.

No fall back plan. let us all help Jim Wang review his code and land sooner than later.

2) Decision on design of hardware support for security storage. Bryon went through each option in his draft explaining pros and cons.

Jim White shared that there are yet to be publicly announced efforts to provide hardware based secure storage but a design decision and software implementation

will ease those efforts, helping efforts to move in parallel with an interface point. **Bryon will update documents based on the decision.**

3) Tingyu shared his thoughts on EdgeX threat model,

a) North (all API calls and export function) – we have protection using the secure proxy,

b) Defining users/groups. (admin task, integrates typically with some enterprise identity and authorization component)

c) South (devices/sensors/actuators)

d) SDKs - Device SDK and Application SDK and watching out for SQL injection type attacks and arbitrary code execution. Cross-site scripting is chiefly a web/UI attack and not "yet" a concern.

e) Inter-microservice communication - crawl/walk/run .. as a first pass we could assume these may be trusted instead of needing to be authenticated and authorized at each call.

f) Device registration – to protect from rogue devices and denial of service.

Tingyu will share his evolving threat model document with the security team, restricted view.

Malini to investigate how other open source projects share their security details or not! She shall also poll her broader open source team at VMware.

4) Time to record our security roadmap. - Malini

Visa Letter Request Process: https://events.linuxfoundation.org/visa-request/

Recommended Airport: Norman Y. Mineta San Jose International Airport, 1701 Airport Blvd. San Jose, CA 95110.

Other possible Airports are SFO, San Francisco airport and OAK, Oakland Airport with further distances,.

Please check Google maps for details relative to your travel plans.

Distance from Airport: Approximately 4.5 miles

Recommended Area Hotel(s): Marriot (Walking distance), Biltmore (across the road on Montague, walk), Hilton (closer to Dell offices, car)

Transportation Options: Self driving, Taxi, Uber, or Lyft