5G SBP Use Case - Remote Attestation Use Case 1- IoT Device Security and Authentication

Use this template to submit Use Cases for submission to the 5G Super Blueprint Use Case & Requirements Advisory Group. All input is required unless marked "(optional)"

- ☐ Muddasar Ahmed work with David Shur to add details and make ready for community consideration
- ☐ Ranny Haiby consult

Use Case Name:	Remote Attestation Use Case 1- IoT Device Security and Authentication
Use Case Description:	Leveraging technics of Peraton Labs add Remote Attestation to existing lab infrastructure This Use Case may be combined with Remote Attestation Use Case 2- IoT Device Onboarding & Maintenance
Epic Problem Statement and how is the problem solved:	**Problem Statement:** How to insure that IoT devices on a network are authentic and have not been tampered with. This is particularly sensitive in remote areas that are not often frequented by people. **Resolution:**
User Stories	- Remote Attestation Protocal (RAP) server is set to periodicaly "inspect" IoT devices by checking by confirming Evidence. Example, remote camera A is passively "inspected" by Remote Attestation server, the server confirms that its evidence (ex; firmware fingerprint) is authentic and permits/allows the camera to stay on the network. - Remote Attestation Protocal server is set to periodicaly "inspect" remote cameras by checking its evidence against pre-configured evidence. Remote camera B is passively "inspected" by Remote Attestation server, the server determines that the evidence does not match evidence that has been pre-configured in the RAP server. The server then denies camera B access on the network and sends an alert. [Placeholder] Active alerting. Camera C sends an alert when its evidence has an unexpected change.
Demo Storyline (optional)	
Interaction with other open source projects and components	- SEDIMENT: See https://sediment-lfproject.github.io/ - KubeArmor: See 5G SBP: KubeArmor + SEDIMENT project
Links to existing documentation (Build Guide, Slideware, etc), if available (optional).	https://sediment-lfproject.github.io/ SEDIMENT Project Alignment
Links to existing demo /video, if available (optional).	
Links to existing code /repos, if available (optional).	https://github.com/sediment-lfproject/remote-attestation

14 Apr 2023

Minutes:

- Quick round of Introductions
- Ta provided description of current SEDIMENT deployment in three parts (following passport model): prover on IoT, verifier, and relying party.
- Rahul provided sescription of Accuknox on securing multi-vendor workloads being pushed to the edge using KubeArmor. Containerized environment, but how do we ensure failure of one container does not compromise other workloads.
- SEDIMENT needs three TCP ports for verifier: prover to verifier, verifier to relying party, RA admin/visualization GUI, and two ports for relying part: verifier to replying party, application GUI. Simple daemons that run on Linux, a few shared library dependencies.
- What is the demo going to be on? Muddasar described use case and demo goals from 5G SBP perspective. Once basic demo of RA with Accuknox is done, we can talk to other folks to integrate with ORAN compliant base station.
- Muddasar will like to see SEDIMENT RA code for attesting an Intel/AMD computer (beyond IoTs), so edge servers can also be attested
- May be a good idea to evaluate each other's products out and do a demo in the lab. Then we can replicate it at Kaloom Lab or other lab available to LF 5G SBP.

Next steps:

- Send meeting minutes to 5G SBP [Rajesh]
- Define requirements for demo. Identify resources (how many cores, memory, disk etc.), IP addresses, ports that need to be open. Topology of services/containers. This will help LF coordinate the use case demo. [Rahul to take lead, Ta to support – draft in a couple of weeks, to discuss tentatively in May 2nd 5G SBP call]
    - Need SEDIMENT to Dockerize the solution
    - Capture requirements in parallel, put it on the LF 5G SBP wiki

11 Apr 2023

Meeting Notes:

- AccuKnox provides run time security and determines security policies
    - Characterizes application behavior
    - Workload hardening
    - SEDIMENT would be one application running under the run time security provided by AccuKnox
- By restricting environment to one application initially (Phase 1), this would reduce the complexity and allow for observations of functionality
- Phase 2: including 5G Core and 5G RAN
- Rajesh: need to consider whether changes are required for the API between the
- Rajesh: need to look at RA as a service rather than an application.
- Rajesh: 1) what is the relying service?; 2) what is the IOT device?
- Rajesh: need to involve SEDIMENT developers in the discussion. Not available today.
- Peraton needs access to the IBM camera demo. Bring up with IBM and Kaloom on the next 5GSBP call
- Accuknox needs to install a "tool server" in the lab
- Gaurav: how do we a