Peraton | LABS

SEcure DIstributed IoT ManagemENT (SEDIMENT) for OPS-5G

PL SEDIMENT Team, PI: David Shur
Members: Rajesh Krishnan, Yow-Jian Lin

The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

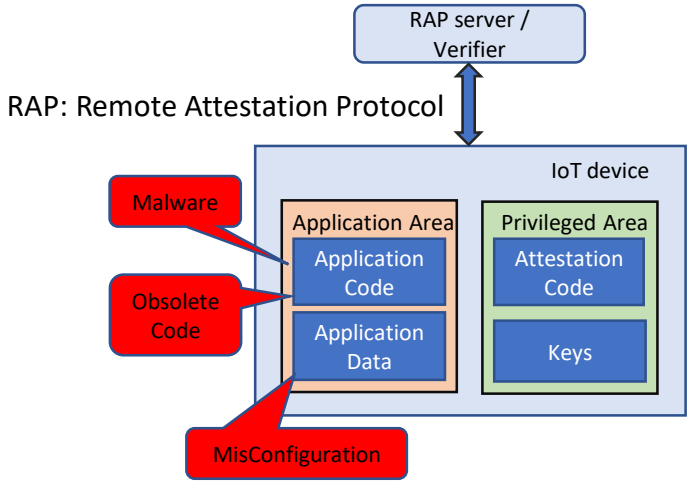
Outline

- SEDIMENT Remote Attestation (RA)
- SEDIMENT RA protocol framework
- IETF Remote ATtestation procedureS (RATS) Architecture
- SEDIMENT transition to a Linux Foundation project
- Engagement with LF 5G Super Blueprint
  - Use case #1
  - Use case #2
- Next steps
- Q/A

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

SEDIMENT Remote Attestation (RA)

- RA goals
  - Detect presence of malware and software tampering
  - Verify IOT device configuration integrity
  - Authenticate
  - Operate across the entire scale of devices on a 5G network

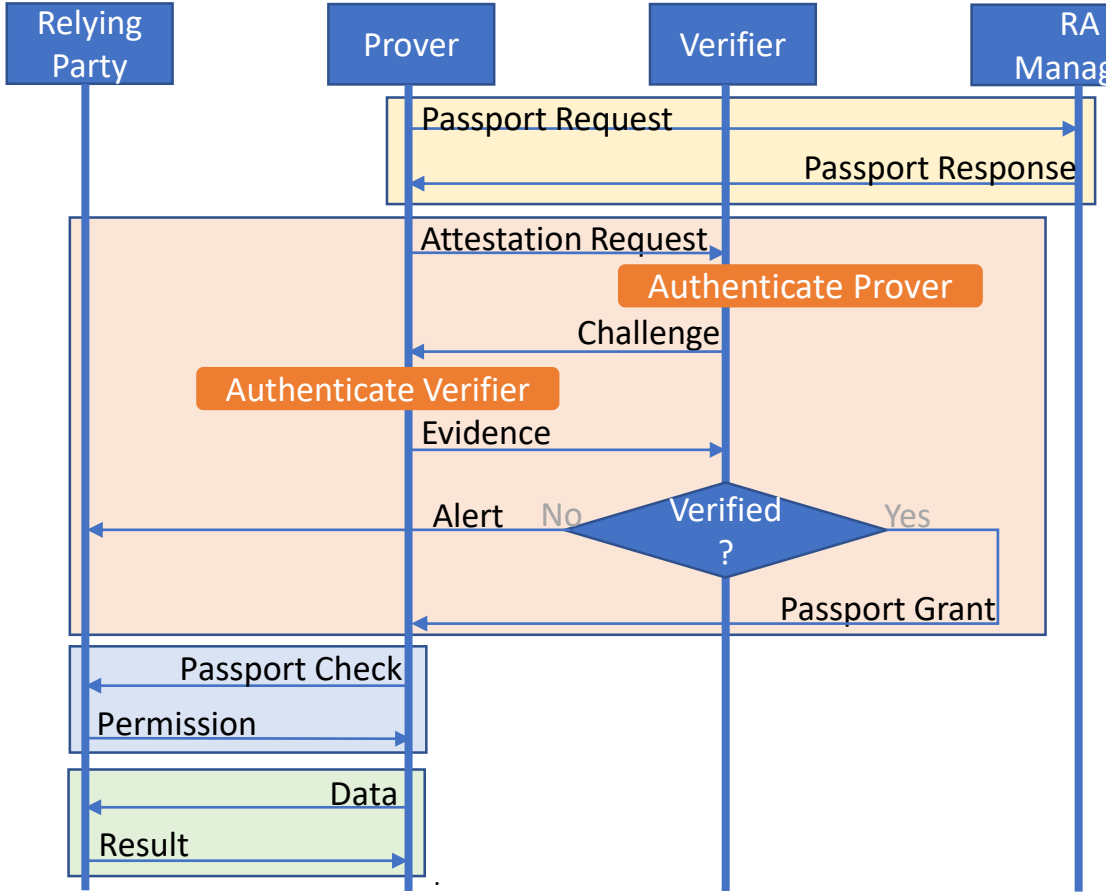


- Key RA components
  - A protocol (cf. next slide) that supports
    - Authentication and authorization among communicating entities
    - Flexibility in requesting various types of evidences for attestation
      - E.g., firmware fingerprint; process status
  - Hardware/software/hybrid Root of Trust (RoT) that ensures the integrity of RA protocol execution [1]
    - Protection of attestation credentials
      - Exclusive access
      - No leaks
    - Safe execution in a protected region
      - Execution atomicity (cannot be interrupted)
      - Immutability (attestation code and everything it depends on cannot be altered after being loaded)
      - Controlled invocation (run attestation code in its entirety)

[1] Karim Eldefrawy, Norrathep Rattanavipanon, and Gene Tsudik. 2017. HYDRA: HYbrid Design for Remote Attestation (Using a Formally Verified Microkernel). *WiSec '17*.

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

Remote Attestation Protocol Framework



Pairing:

- Prover authenticates itself to Relying Party and acquires Verifier connection information

Attestation:

- Prover initiates attestation, *instead of continuously keeping a communication channel open waiting to be attested, with significant energy savings*.
- Verifier can issue a variety of challenges to request Prover to produce evidences.
- Authentication digests signed with the shared key enables both parties to authenticate.
- Verifier evaluates evidence. Either grants a passport to Prover or sends an Alert to Relying Party. Prover must restart the procedure after some time if it does not get expected positive response from Verifier.

Join:

- Prover submits granted passport to the Relying Party to gain permission to communicate.

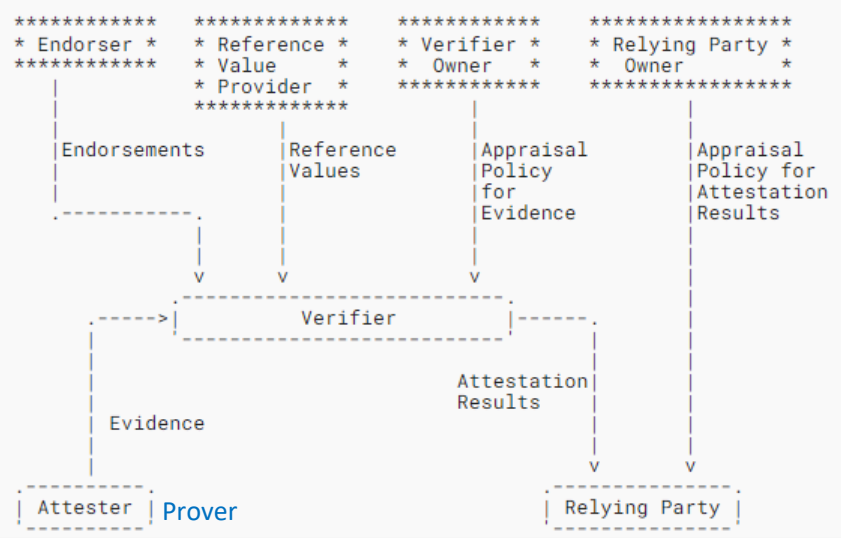
Report:

- IoT device sends application data after Passport has been accepted.

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

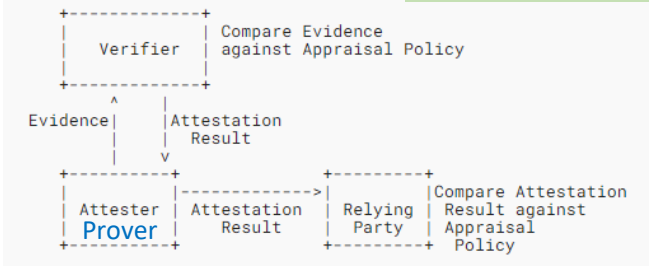
IETF RATS WG Architecture

https://datatracker.ietf.org/doc/rfc9334/

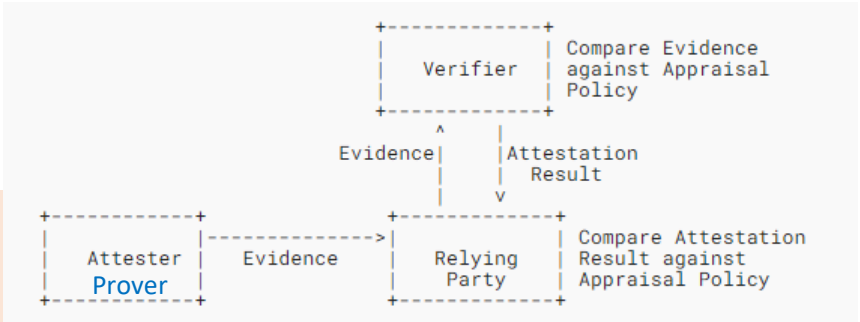


Conceptual Information Flow

SEDIEMENT RA is being aligned with RATS, following Passport model



Passport Model



Background Check Model

Relying Party:	Network equipment for network access admission; Server holding confidential data for release; Entity that needs trustworthiness of remote elements
Evidence:	Claims about the target environment
Reference Values:	Values used in appraising evidences
Endorsements:	Statements that help authenticating device info

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

SEDIMENT Transition: Linux Foundation Project

Peraton | LABS

- "SEDIMENT, a Series of LF Projects" has been set up with the following mission statement:
  - "to provide open-source software implementing a distributed and scalable security architecture with remote attestation for networked IoT devices"
- Documents have been adopted/executed by LF and Peraton Labs:
  - Technical Charter, Series Agreement, and Contributor's Agreement (word mark transfer)
- Project supporters including one LF member:
  - NIWC (LF member), DARPA, Peraton Labs, UCI, Kryptowire Labs, Aarno Labs, USC/ISI
- Apache v2.0 License for code and CC-BY-4.0 for documentation chosen
- Code and documentation released by DARPA DISTAR and Peraton
- Repositories for code and webpages: https://github.com/sediment-lfproject
- LF Project public announcement on February 22nd, 2023

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

Engagement with LF 5G SBP

- Develop use cases for RA in collaboration with Muddasar Ahmed and Ranny Haiby
  - Ensure that IoT devices on a network are authentic and have not been tampered with
  - Ensure that IoT devices can be seamlessly maintained and securely updated
- Develop and integrate SEDIMENT RA onto existing 5G SBP lab infrastructure as proof of concept of ways to realizing 5G SBP use cases

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Use Case #1

- 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.

- How would remote attestation help?
  - RA Verifier is set to periodically "inspect" remote cameras by checking their firmware fingerprint.
    1. RA Verifier confirms that the firmware fingerprint of Remote Camera A is authentic and permits/allows the camera to stay on the network.
    2. RA Verifier determines that the firmware fingerprint of Remote Camera B is not authentic. RA Verifier then alerts Relying Party (e.g., firewall) to deny Remote Camera B access on the network.

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

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Use Case #2

- Ensure that firmware of IoT devices can be seamlessly maintained and securely updated, especially when IoT devices are deployed at scale.

- How would remote attestation help?
  - With a hardware/software co-design, RA Prover enforces software immutability and prevents unauthorized updates.
    1. Unauthorized software updates on Remote Camera C triggers its MCU reset.
    2. Secure updates issued by RA Verifier to Remote Camera D as the sole means of software updates.

5G SBP Use Case - Remote Attestation Use Case 2- IoT Device Onboarding & Maintenance

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)

Next Steps

- Continue use case refinement with the working group and update draft on the LF 5G SBP site.

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)