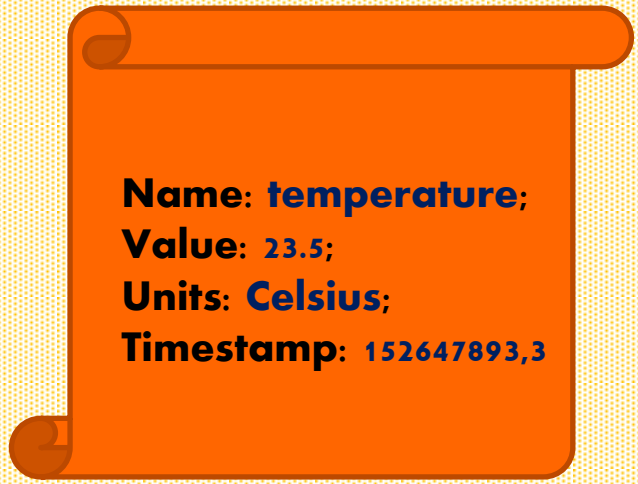
Secure Swarm Attestation for IoT Networks

Aïda Diop
(Orange Labs - Télécom SudParis)

12/02/2019

Trust in Remote Devices: example

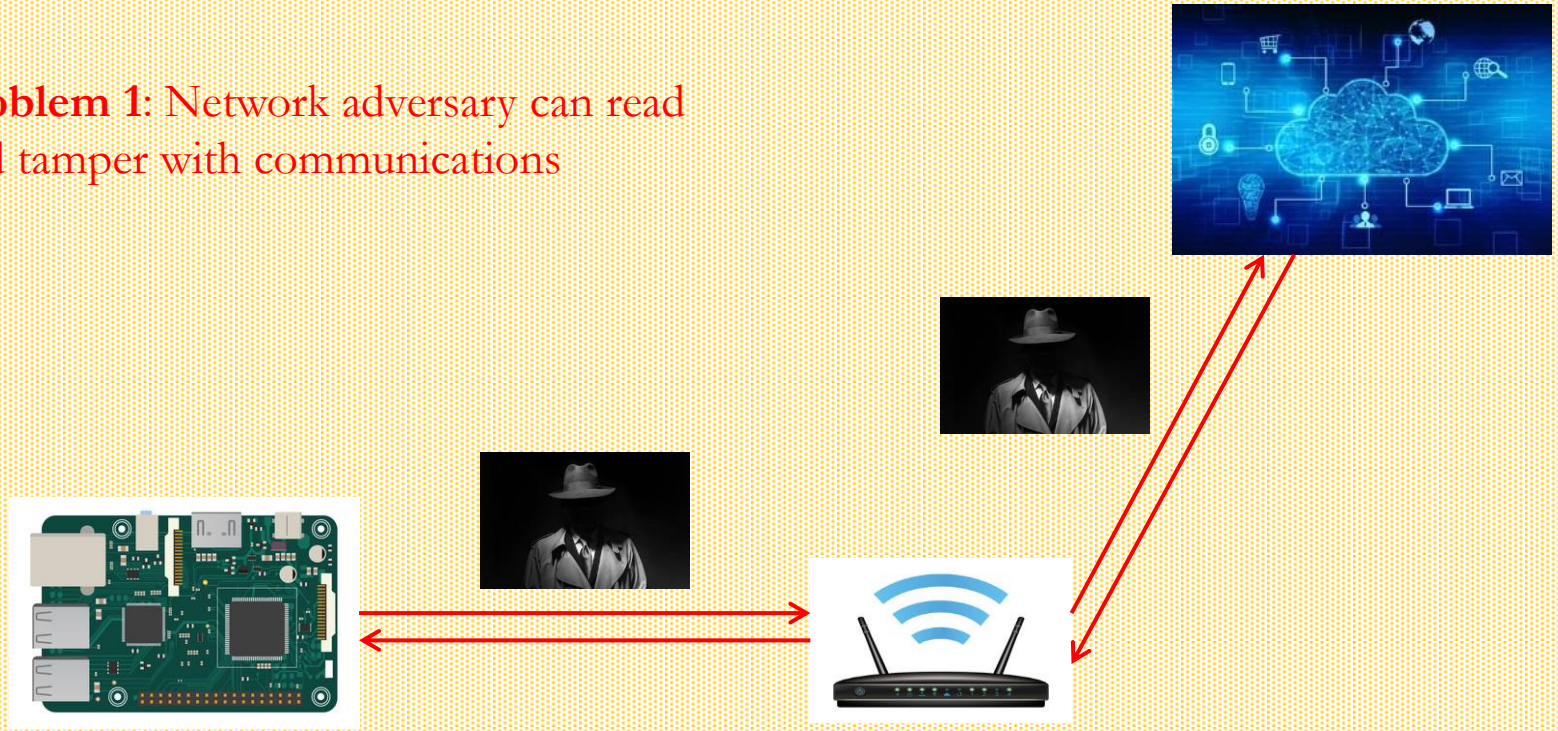
- A sensor sends the following message over a Bluetooth, BLE or Thread network:



- Can it be **trusted**?

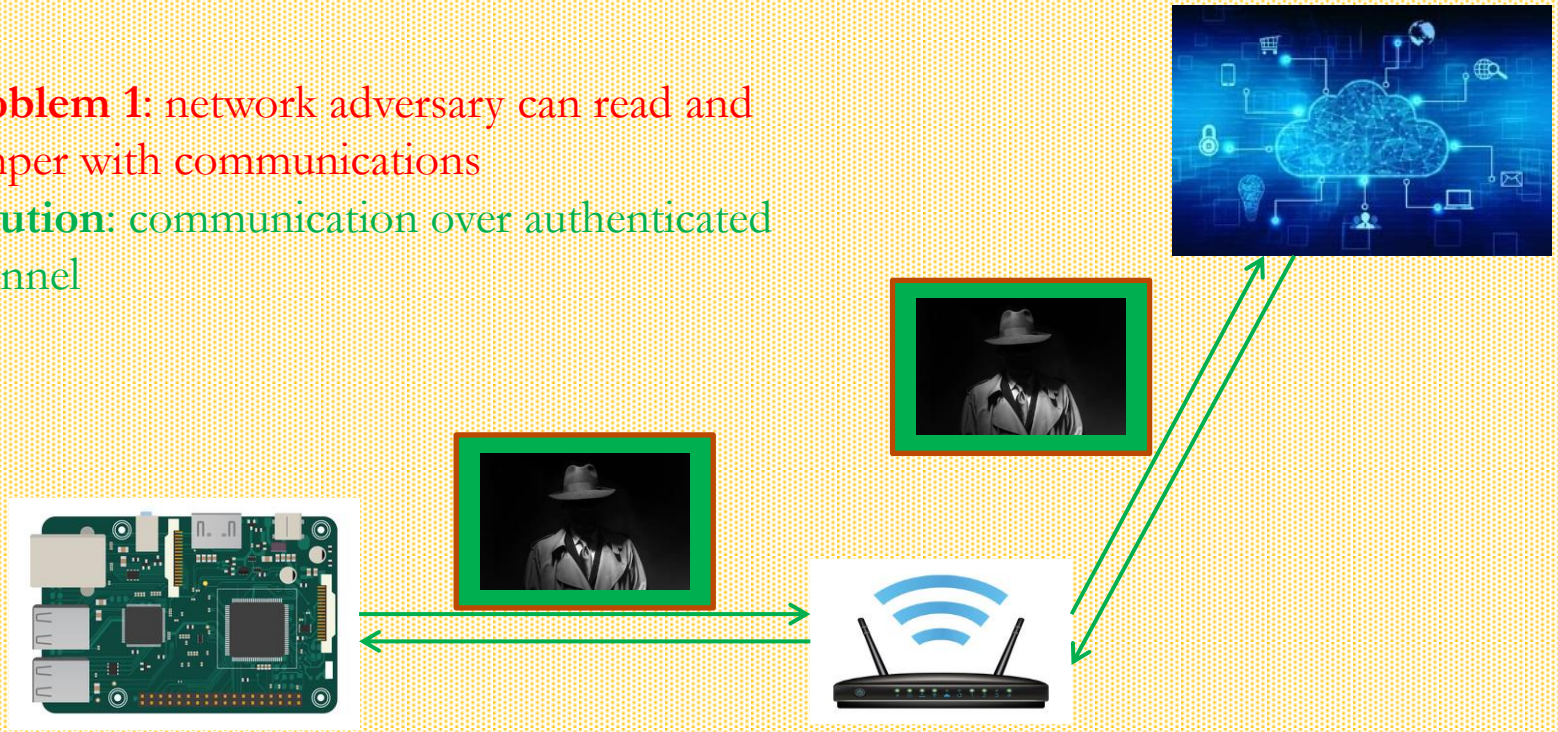
Trust in Remote Devices: example

- **Problem 1**: Network adversary can read and tamper with communications



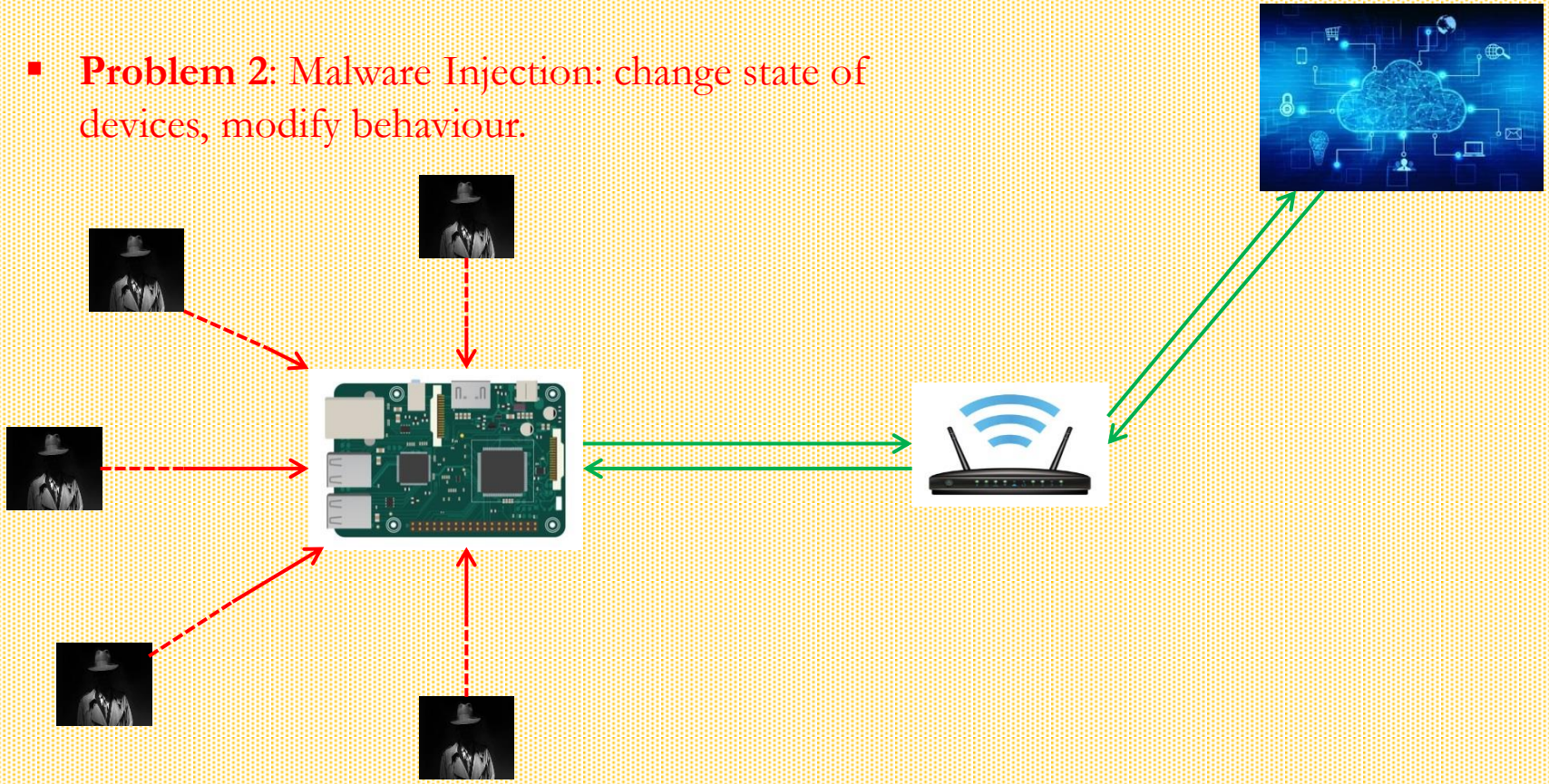
Trust in Remote Devices: example

- **Problem 1**: network adversary can read and tamper with communications
- **Solution**: communication over authenticated channel



Trust in Remote Devices: example

- **Problem 2**: Malware Injection: change state of devices, modify behaviour.



Trust in Remote Devices: example

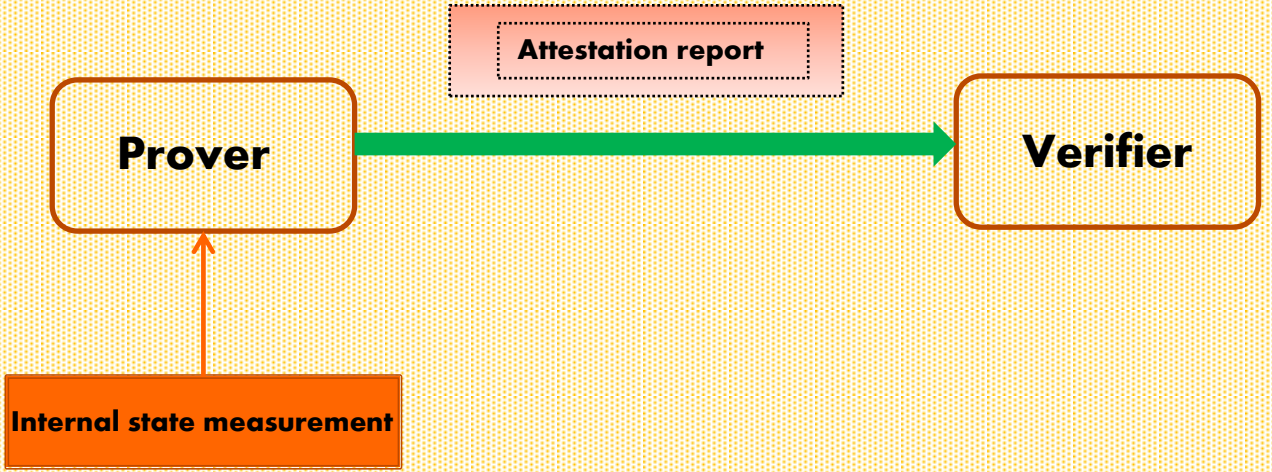
- **Problem 2:** IoT Malware attacks

https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/

https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

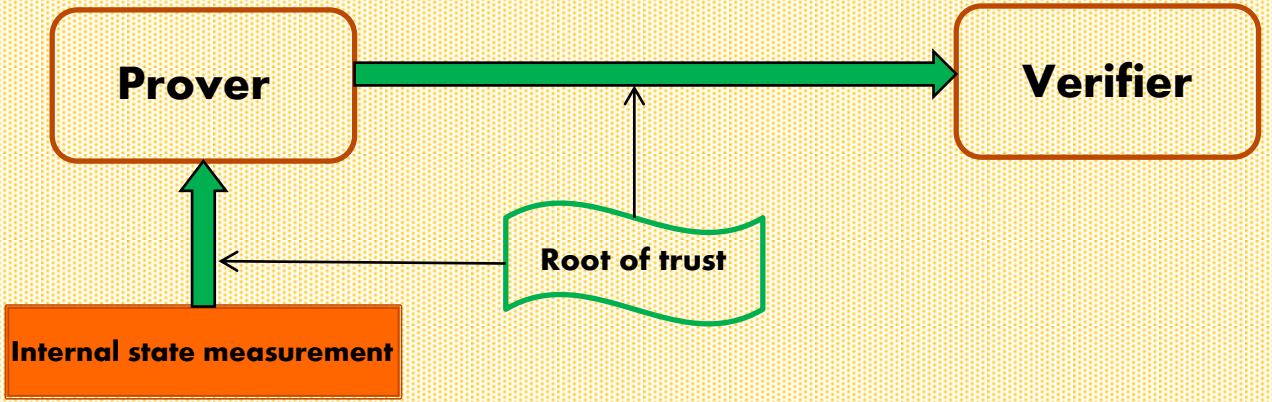
Remote Attestation

- **Problem 2**: Malware Injection
- Solution: **Remote Attestation**
  - Interactive protocol between a **prover** and a **verifier.**
  - Verifier attests of the **current** state of the prover.



Remote Attestation

- **Properties:**
  - **Authenticity**: protocol represents the real state of the system.
  - **Freshness**: protocol represents the current state of the system.



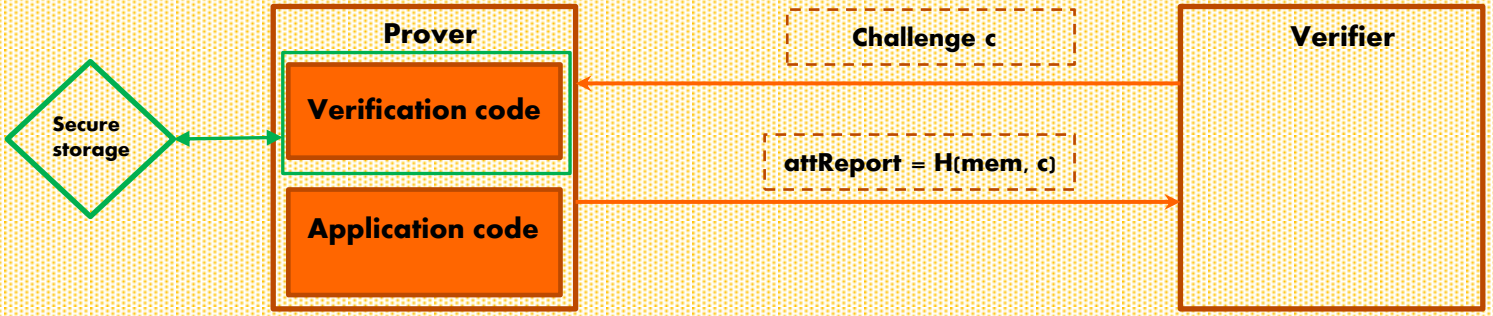
Hardware VS Software-based Attestation

- **Hardware-based attestation:**
  - Hardware module: Trusted Platform Module (TPM);
  - Platform Configuration Registers (PCRs) stores platform «state» measurement;
  - Stores cryptographic secrets in hardware;
  - Limitations:
    - Requires a root of trust for measurement;
    - Expensive hardware for low-power devices;
    - Attestation measurement during initial software loading only.

- **Software-based attestation:**
  - No secret stored on prover's platform;
  - Limitations:
    - Unrealistic security assumptions: passive adversary;
    - Weak security guarantees;
    - Verifier must always the know the exact configuration of the device;
    - Requires authenticated channel (e.g. physical connection).

Hybrid Attestation

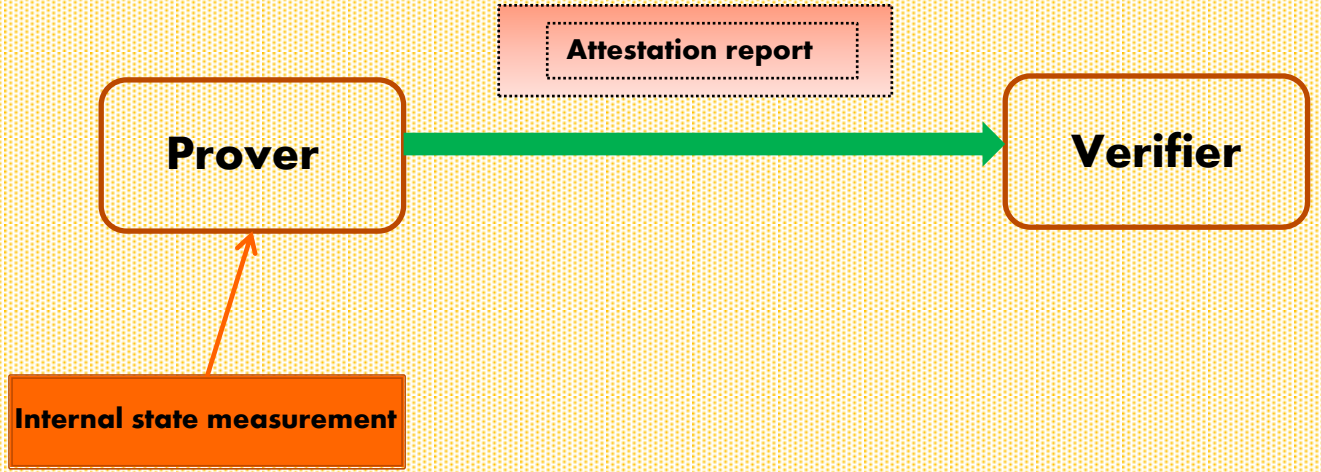
- Minimal hardware requirement:
  - Read-only memory (ROM) that stores cryptographic keys and the attestation protocol.
  - Memory-protection unit (MPU) that controls access to the restricted data in the ROM.



- Practical implementations: SMART[1] & TrustLite[2]

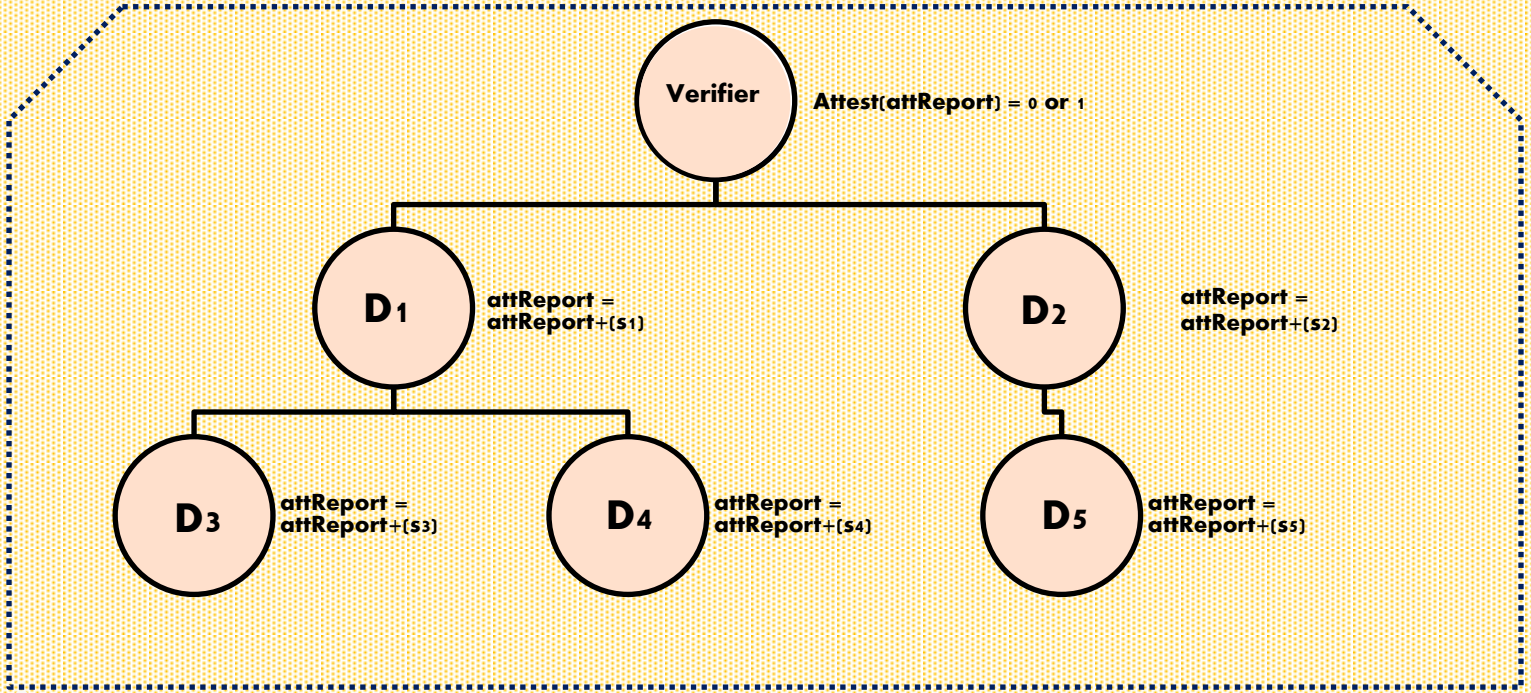
Remote Attestation: application to IoT

- **Problems:**
  - Single prover – single verifier scenario: efficiency and scalability issues.
  - Unfeasible to attest millions of devices one device at a time.
- **Solution**: **Swarm attestation**.



Swarm Attestation: Model

Attestation process where all devices in the network collaborate to produce a **single attestation report** for the verifier.



Swarm Attestation: Properties

- **Functionality**:
  - Network topology: static, quasi-static or dynamic;
  - Architecture: software – hardware – hybrid;
  - Attestation model: interactive VS non-interactive.

- **Security & Privacy**:
  - Authenticity & Integrity of the attestation process;
  - Adversary type: network adversary, remote malware injection, or physical adversary;
  - Adversary's power: read communication, modify attestation, falsify internal state;
  - Underlying cryptographic primitive: symmetric or asymmetric scheme.

- **Implementation**:
  - Topology of the network: computational complexity, memory footprint;
  - Simulation criteria: number of devices, underlying hardware.

Swarm Attestation: Attacks

- **Network attacker:**
  - Eavesdrop on communication routes in the swarm;
  - Read/re-order partial attestation result;
  - Drop attestation report packets in the network.

- **Remote attacker**:
  - Corrupt devices offline in order to « trick » secure boot;
  - Inject malware in devices in the swarm;
  - Perform DoS attacks on devices/provers therefore compromising the overall attestation process.

- **Physical attacker**:
  - Physically remove a device from the swarm therefore compromising result of the swarm attestation;
  - Retrieve cryptographic keys from a target device thus generating valid attestation for said device.

Swarm Attestation: Solutions

- Scalable Secure Embedded Device Attestation (**SEDA**)[3]:
  - First swarm attestation solution based on hybrid model;
  - Offline phase: device initalisation – Online phase: attestation generation.
- Lightweight swarm attestation (**LISA**)[4]:
  - Lightweight alternative to SEDA;
  - Provides classification of swarm attestation models.
- Secure non-interactive attestation for embedded devices (**SeED**)[5]:
  - Non-interactive attestation protocol;
  - Mitigates against DoS attacks.
- Scalable attestation protocol to detect software and physical attacks (**SCAPI**)[6]:
  - Mitigates against physical attacks.
- Secure and scalable aggregate network attestation (**SANA**)[7]:
  - Attestation protocol based on asymmetric primitives (aggregated signatures verifiable in constant time);
  - Formal security proof.

Swarm Attestation Solutions: Limitations

- **Scalability**. Attestation aggregation done by first computing the verification function (MAC or signature) on individual software binaries, and then aggregating said functions (either using the built-in aggregation mechanism (e.g. SANA), or using an XOR) for all devices in the swarm.

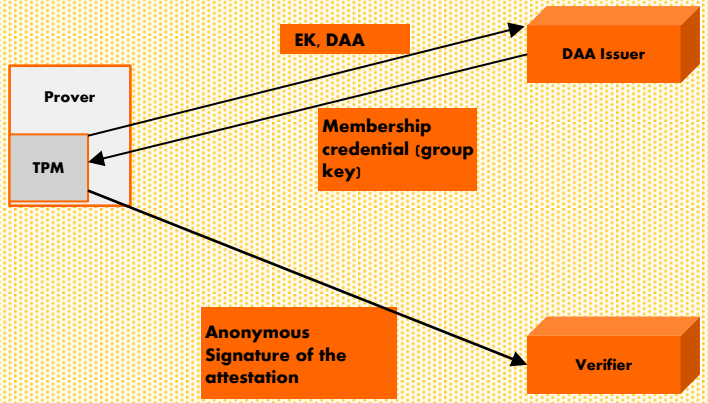
- **Privacy**. No existing attestation protocol that caters to privacy concerns. (Limitation for use cases such as VaNET).

- **Security**.
  - Mitigation techniques against DoS attacks against the prover are still limited;
  - Only SANA provides a formal security proof.

- **Performance**. Need for a model that finds a trade-off between devices' computational capabilities and security needs.

Direct Anonymous Attestation (DAA)

- **Direct Anonymous Attestation (DAA)**. Introduced by Brickell et al. [8]



- Variant of a group signature scheme with efficient zero-knowledge proofs;
- Secure hardware (TPM) to create and store cryptographic keys;
- Privacy-preserving attestation scheme that conceals the identity of provers.

New Solution based on Direct Anonymous Attestation

- **DAA-based solution**:
  - Avoid targeted attacks on device identity – application to networks such as Vehicular Ad-hoc Networks (VaNET);
  - Non-interactive attestation protocol that mitigates DoS attacks.

- **Scalability:**
  - Construction based on aggregate signatures thus providing better efficiency and scalability.

- **Privacy:**
  - Scheme does not reveal the structure of the network (conceals identities of individual devices).

- **Security:**
  - Formal security proof and security based on standard cryptographic assumptions.

References

- [1] Eldefrawy, K., Tsudik, G., Francillon, A., Perito, D.: SMART: secure and minimal architecture for (establishing dynamic) root of trust.
- [2] Koeberl, P., Schulz, S., Sadeghi, A., Varadharajan, V.: Trustlite: a security architecture for tiny embedded devices.
- [3] Asokan, N., Brasser, F.F., Ibrahim, A., Sadeghi, A., Schunter, M., Tsudik, G.Wachsmann, C.: SEDA: scalable embedded device attestation.
- [4] Carpent, X., Defrawy, K.E., Rattanavipanon, N., Tsudik, G.: Lightweight swarm attestation: A tale of two lisa-s.
- [5] Ibrahim, A., Sadeghi, A., Zeitouni, S.: Seed: secure non-interactive attestation for embedded devices.
- [6] Kohnhauser, F., Buscher, N., Gabmeyer, S., Katzenbeisser, S.: SCAPI: a scalable attestation protocol to detect software and physical attacks.
- [7] Ambrosin, M., Conti, M., Ibrahim, A., Neven, G., Sadeghi, A., Schunter, M.: SANA: secure and scalable aggregate network attestation.
- [8] Ernest F. Brickell, Jan Camenisch, Liqun Chen: Direct anonymous attestation.