Enhancing Remote Healthiness Attestation for Constrained IoT Devices

Y. Jia, B. Liu, W. Jiang, B. Wu, C. Wang

IEEE ICNP 2020
Madrid, Spain, October 13-16, 2020

HUAWEI TECHNOLOGIES CO., LTD.

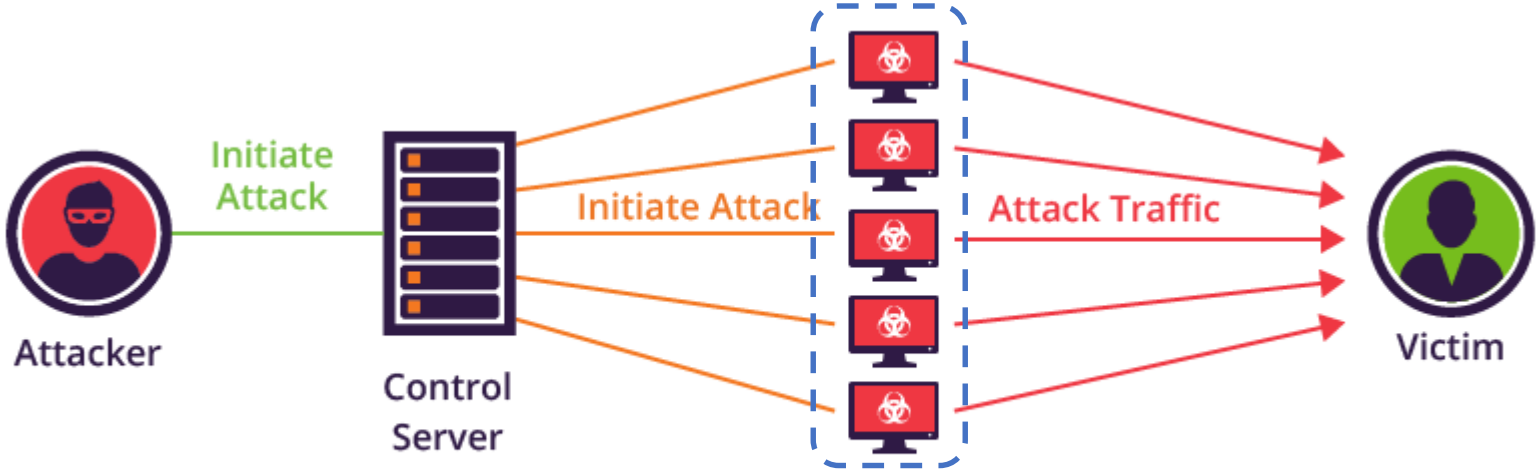
IoT Devices are keeping losing control…

IoT devices remain **vulnerable**…

Hackers are lunching **DDoS** with IoT devices…

Mirai attacks…

Peak **1.7 Tbps**



Reasons behind the constantly vulnerabilities

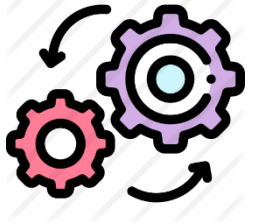
Market

Shaping

Constrained Resources…

Hacker

Hacking



Unaffordable
Security mechanisms

IoT Hacked!

Given that IoT devices are inevitably vulnerable, the question goes to:

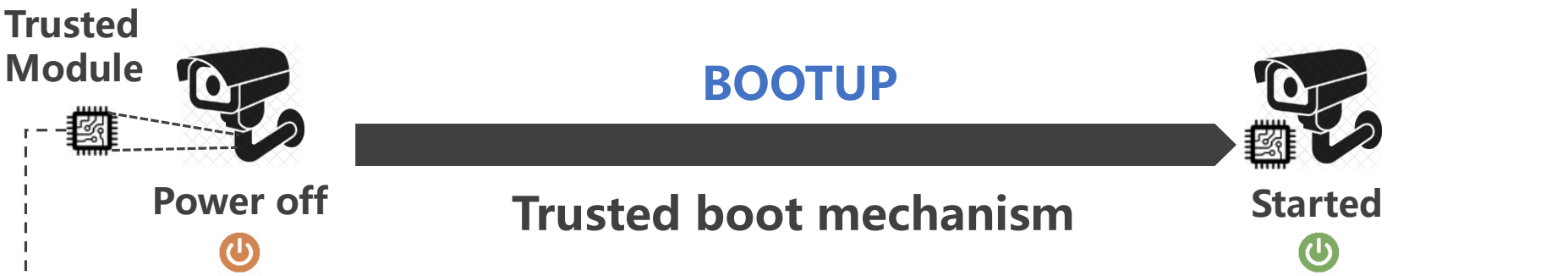
How could we timely identify hacked IoT devices?

Remote Attestation

Universal Remote Attestation

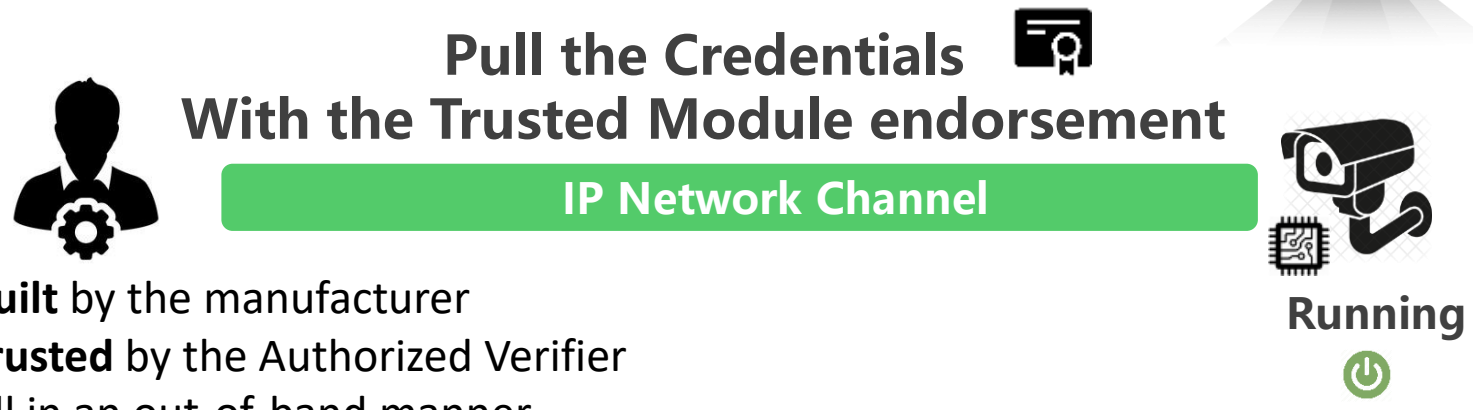
STEP 1

Trusted Boot

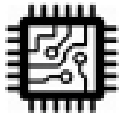


STEP 2

Remote attestation



- **Built** by the manufacturer
- **Trusted** by the Authorized Verifier
- All in an out-of-band manner



A dedicated Trust Module is way too heavy/expensive…

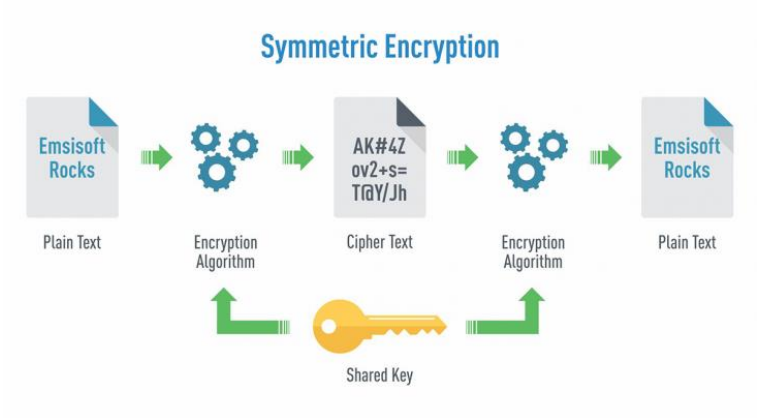
Could it be evolved for the constrained IoTs?

DICE(Device Identifier Composition Engine)

The DICE(Device Identifier Composition Engine) Proposal

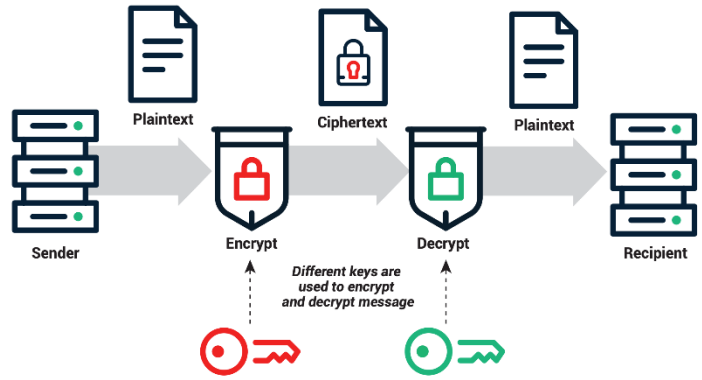
- Initially proposed by Microsoft
- Standardized by TRUSTED COMPUTING GROUP
- TRUSTED COMPUTING GROUP standardize **2** specifications of **the DICE-based remote attestation**

① **symmetric** crypto DICE



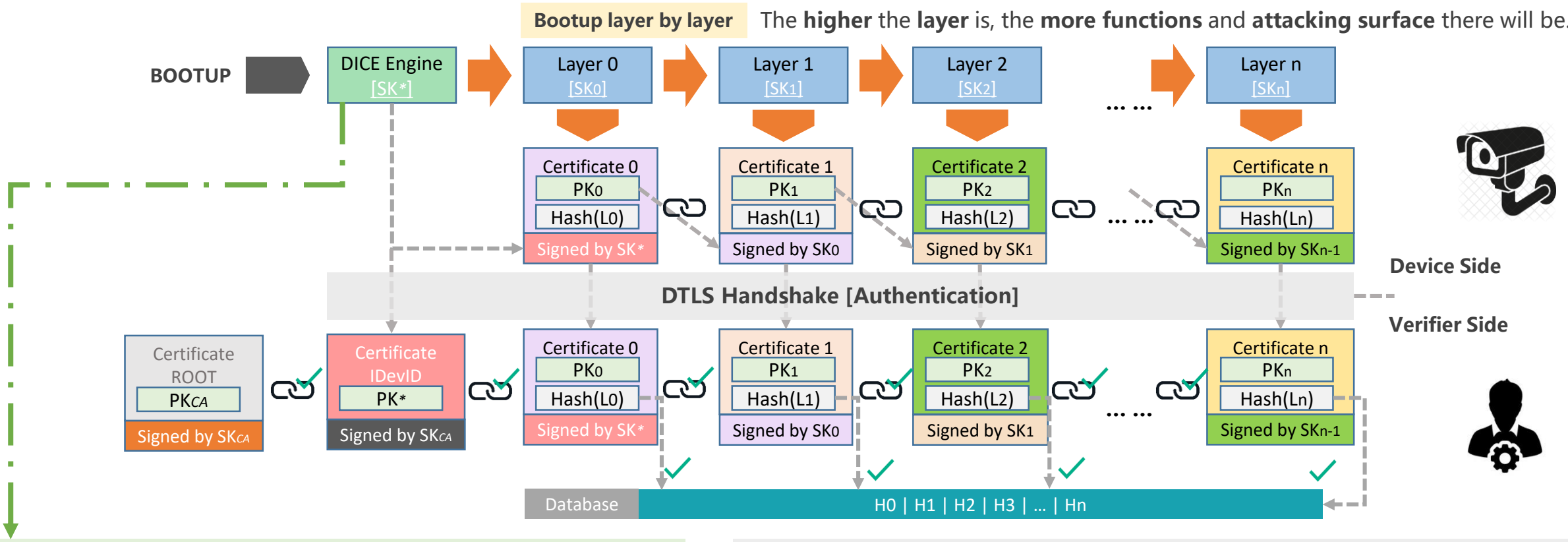
Standardized by 2020

② **asymmetric** crypto DICE



Standardized by 2018

DICE with the Asymmetric crypto



Prerequisites

- DICE Engine **is developed** and **installed** by the **manufacturer;**
- The source code of the DICE Engine too **tiny** to be **hacked**;
- DICE Engine is **unconditionally trusted** by the Verifier;

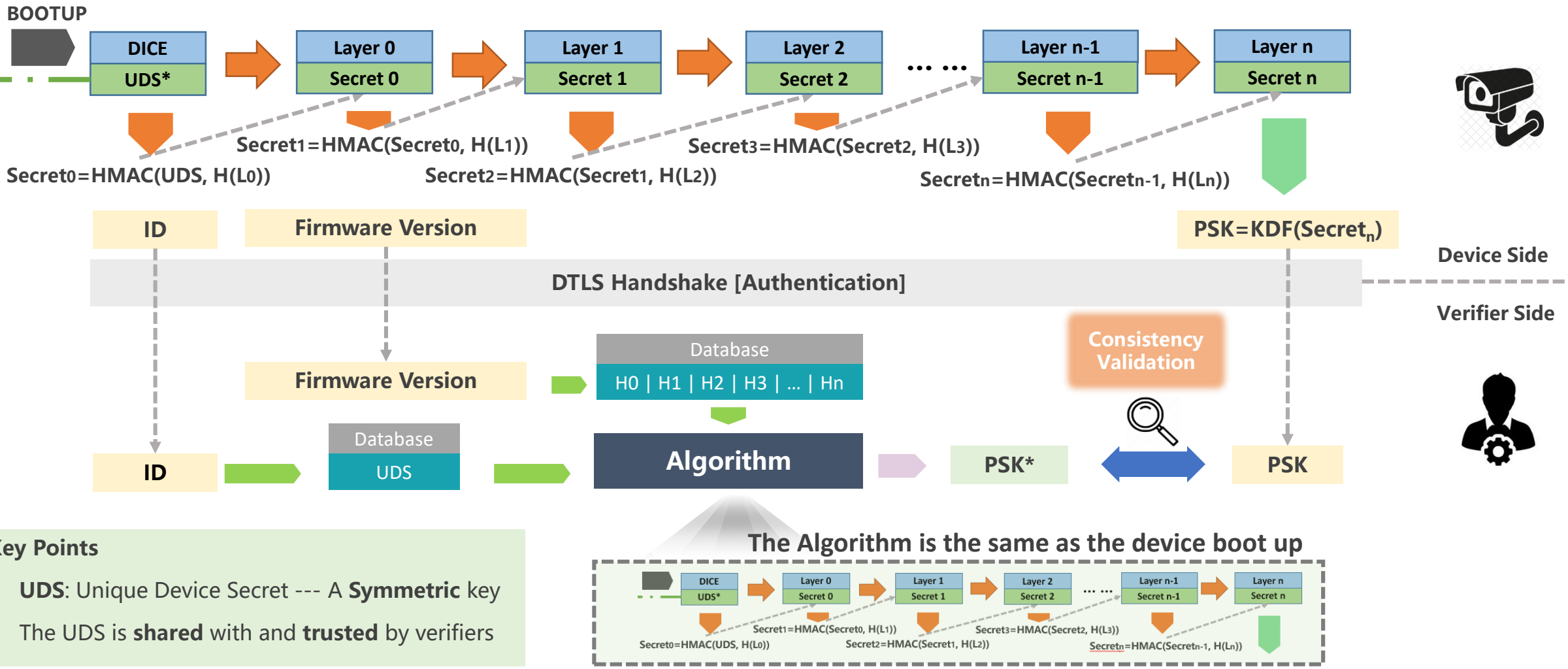
Design Key:

- DICE Engine stores a **SK(private key)/PK(public key)** pair for the endorsement;
- DICE Engine will be **shut down immediately** once layer 0 booted up;
- The short running interval guarantees that the SK(private key) is **only readable for the DICE Engine** itself, and thus **inaccessible** by any other layers;

The validation is based on the certificate-chain

DICE with the Symmetric crypto

The design principles are all the same as the Asymmetric crypto based DICE



Key Points

- **UDS**: Unique Device Secret --- A **Symmetric** key
- The UDS is **shared** with and **trusted** by verifiers

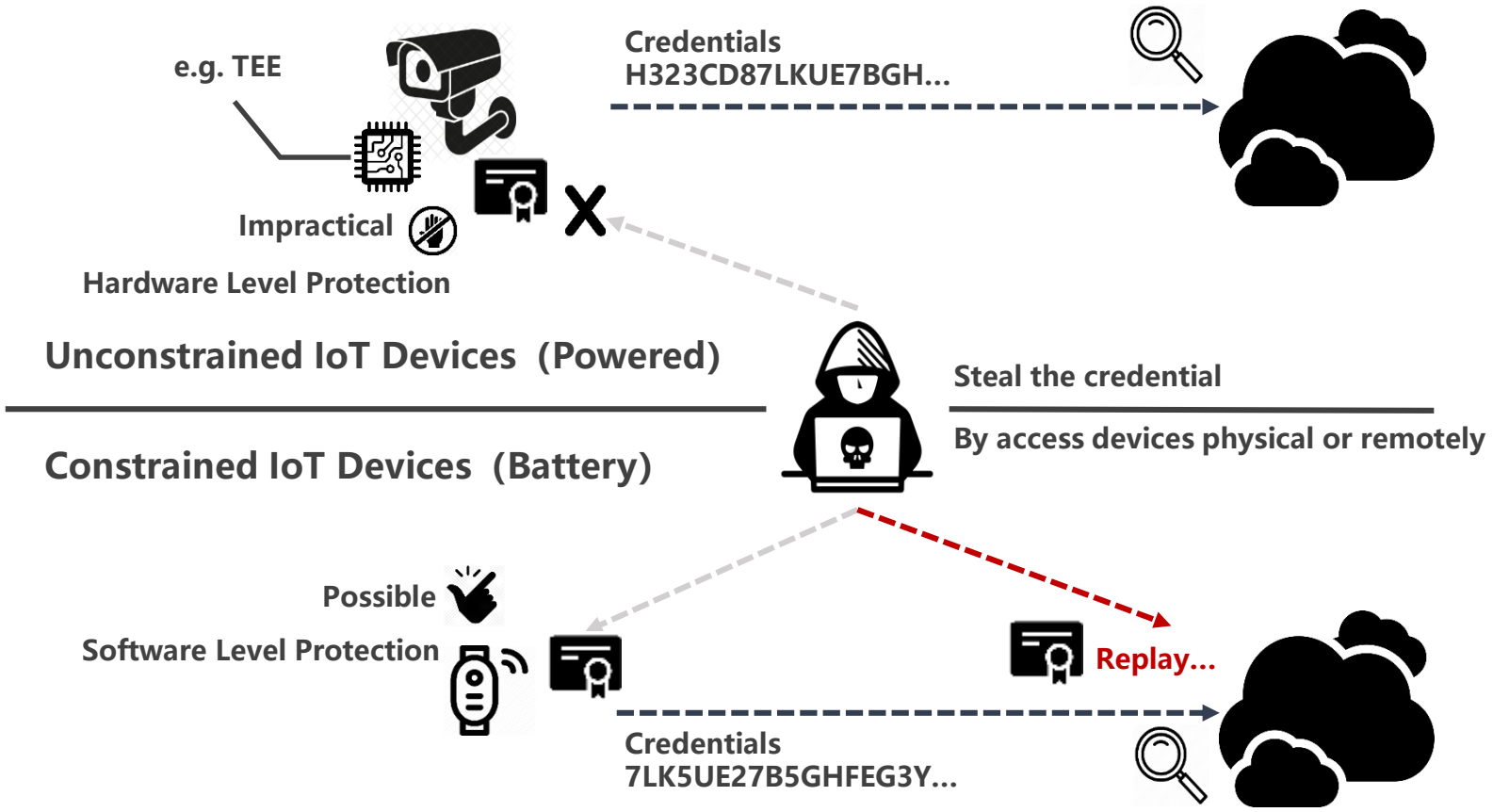
The validation is based on the **Hash-chain**

NEVERTHELESS

Replay Attacks are behind DICE…

Threat: steal the credentials and then replay...

NOTE: DICE DO NOT offer the capability of the secure storage



The credential is static...
Once stolen
the replay attacks survives...

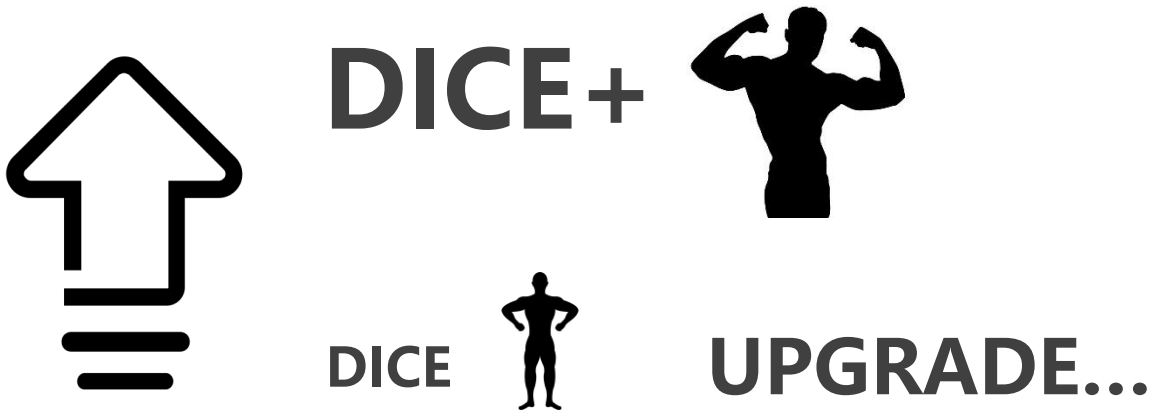
DICE+: Design Consideration

Main Consideration

Direction 1: Replay attack resilience — Secure

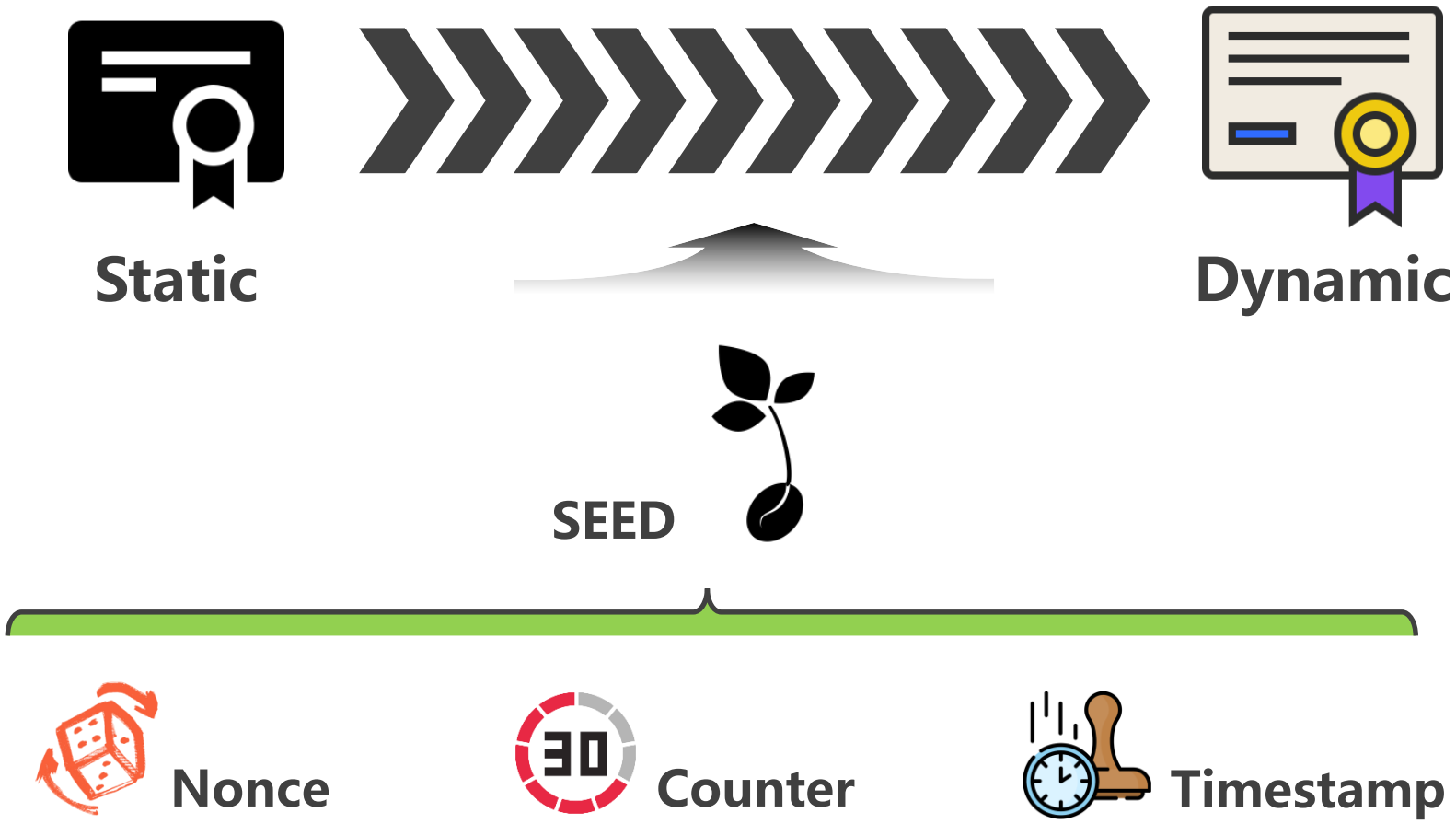
Direction 2: adaptive for the constrained IoT Devices — Light-weight

Direction 3: Fine-grained firmware attestation — Accuracy

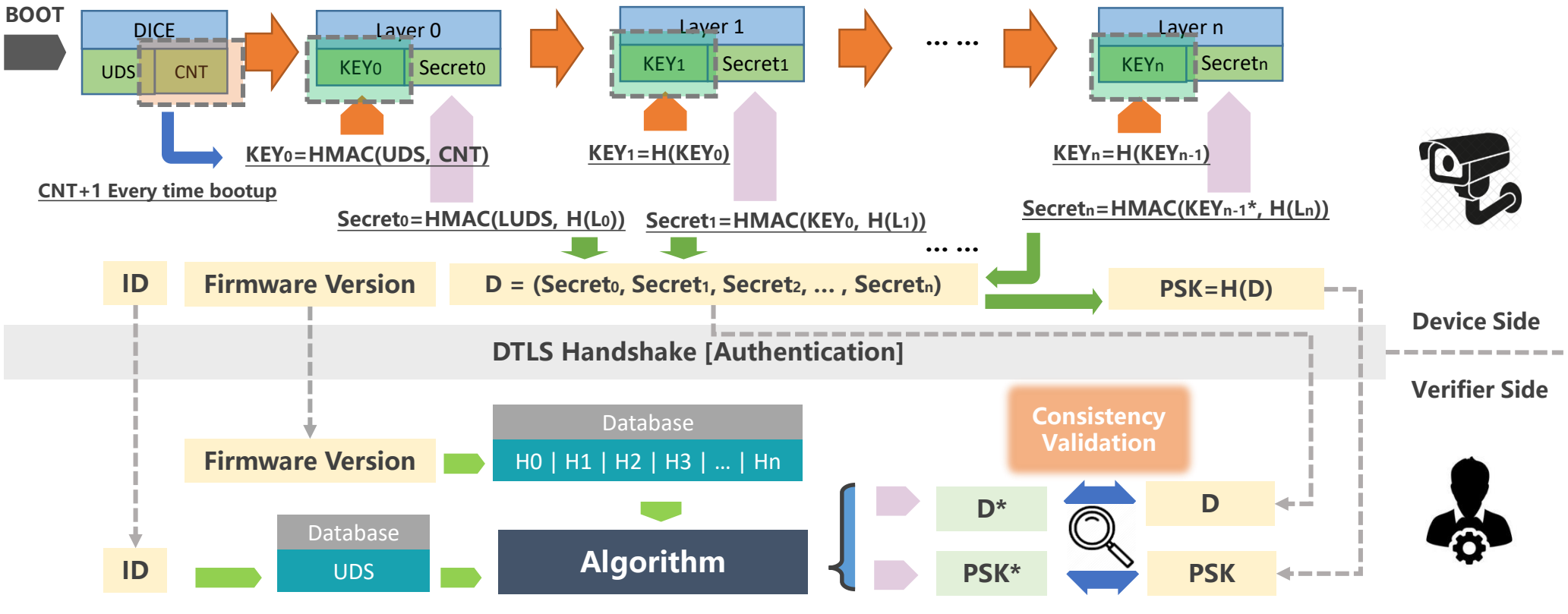


Identifying the replay...

Convert the Credential from STATIC to DYNAMIC !



DICE+: Design Details Evolution from the Symmetric crypto DICE



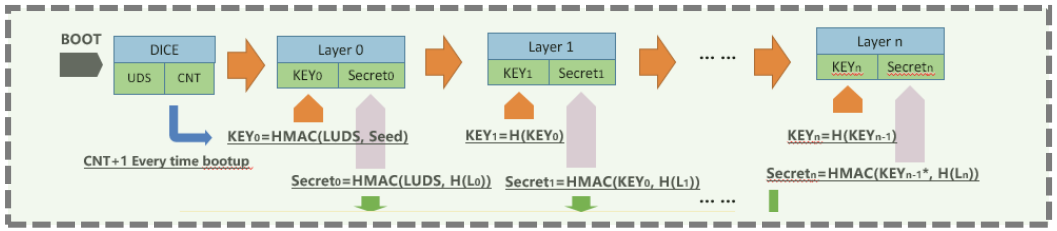
MAIN CHANGES

- **Seed involved:** A **counter** is introduced in the DICE engine

OTHER OPTIMIZATIONS

- **Symmetric crypto:** remain the extreme light-weight overhead
- **New algorithm**: A **parameter** is introduced in every layer boot up

The Algorithm is the same as the device boot up



Conclusion: What DICE+ Improve?

DICE+

DICE [Asymmetric]

DICE [Symmetric]

CHALLENGE 2: Computationally costly

- Asymmetric crypto computation consumes energy
- Certificate-chain transfer consumes energy

CHALLENGE 1: Replay Attack

- **The static credentials are easy to replay...**

CHALLENGE 3: Coarse-grained attestation

- Verifiers are unable to identify the specific hacked layer

UPDATE 2: Extreme constrained IoT

1. energy consumptions **reduce 1000x**
2. chip size for security area can reduce **~60%**

UPDATE 1: Resilient for Replay

- Verifiers can adjust the **period of the validity** of the seed
- Verifiers is able to identify the hacked devices that have been **imitated** by the **replay attacks**.

UPDATE 3: Hacked Layer Identification

- Verifiers are able to identify in which layer the IoT devices have been hacked.

THANKS!

IEEE ICNP 2020
Madrid, Spain, October 13-16, 2020

HUAWEI TECHNOLOGIES CO., LTD.