Remote Attestation

Building trust in things you can't see

N. Asokan ***asokan@acm.org***

Andrew Paverd ***andrew.paverd@ieee.org***

Aalto University

UNIVERSITY OF HELSINKI

Acknowledgements

(including co-authors of the presenters on papers cited in this tutorial)

Tigist Abera
Ferdinand Brasser
Lucas Davi
Ghada Dessouky
Jan-Erik Ekberg
Kari Kostiainen
Ahmad Ibrahim
Patrick Koeberl
Pekka Laitinen
Thomas Nyman
Ahmad-Reza Sadeghi
Matthias Schunter
Sandeep Tamrakar
Gene Tsudik
Christian Wachsmann
Shaza Zeitouni

Outline

- Remote Attestation in Principle
  - What is *remote attestation*?
  - What technologies have been proposed?
- Break
- Remote Attestation in Practice
  - What technologies are being used?
  - What challenges remain?

Motivating Example

Motivating Example: IoT

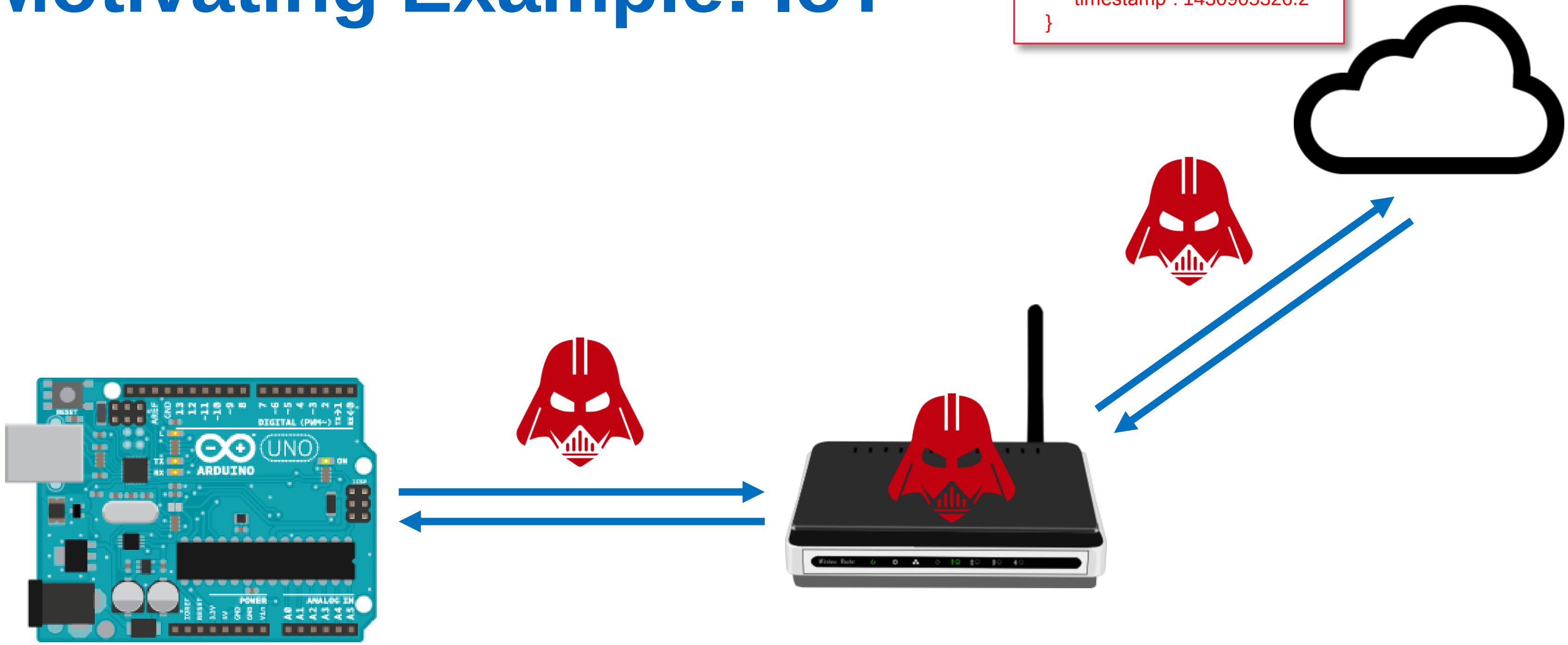
The following message is received:


```
{
        "name": temperature,
        "value": 23.5,
        "units": Celsius,
        "timestamp": 1430905326.2
}
```


What does it mean?

Motivating Example: IoT

{
"name": temperature,
"value": 23.5,
"units": Celsius,
"timestamp": 1430905326.2
}



Network adversary: read, modify, falsify communication

Motivating Example: IoT

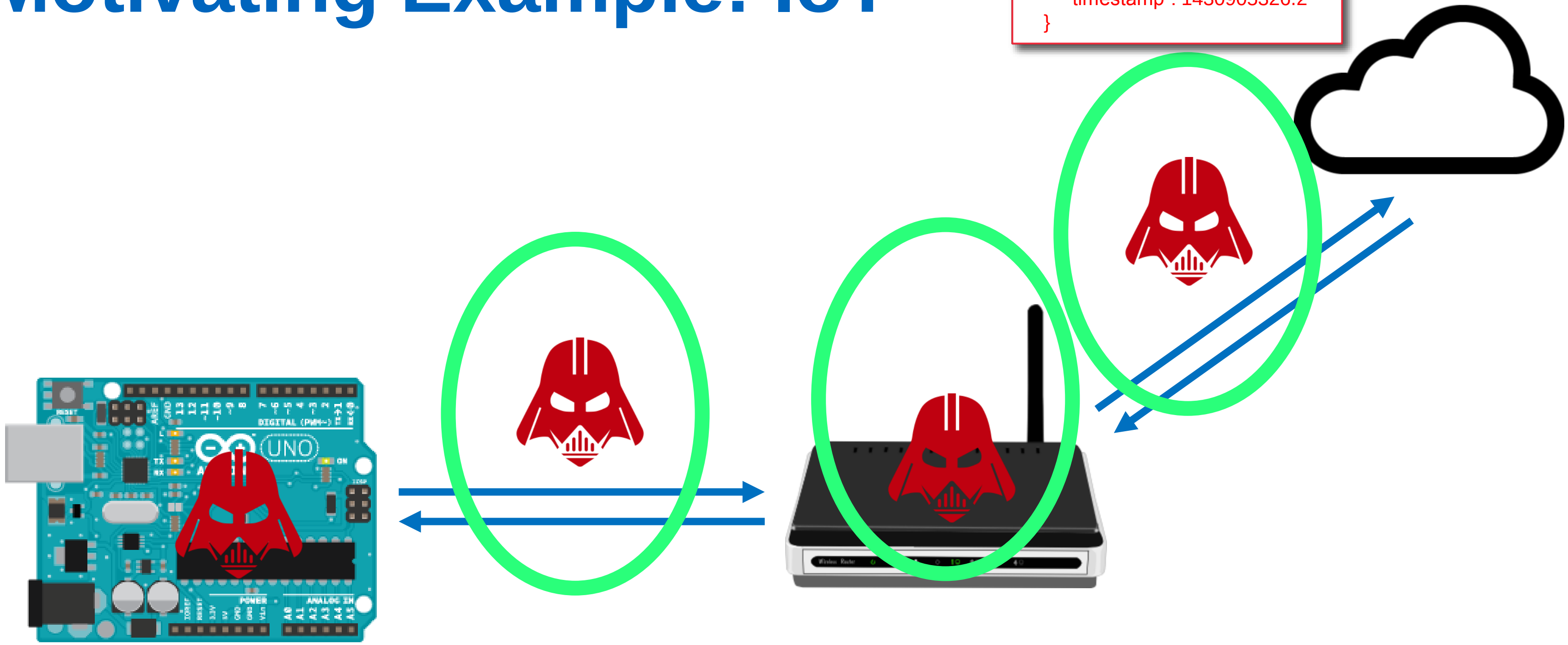
The following message is received over an authenticated, integrity-protected communication channel:


```
{
    "name": temperature,
    "value": 23.5,
    "units": Celsius,
    "timestamp": 1430905326.2
}
```


What does it mean?

Motivating Example: IoT

{
"name": temperature,
"value": 23.5,
"units": Celsius,
"timestamp": 1430905326.2
}



Network adversary: read, modify, falsify communication

✓ authenticated, integrity-protected communication

<u>**Malware:** extract secrets, change state, modify behaviour</u>

Physical adversary: has physical access to device

IoT Malware

WIRED An Unprecedented Look at Stuxnet, the World's Firs... SUBSCRIBE

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

KIM ZETTER SECURITY 11.03.14 6:30 AM

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

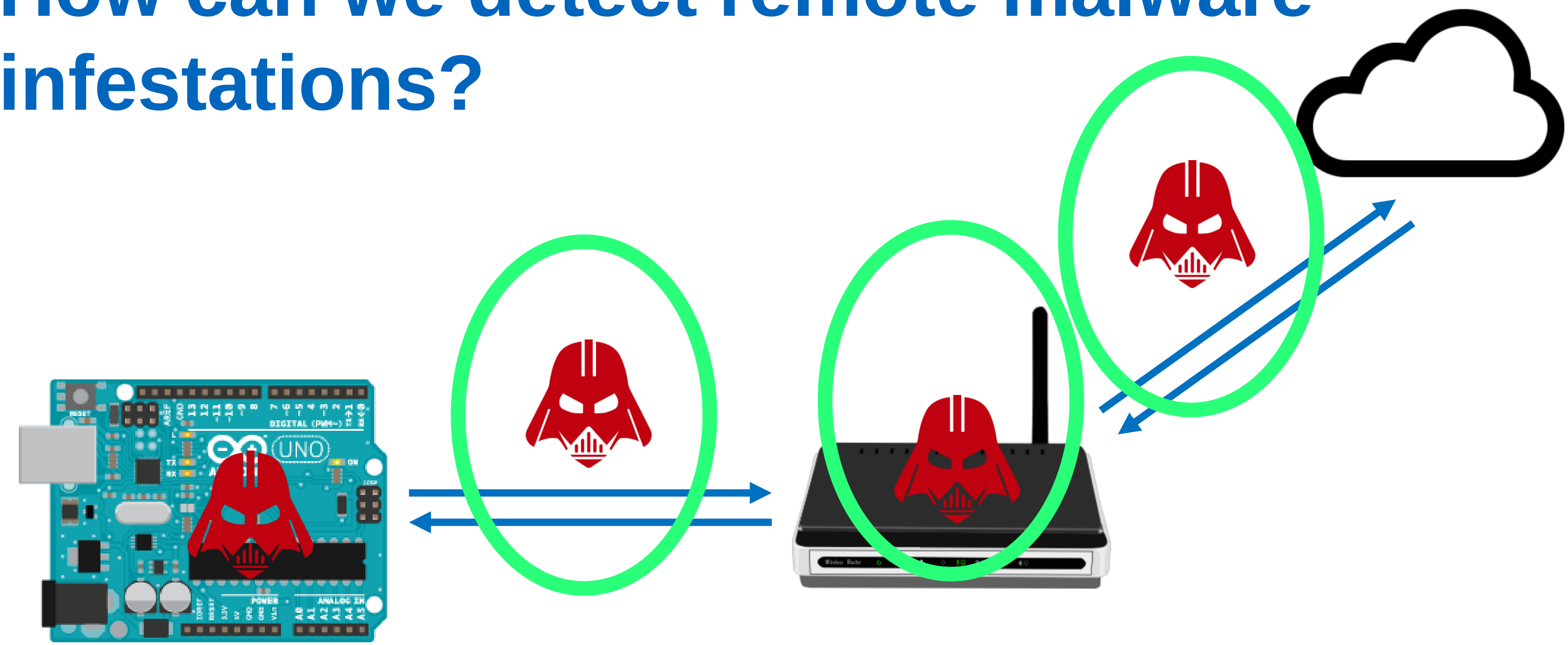
IoT malware and ransomware attacks on the incline: Intel Security

Intel Security has released a five-year retrospective report on industry threats, finding people have become dependent on devices at the cost to their security and privacy, allowing malware and ransomware attacks to rapidly grow.

By Asha Barbaschow | September 2, 2015 -- 01:11 GMT (02:11 BST) | Topic: Security

http://www.zdnet.com/article/iot-malware-and-ransomware-attacks-on-the-incline-intel-security/

How can we detect remote malware infestations?



Network adversary: read, modify, falsify communication

✓ authenticated, integrity-protected communication

Malware: extract secrets, change state, modify behaviour

Physical adversary: has physical access to device

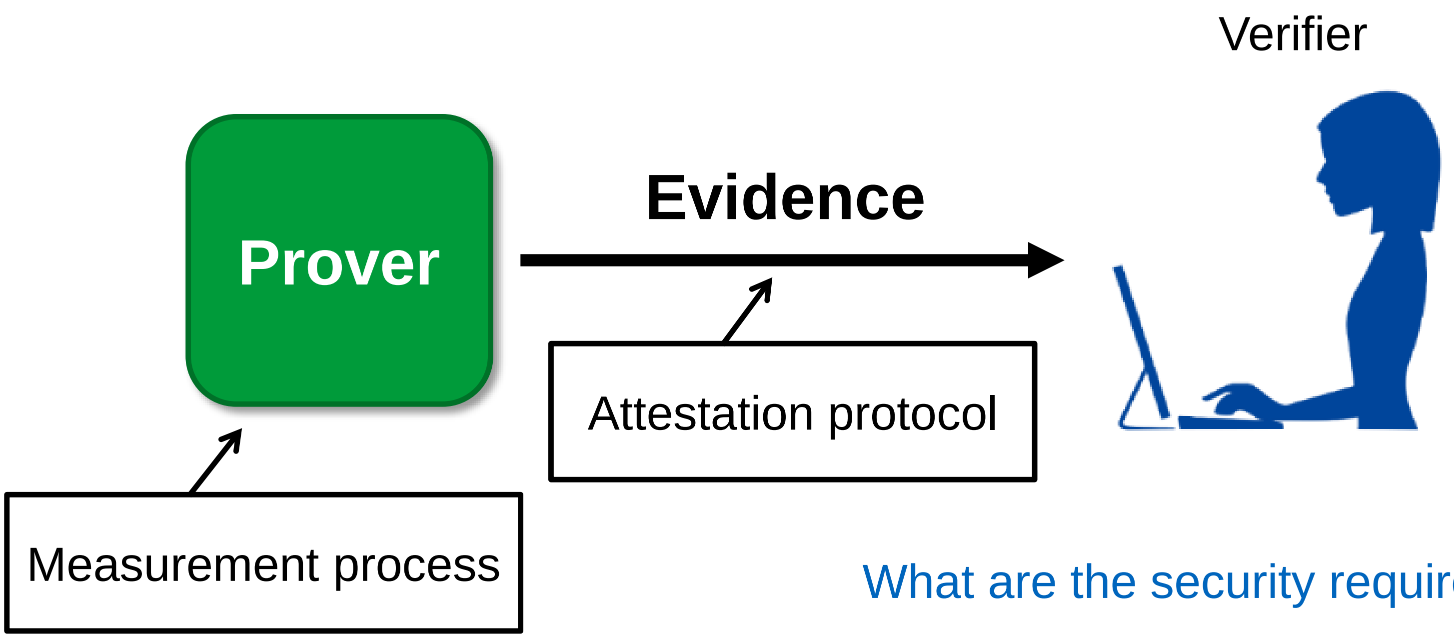
Remote Attestation in Principle

Aalto University

UNIVERSITY OF HELSINKI

Remote Attestation in Principle

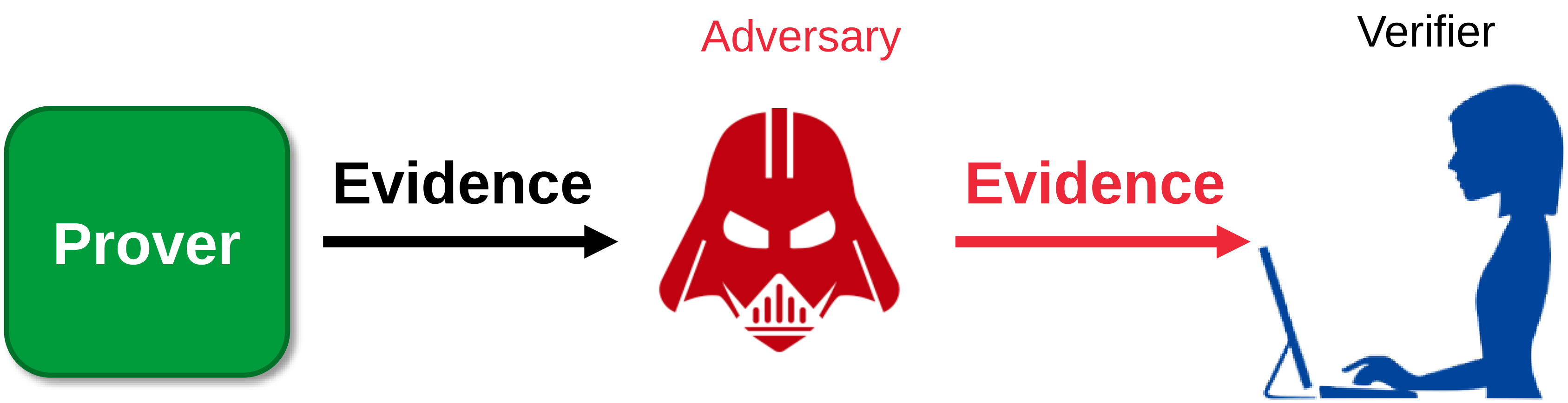
Verifier ascertains current state and/or behaviour of *prover*.



What are the security requirements?

Attestation Requirements

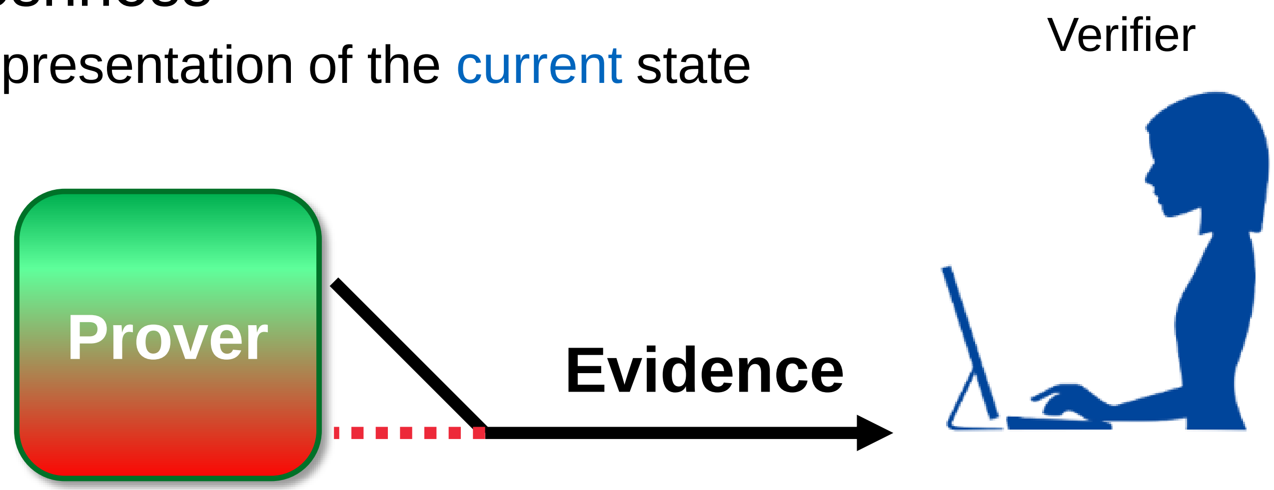
1. Authenticity
   - representation of the real state of the system



Attestation Requirements

1. Authenticity
   – representation of the real state of the system

2. “Freshness”
   – representation of the current state

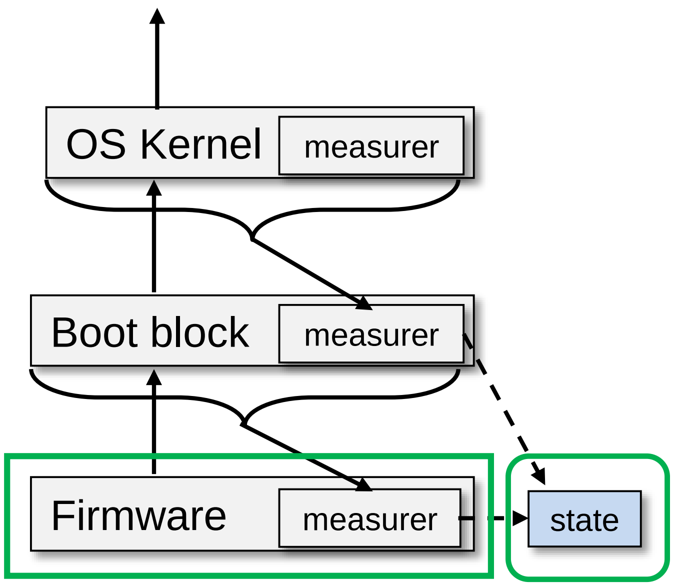


Trusted Platform Module (TPM)

Authenticated Boot

- Measure and record booted components ("state")

- State can be:
  - bound to stored secrets - sealing
  - reported to external verifier - remote attestation

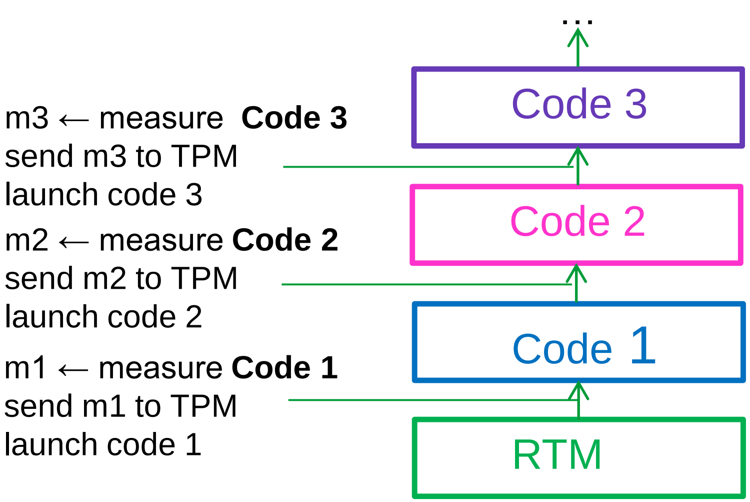


Authenticated boot

TPM Measurement Process

Platform Configuration Registers (PCRs) store aggregated platform "state" measurement

- Requires a root of trust for measurement (RTM)
- A given state reached ONLY via correct extension sequence
  - "PCR extension rule"



$H_{new} = H(H_{old} \mid new)$ *[PCR extension rule]*

$H_0 = 0$

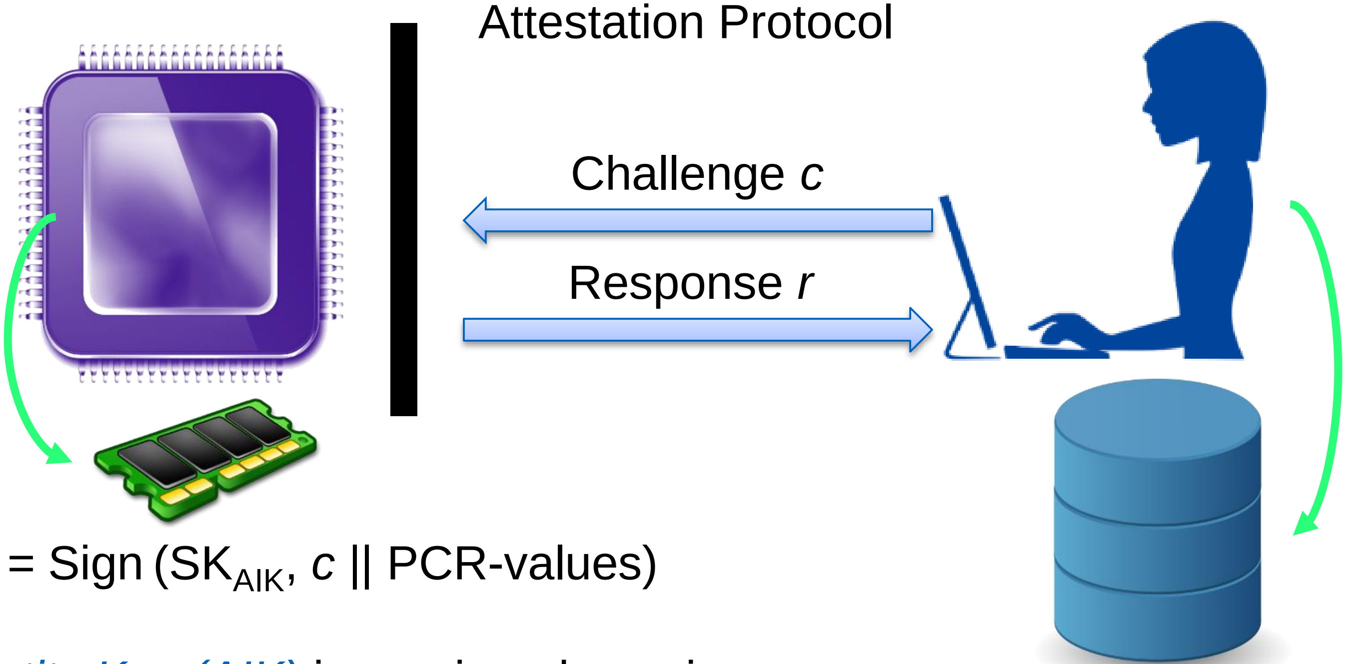
$H_1 = H\,(0|m1)$

$H_2 = H\,(H\,(0|m1)\,|m2)$

$H_3 = H\,(H\,(H\,(0|m1)\,|m2)\,|m3)$

TPM Attestation Protocol

- **Goal**: Check whether the prover is in a trustworthy state



“TPM Quote” r = Sign (SK_{AIK}, c || PCR-values)

Attestation Identity Key (AIK) is a unique keypair whose private key (SK_{AIK}) is *TPM-protected*

Database of acceptable measurements

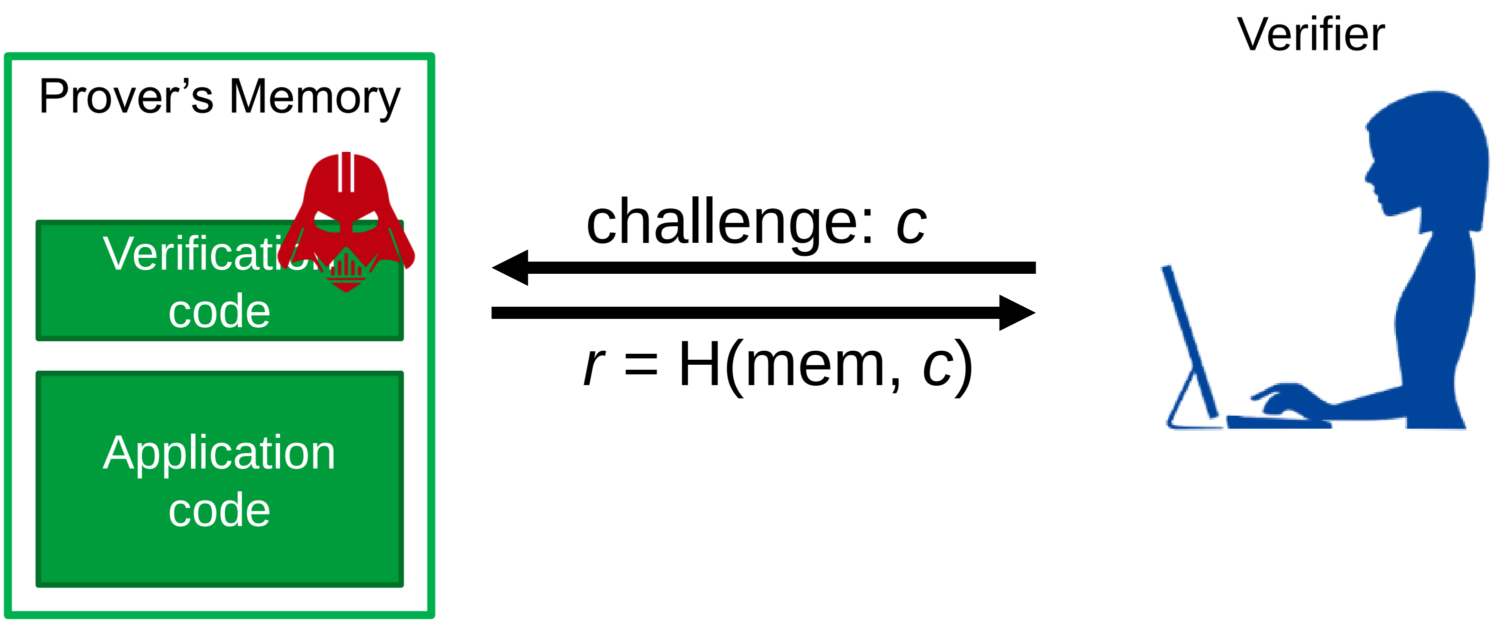
Drawbacks of TPM Attestation

- Needs additional hardware and software
- Not suitable for "anaemic" provers
- Covers only the initial loading of software
- Deals with only one prover and one verifier
- Database of acceptable measurements does not scale

Software-Based Attestation

Software-Based Attestation

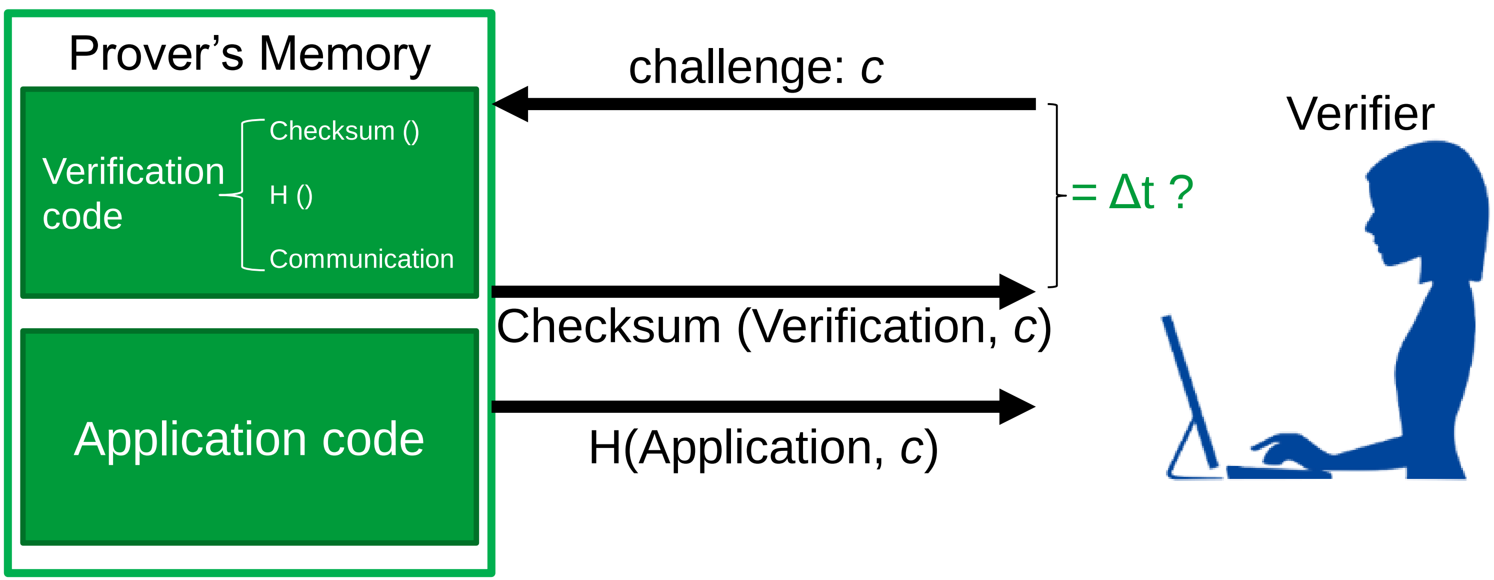
- Assumes no hardware features to support attestation
  - No secrets on prover (e.g. no AIK)



Software-Based Attestation

- Pioneer system
  - compute time-optimal checksum of verifier

Authenticity?



A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. [Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms](). SOSP ‘05

Software-Based Attestation: Summary

Limitations of timing side channels

- verifier must know exact hardware configuration
- difficult to prove time-optimality
- assumes "adversarial silence" during attestation
- limited to "one-hop" networks
  - requires authenticated channel (e.g. physical connection)

Hybrid Attestation

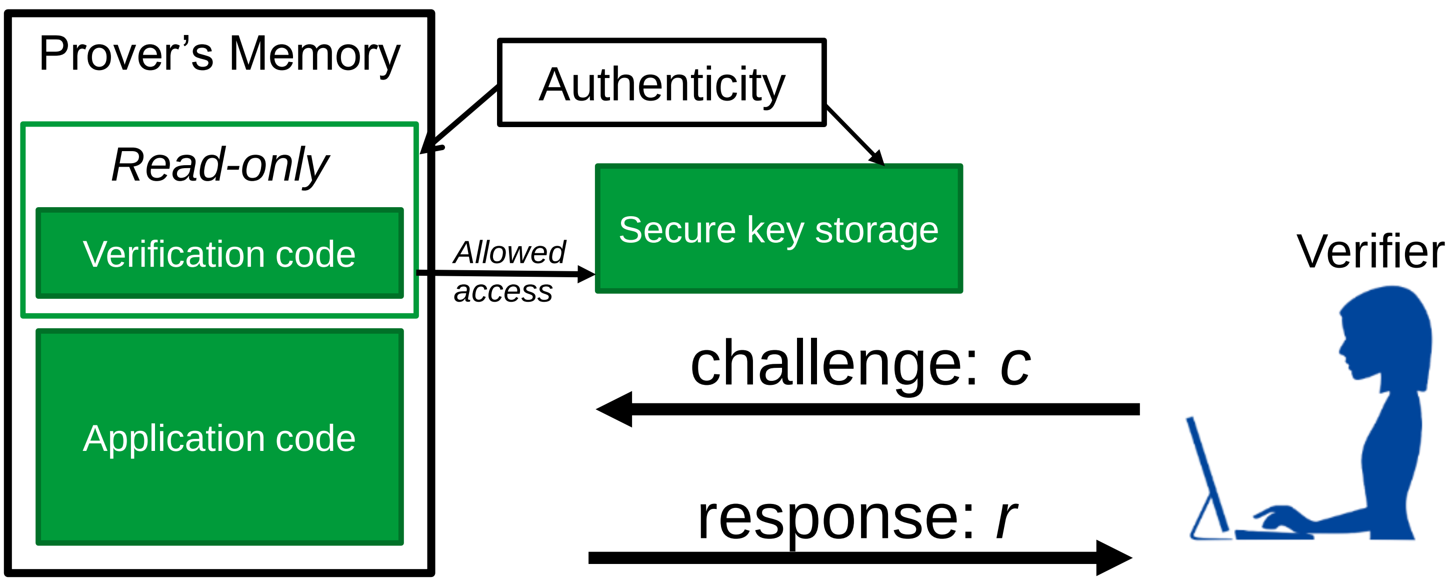
Hybrid Attestation

Minimal trust anchors: small changes to hardware

Hybrid Attestation: SMART

Minimal trust anchors: small changes to hardware

Read-only Verification code, secure key storage and atomicity of execution of Verification code

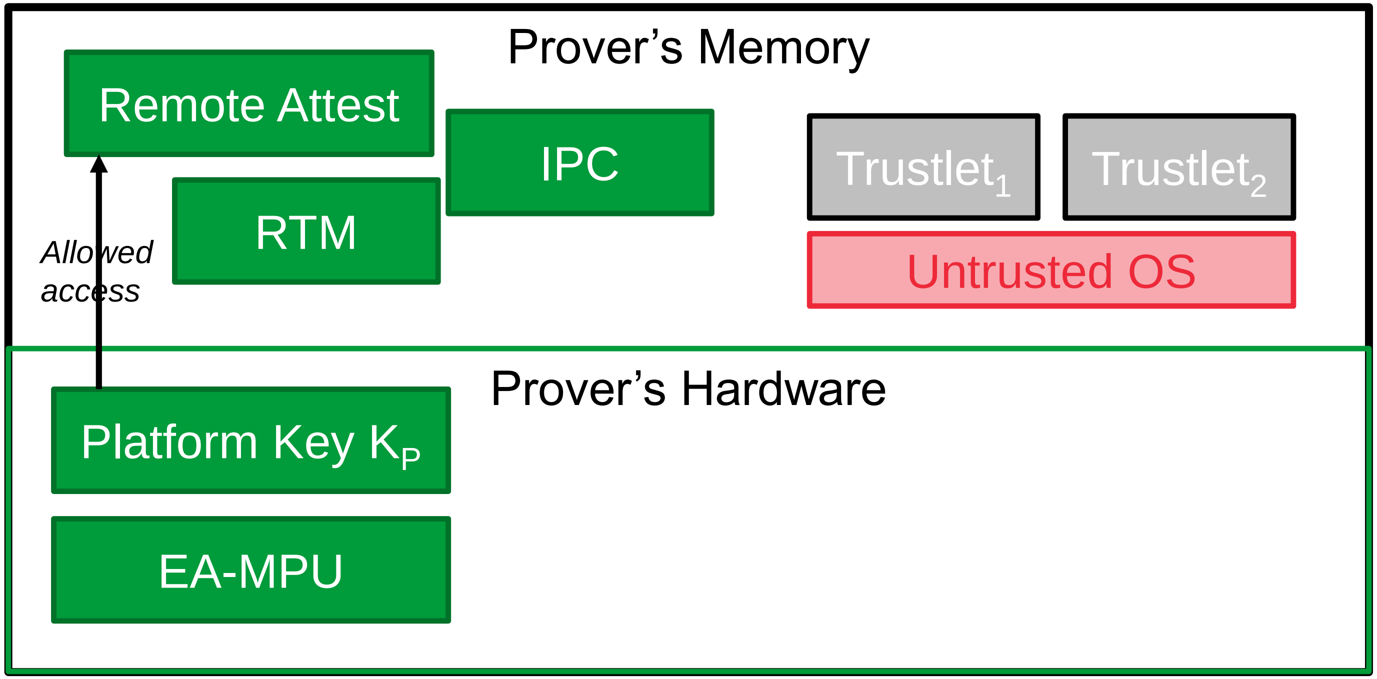


K. El Defrawy, A. Francillon, D. Perito, and G. Tsudik. [SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust](). NDSS '12

A. Francillon, Q. Nguyen, K. Rasmussen and G. Tsudik, [A Minimalist Approach to Remote Attestation](), DATE 2014

Hybrid Attestation: TrustLite & TyTAN

- Execution-Aware Memory Protection Unit (EA-MPU)
  - Access control based on memory request target and origin



P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan. [TrustLite: A Security Architecture for Tiny Embedded Devices](). EuroSys '14

F. Brasser, B. El Mahjoub, A.-R. Sadeghi, P. Koeberl, [TyTAN: Tiny Trust Anchor for Tiny Devices](), DAC '15

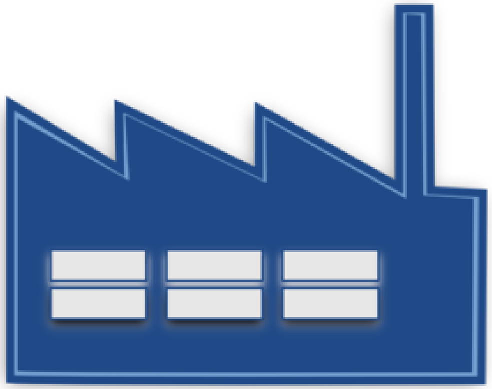
Hybrid Attestation: Summary

- Advantages of hybrid approaches
  - Can be used across a network / over an untrusted channel
  - Verifier need not know prover's exact hardware configuration
- Drawbacks
  - Needs additional hardware support
  - But minimal MCU trust anchors available commercially
    - TrustZone-M (ARM v9), …

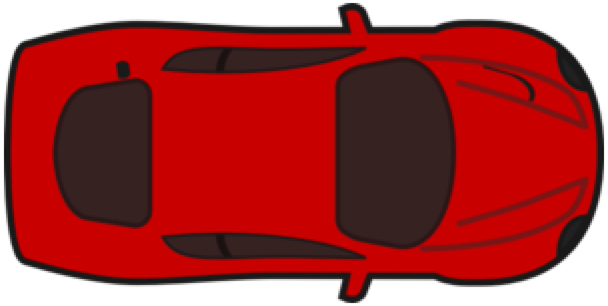
Scalability of Attestation

Scalability of Attestation

- Attestation protocols usually assume a single prover
  - but IoT scenarios may involve groups of (many) provers



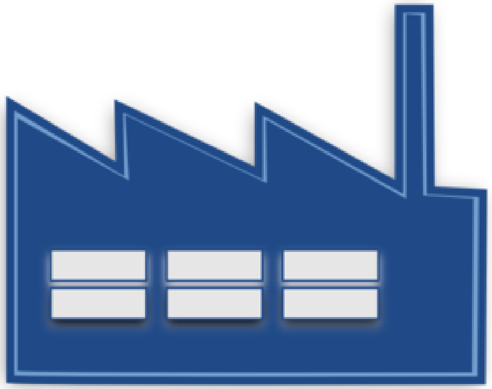
Smart factories



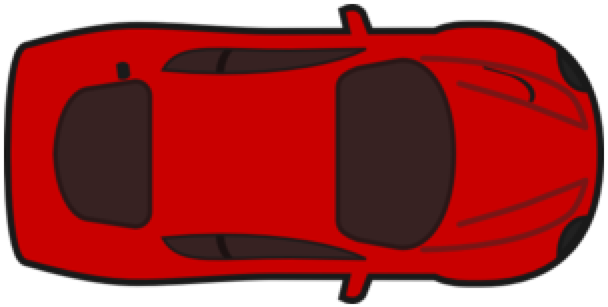
Smart vehicles

Scalability of Attestation

- Device *swarms*
  - dynamic topology: nodes move within swarm
  - dynamic membership: nodes join and leave the swarm



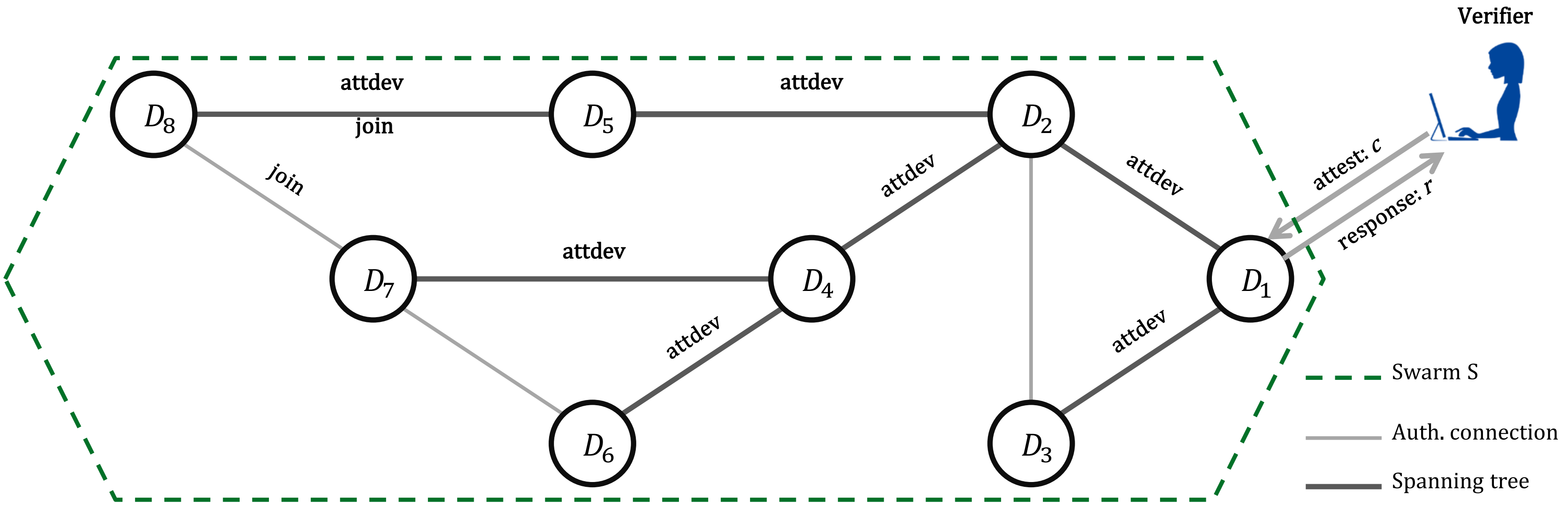
Smart factories



Smart vehicles

Scalability of Attestation: SEDA

SEDA: Scalable Embedded Device Attestation
- More efficient than attesting each node individually
- Can use any type of measurement process



N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, C. Wachsmann. SEDA: Scalable Embedded Device Attestation. CCS '15

Scalability: DARPA, SANA, LISA-s

DARPA: Device Attestation Resilient to Physical Attacks

– Absence detection to detect physical attacks

SANA: Secure & Scalable Aggregate Network Attestation

– Optimistic Aggregate Signature (OAS) scheme

LISA-s: Lightweight Swarm Attestation schemes

– Quality of Swarm Attestation (QoSA): binary; count; list; full

A. Ibrahim, A-R. Sadeghi, G. Tsudik, S. Zeitouni. DARPA: Device Attestation Resilient to Physical Attacks. ACM WiSec '16

M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A-R. Sadeghi, M. Schunter. SANA: Secure and Scalable Aggregate Network Attestation. CCS '16

X. Carpent, K. El Defrawy, N. Rattanavipanon, G. Tsudik. LIghtweight Swarm Attestation: a Tale of Two LISA-s. ASIACCS '17

Scalability of Attestation: Summary

- Different types of schemes proposed to:
  - improve security (e.g. physical attack resilience) *or*
  - improve performance (e.g. optimistic aggregation) *or*
  - improve in functionality (e.g. QoSA)

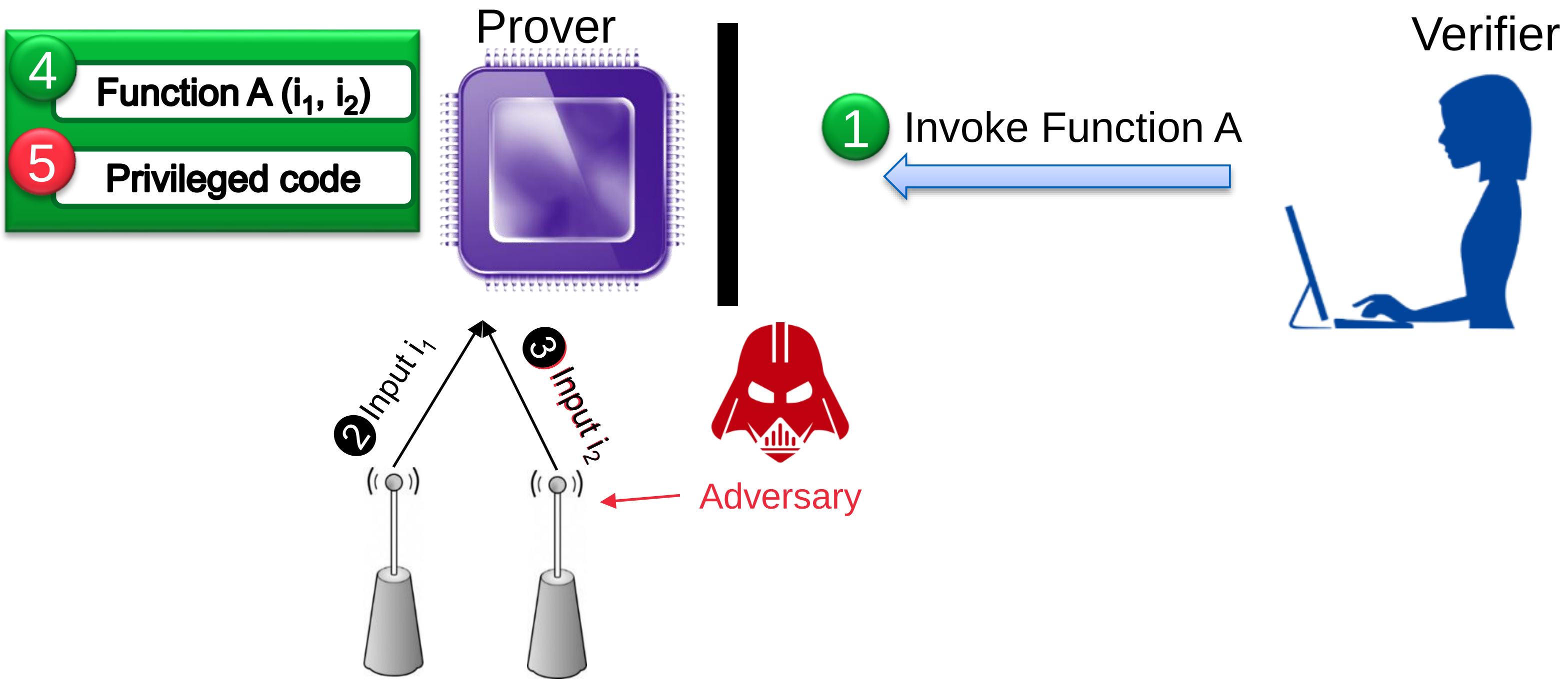
- What are the real-world application requirements?

Run-Time Attestation

Why Run-Time Attestation?

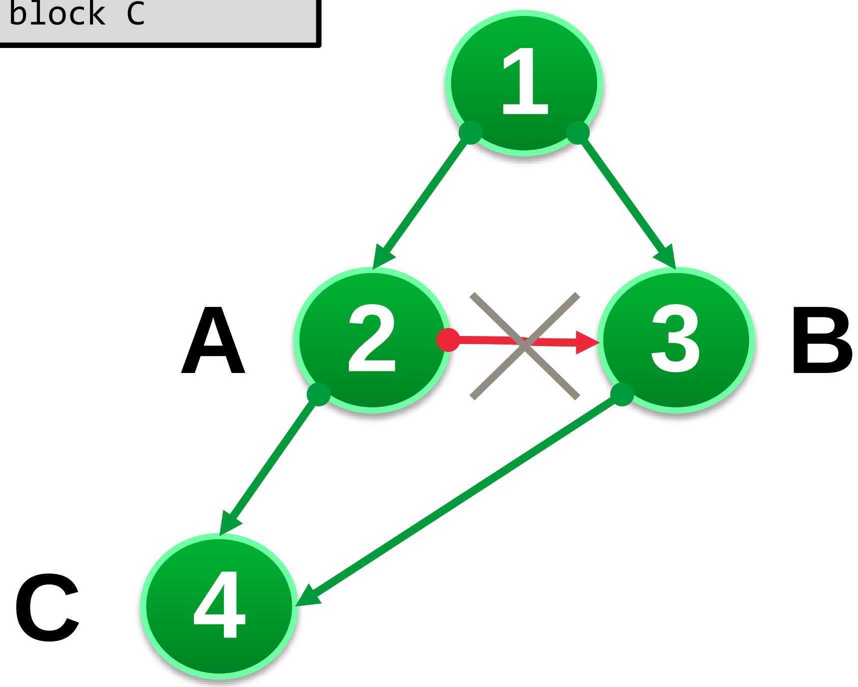
- Traditional attestation measures binaries at load time
- Cannot capture run-time attacks
  - return-oriented programming
  - control data attacks

Run-Time Attacks



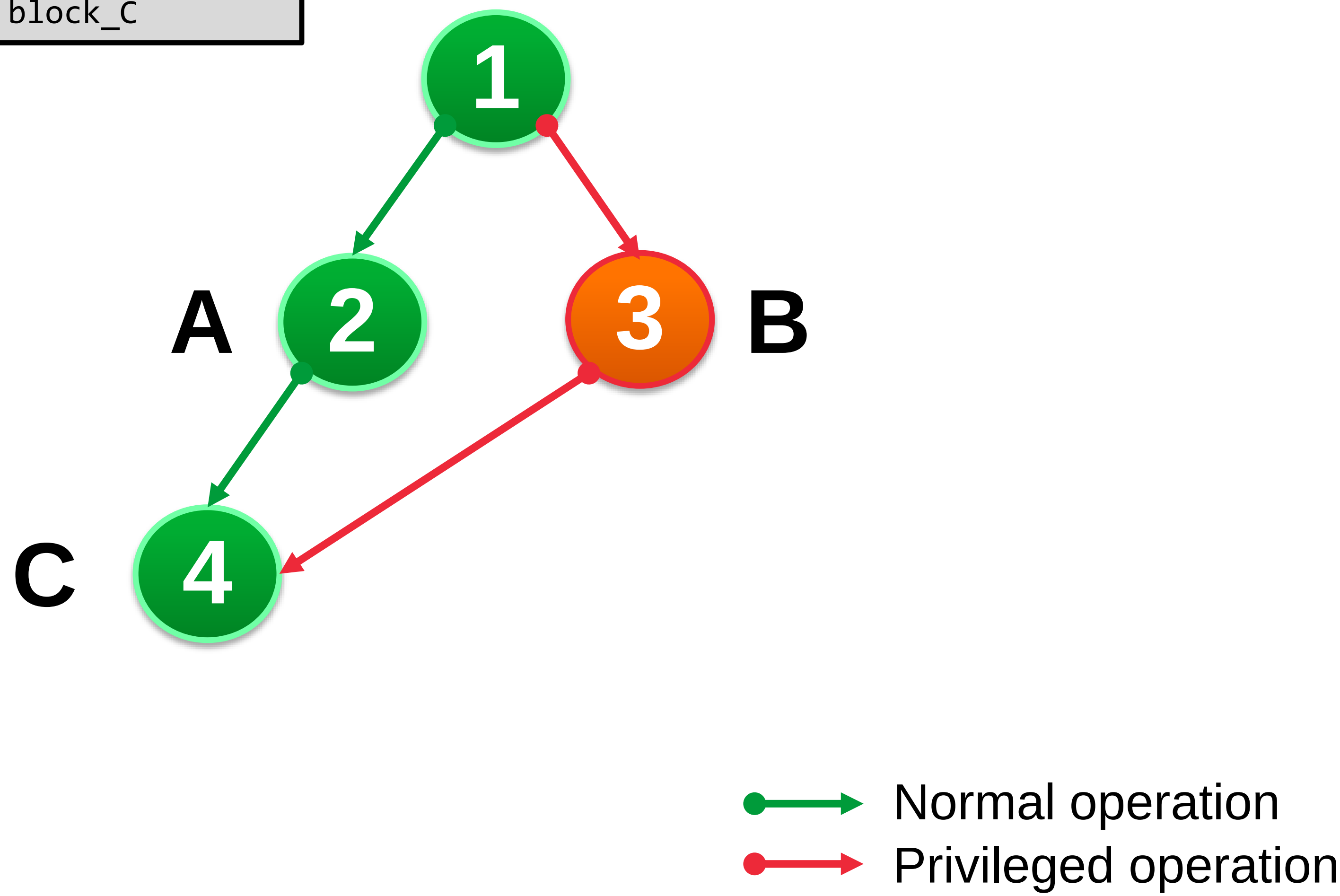
Control Flow Integrity (CFI)

```
① if (cond)
②  then: block A
③  else: block B
④ block C
```

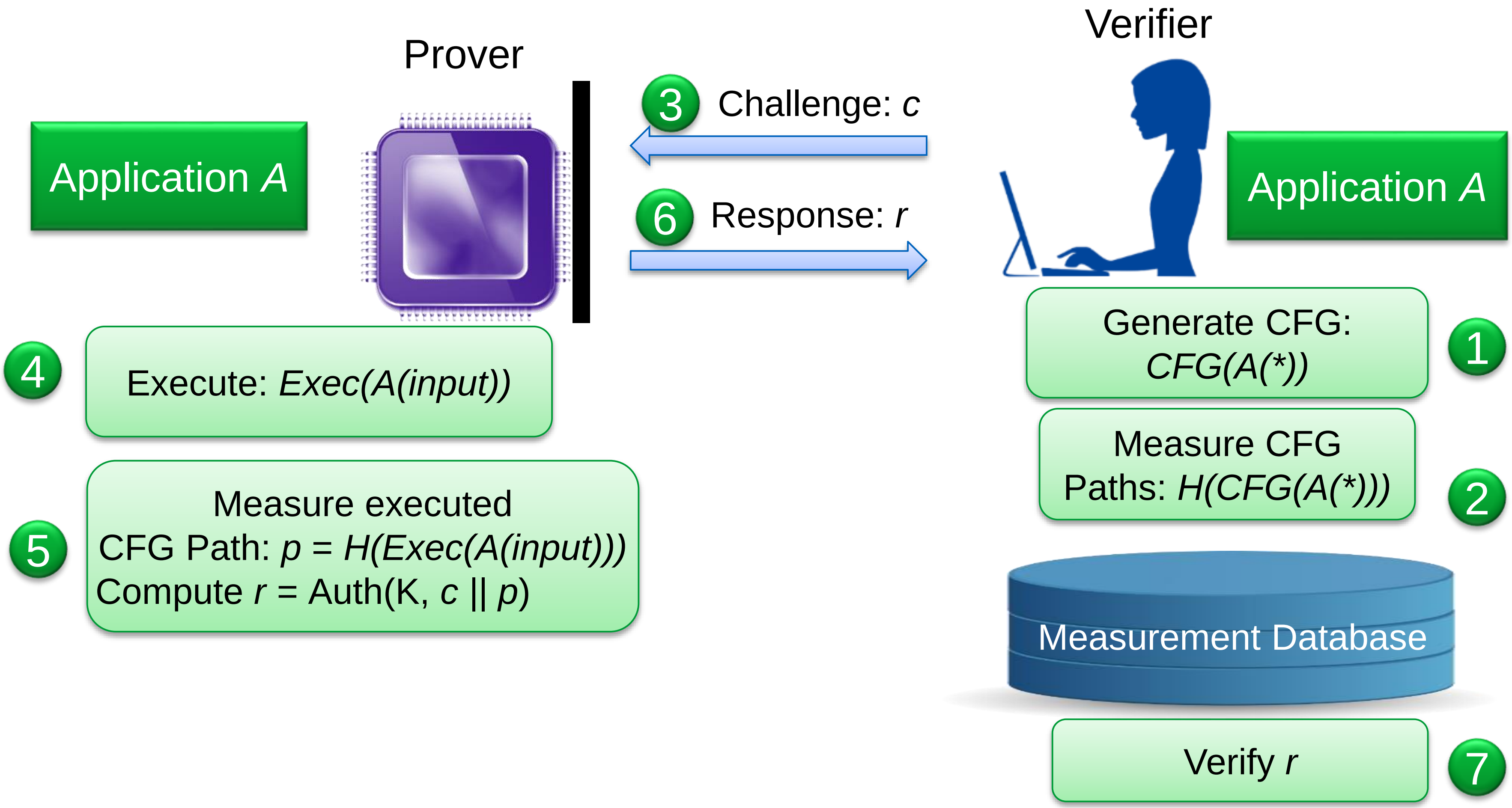


Run-Time Attacks Without Violating CFI

```
① if (cond)
②  then: block_A
③  else: block_B
④ block_C
```



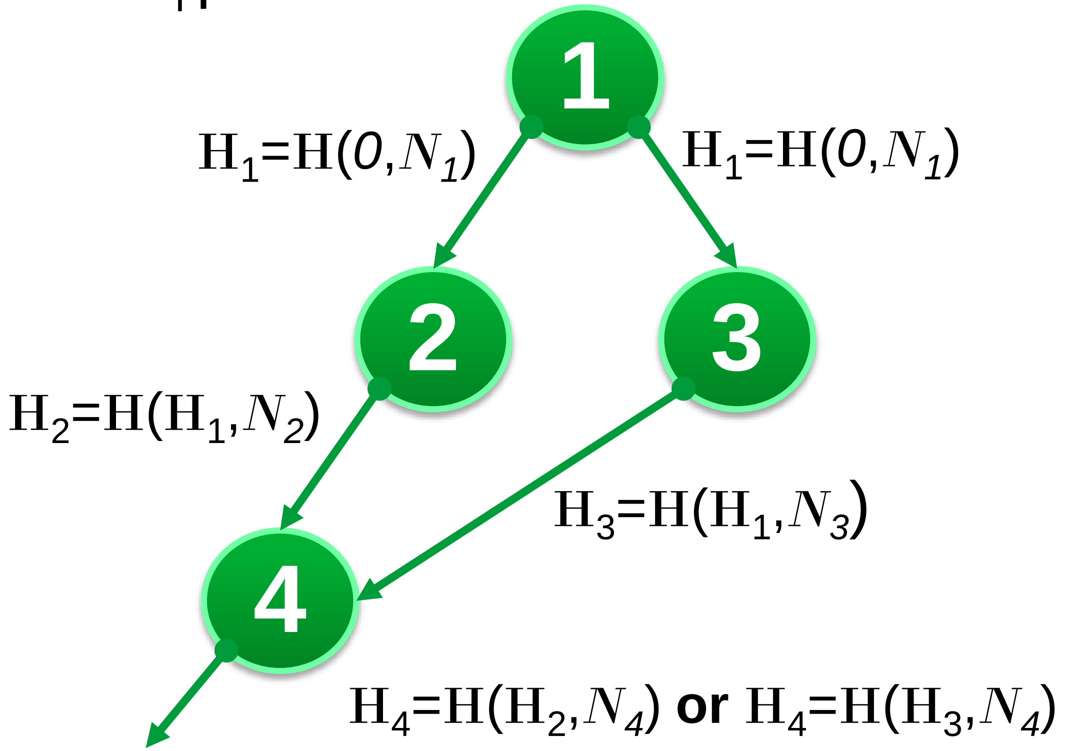
Control-Flow Attestation (C-FLAT)



T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, *C-FLAT: Control Flow Attestation for Embedded Systems Software, CCS '16.*

C-FLAT: High-Level Idea

- Cumulative Hash Value: $H_j = H(H_i, N)$,
  where H_i previous hash result and N is the current node

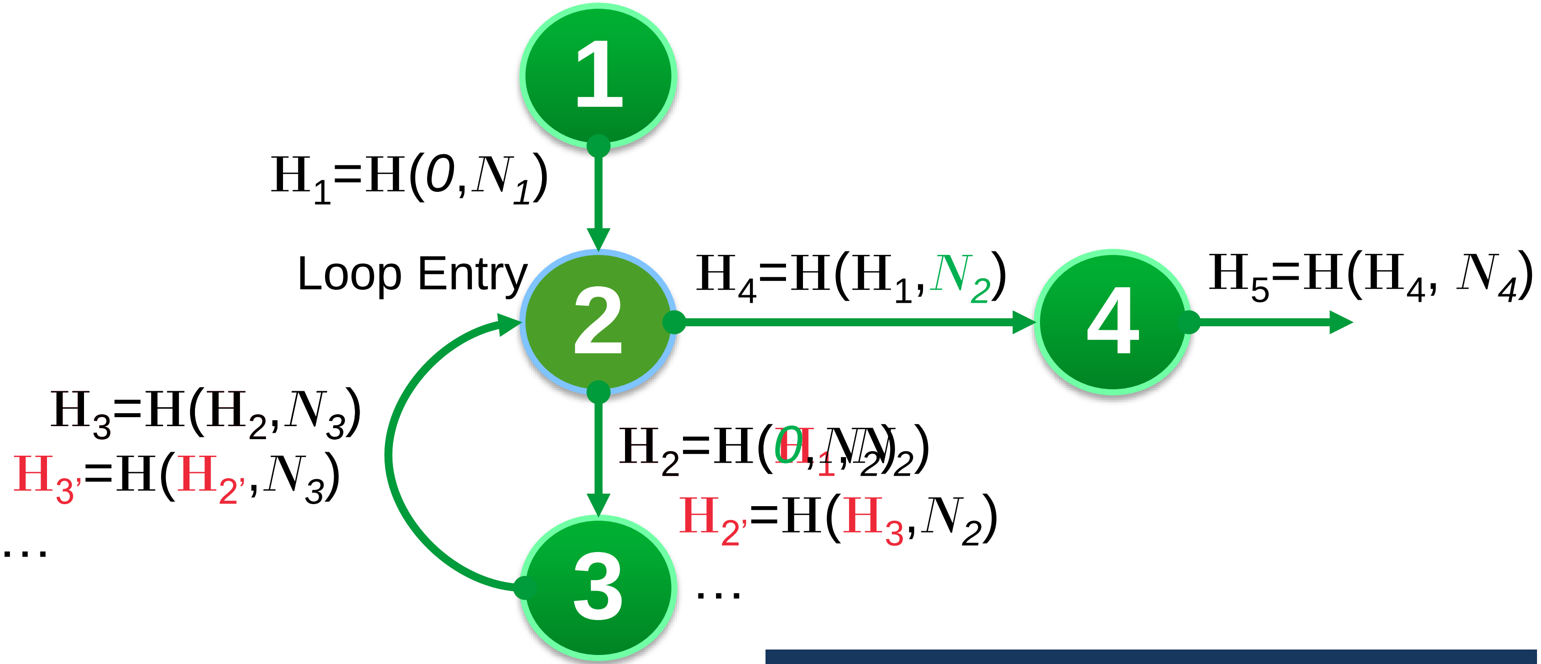


$p = H_4$

T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, *C-FLAT: Control Flow Attestation for Embedded Systems Software, CCS '16.*

Handling Loops

- Different loop paths/iterations → many valid hash values
  - Our approach: treat loops as separate sub-graphs



$p = H_5, <H1, \{H_3\ , \#H_3\}>$

H_x different for each loop iteration

T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, *[C-FLAT: Control Flow Attestation for Embedded Systems Software](), CCS '16.*

Proof-of-Concept Implementation

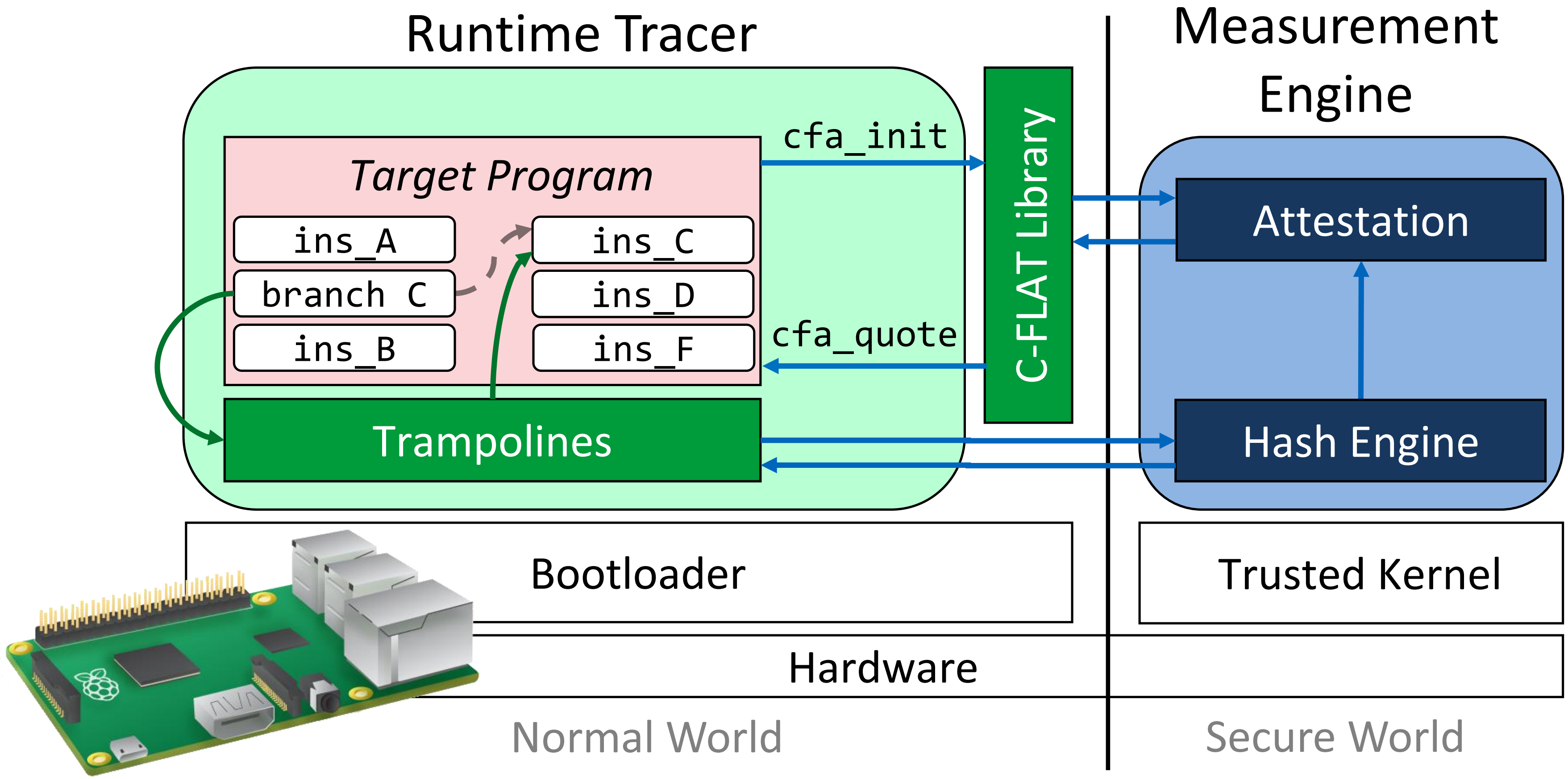
- Bare-metal prototype on Raspberry Pi 2
  - Single-purpose program instrumented using binary-rewriting
  - Runtime Monitor written in ARM assembler
  - Measurement Engine isolated in TrustZone-A Secure World

cfa_quote: 7c 16 d6 51 20 a2 a0 c7 90 f5 ef 04 0c 2e ba bc
  loop[000]: 78 22 5b 62 92 41 ca 02 7b ff 29 57 c6 6f 9b a2
    path[000]: 2f a5 8c dc 1b 35 41 29 ab dd 35 5c f2 69 08 37 (1)
  loop[001]: d6 90 9e a0 8c ae 90 84 9e 66 09 f8 a6 7b 52 04
    path[000]: 92 fb d1 e8 90 cb 02 e5 6c f2 65 8c 86 72 0e d3 (2)
....
  loop[006]: 05 e3 92 40 95 ef 7b 46 13 7d 6e 8b 05 be bf 41
    path[000]: 67 c6 5e d4 18 13 02 bc 4a 5d 60 a0 16 85 f4 ed (9)
    path[001]: 78 19 af 09 0f d5 64 f4 39 b4 7a 0d 97 57 77 8c (2)

Source: https://github.com/control-flow-attestation/c-flat/blob/master/samples/syringe/syringe-auth.txt

T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, C-FLAT: Control Flow Attestation for Embedded Systems Software, CCS '16.

Proof-of-Concept Implementation



Source code at https://github.com/control-flow-attestation/c-flat

T. Abera, N. Asokan, L. Davi, J-E. Ekberg, T. Nyman, A. Paverd, A-R. Sadeghi, G. Tsudik, [C-FLAT: Control Flow Attestation for Embedded Systems Software](), CCS '16.

LO-FAT

- Low-Overhead Control Flow Attestation in Hardware
  - Same security guarantees as C-FLAT
  - No performance overhead
  - No need for software instrumentation

- Utilizes existing IP building blocks
  - Branch filter used for detecting repeated paths
  - Hash engine for compressing attestation evidence

- Proof-of-concept implementation of main components
  - Targeting RISC-V SoC ("*Pulpino*")

G. Dessouky, S. Zeitouni, T. Nyman, A. Paverd, L. Davi, P. Koeberl, N. Asokan, A-R. Sadeghi, LO-FAT: Low-Overhead Control Flow Attestation in Hardware, DAC '17.

Run-Time Attestation: Summary

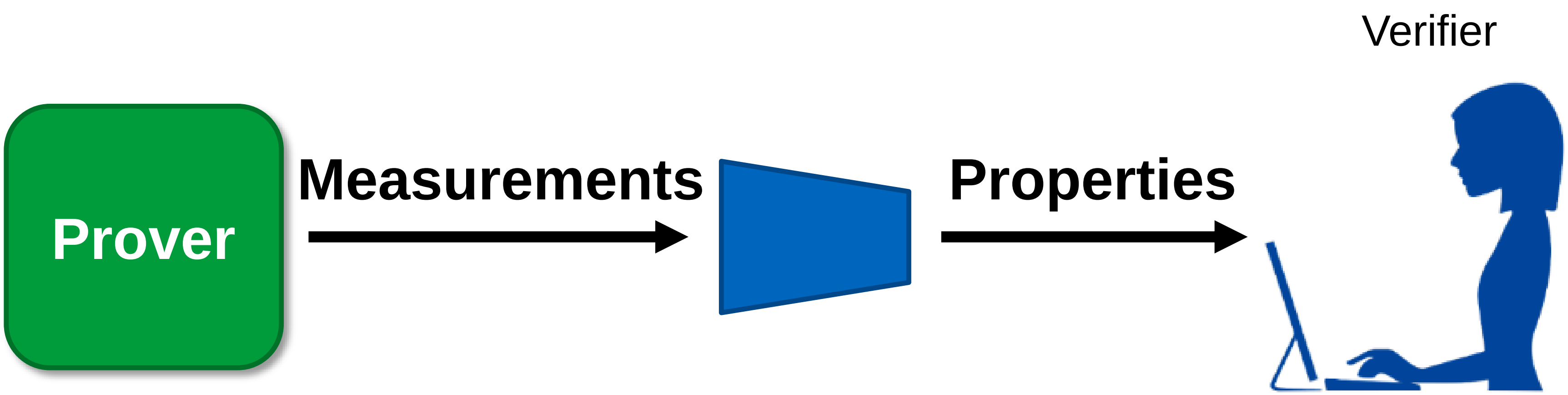
- How can we scale control flow attestation?
  - Better ways to encode/aggregate measurements?
  - Faster/simpler purpose-built hash functions?
  - Attestation of properties rather than measurements?
    - From attestation to checking compliance with a (dynamic) policy?

Property-Based Attestation

Property-Based Attestation

Attest properties of interest instead of program binaries

- scalability of maintaining acceptable measurements



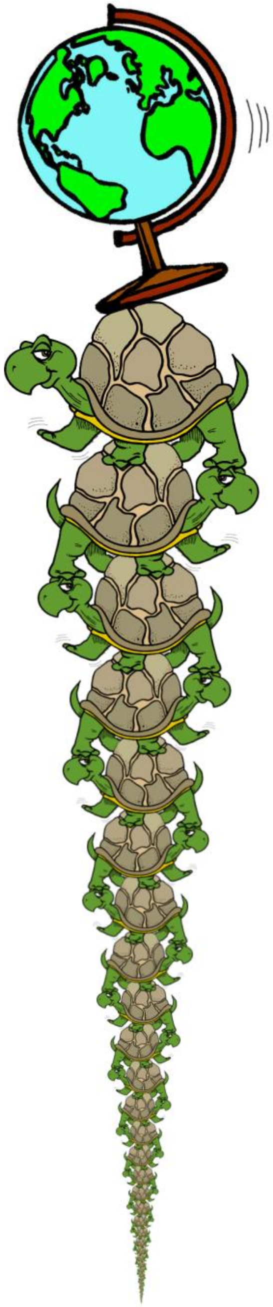
Use a trusted third party to convert from binary evidence to properties

A-R. Sadeghi, C. Stüble. Property-based attestation for computing platforms: caring about properties, not mechanisms. New Security Paradigms Workshop, 2004.

Mid-Point Review: Attestation in Principle

- TPM attestation
- Software-based attestation
  - Pioneer
- Hybrid attestation
  - SMART
  - TrustLite & TyTAN
- Scalable attestation
  - SEDA
  - SANA & LISAs
- Control-Flow Attestation
  - C-FLAT
  - LO-FAT
- Property-based attestation

Which of these are:
1. “Paperware” 2. Testable 3. Deployed



Short Break

On Roots of Trust …

A well-known scientist (some say it was Bertrand Russell) once gave a public lecture on astronomy. He described how the earth orbits around the sun and how the sun, in turn, orbits around the center of a vast collection of stars called our galaxy. At the end of the lecture, a little old lady at the back of the room got up and said: "What you have told us is rubbish. The world is really a flat plate supported on the back of a giant tortoise." The scientist gave a superior smile before replying, "What is the tortoise standing on?" "You're very clever, young man, very clever," said the old lady. "**But it's tortoises all the way down**!“

- Stephen Hawking, in *A Brief History of Time*

http://transversalinflections.files.wordpress.com/2011/06/turtles-all-the-way-down.png

Remote Attestation in Practice

Aalto University

UNIVERSITY OF HELSINKI

TPM Attestation

- Where are TPMs used?

- Where is TPM attestation used?

- Main challenge: verifier database scalability
  - Very large number of software packages
  - Frequently changing due to updates
  - Therefore: very hard to maintain whitelists

- Other challenges?

Property-Based Attestation in MirrorLink

- MirrorLink allows use of smartphone services in vehicles
- Car head-unit must enforce driver distraction regulations

http://www.mirrorlink.com

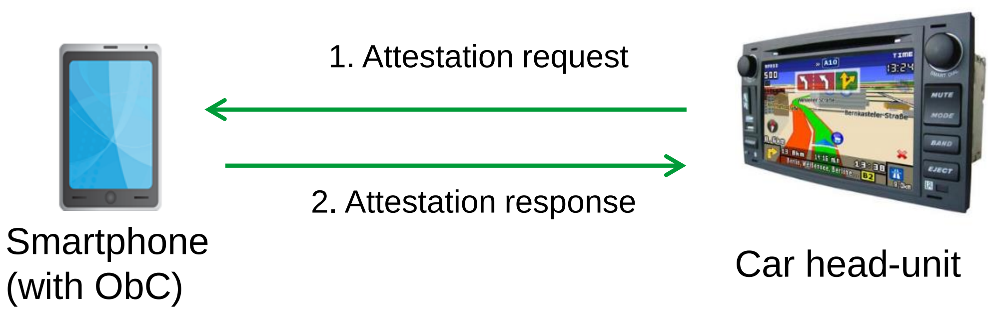
CARCONNECTIVITY consortium

R. Bose, J. Brakensiek, K-Y Park. Terminal Mode – Transforming Mobile Devices into Automotive Application Platforms. AutomotiveUI 2010.

Content Attestation in MirrorLink

- Head unit only allows some types of content while driving
  - Needs to know what content it is asked to render
- Content Attestation
  - Defined using TPM structures (part of MirrorLink standard)
  - Initially implemented using On-board Credentials (an early TEE)

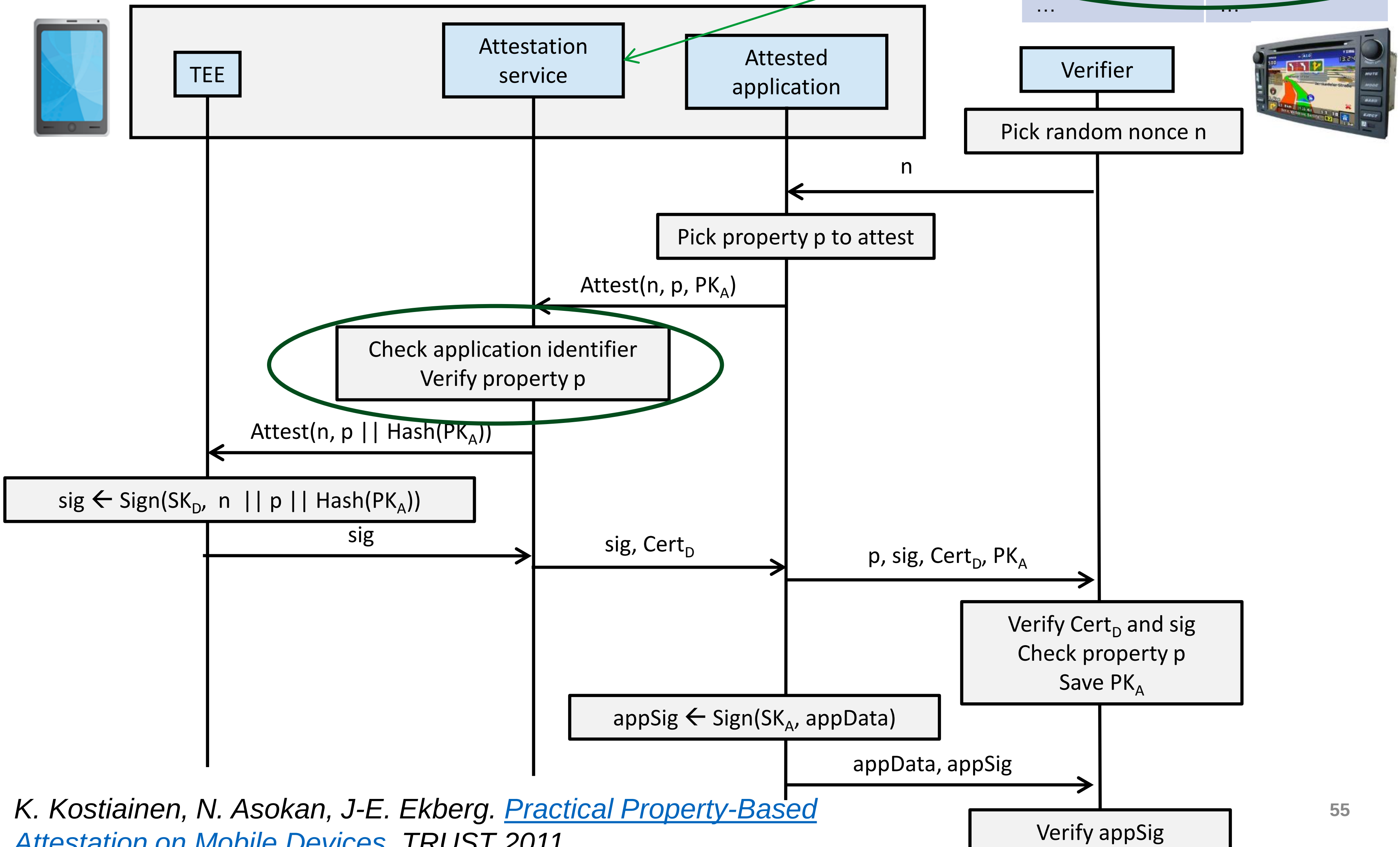
3. Enforce driver distraction regulations



K. Kostiainen, N. Asokan, J-E. Ekberg. Practical Property-Based Attestation on Mobile Devices. TRUST 2011.

MirrorLink Data Attestation

Application Identifier	Property
App1	P1, P2
App2	P3
…	…



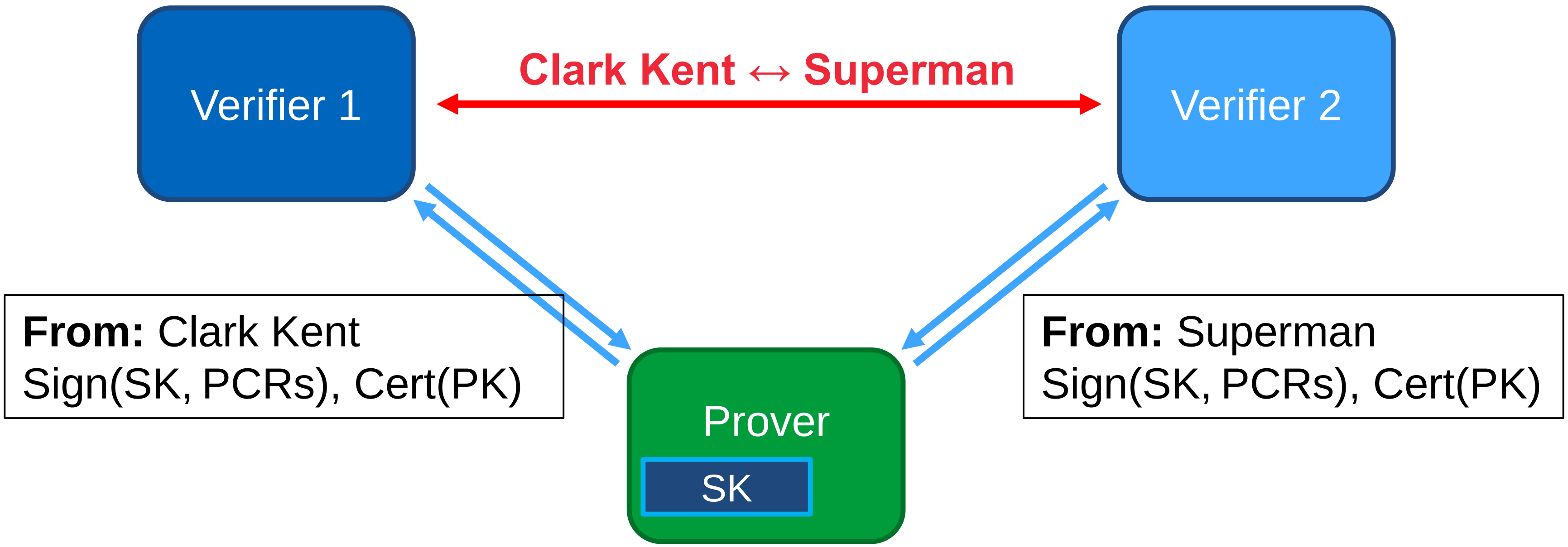
K. Kostiainen, N. Asokan, J-E. Ekberg. [Practical Property-Based Attestation on Mobile Devices](). TRUST 2011.

Privacy in Attestation

Privacy in TPM Attestation

PK	Public key
SK	Private key

- *(Recall)* Prover provides TPM-signed quotes to verifiers



See also [Intel Pentium III Processor Serial Number controversy] (1999)

Privacy in TPM Attestation

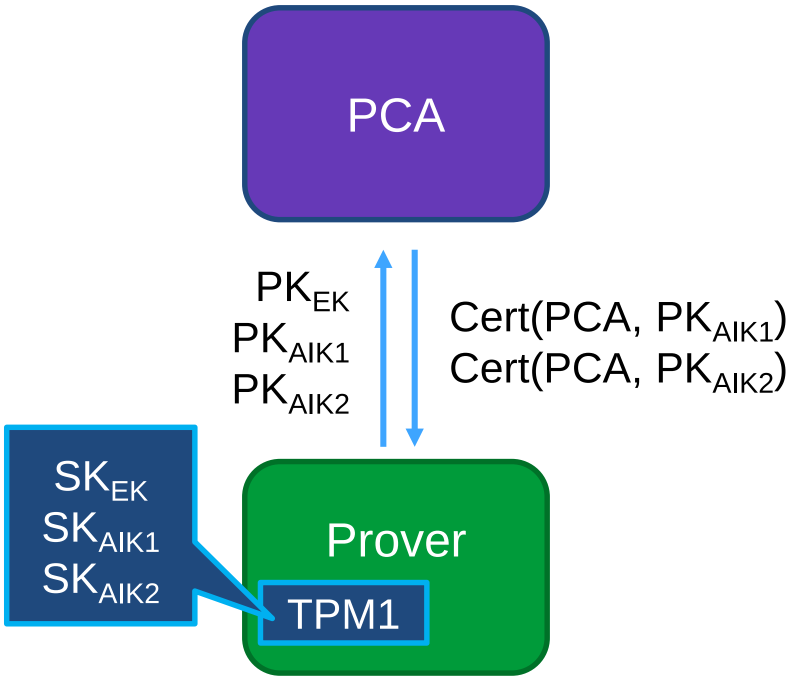
- Solution: use different attestation key pairs
  - *Endorsement Key (EK)*
    - One EK per TPM
    - Certified by manufacturer

  Used to prove this is a real TPM

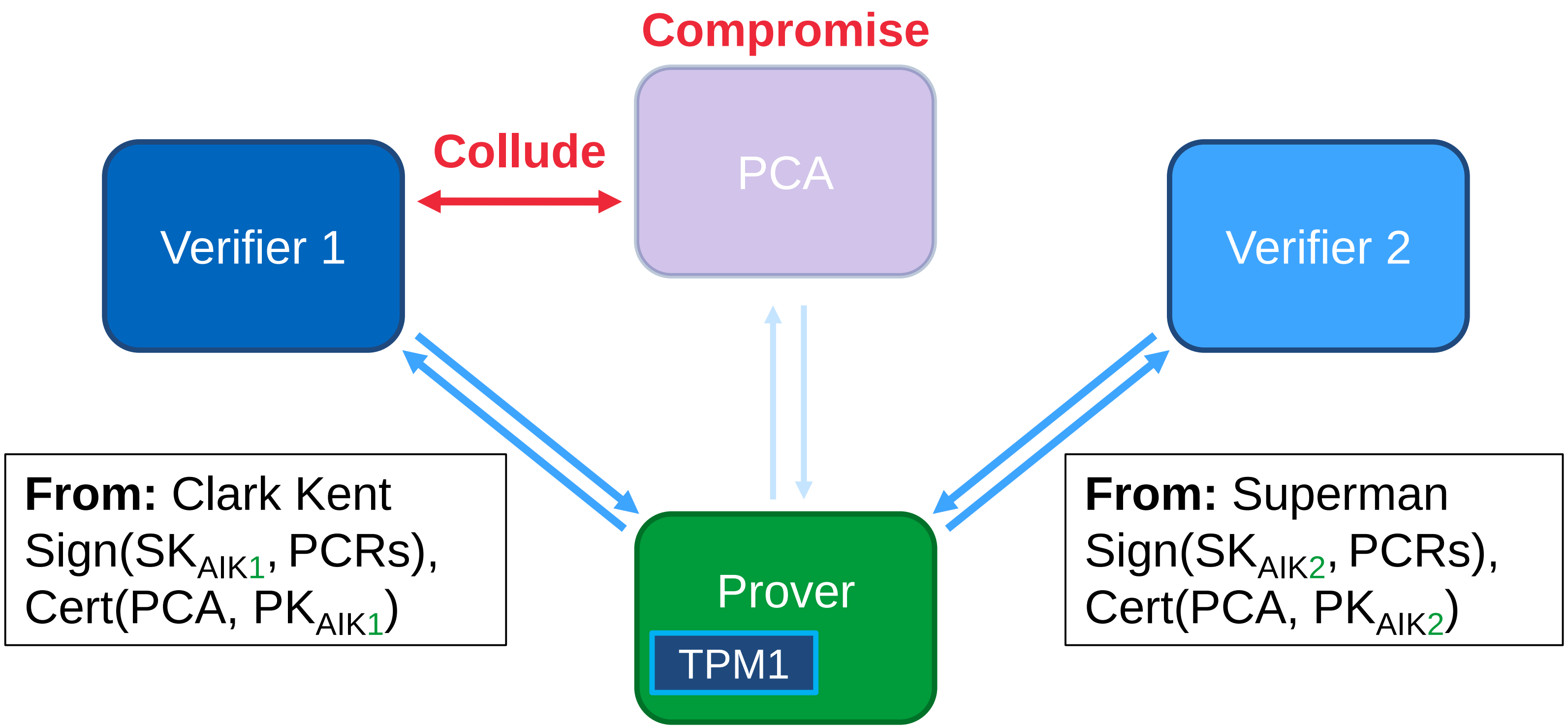
  - Attestation Identity Key (AIK)
    - (Virtually) unlimited number of AIKs
    - Certified by a Privacy CA or through Direct Anonymous Attestation (DAA)

  Used during attestation

Privacy Certificate Authority (PCA)



Privacy Certificate Authority (PCA)



Direct Anonymous Attestation

- Mechanism of certifying AIKs without a trusted third party
- Based on group signature schemes
  - Secure in random oracle model with strong RSA and decisional Diffie-Hellman assumptions
  - Prover controls linkability between signatures
  - Revocation of anonymity intentionally not possible
- Rogue TPMs can be excluded only if private key is known

E. Brickell, J. Camenisch, L. Chen. Direct Anonymous Attestation. ACM CCS, 2004.

Direct Anonymous Attestation

DAA_join: Protocol between TPM and DAA issuer (e.g. manufacturer) through which TPM obtains a DAA key.

DAA_sign: TPM signs an AIK using its DAA key.

DAA_verify: Protocol through which TPM proves to a verifier that it has a valid DAA signature on AIK (without revealing DAA key).

E. Brickell, J. Camenisch, L. Chen. Direct Anonymous Attestation. ACM CCS, 2004.

Privacy in TPM Attestation

- *(Recall)* Prover provides TPM-signed quotes along with the full list of executed software to verifiers

Concern 1: Infer private information from installed apps

- Possibility for profiling/discrimination

Concern 2: Track users through “software fingerprints”

- Negates use of DAA or Privacy CA

Attestation in Trusted Execution Environments (TEEs)

Intel Software Guard Extensions (SGX)

Objective

– Protect a small amount of code and data against all other software (including the OS)

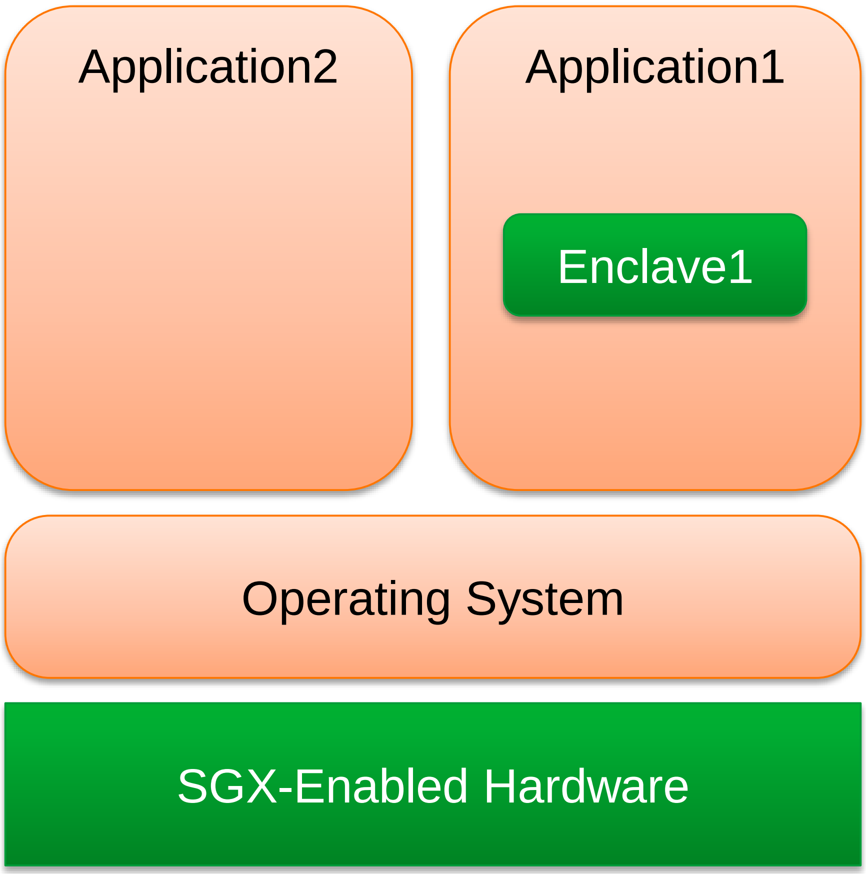
Mechanism

– Processor-enforced isolated execution environment: *enclave*

Enclave features

– Secure storage (sealing)
– Secure provisioning (remote attestation)

Intel Software Guard Extensions (SGX)



- Enclave runs in user process
- Enclave memory encrypted before leaving CPU boundary
- Ensures confidentiality and integrity of enclave data

F. McKeen, et al. [Innovative Instructions and Software Model for Isolated Execution], HASP 2013

SGX Remote Attestation

- Verifier database scalability
  - Only enclave code and configuration are attested

- Privacy
  - Limited amount of code attested
  - *Enhanced Privacy ID (EPID)*

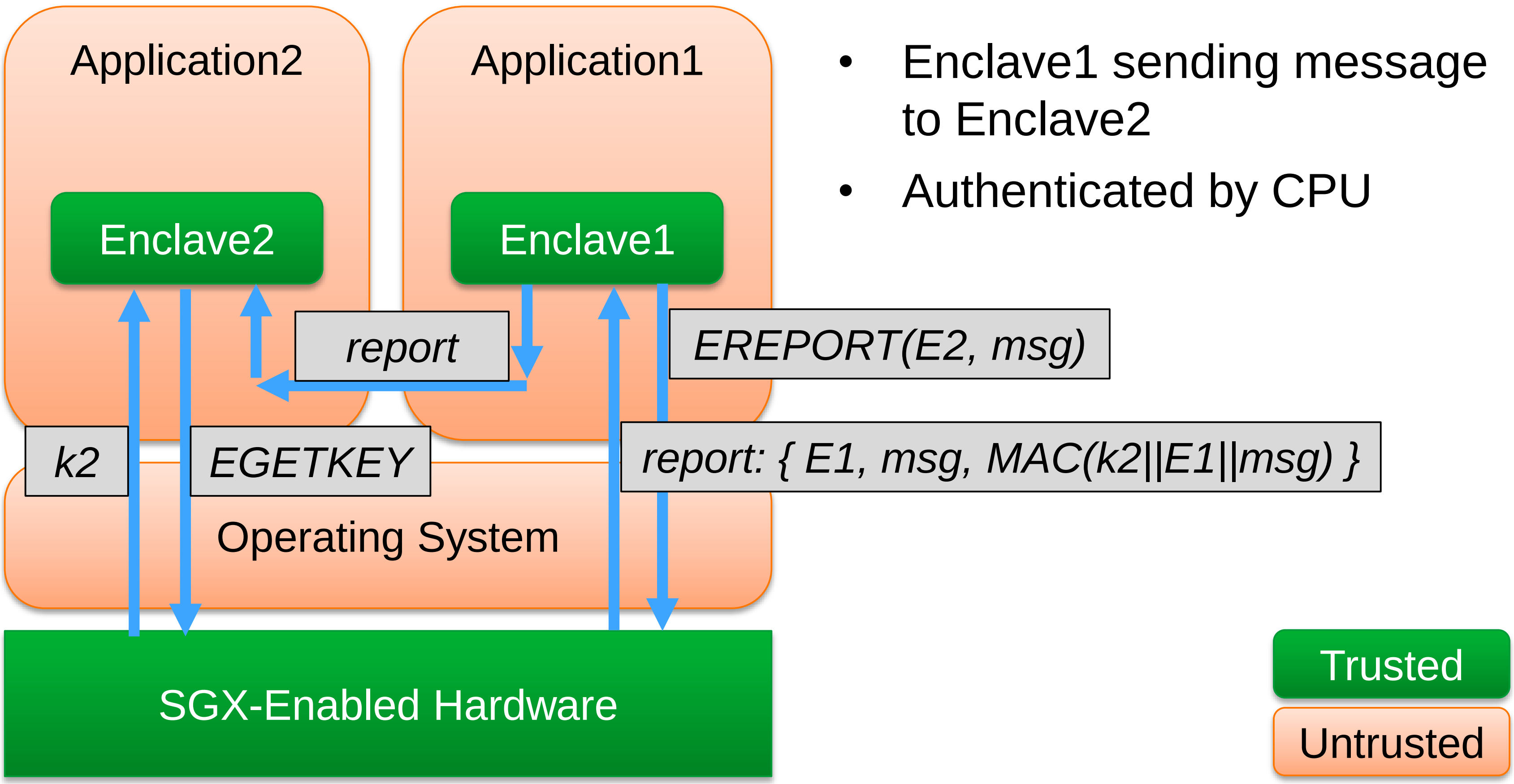
Enhanced Privacy ID (EPID)

A DAA scheme with enhanced revocation capabilities

- Same privacy guarantees as DAA
  - Also assumes random oracle model with strong RSA and decisional Diffie-Hellman assumptions
- Improved revocation capabilities
  - Revocation possible even if private key not publically known

E. Brickell, J. Li. Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. WPES 2007.

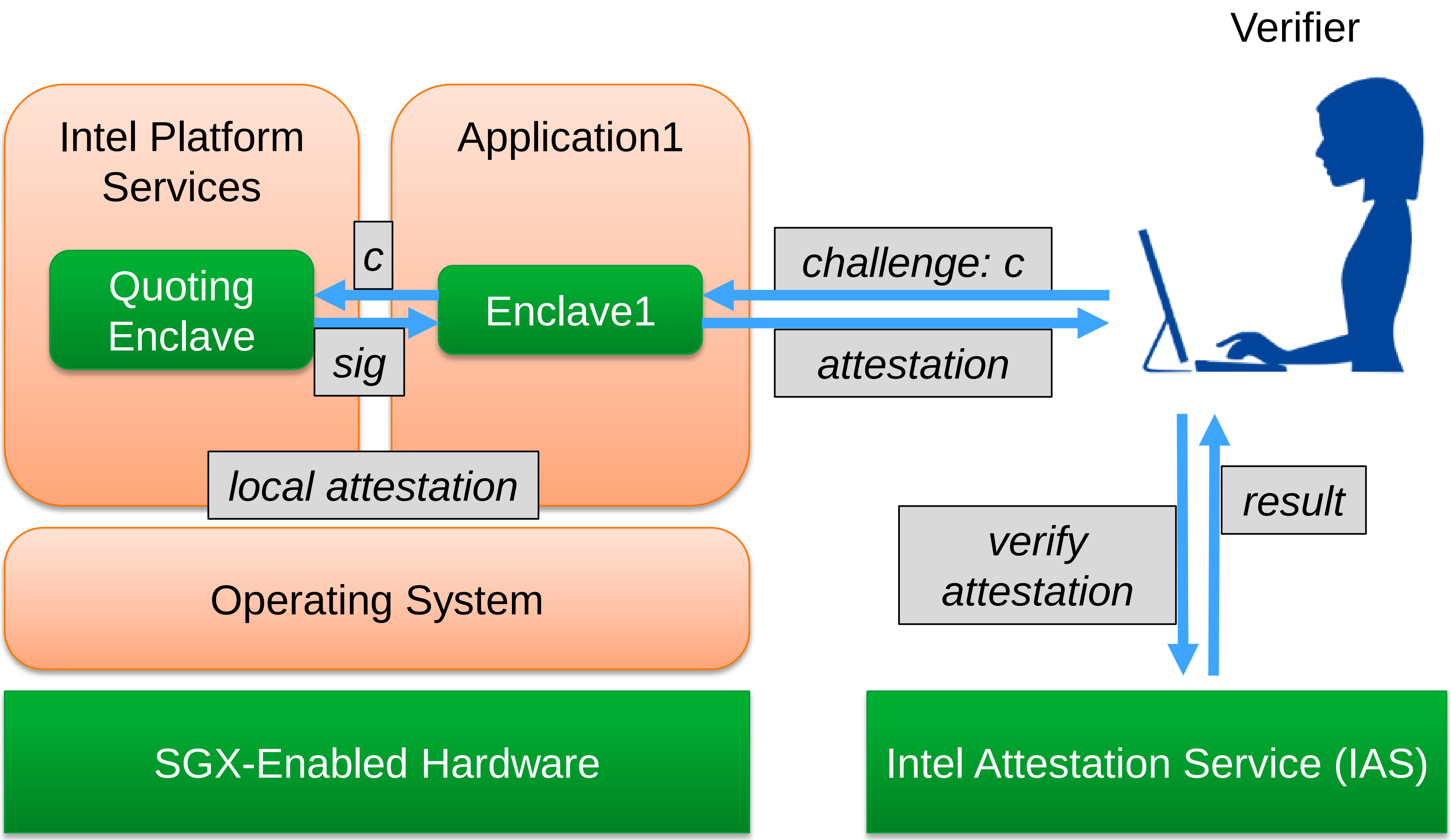
SGX *Local* Attestation



- Enclave1 sending message to Enclave2
- Authenticated by CPU

I. Anati, S. Gueron, S. Johnson, V. Scarlata. Innovative Technology for CPU Based Attestation and Sealing, HASP 2013

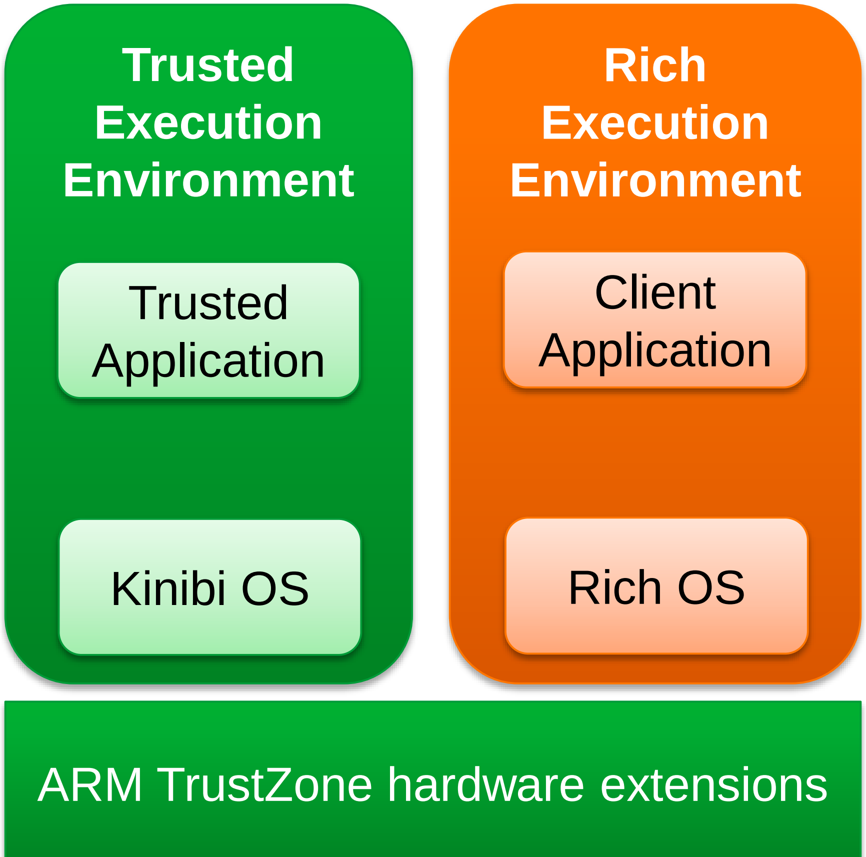
SGX Remote Attestation



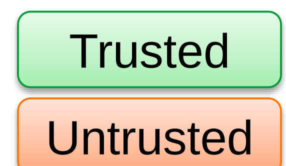
I. Anati, S. Gueron, S. Johnson, V. Scarlata. [Innovative Technology for CPU Based Attestation and Sealing](), HASP 2013

Kinibi on ARM TrustZone

Kinibi on ARM TrustZone

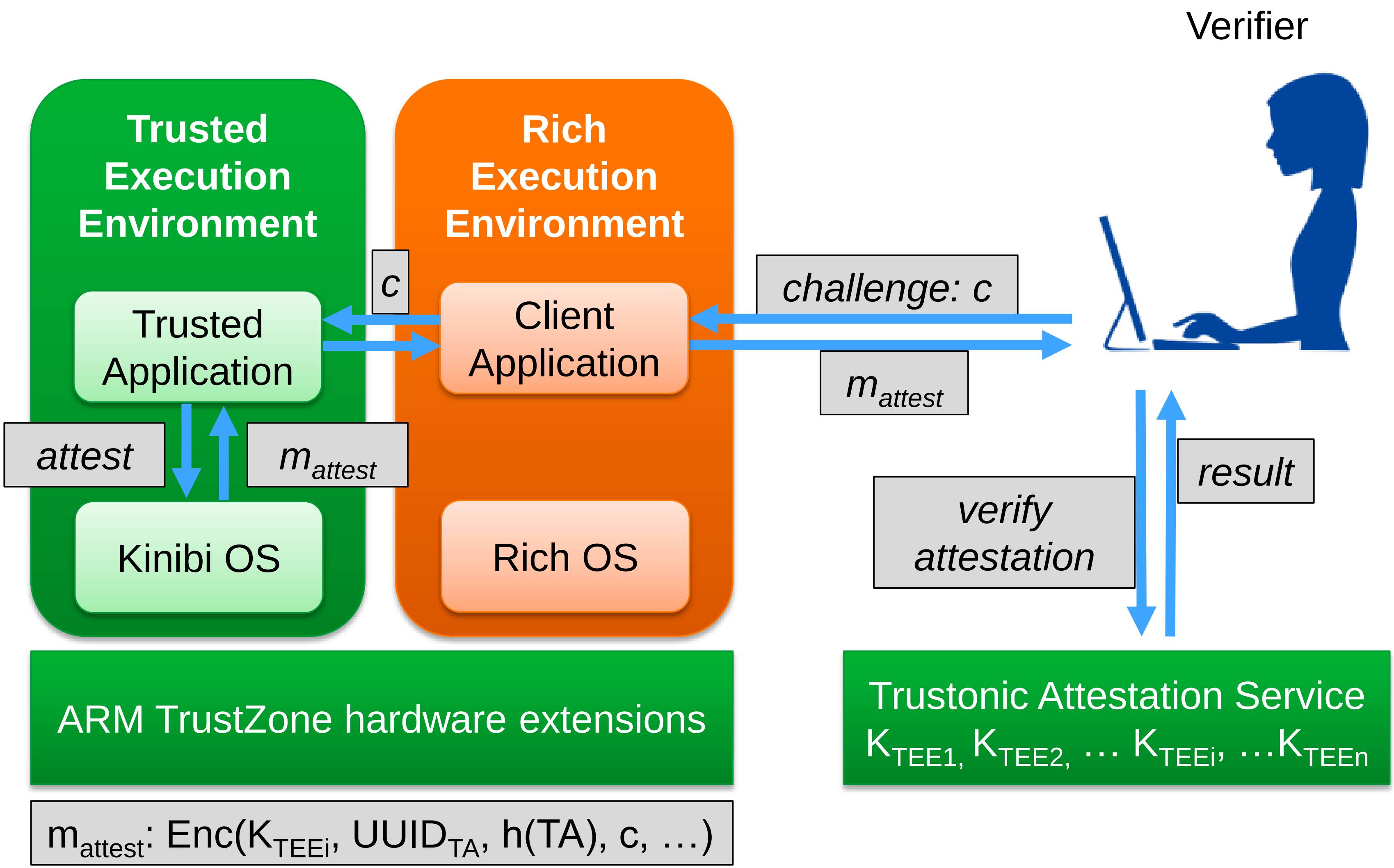


- Single hardware-enforced TrustZone TEE per platform
- Kinibi trusted OS:
  - manages trusted applications
  - isolates them from each other



S. Tamrakar, J-E Ekberg, P. Laitinen, [On Rehoming the Electronic ID to TEEs](), TrustCom 2015

Remote Attestation in Kinibi



S. Tamrakar, J-E Ekberg, P. Laitinen, [On Rehoming the Electronic ID to TEEs](), TrustCom 2015

Common use case: Key Attestation

Key Attestation

How to attest that a key is protected by hardware?

- Must also prevent linkability between keys

- TPM_CertifyKey command
  - Non-migratable TPM key certified using AIK
  - Subject Key Attestation Evidence (SKAE) extension X.509 cert.
  - Now supported by Windows Server (Feb 2017)

- Using normal SGX attestation
  - Verifier checks that enclave generated key securely

Android Keystore Attestation

- Available from Android 7.0 (API level 24) onwards
  - But currently few devices with hardware-backed attestation
- Keystore produces an *attestation certificate* for key pair
  - Standard X.509, signed by on-device attestation key
- On-device attestation keys
  - Injected into device during manufacture
  - Signed by device manufacturer or Google
  - Injected in batches: “minimum 10,000 devices per key”

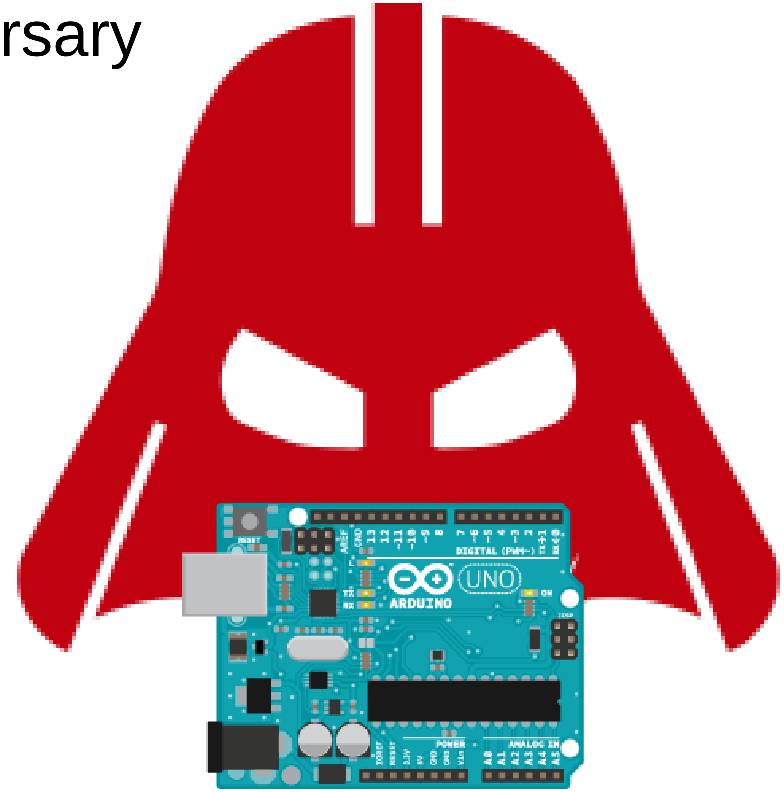
Summary: Attestation in Practice

- TPM-based Attestation
- MirrorLink Data Attestation Protocol
- Privacy in Attestation
- Attestation in TEEs
  - SGX
  - TrustZone
- Key Attestation

Open Challenges

Open Challenges

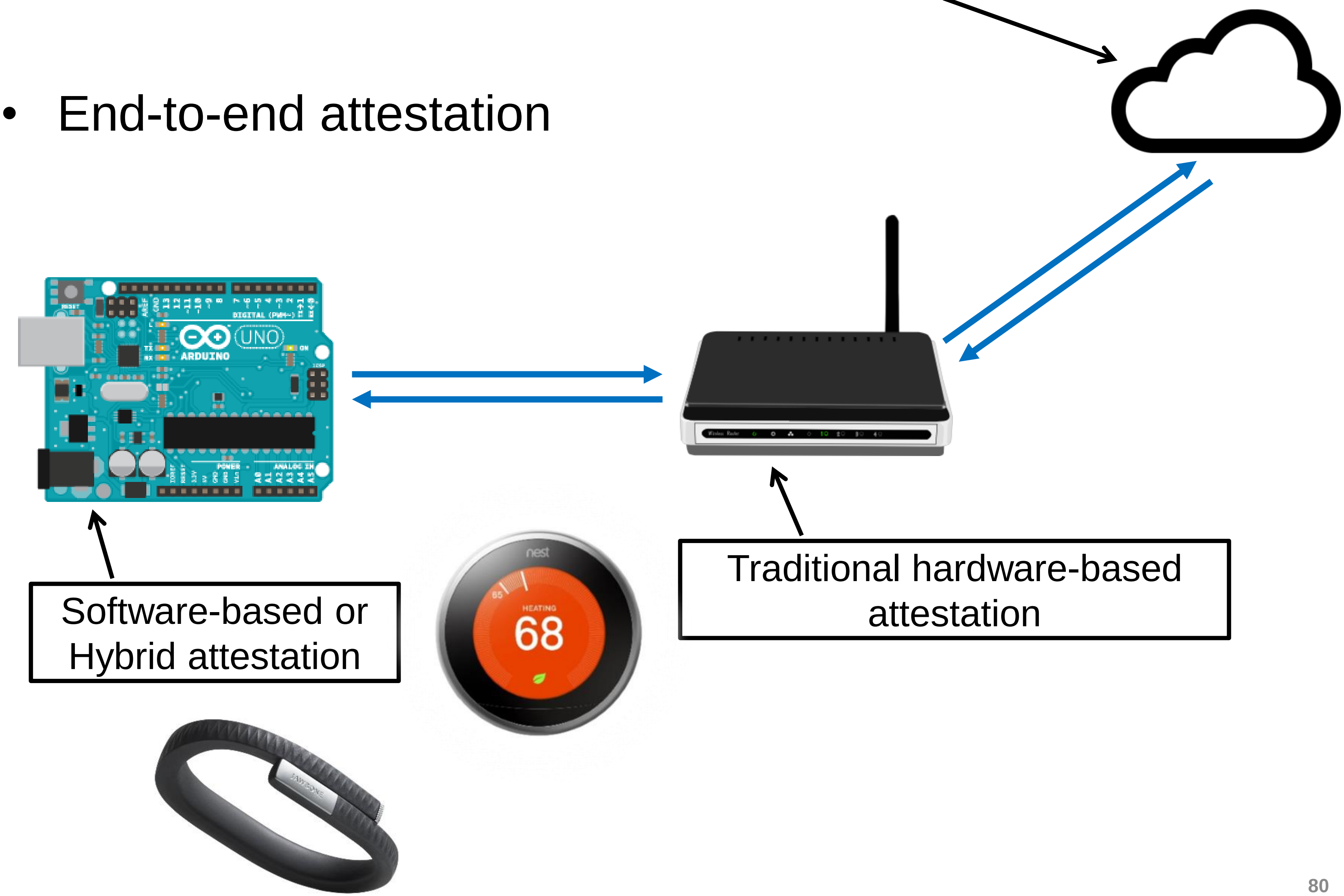
- Physical adversary



Open Challenges

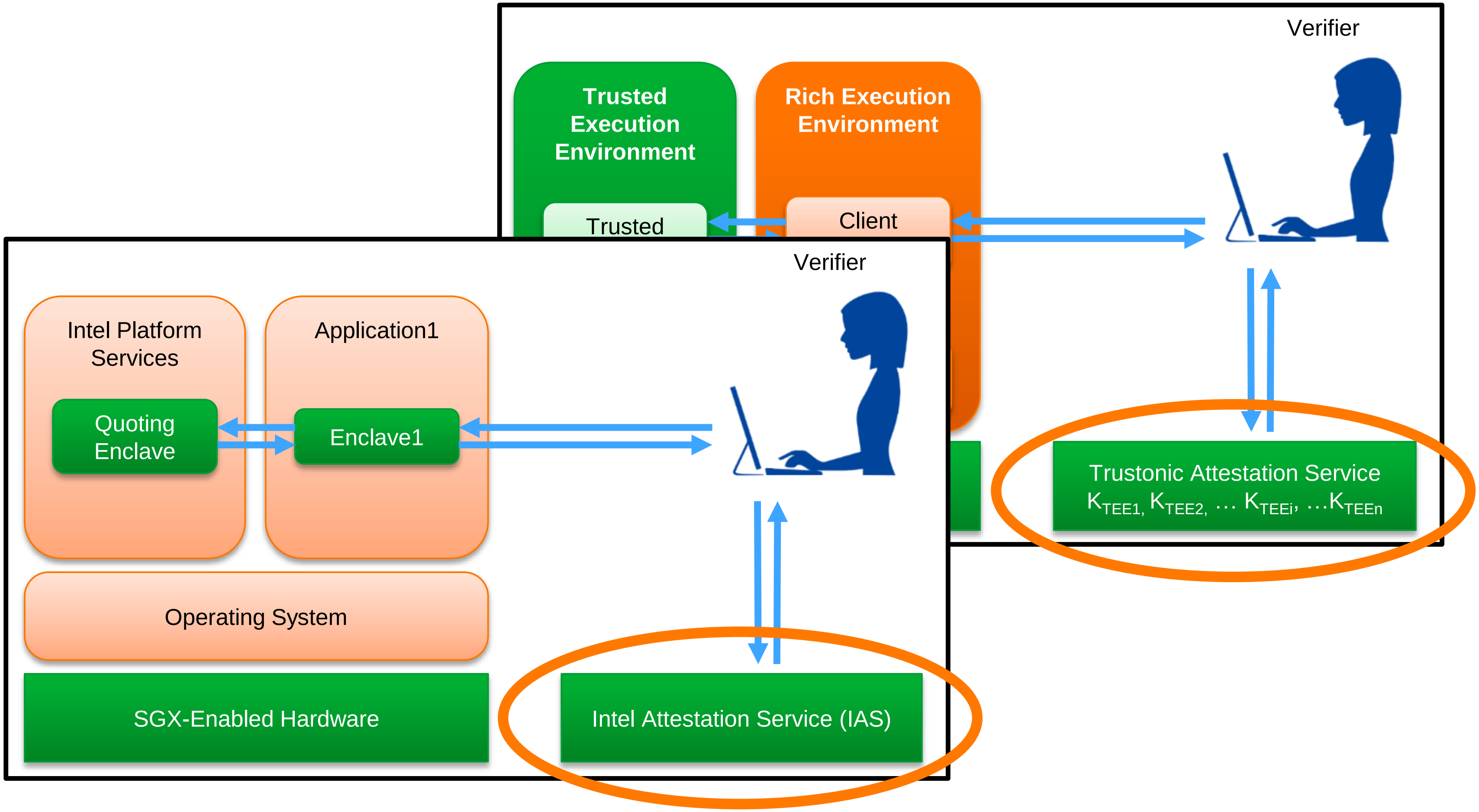
Traditional attestation based on virtualized hardware (e.g. virtual TPM)

- End-to-end attestation



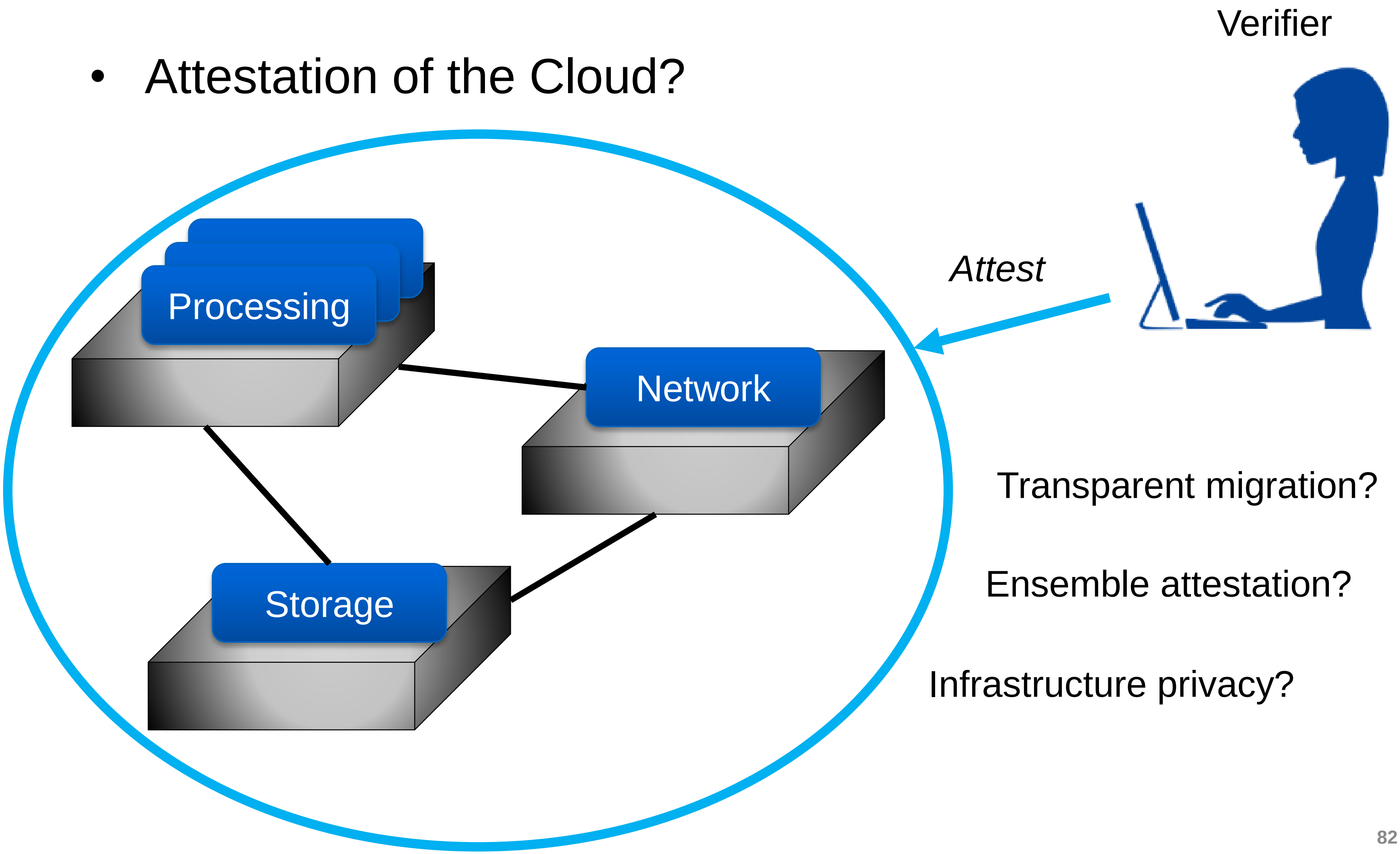
Open Challenges

- Attestation Servers?



Open Challenges

- Attestation of the Cloud?



Transparent migration?

Ensemble attestation?

Infrastructure privacy?

Conclusions

- Increasing need for remote attestation
- Various schemes proposed, developed, deployed
- Building deployable attestation schemes is challenging