Secure Systems Groups

Demo Day 2016

N. Asokan, Tuomas Aura, Valtteri Niemi

Aalto University

UNIVERSITY OF HELSINKI

“State of the Union”

Who are we?

- Aalto University
  - 2 professors
  - 2 postdocs
  - Several PhD and MSc thesis students
  - Several interns
- University of Helsinki
  - 1 full-time + 1 part-time professor
  - 1 postdoc
  - 1 PhD student and several MSc thesis students

How are we funded?

- Cyber Trust SHOK (Aalto & UH)
- 2 Academy of Finland projects: ConSec (Aalto), CloSe (Aalto & UH)
- Tekes project: Take5 (UH)
- Intel CRI for Secure Computing (ICRI-SC) (Aalto & UH NODES)
- Basic university funding (Aalto & UH)
- Industry collaboration: NEC Labs (Aalto), Huawei (UH)
- MATINE (Ministry of Defense) project (Aalto)

What do we work on?

- (Mobile) Platform Security
- Contextual Security
- Cloud Security
- New: Blockchains

- 5G Security

- Security Protocol Engineering
- Network Security
- Security for Ubiquitous Computing

What do we work on?

Security

Usability

Deployability

Where are we publishing?

Self evaluation:
Good but room
to improve

- Top-tier infosec venues: ACM CCS (2), NDSS (2)
- Other top-tier venues: UbiComp, ICDCS, PerCom
- Thematic venues: **IOT (best paper)**, Financial Crypto, TrustCom, TRUST

- Industry exposure: BlackHat EU, **CeBIT (MAPPING app competition)**

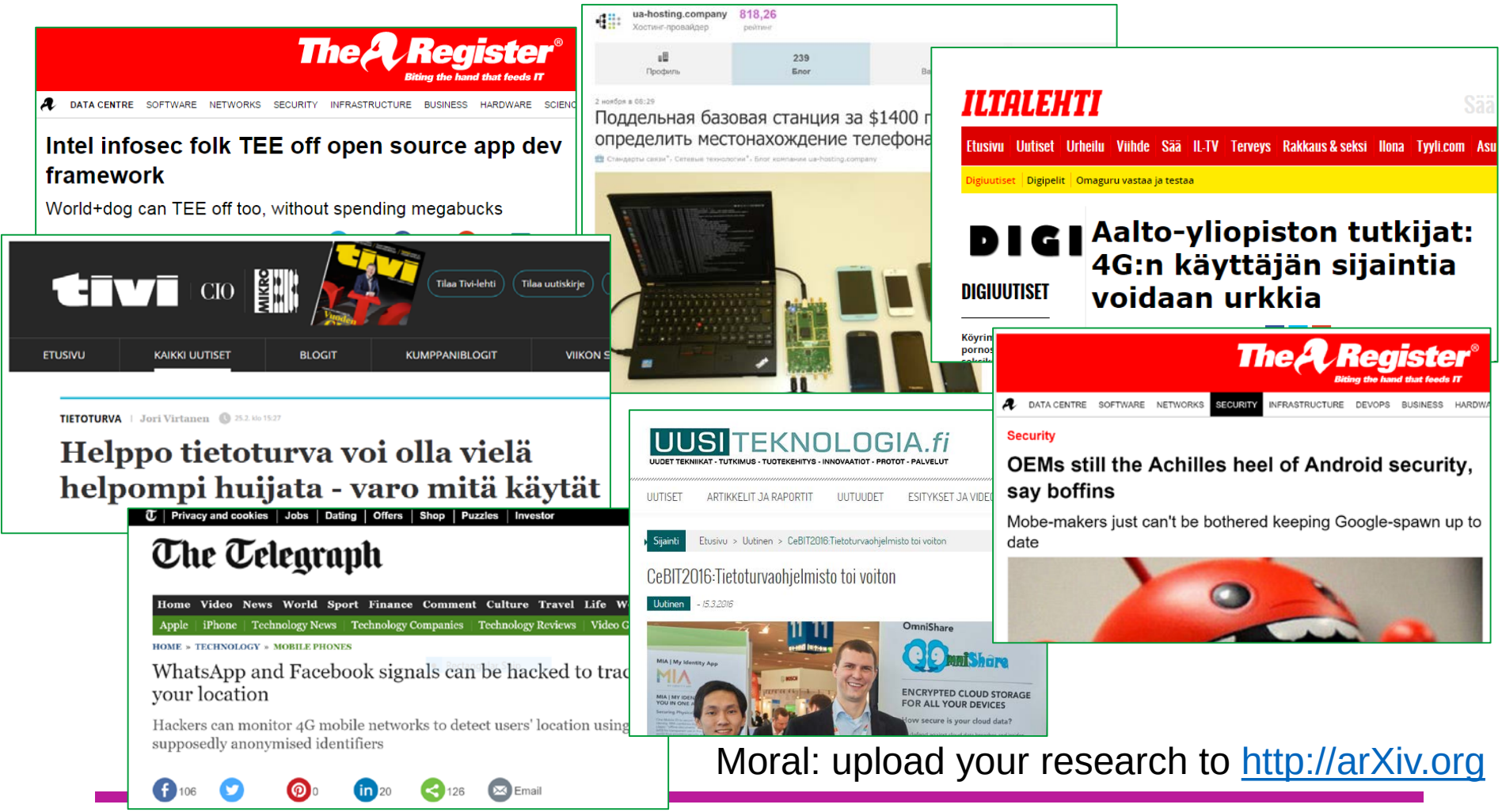
What do we teach?

- Information Security courses
  - Bachelor level course on Information Security
  - MSc level courses on network security, mobile system security
  - Seminar and laboratory courses
  - Shared courses between Aalto and UH
- Courses taught by industry experts
  - Reverse engineering Malware(F-Secure)
  - Software Security (Vähä-Sipilä)
- **Highest scoring courses in student feedback**

Industry Collaboration

- Industry-funded collaborative projects
  - Intel, NEC Labs
- Publicly-funded collaborative projects
  - Electrobit, Ericsson, F-Secure, Ministry of Defense, Nokia, nSense, Huawei, Trustonic
- Other collaboration with industry sector
  - Trustonic, SSH
- Collaboration with state sector
  - VTT, Väestörekisterikeskus

Media coverage of our research



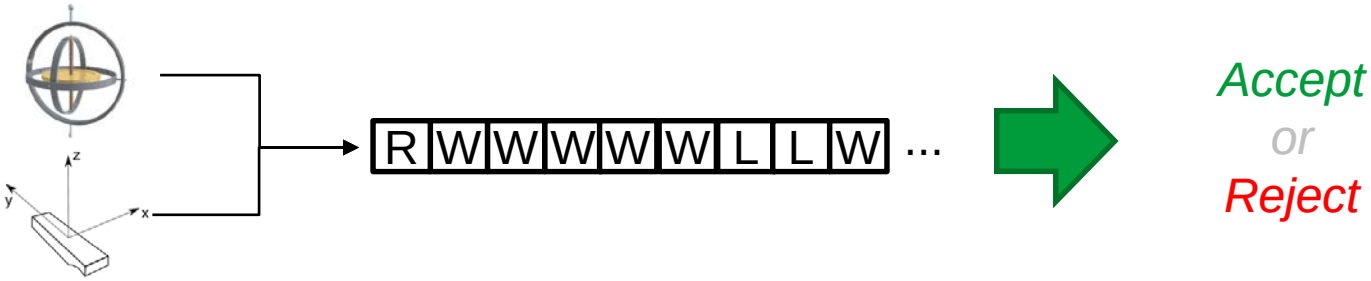
Moral: upload your research to http://arXiv.org

Demo Teasers

Relay Resilient Zero-Effort Authentication

Can on-board devices alone be used for proximity assertion in theory and in practise?

- Attacker can emulate proximity with high-speed link between prover and verifier
  - Prevented by moving proximity verification to prover itself
- Prover maintains internal state or perceived events (left, right, walk, stationary, ...)
  - Participates in challenge-response protocol only if in appropriate state



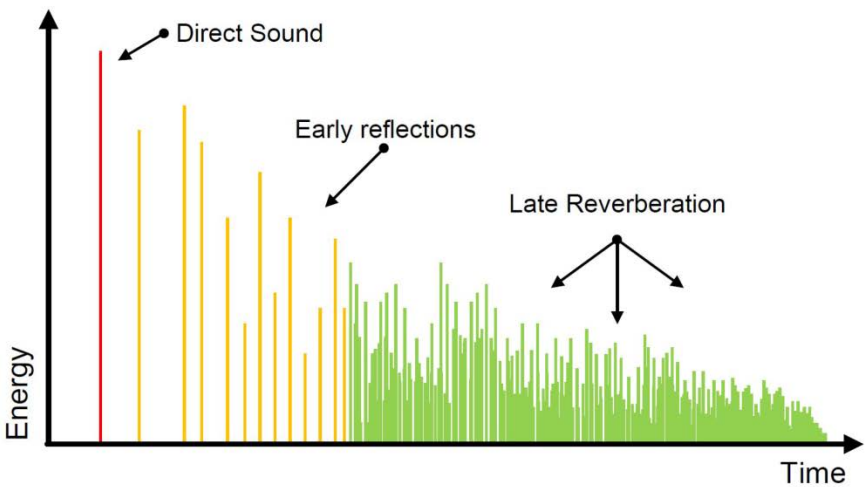
Asymmetric design ideal for IoT devices

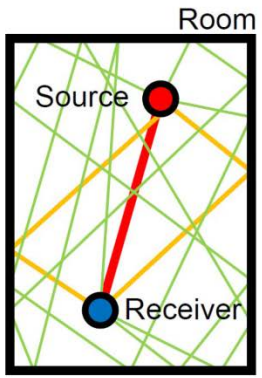
Mika Juuti

Co-presence detection using RIR

Can RIR help thwart relay attacks in proximity-based authentication?

Room Impulse Response (RIR)





Solutions:

- 3 frequency domain features: RT60, Direct-to-Reverberation ratio, Echo
- Features on different freq. bands
- Automatic calibration

Results:

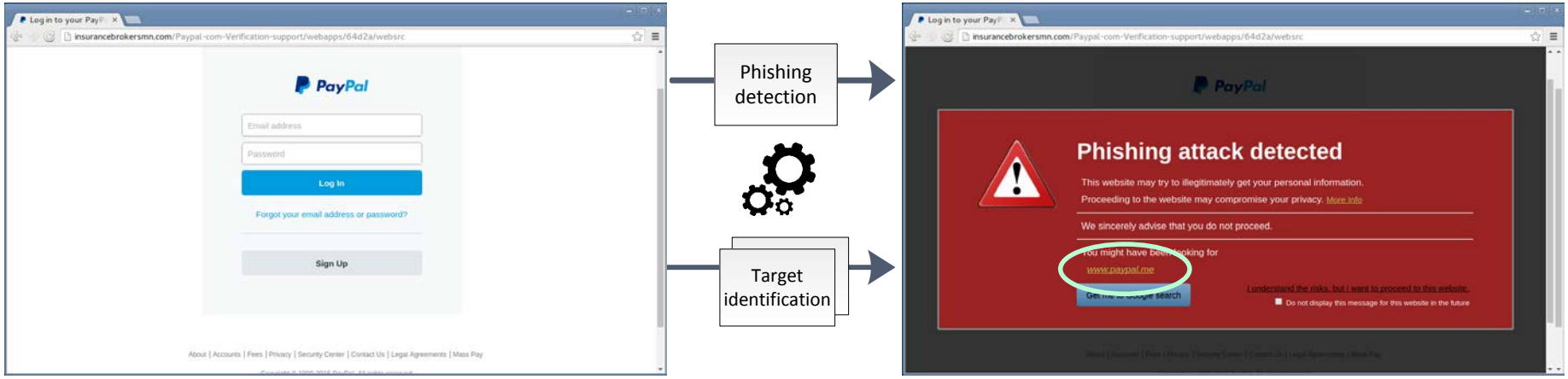
- Single device: >80% accuracy
- Multiple devices: better calibration for input signal loudness?

Challenges of using RIRs in commodity devices:

- Unexpected effects: clipping, harmonic distortion
- Difference in frequency responses, loudness of mics/speakers

Real-Time Client-Side Phishing Prevention Add-on

How to efficiently detect phishing websites and steer users away from them?



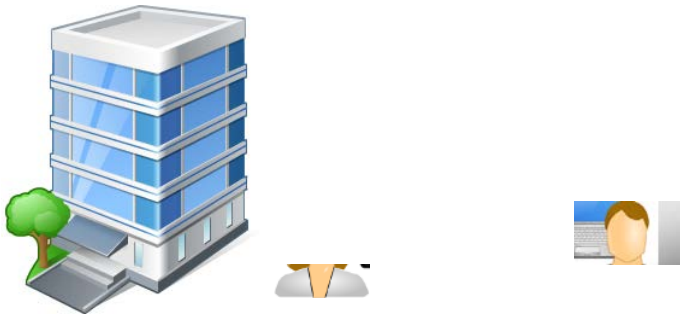
- Resilient to adaptive attacks
- Language and brand independent
- Redirect to legitimate website

- High accuracy: 99 %
- Low FPR: 0.1 %
- Fast warning: 473 ms median time

Giovanni Armano

Risk Engine for User Behavior Analytics

How to control Internet transactions to protect enterprise assets while preserving usability?

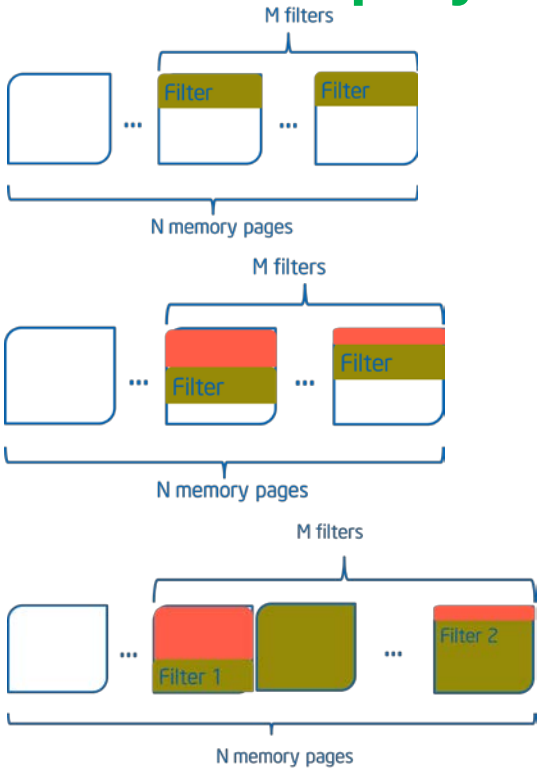


- Context-aware transaction authorization
- Analyze transaction sequence (e.g. intranet download + upload to cloud)
- Build user-specific transaction profile

Randomization can't stop BPF JIT spray

Is upstream Linux kernel still vulnerable to JIT spray?

- 2012: Berkeley Packet Filter (BPF) JIT spray
- Upstream Linux kernel fix has held till 2016 despite concerns
- We show that the fix is vulnerable to a new modified attack



Impact:

- New patches scheduled for merge with upstream kernel
- Takeaway: fix causes, not symptoms

Elena Reshetova

https://github.com/01org/jit-spray-poc-for-ksp

SEAndroid policy analysis: SELint

How to help OEMs improve their SEAndroid policies?

SEAndroid mandatory from 5.0:

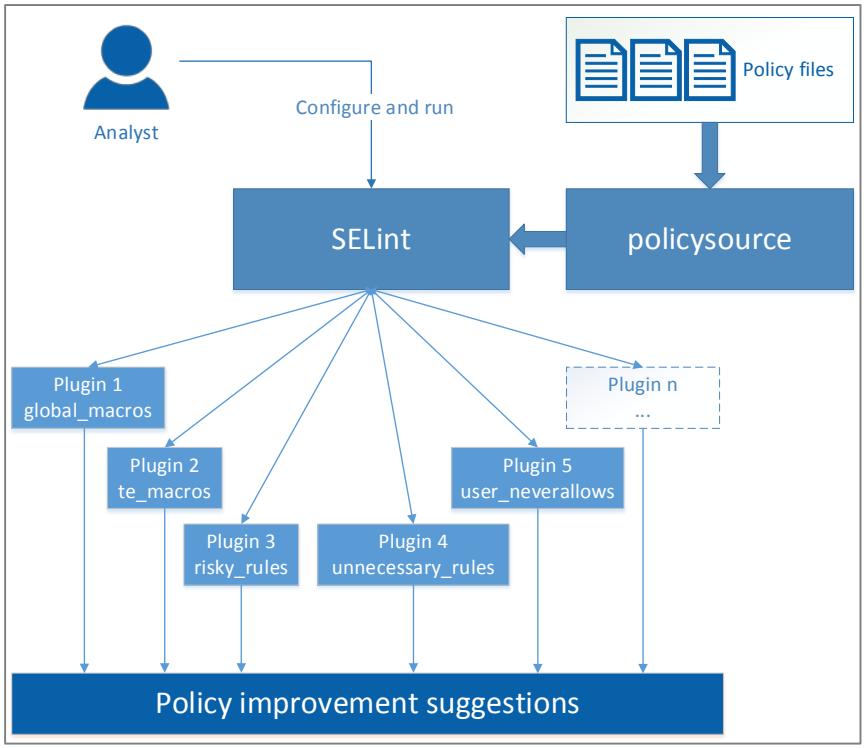
- OEMs make mistakes when writing policies (See https://ssg.aalto.fi/projects/seal/)
- Mistakes also due to lack of tools

Need for tools that can

- work with source policy
- be used without expert knowledge

Our proposal: SELint

- Extensible: plugins
- Configurable



Use SELint to simplify and speed up analyst workflow

Filippo Bonazzi

Aalto University

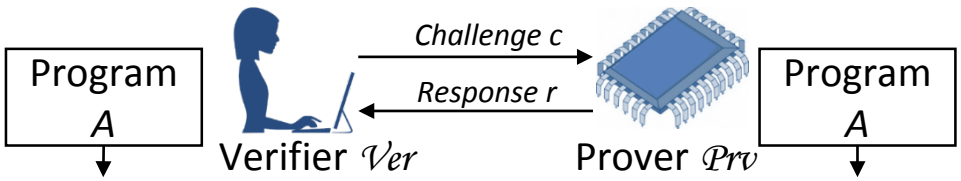
Collaborative Research Institute for Secure Computing

INTEL OPEN SOURCE TECHNOLOGY CENTER

https://ssg.aalto.fi/projects/selint/

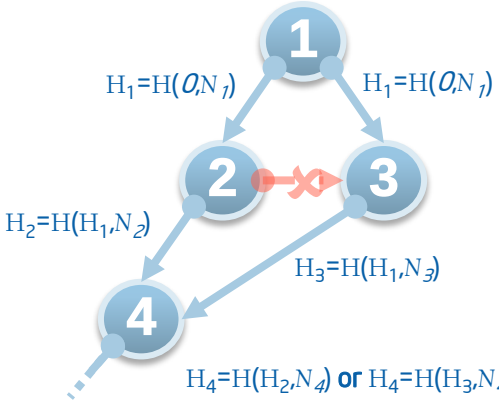
C-FLAT: Control Flow Attestation of Embedded Systems Software

How can a trusted **verifier** learn about **run-time attacks** and the **dynamic behavior** of an **embedded device**?



TrustZone-A PoC on Raspberry Pi 2

```
① if (cond)
②  then: ins_A
③  else: ins_B
④ ins_D
```



Novel **attestation scheme** for **runtime behaviour**

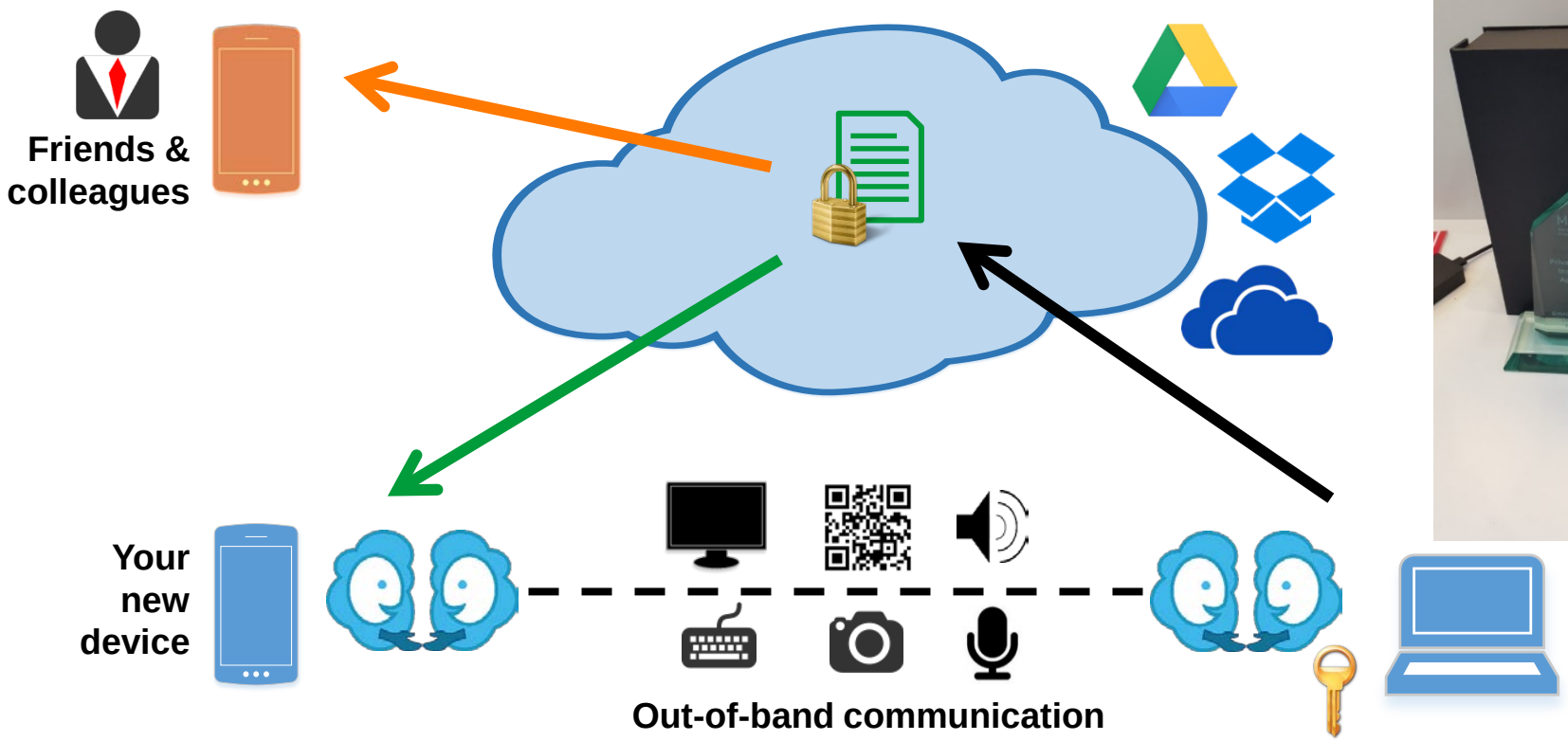
$Auth = H_4$

Thomas Nyman

OmniShare

Privacy via IT Security App Competition: 1st Prize CeBIT 2016

How can you share your data securely with anyone you like, anywhere you like?



Andrew Paverd

Aalto University

Collaborative Research Institute for Secure Computing

Technische Universität Darmstadt

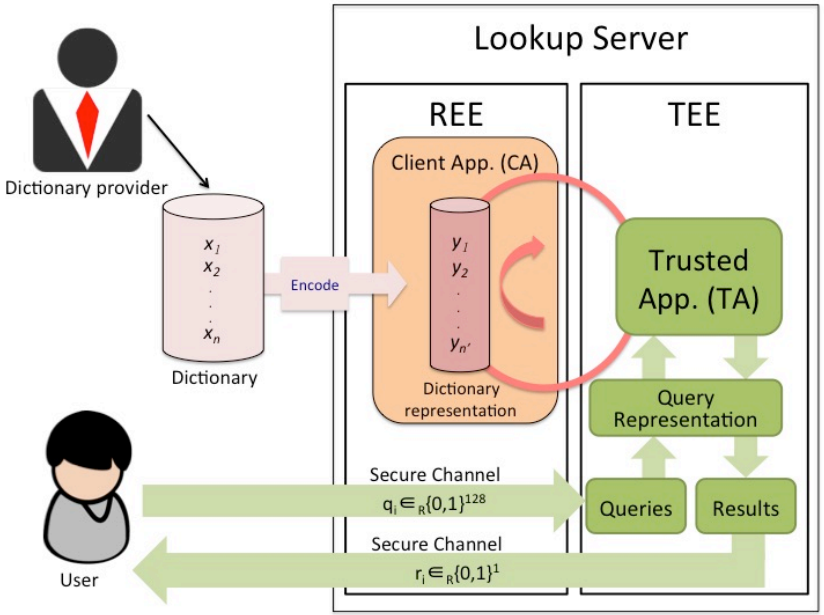
Academy of Finland

CloSe

https://ssg.aalto.fi/omnishare/

Scalable Private Membership Test Using Trusted Hardware
ARM TrustZone and Intel SGX

How to design efficient yet privacy preserving membership test using trusted hardware, for a malware checking scenario?



- Carousel approach – continuously circle malware dictionary through trusted hardware
- Different data structures for efficient response computation
  - E.g. Sequence of Differences, Bloom filter, and Cuckoo hash
- Carousel outperforms Path ORAM (using Cuckoo hash)

- Supports ~67 million malware identifiers with < 2^{-10} false positive rate
- 1025 queries/sec on ARM TrustZone and 3720 queries/sec on Intel SGX

Sandeep Tamrakar

Private Membership Test with Homomorphic Encryption

How to look up a keyword in a cloud-hosted database without sacrificing privacy?

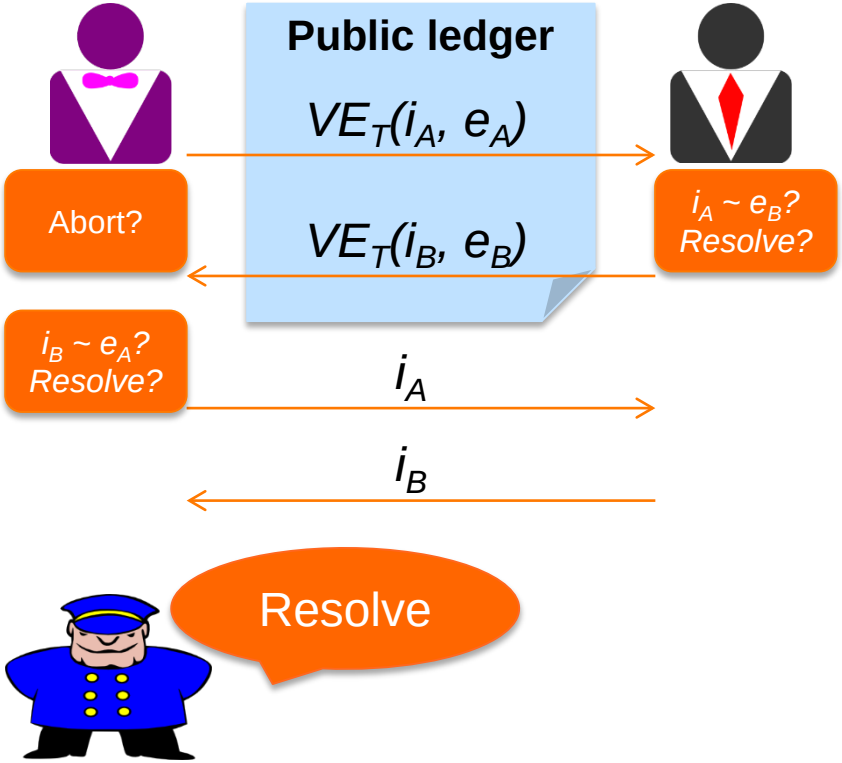
- Server maps items in the database into items of a matrix
- Client finds the matrix index corresponding to his/her query keyword and encrypts the index utilizing Homomorphic Encryption
- Homomorphic encryption allows server to search in the matrix without knowledge of client's keys
- Client decrypts the result and finds out whether index corresponds to an item in the matrix or not

After executing this protocol, the secrecy of both parties is preserved.

Applications on Blockchain: Promise and Limits

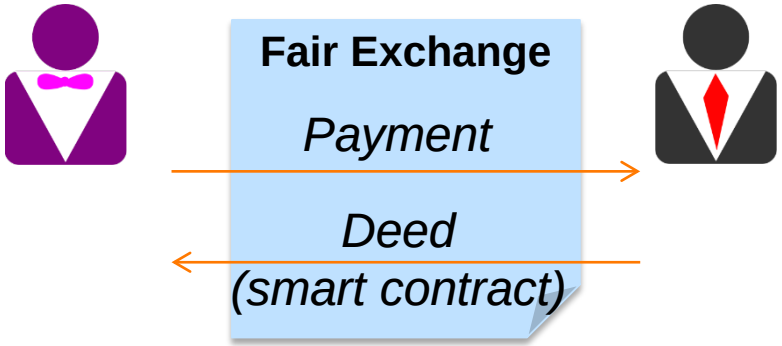
How can we use blockchains in new ways?

Improving optimistic fair exchange using a blockhain



Improving *timeliness* of cryptocurrency transactions

But Bob does not know when the contract becomes valid!



Jian Liu

Aalto University

NEC

Java API for Trusted Execution Environments

NordSecMob
Master's Programme in Security and Mobile Computing

How can a Java developer use a GlobalPlatform-compliant Trusted Execution Environment?

Realizing GlobalPlatform TEE Client API in Java:

1. Full coverage of functionality;
2. Conforming to Java conventions;
3. Easy to use: no need for native code.

Prototype implementation using Open-TEE and OmniShare.

```
ret = TEEC_InitializeContext(&context, ...);
if( ret != TEEC_SUCCESS ) return ret;
ret = TEEC_OpenSession(&context, &session, ...);
operation.params[0].memref.parent = &shared_memory;
operation.params[1].value.a = a;
operation.params[1].value.b = b;
ret = TEEC_InvokeCommand(&session, CMD_DO_ENC, &operation,
&retOrigin);
```

GP TEE Client API example

```
try {       ITEEClient.IContext context = client.initializeContext(...);
            ITEEClient.ISession session = context.openSession(...);
            ITEEClient.IValue value = client.newValue(a, b, ...);
            ITEEClient.IRegisteredMemoryReference rmr =
client.newRegisteredMemoryReference(shared_memory, ...);
            ITEEClient.IOperation operation = client.newOperation(rmr,
value);
            session.invokeCommand(CMD_DO_ENC, operation);
} catch (TEEClientException e) retOrigin = e.getReturnOrigin();
```

Java API example

Rui Yang

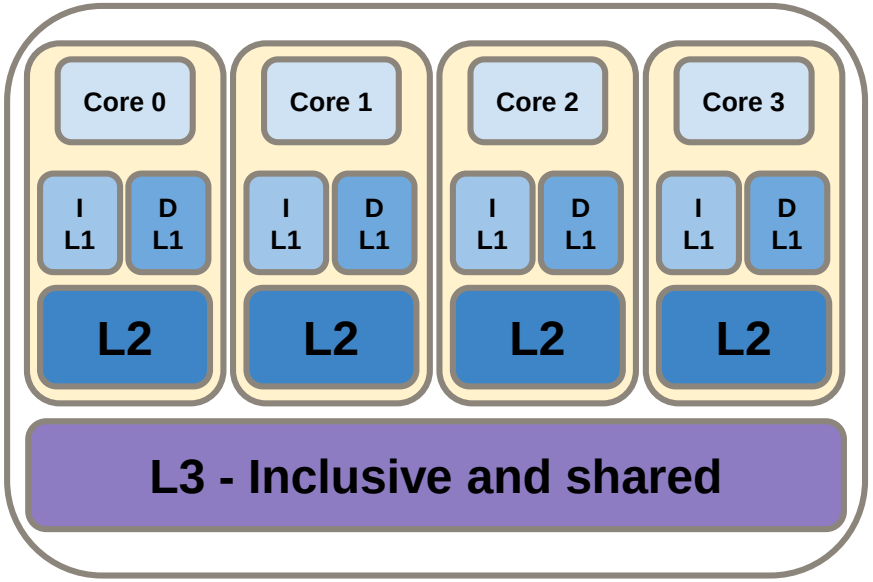
Aalto University

HUAWEI

Let Me CLFLUSH Your Cache: Cache-Timing Techniques

What techniques are used for side-channel cache-timing attacks?

- Trace-driven techniques are powerful.
- Last-Level Cache is the new target.
- Techniques are adaptable to specific algorithms/scenarios.



Cache-timing attacks are a real threat.

Stepping Stone Detection in Software Defined Networks

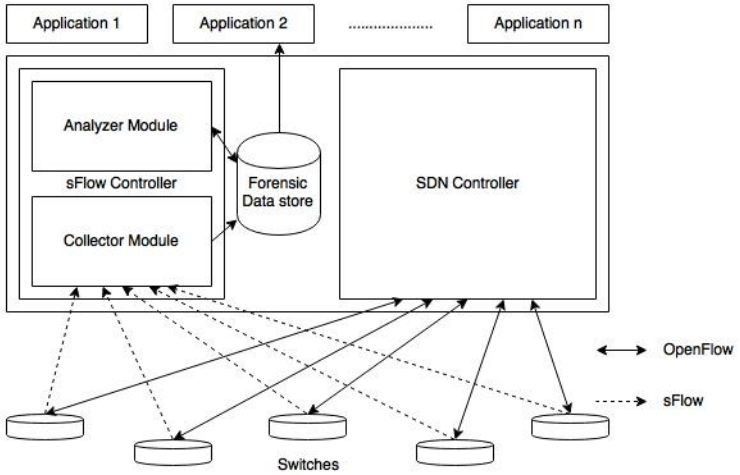
Proposal of an SDN+NFV based architecture that supports stepping stone detection

Detection techniques based on

- Timing of packets, Content-size
- Anomaly-based detection techniques for jitter and chaff

Proposed SDN-based Architecture

- sFlow enabled switches
- Collector and analyzer modules
- Forensic data store



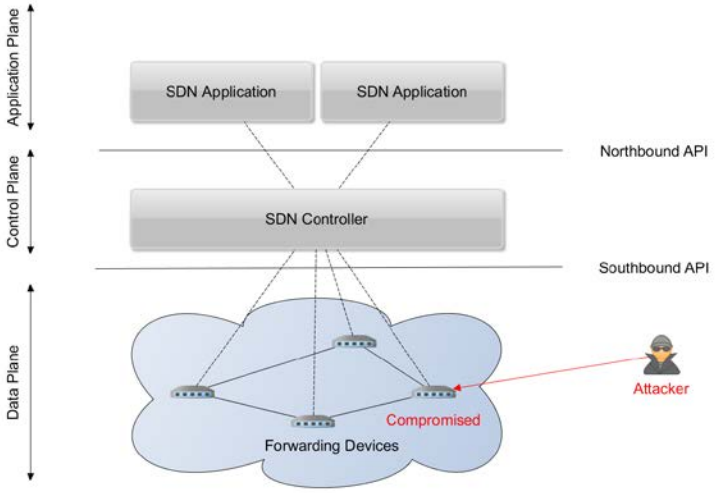
Debopam Bhattacherjee

NordSecMob
Master's Programme in Security and Mobile Computing

Security Testing SDN Controllers

Improve the software quality of open-source SDN controllers

- Fuzz testing
- Targets: OpenDaylight and ONOS SDN controllers
- Threat modeling



- Several vulnerabilities found

Andi Bidaj

Aalto University

Tekes

Potentially Unwanted Programs

How to automate PUP Installer analysis?

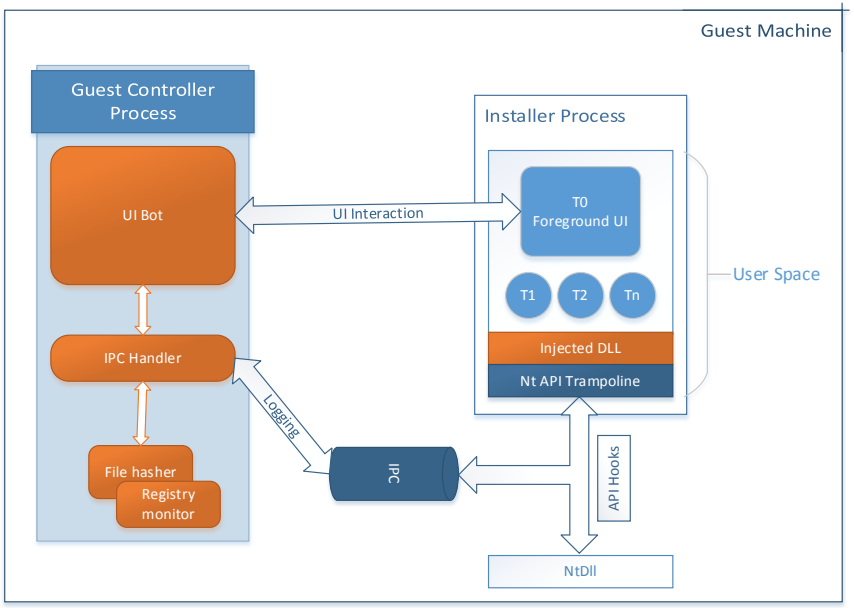
Freeware installers are notorious for bundling *potentially unwanted programs* (toolbars etc.) alongside with the applications they are expected to install.

→ Automate interaction with installer UI

→ Dynamic malware analysis techniques to track fs / registry changes

→ Track back affected files to their network origin

→ Virtualization/Metalization & Cloud support

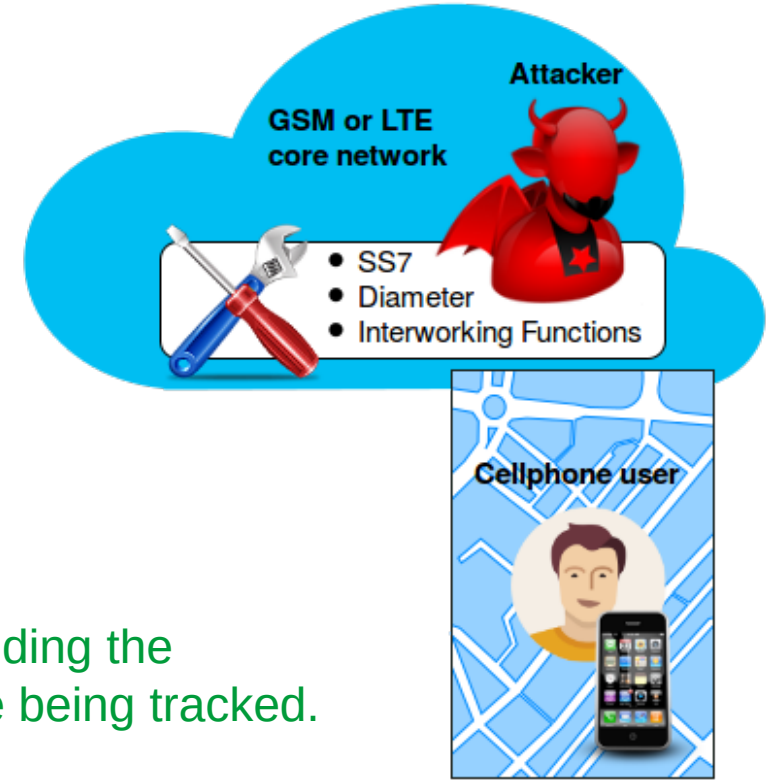


Alberto Geniola

Cellular location tracking attacks using signaling protocols

How accurately can attackers track your cellphone location?

- Attackers can misuse the signaling protocols (SS7) to track the location within 2G/GSM networks.
- Interoperability functionalities make 4G/LTE networks as vulnerable as their predecessors.
- Such methods have also been used for mass surveillance.



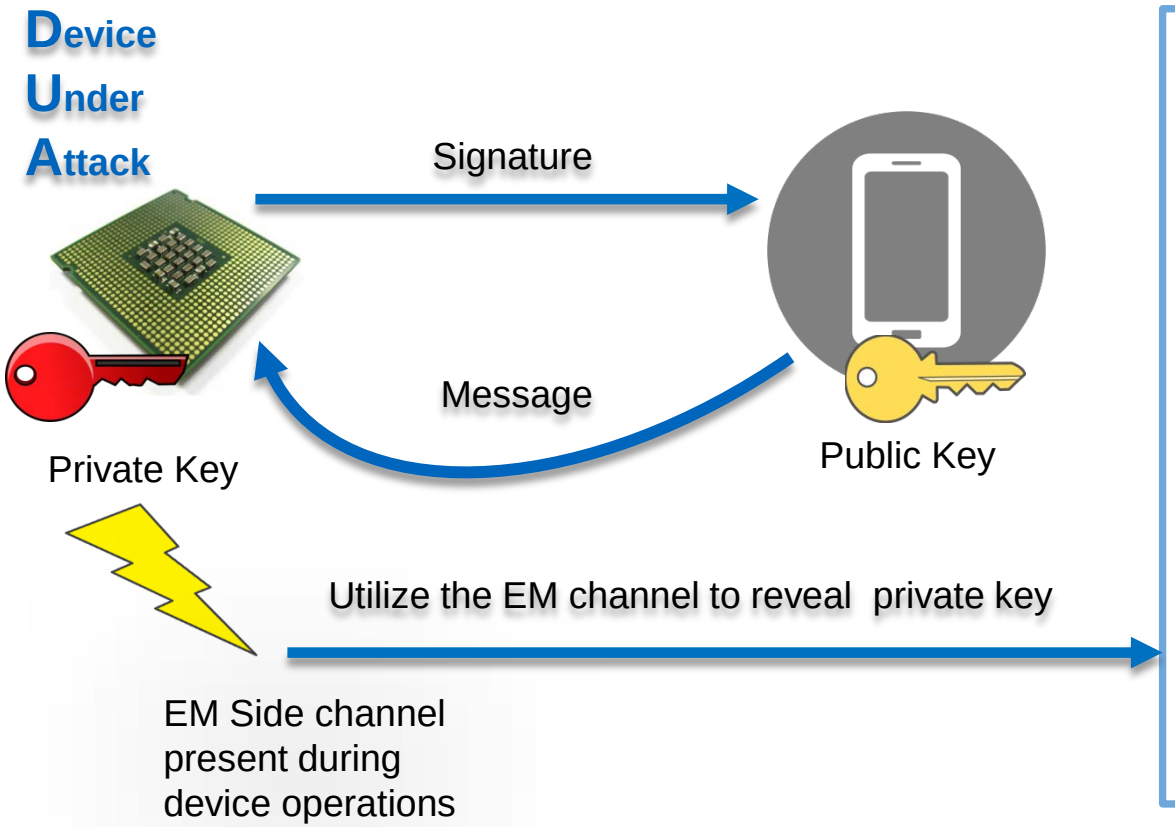
There is no way that the end-users (including the telecom experts) will realize that they are being tracked.

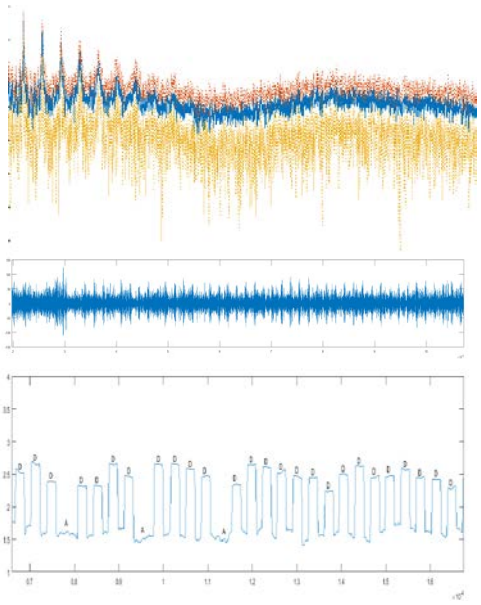
Siddharth Rao

Visitor Demos

EM Side Channel Analysis on Complex SoC Architectures

Can your device radiate secrets ?

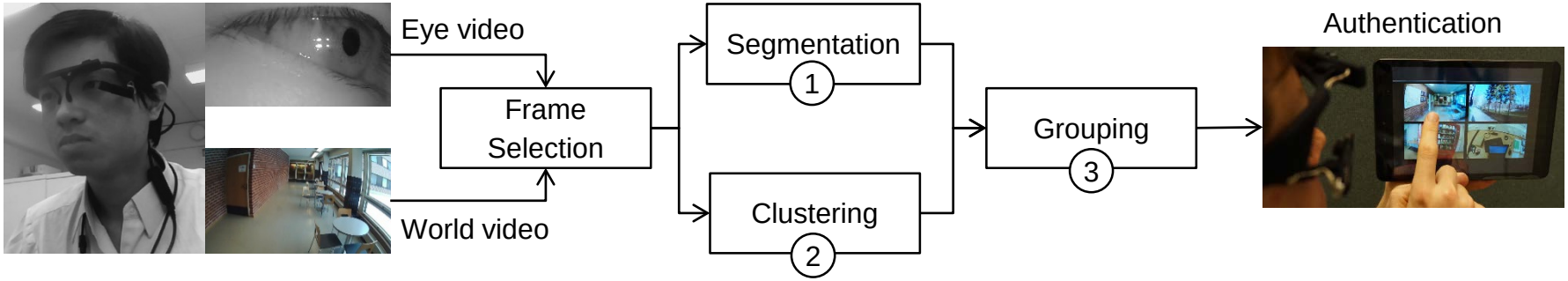


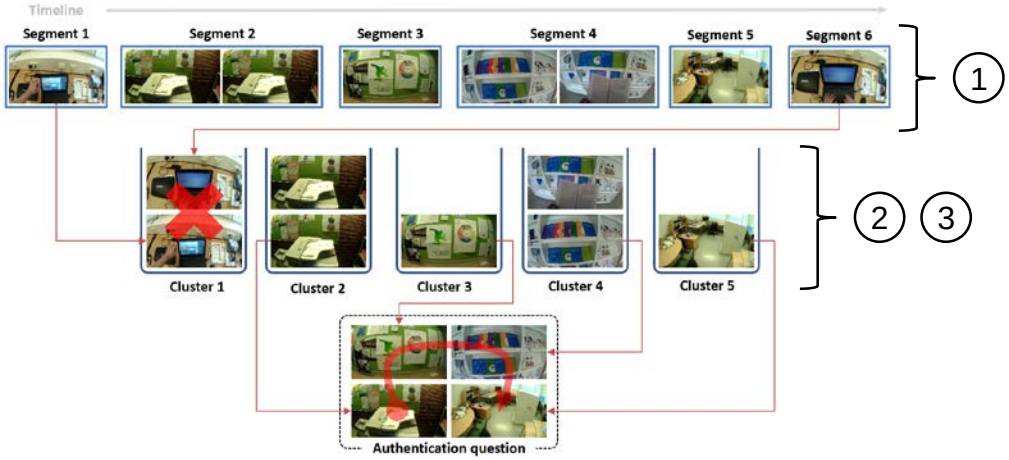


c5df277b41d6cc4067decf09
2e98591171535de7a3605c
89cf6894174cd51832

Authentication based on egocentric vision

How to exploit egocentric videos to authenticate users?





- Authentication password: a set of images
- User authentication: re-arranging the images
- Selection criteria:
  - ✓ High memorability
  - ✓ Low popularity
- Temporal segmentation: discriminating scenes
- Clustering: removing repetitive scenes

The password is what you have seen

Le Nguyen Ngu Nguyen

Where do we go next?

2014
DemoDay

- Secure Systems will continue at UH
  - Hien Truong continues as postdoc ✓
  - I will be actively involved ✓
  - UH will recruit a new professor for information security ✓
- My wishlist
  - Aalto and UH Secure Systems groups work together ✓
  - Courses in both universities open to both universities ✓
  - Supervision across university boundaries ✓
  - Industry collaboration to attract the best students

Thank you for coming!
We appreciate your feedback.

Next:
Library:

Coffee served outside the library
13:15 – 16:00 Demos & Posters
15:00 Joint Aalto-UH announcement by Deans/Heads