Aalto University

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Secure Systems Groups

Demo Day 2017

N. Asokan, Tuomas Aura, Valtteri Niemi

“State of the Union”

Who are we?

Aalto University

- **2 professors**
- **6 (3+2+1) postdocs**
- **Several PhD/MSc students and research interns**

University of Helsinki

- **1 Professor**
- **2 senior researchers**
- **2 postdocs**
- **Several PhD/MSc students**

How are we funded?

CyberTrust SHOK (Aalto and UH) (→ summer ’17)

3 Academy of Finland projects:

ConSec (→ summer ’17), SELIoT (spring ’17 →), SecureConnect (autumn ’16 →)

BCon (autumn ’17 →) (Blockchains, Consensus and Beyond)

2 Tekes projects:

CloSer (autumn ’16 →), Take5 (autumn ’16 →)

Intel Collaborative Research Center for Secure Computing (Aalto and UH Nodes)

Other industry collaboration: NEC Labs, Ericsson (Aalto), Huawei (UH)

Basic funding from universities (Aalto and UH)

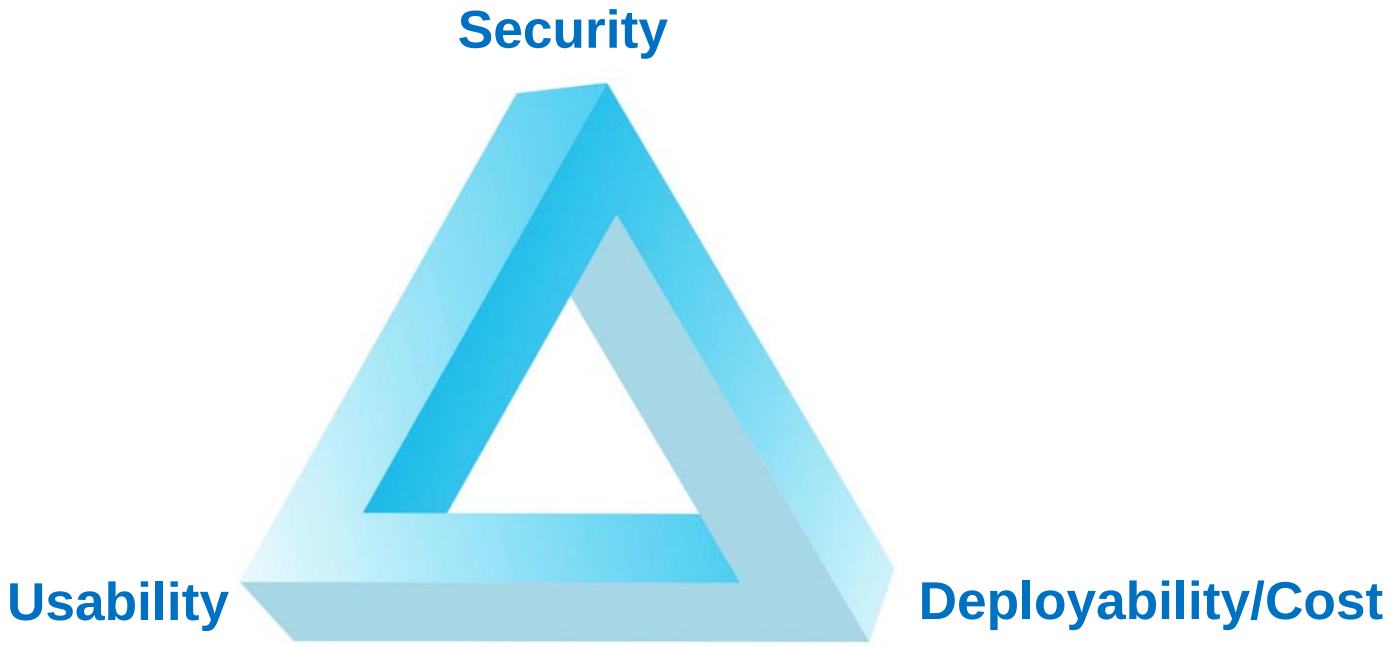
What do we work on?

(Mobile) Platform Security
Machine Learning and Security
Cloud and IoT Security
Blockchains and consensus
New direction: Stylometry and security

5G Security

Security Protocol Engineering
Network Security
Security for Ubiquitous Computing

What do we work on?



Where are we publishing?

Top-tier infosec venues: ACM CCS

Other top-tier venues: IEEE ICDCS (2), IEEE Trans. Comput., IEEE/ACM DAC

Focused thematic venues: PETS, SECON

Other venues: ACM ASIACCS, IEEE IC, NSS

Recognition: **Best poster, IEEE ICDCS**
Honorable mention for best paper, ACM ASIACCS

What are we teaching?

Information Security courses

- **Bachelor level course on Information Security**
- **MSc level courses on network security, cryptography, mobile system security**
- **Seminar and laboratory courses**
- **MOOC: Cybersecurity Base with F-Secure**
- **Shared courses between Aalto and UH**

Courses taught by industry experts

- **Reverse engineering Malware(F-Secure)**

Recognition: **Teacher of the year (Aura)**
Top-5 among small courses
Best Infosec thesis in Finland

Helsinki-Aalto Center for Information Security
HAIC

June 2016: Strategic initiative by Aalto and UH Deans of Science

Initial focus: attract top students to our MSc programs in information security

Spring 2017: Tuition waivers (Aalto, UH), funding for “honours contracts” (Aalto)

Spring 2017: Reached out to industry for donations

F-Secure and Intel (HAIC donors), Nixu (HAIC supporter)

Summer 2017: 3 HAIC scholars (Aalto), 1 HAIC scholar (UH), Annual Report

Call to action: donors for next year

https://haic.aalto.fi/

“Demo/Poster Teasers”

Aalto SSG posters/demos

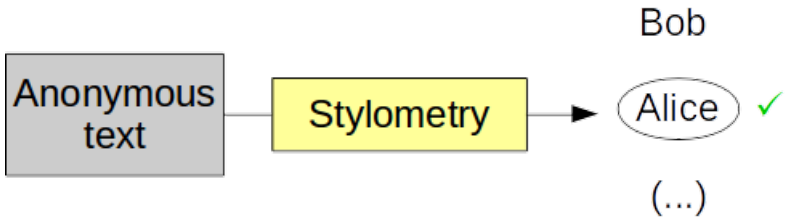
Stylometry and Information Security

How can stylometric techniques be used in security/privacy appications?

Stylometry: text classification (author, text type etc.) based on linguistic style

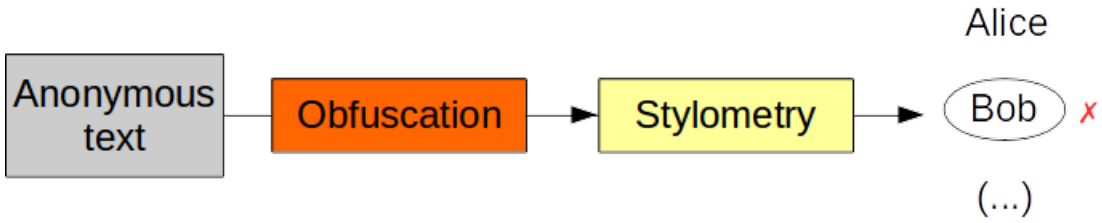
Using stylometry in security analysis

- Detecting online deception
- Classifying troll-messages
- Detecting threats and cyberbullying
- Connecting multiple identities of an author



Adversarial stylometry

- Anonymization via text style obfuscation
- Methods:
  - Manual
  - Computer-assisted
  - Automatic



Detecting Fake Base Stations with Accurate Positioning

How to detect fake base stations based on signal strength and estimated location?

Fake base station detectors exist but:

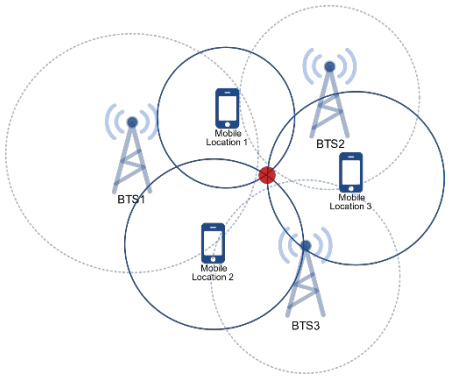
- How to prevent user device from talking to base station prior to detection?
- What if attacker imitates genuine base station details (LAC, CID, MNC, MCC)?

Proposed approach:

- Locate base station using signal power.
- Approximate path loss function using ML with regards to topography.

Add on top of existing solutions:

- Power estimation
- Position estimation



Security analysis of direct carrier billing

Poster

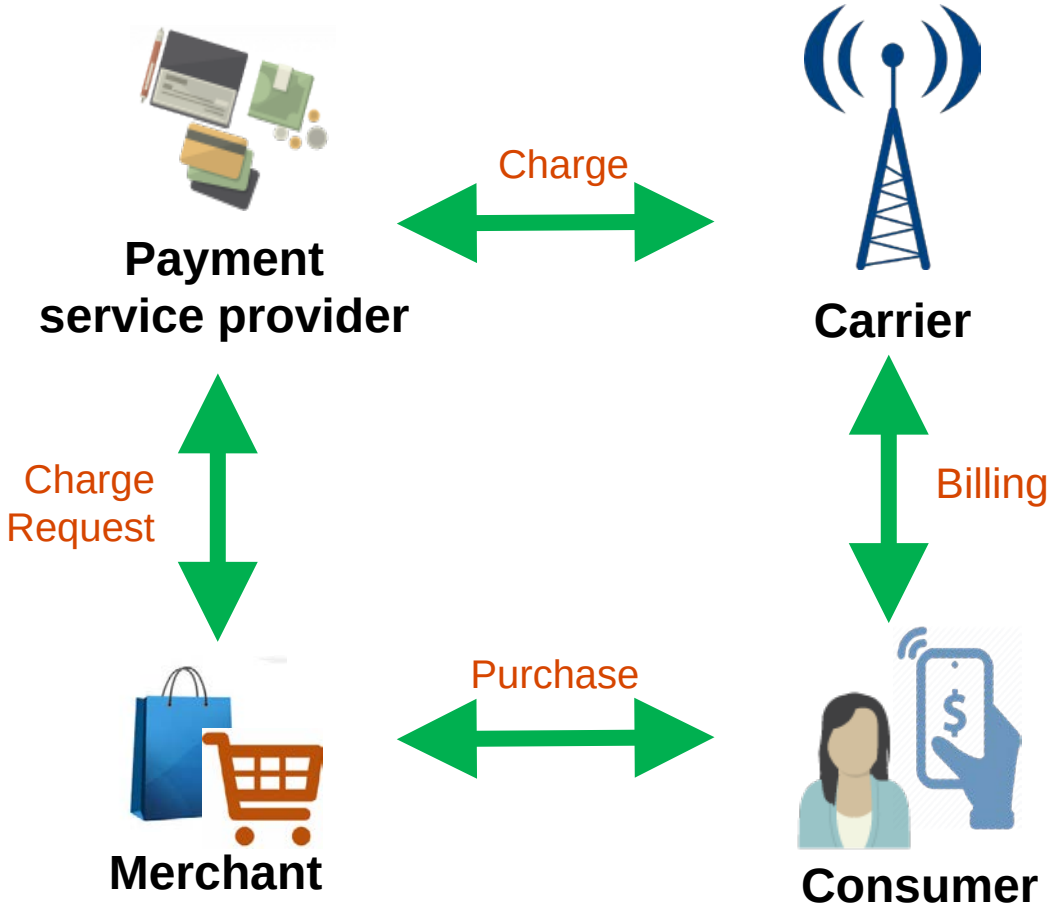
Demo

Can merchants, carriers and payment service providers be trusted with this payment method?

Security Observed

- Access to the service relies on Identification / Authentication features of 3G / 4G networks.
- HMAC codes to authenticate and protect the integrity of messages during the transaction.
- Tokenization to mask sensitive data.
- In-App security checks.
- User acount linked to the phone number.

Vulnerabilities already discovered.



Nadin Vazquez Torralba

Linux Kernel Memory Safety

How to prevent spatial and temporal memory errors in the Linux kernel?

Prevent Ref. Counter overflows

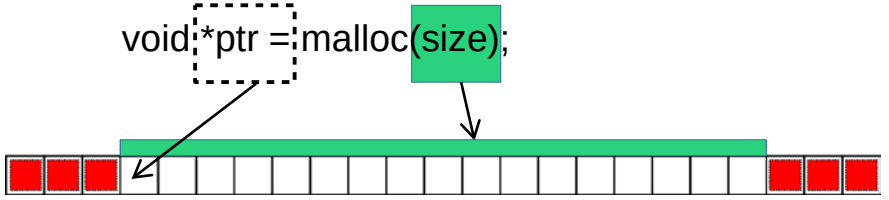
- Contribute to upstream kernel via KSPP
- PaX/Grsecurity based feature
  - High-performance, safe-by-default
  - High maintenance overhead
- New design *refcount_t*
  - Generic implementation, still in flux
  - Restricted API discourages unsafe use
- Working on kernel wide adoption
  - 233 patches submitted, ~70 landed

```
01  if (refcount_dec_and_test(obj->refc) {
02      free_obj(obj);
03  }
```

bit.ly/ssg-kernel

Use Intel MPX for pointer bound checks

- Intel MPX support unwieldy for in-kernel
  - Large memory use
  - Reliance on Page Faults
- Adapt MPX for in-kernel usage
  - Support modular coverage
  - Bounds from kernel MM metadata
  - Using custom Linux GCC-plugin
- Working prototype with basic functionality



Hans Liljestrand

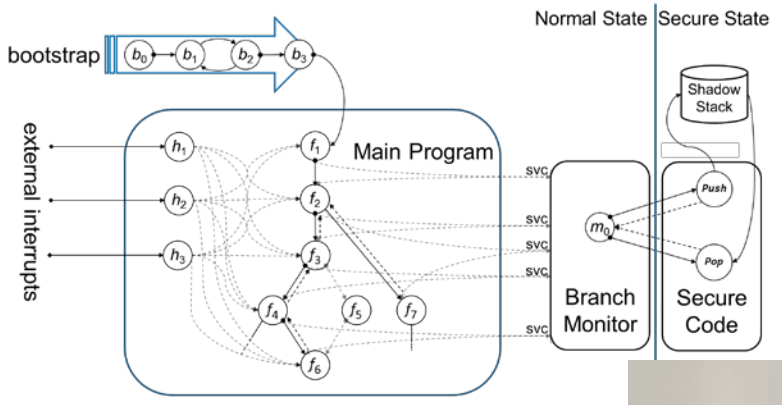
Poster

Hardware-supported Call and Return Enforcement for Commercial Microcontrollers

How can Control-Flow Integrity be realized on low-end IoT devices?

CFI CaRE

- First interrupt-aware CFI scheme for low-end (ARM) microcontrollers
- Hardware-based shadow stack protection using ARM TrustZone-M
- Memory layout-preserving binary instrumentation realizable on-device
- PoC implementation on ARM Versatile Express MPS2+



CaRE architecture overview

PoC implementation platform

https://arxiv.org/abs/1706.05715

Thomas Nyman

Poster

Demo

HardScope: Thwarting DOP with Hardware-assisted Rn-time Scope Enforcement

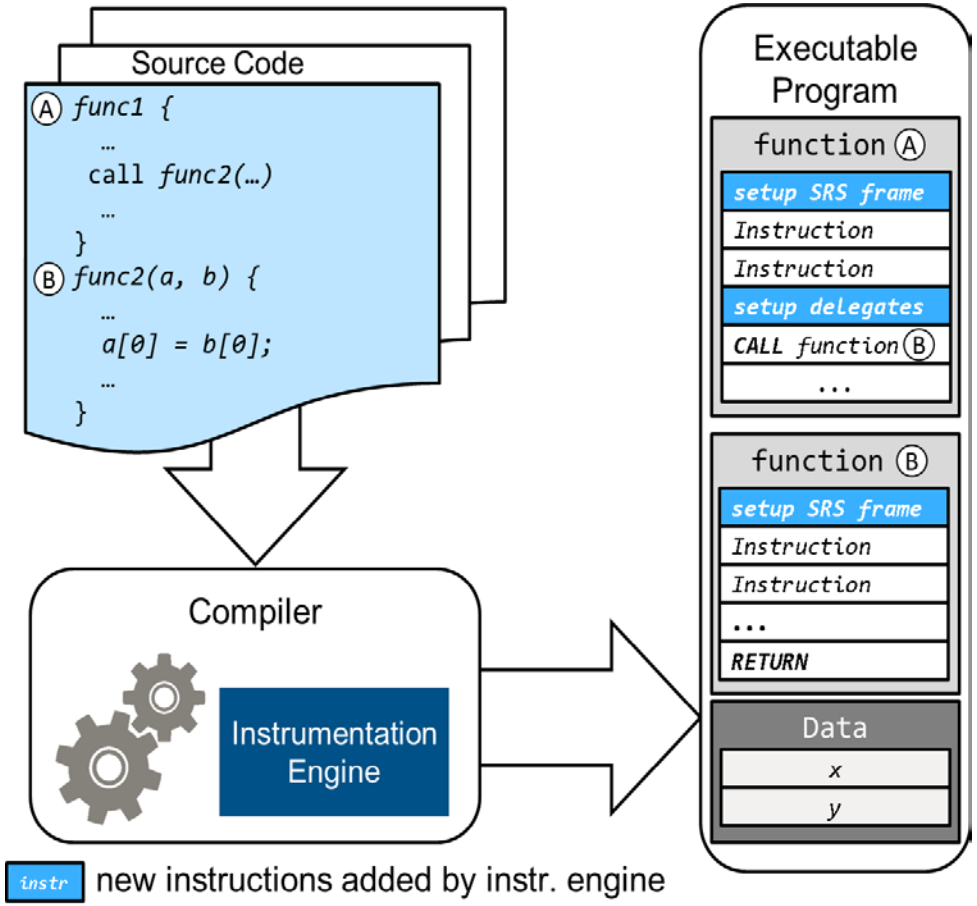
How to defend against Data-Oriented Programming attacks?

Existing security features (*NX*, *ASLR*, *CFI*) cannot resist Data-Oriented Programming (DOP) attacks

DOP attacks access out-of-scope data in memory

HardScope

- enforces variable visibility rules at run-time to stop DOP attacks
- new instructions, compile-time instrumentation, processor h/w extension
- implementation on RISC-V (simulator, h/w) and compiler support



https://arxiv.org/abs/1705.10295

Poster

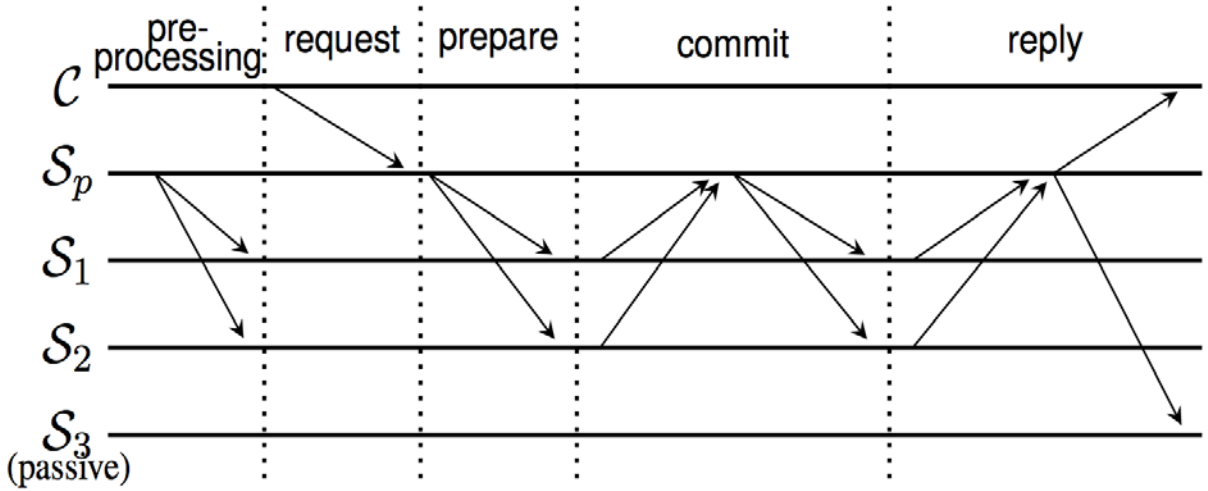
Scalable Byzantine Consensus via Hardware-assisted Secret Sharing

How to improve speed and scalability of blockchain consensus?

FastBFT uses hardware-based TEEs

Fastest and most scalable Byzantine Fault Tolerant (BFT) protocol to-date

Framework representing various design choices;



Improved complexity

- Communication: $O(n^2)$ to $O(n)$
- Computation: minimize public-key operation

Optimized number of active replicas

- Balanced load
- Strong resilience

https://arxiv.org/abs/1612.04997

Jian Liu

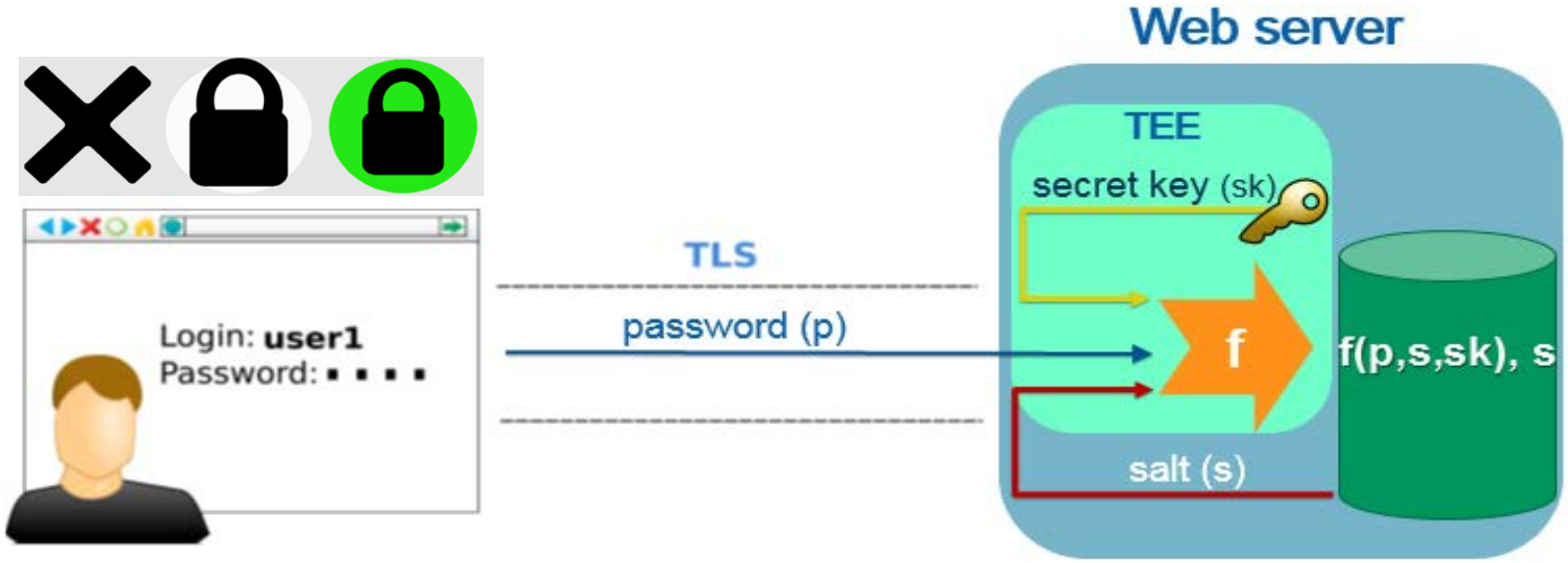
Protecting Web Credentials with Trusted Hardware

Poster

Demo

SAFE KEEPER

How to prevent password database breaches using off-the-shelf hardware and without affecting the performance?



- Browser extension that checks if a web server uses SafeKeeper.
- User study with 64 participants showed that average efficiency is nearly 87%.

- Web server applies keyed one-way function.
- Key protected in Trusted Execution Environment.
- Prototype using Intel SGX adds less than 2% performance overhead.

Klaudia Krawiecka

Improving Security and Efficiency of Blockchain-based Cryptocurrencies

How to prevent double-spending in cryptocurrencies?

Problem: Double-spending attack

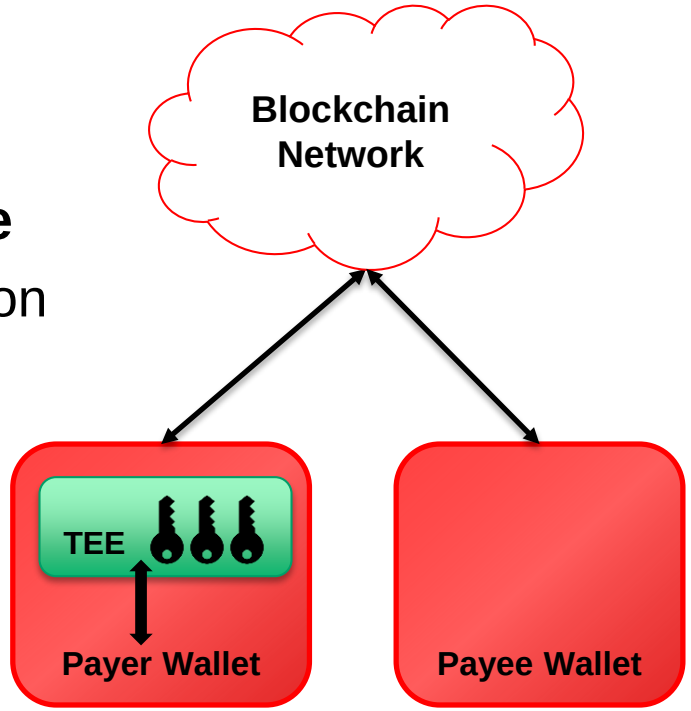
- Malicious payer can double-spend bitcoins
- Bitcoin recommends waiting for 6 blocks (60 mins)
- Payee can accept payments sooner, but risks loss

Solution: Use Trusted Execution Environment (TEE) to enforce

- Sign-once semantics – Ensure each key signs only one transaction
- Verifiable guarantee to payee – Remote Attestation quote

Proof-of-Concept using Intel SGX technology

- No modifications to Bitcoin protocol or miners
- Instant Bitcoin payments; similar to credit cards



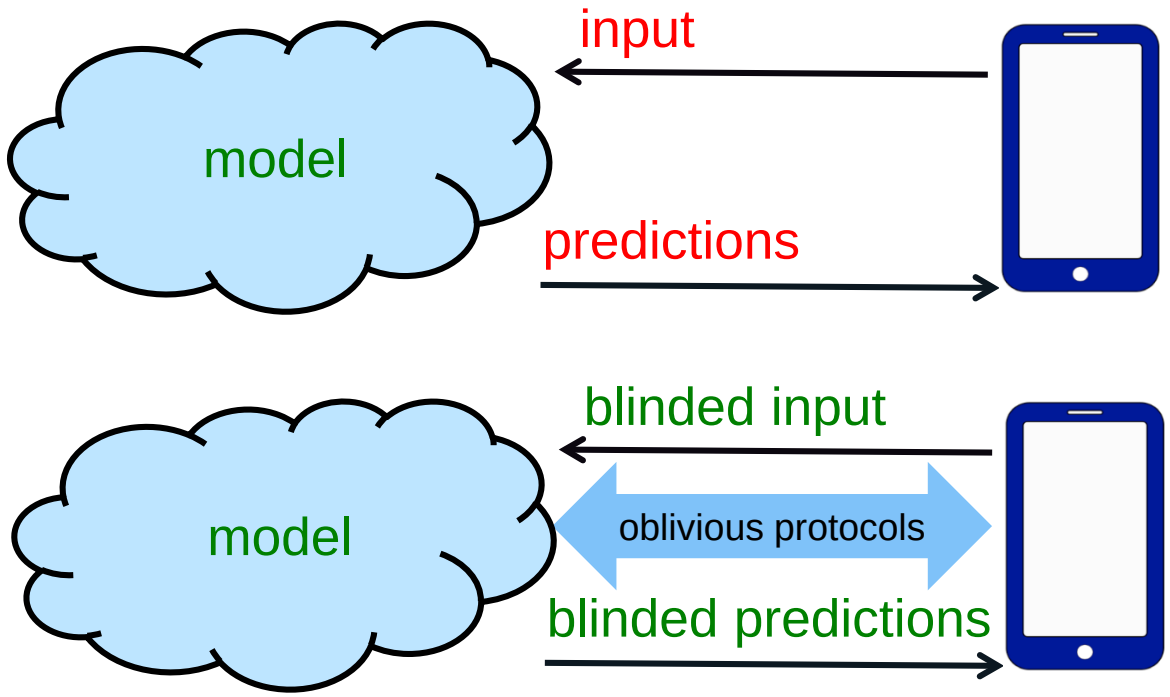
Rakesh Gopinath Nirmala

Poster

Demo

Oblivious Neural Network Predictions via MiniONN Transformations

How to preserve privacy in machine learning predictions?



Cloud-based prediction models increasingly popular but risk privacy:

- clients disclose potentially sensitive input data to server.

MiniONN allows any neural network to be made privacy-preserving

- server does not learn clients' input;
- clients learn nothing about the model;
- More general, significantly faster than prior work.

https://eprint.iacr.org/2017/452

Jian Liu

Poster

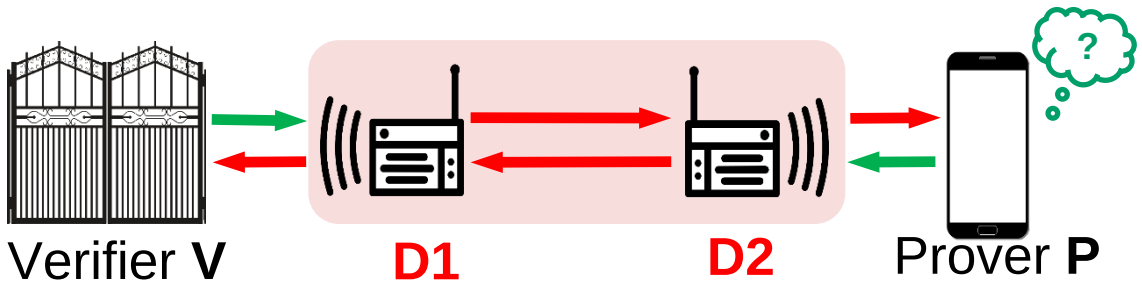
Demo

Securing Transparent Authentication

Can we make transparent authentication safer with inertial data?

Transparent authentication (TA) protocols very convenient, but insecure due to relay attacks

- User carries a prover device **P** (e.g. key, phone), and verifier device **V** (e.g. gate) senses its proximity
- Attacker can defeat this proximity assumption by deploying a pair of relay devices D1 & D2



STASH

- P participates in TA **iff** current trajectory similar to authorized trajectories to V
  - → Accelerometer & gyroscope measurements
  - → Usability-security tradeoff
- Retains high usability of TA, while resisting fraudulent TA requests

https://wiki.aalto.fi/display/sesy/Contextual+Security+Project

Automated Deauthentication using Web Transaction Analysis

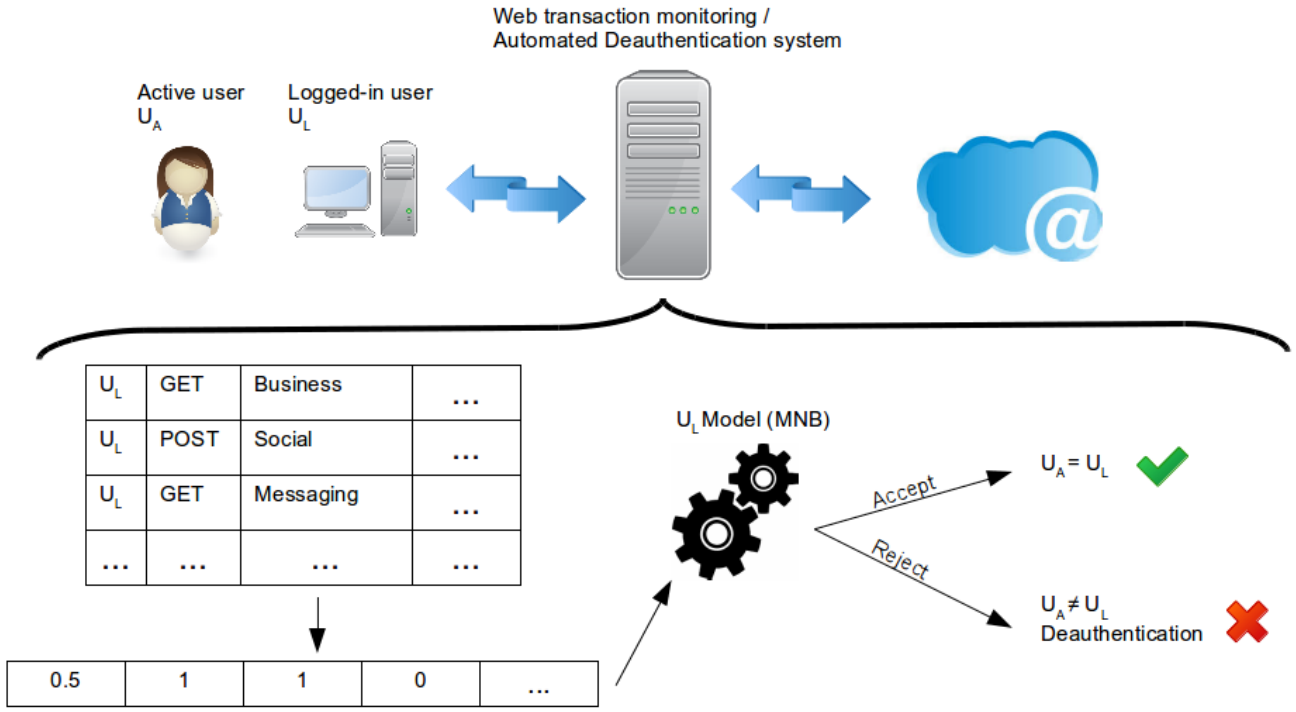
How to detect unauthorized/risky usage of a user account with low overhead ?

Automated Deauthentication systems:

- Mostly rely on biometrics
- Need local software / additional hardware
- Do not prevent malicious behavior of authorized users

Our solution:

- Centralized monitoring: no overhead on client host
- Deauthenticates logged-in user deviating from the expected/learned behavior
- Speed: 5.5 minutes
- Accuracy: Recall = 54.5%, FPR = 3.3%



Radek Tomšů

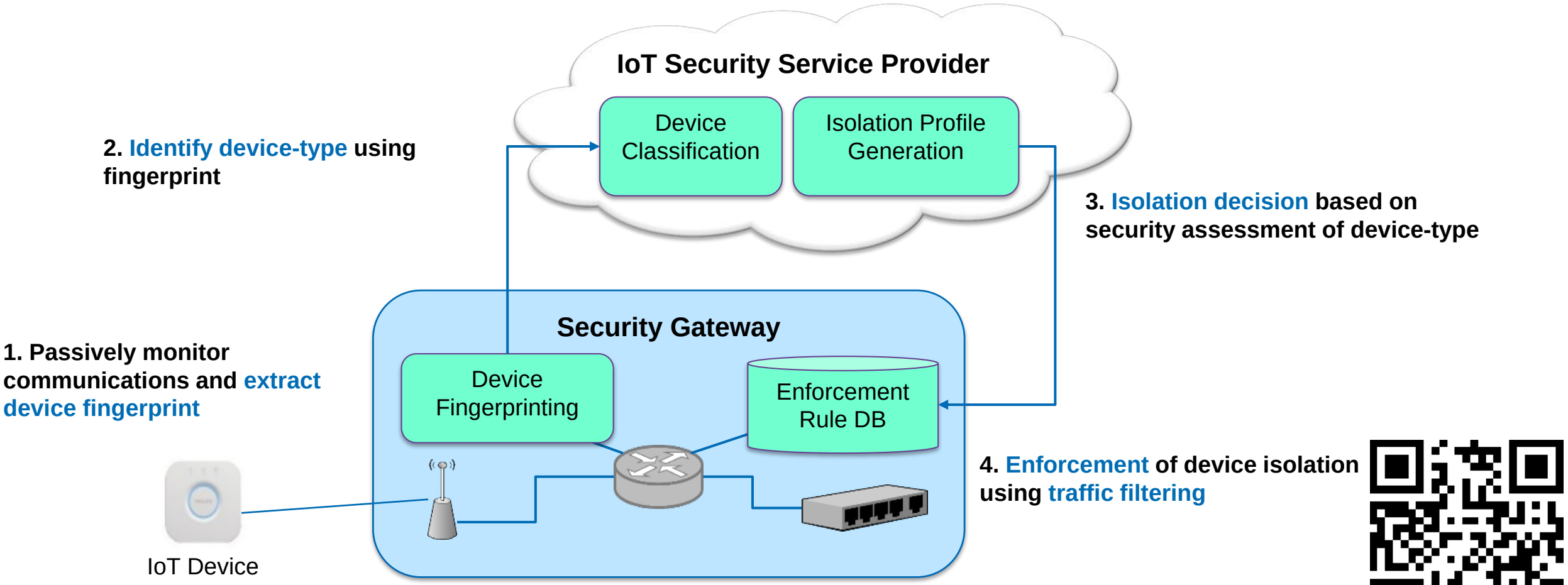
https://arxiv.org/abs/1703.09745

Poster

Demo

IoT Sentinel: Automated device-type identification for security enforcement in IoT

How to protect smart home network from inherently vulnerable IoT devices ?



Samuel Marchal

https://arxiv.org/abs/1611.04880

Poster

Demo

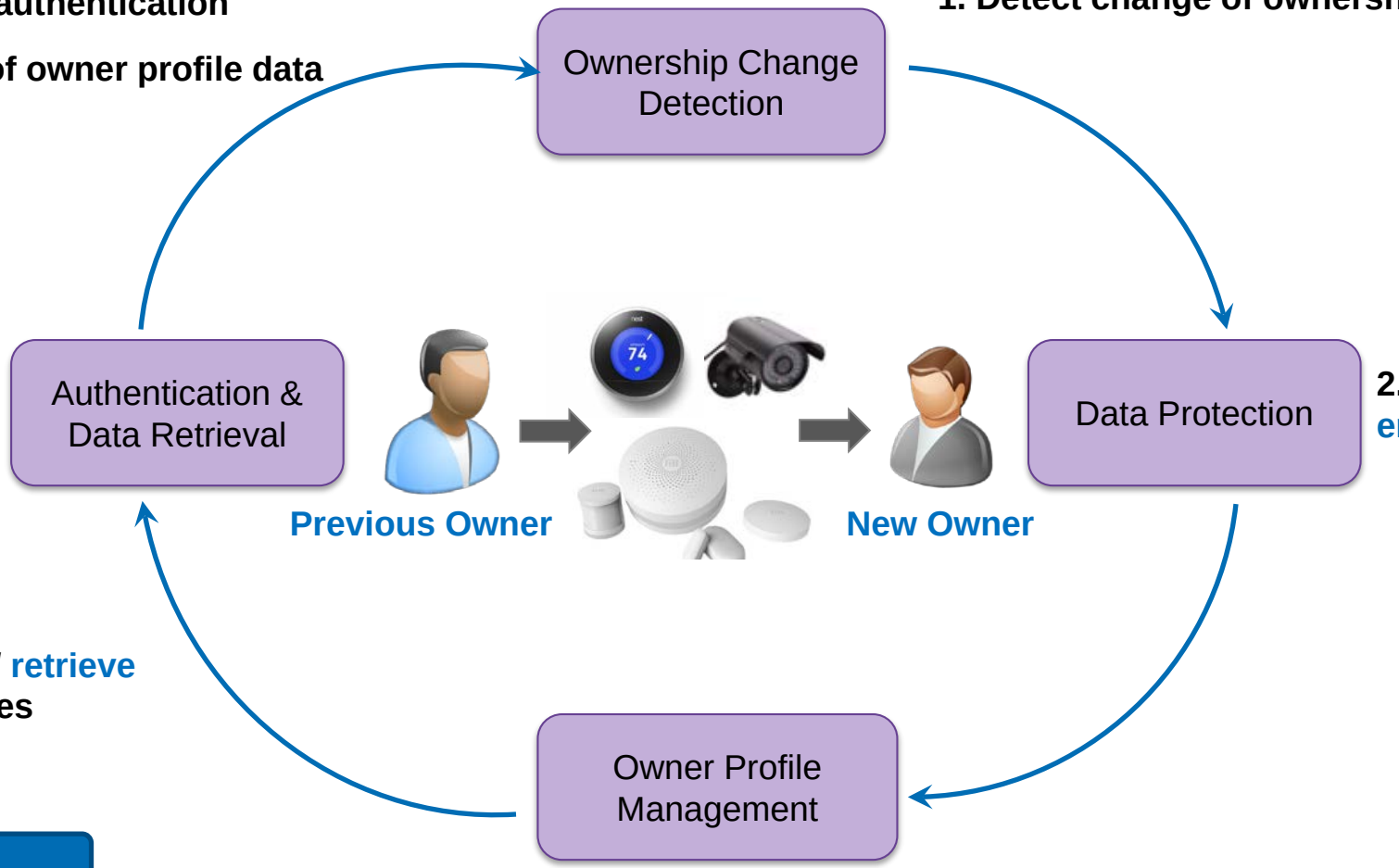
Securing Ownership Change of IoT Devices

How to protect privacy sensitive data during ownership change of IoT devices ?

4. Password based authentication

⟶ decryption of owner profile data

1. Detect change of ownership based on context



2. Protect owner data using encryption

3. Create new profile/ retrieve existing profile profiles

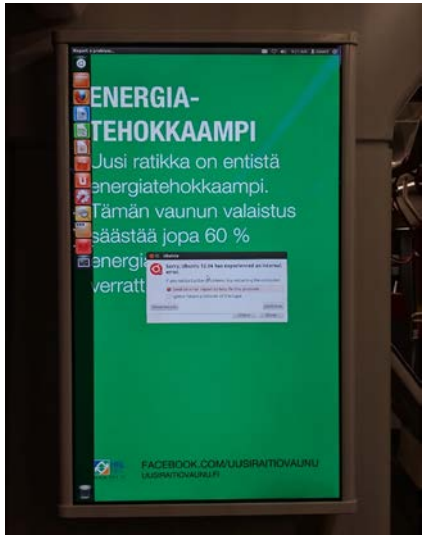
Sakib Khan

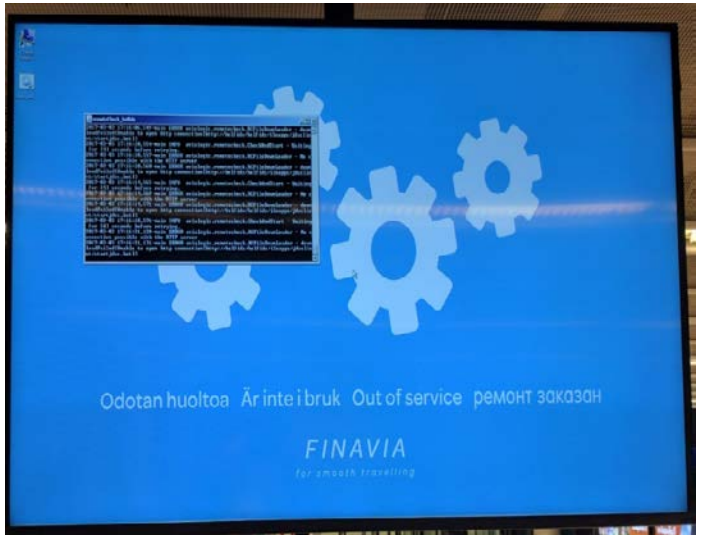
Poster

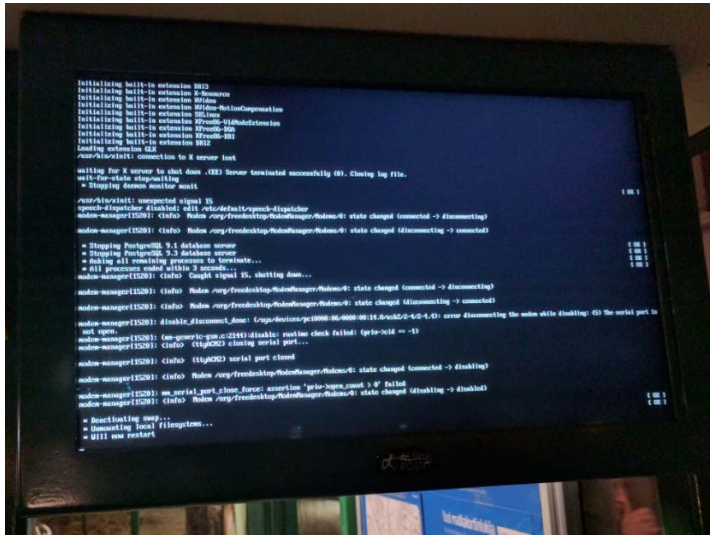
Demo

Remote Monitoring and Failure Recovery of Cloud-Managed Digital Signage

Displays fail everywhere. What can we do?







Better diagnosis and recovery for digital signage failures

- Display sends screenshots and logs to the cloud
- Automated log analysis in cloud
- Display configuration managed remotely
- Management scripts from cloud to the display
- Minimize downtime and on-site service

Ashish Sultania

Poster

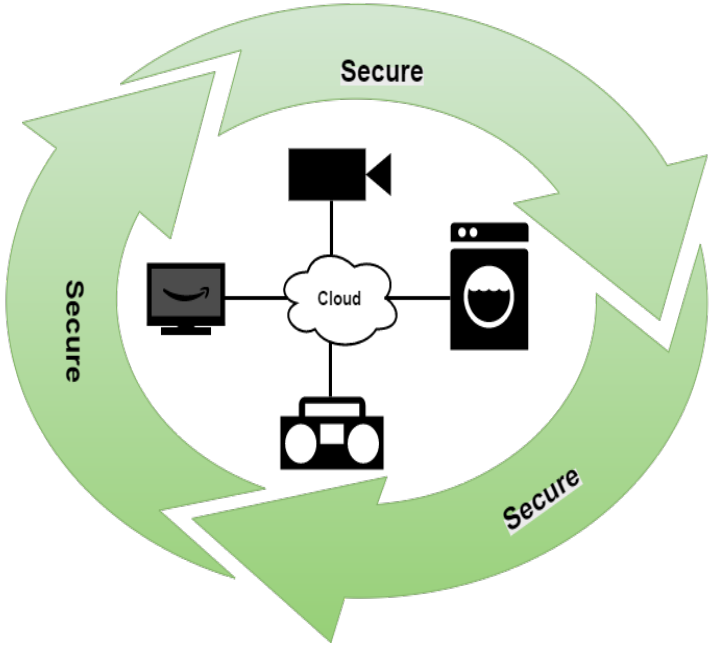
Demo

Enhancements to Secure Bootstrapping of Smart Appliances

How to enhance the EAP-NOOB protocol?

Nimble out-of-band authentication for EAP (EAP-NOOB) is a protocol for simple and secure bootstrapping of IoT appliances

- **Rekeying and Algorithm Agility**
- **Timeouts and Failure Recovery**
- **Handling Parallel Sessions**



- **Access Control to Network Resources**
- **Isolation of IoT Devices**
- **Wired Access**
- **OOB channel with NFC**

Shiva Prasad T P

https://tools.ietf.org/html/draft-aura-eap-noob-02

UH SSG posters/demos

Poster

Demo

PMT with Low Communication Complexity

How to preserve end user privacy when querying cloud-hosted databases?

- **Server** divides its database into 2^{2a} subsets and inserts each subset into a Bloom/Cuckoo filter.
- Divides the filter to $\mathfrak{b}$ fragments and arranges $\mathfrak{b}$ matrices of size $2^a \times 2^a$ with fragments of the filters as their elements.

- **Client** finds the matrix index corresponding to his item x.
- Encrypts the index utilizing Homomorphic Encryption.
- Homomorphic encryption allows **server** to search in the matrix without knowledge of client's private key.
- **Client** decrypts the result : ■ ■ ⋯ ■

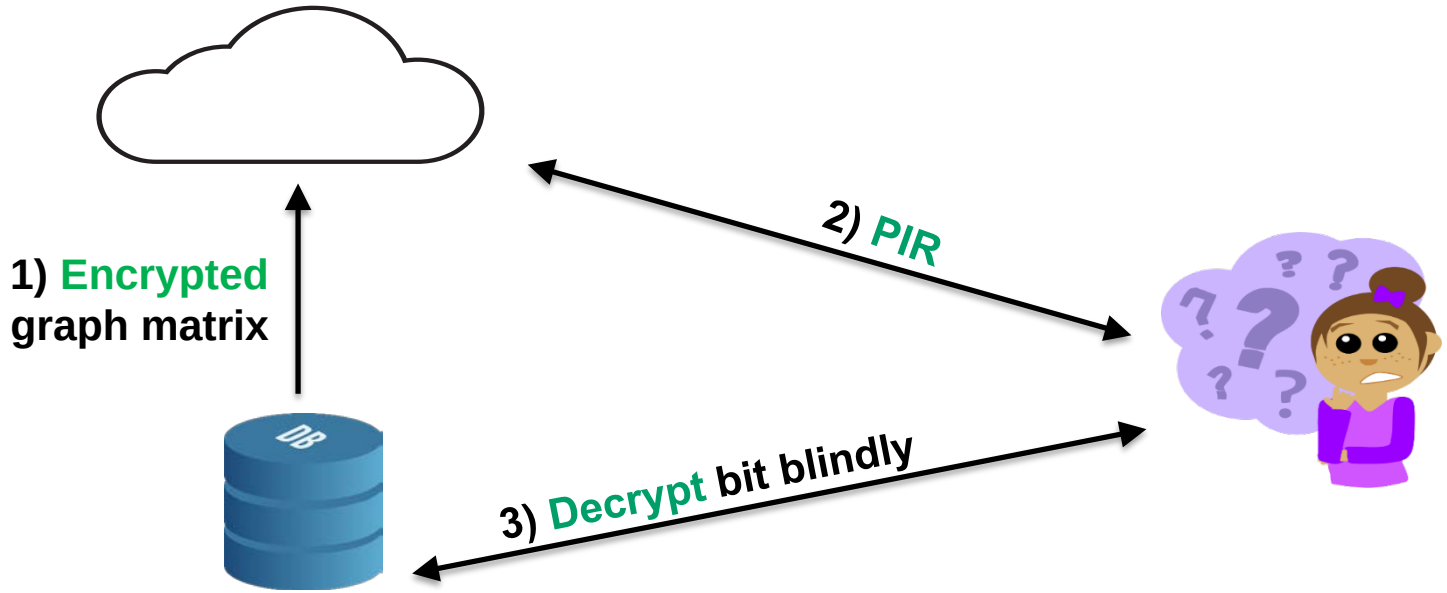
Our implementation shows that this protocol can be used in real world applications, for example, for Android app or website reputation services.

Sara Ramezanian

Private Graph Search

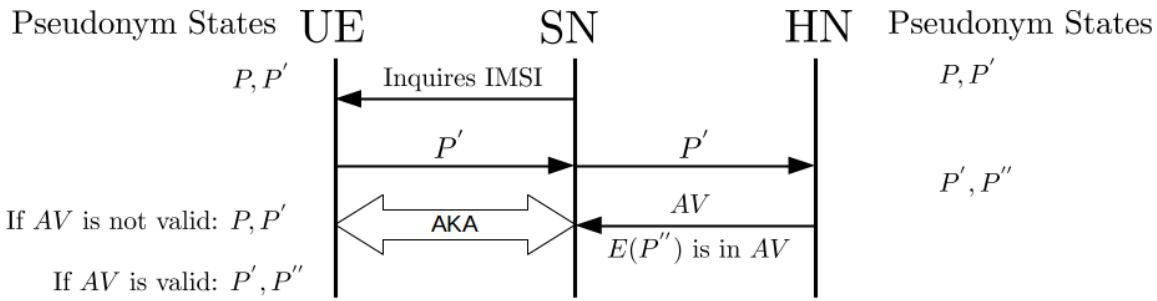
How can an entity query the graph to find "if there is a path from A to B", without sacrificing the privacy?

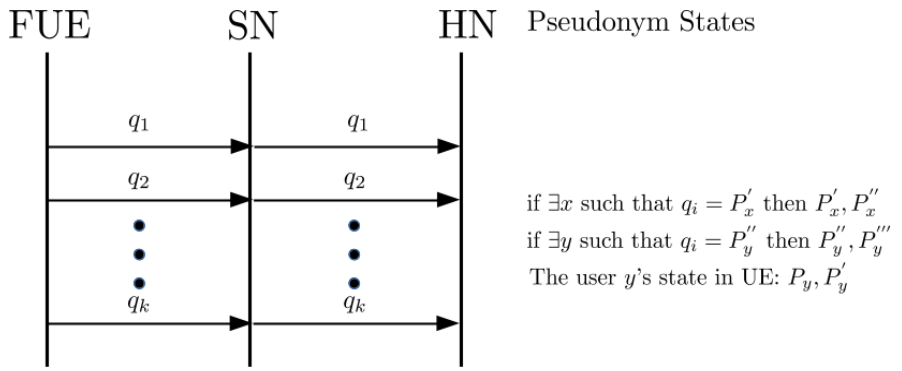
- Two lists of triplets: (user, host, fingerprint) and (fingerprint, user, host), define **trust relations** between users on different hosts.
- This database can be illustrated as a directed graph.
- The graph owner constructs the transitive closure of the directed graph (tc-graph) and stores the tc-graph into a matrix.
- There are three parties involve in this protocol: Owner of the graph, user and the Cloud.



DoS Attack Against a Solution of Identity Privacy in Cellular Network

How can a pseudonym based solution to defeat IMSI-catchers open a vulnerability to DoS?





Defeating IMSI-Catchers Using Pseudonyms

- Temporary identifiers known as pseudonyms are used instead of IMSI
- Home network (HN) generates pseudonyms and send it to user equipment (UE) piggybacked in authentication vector (AV)
- Pseudonyms keep changing according to a agreed protocol

DoS Attack

- The DoS attack is mounted by a fake UE (FUE) against the whole network
- All the users lose synchronization of the pseudonyms with the home network
- A solution to defeat the attack is proposed in the poster

Mohsin Khan

Database leakage attack against a WiFi fingerprint location scheme using Paillier encryption

How to steal the server's database and how to fix the problem?

WiFi fingerprint localization (WFL)

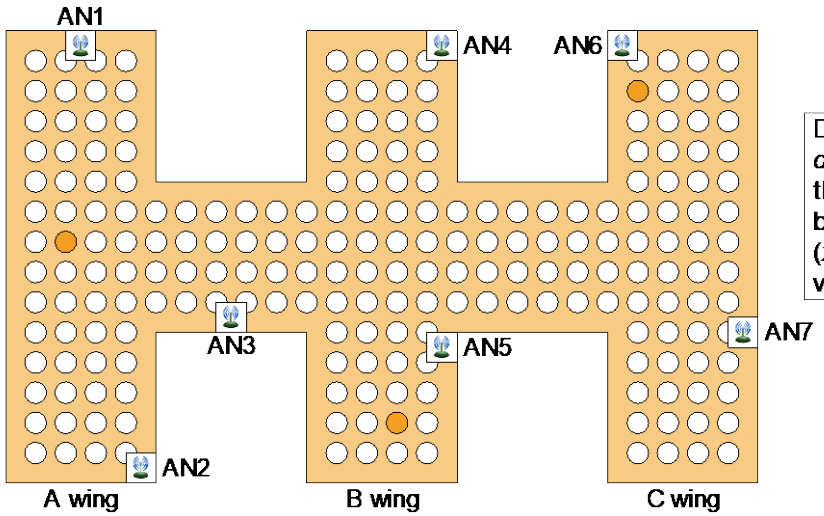
- **User**: Measure and send WiFi signal strengths (RSS)
- **Server**: Calculate the user's location using a RSS database

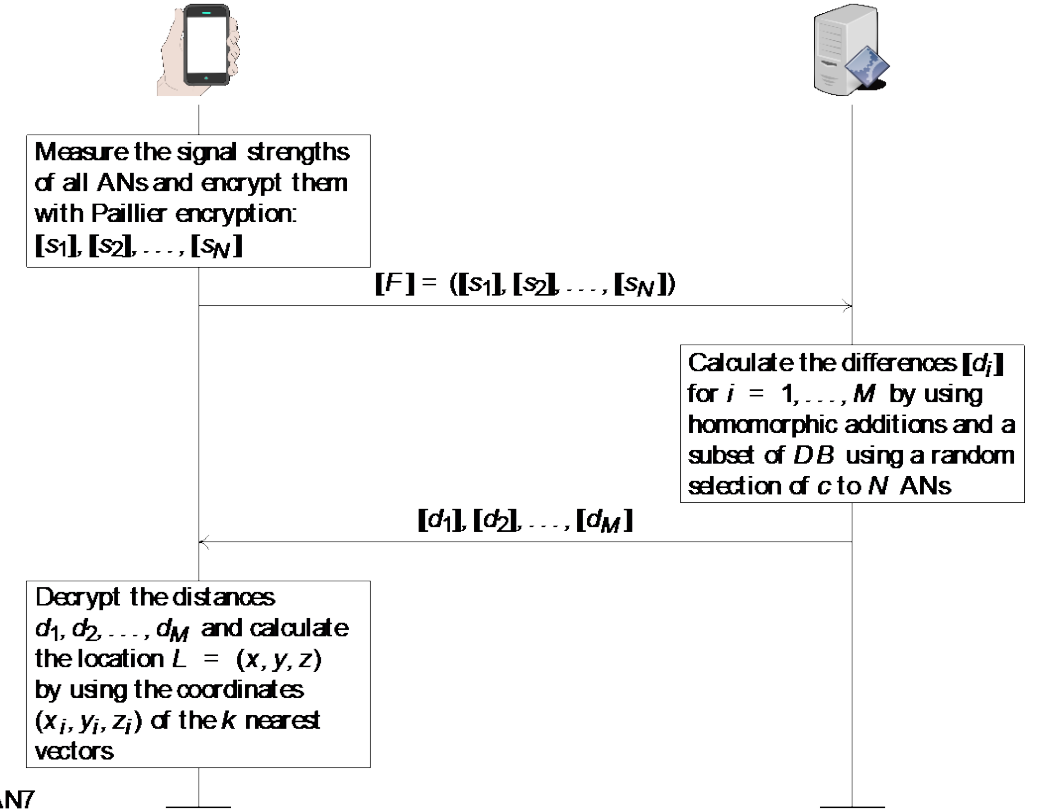
Privacy-Preserving WFL by Li et al. in INFOCOMM'14

- Paillier encryption protects the user's location
- Random masking and selection of ANs protect the database

Our attack fully exposes the server's database

- **A realistic assumption**:
  User knows 2 locations, where an AN is not available, for each AN





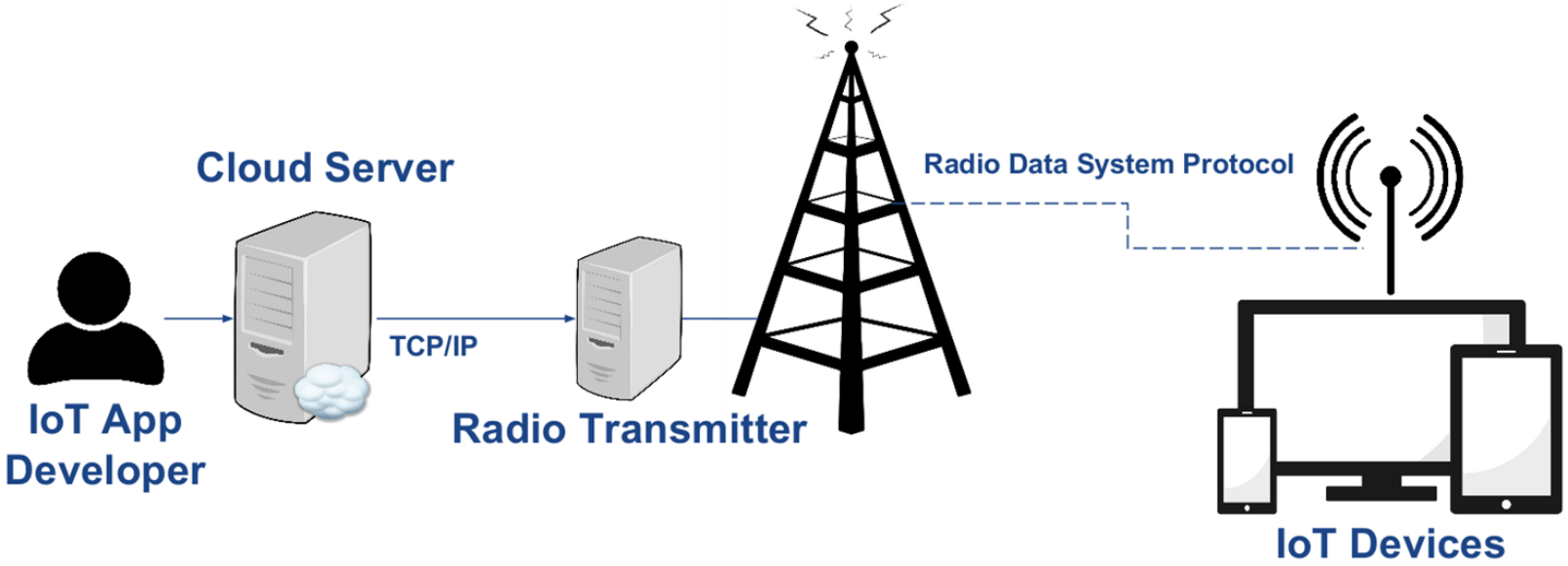
Guest posters/demos

Poster

Demo

IoT Application Provisioning Service

How to realize a software provisioning service for IoT devices using long-range broadcast communications?



Requirements

- Each app is bound to a specific class of devices
- IoT devices perform seamless updates
- Two major requirements in the update process: authentication and integrity

What is the value?

- The system does not rely on any specific communication technology as long as it is long-range broadcast digital data
- Cheaper alternative to cellular solutions
- No Internet connection-related security threats on IoT devices

Jose Viquez Zamora

Poster

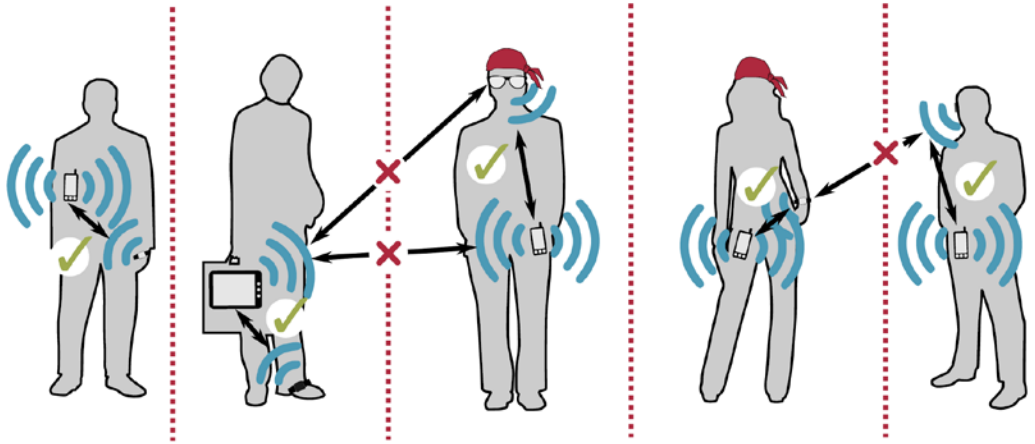
Demo

Context-based Authentication and Device Pairing

How to pair on-body devices without user interaction?

Device pairing schemes exist but:

- Explicit user interaction, e.g. PIN input
- Revocation only with user interaction
- Static pairing



Our approach

- Gait-based device pairing
- Ad-hoc device-to-device authentication
- Secure session confined to context of use

Evaluation

- 15 subjects
- 7 on-body device locations
- 5 locomotion types (walking, running, descending, ascending, jumping)

Poster

Demo

Designed for Security. *LastPass uses leading technologies to secure data and protect user privacy. Our proven security model sets the standard for transparency and best practices.*

-- LastPass Password Manager

Security Evaluation of Password Manager Browser Extensions

LastPass security flaw could have let hackers steal passwords through browser extensions

--theverge.com, March 2017

Password manager OneLogin hit by 'malicious actor' who may be able to de

--wired.co.uk , June 2017

9 Popular Password Manager Apps Found Leaking Your Secrets

--thehackernews.com , Feb 2017

A!

-- Viswanathan Manihatty Bojan, Thanh Bui, Tuomas Aura

F-Secure.

Automated analysis of freeware installers

How to automate the analysis of freeware installers?

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

What we did

- Automated the whole installation process of an application, including UI interaction
- Monitored system modifications during installation (registry and fs access, network)
- Analyzed hundreds of freeware installers crawled from download portals
- The analysis system supports virtualization as well as analysis on bare metal nodes

What we have learned (so far)

- UI automation is possible with relatively simple heuristics
- Freeware installers often download binaries over insecure channel, which are then executed with elevated priviledges (MitM-vulnerability)
- Installers from download portals often distribute PUP, but rarely malware

Aalto University

Alberto Geniola
Markku Antikainen
Tuomas Aura