Secure Systems Groups

Demo Day 2015

N. Asokan, Tuomas Aura, Valtteri Niemi
“State of the Union”
Who are we?

- **Aalto University**
  - 2 professors
  - 1 (+1) postdocs
  - 5 full-time & several industrial PhD students
  - Several MSc thesis students
  - Several interns

- **University of Helsinki**
  - 1 full-time + 1 part-time professor
  - 1 postdoc
  - 1 MSc thesis student
How are we funded?

• Aalto
  – 2 Academy of Finland projects
  – Intel CRI for Secure Computing (ICRI-SC) at Aalto
  – Basic funding from Aalto
  – Research collaboration with Huawei
  – MATINE (Ministry of Defense) project
  – IoT SHOK
  – New: Cyber Trust SHOK

• University of Helsinki
  – Basic funding from UH
  – (close collaboration with ICRI-SC at UH at the NODEs unit)
What do we work on?

- (Mobile) Platform Security
- Contextual Security
- Cloud Security
- 5G Security
- Security Protocol Engineering
- Network Security
- Security for Ubiquitous Computing
What do we work on?

Security

Usability

Deployability
Where are we publishing?

- Proc. IEEE, ACM CCS, **ACM UbiComp**, PMC journal
- ACM WiSec, **ACM ASIACCS**, Financial Crypto
- NordSec, NordiCHI

- Best Paper Awards
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
  – “Malware course” (F-Secure), Software Security (Vähä-Sipilä)
Who did we train?

• Aalto: ~12 MSc theses, ~10 BSc theses
  – Olli Jarva: won best infosec thesis prize (Finnish Information Security Association); runner-up best CS thesis (Finnish Computer Science Association)

• UH: 3 MSc theses

• Invited sessions at summer/winter schools
  – 2014: Padova Summer School, Technion TCE Summer School, Estonian Summer School in Computer Science
Industry Collaboration

• Industry-funded collaborative projects
  – Intel, Huawei

• 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
  – Väestörekisterikeskus (eID), Ministry of Justice (Internet elections), FICORA (cryptography)
Where do we go next?

- 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
Demo Teasers
SEAndroid Policy Analytics

How to enable OEMs to design better SEAndroid policies?

SEAndroid is now mandatory

SEAL: A suite of tools for SEAndroid policy Analytics

Manual analysis: examples of ineffective and potentially unsafe rules added by OEMs
Open Virtual TEE

What is needed to enable app developers to use trusted h/w?

- Open-TEE is a GlobalPlatform (GP)-compliant virtual trusted execution environment (TEE)
  - Intended as a developer aid; can also be a fall-back TEE
- Open-TEE session for **GP App Developers Workshop**

---

Open-TEE

Welcome to the homepage of the Open-TEE project!

The goal of the Open-TEE open source project is to implement a "virtual TEE" compliant with the recent GlobalPlatform TEE specifications.

Our primary motivation for the virtual TEE is to use it as a tool for developers of Trusted Applications and researchers interested in using TEEs or building new protocols and systems on top of it. Although hardware-based TEEs are ubiquitous in smartphones and only ordinary developers do not have access to them. While the emerging GlobalPlatform specifications may change that in the future, a fully functional virtual TEE can help developers and researchers alike.

http://open-tee.github.io/DemoDay

UNIVERSITY OF HELSINKI

Collaborative Research Institute for Secure Computing
Deploying TEE-based Authentication

What do service providers need in order to improve security/privacy in their services using TEEs?

• Support entire user base:
  – Devices with different types of TEEs, no TEEs

• Showcase: eID scheme specified by VRK

Thomas Nyman

https://se-sy.org/projects/eid/
Person authentication in Finland

• **Transaction Authentication Number**
  – One time passcode cards
  – Widely used
  – High logistics costs, controlled by banks

• **Citizen PKI (Kansalaisvarmenne)**
  – Deployed for over a decade
  – Expensive, requires a reader

• “**Mobile PKI**” (**Mobiilivarmenner**)
  – Controlled by mobile carriers
Deploying TEE-based Authentication

What do service providers need in order to improve security/privacy in their services using TEEs?

• Support entire user base:
  – Devices with different types of TEEs, no TEEs

• Showcase: eID scheme specified by VRK
  – TPM 2.0 on a PC
  – Open-TEE on a legacy Android device
  – [Trustonic <t-Base on GS6]
Developing apps for emerging TEEs

How to make it easy for developers to benefit from emerging new TEE architectures?

• “Make it easy for developers to benefit from TEEs”
  – On-board Credentials, Open-TEE, …
  – GlobalPlatform standards

• New TEEs are emerging
  – SGX: Servers and PCs
  – TrustLite, SMART, …: tiny IoT devices
  – Come with their own SDKs, programming paradigms, ..!

• But existing standards are for “split-world” TEEs
  – inspired by “TrustZone”
LookAhead: Augmenting Website Reputation Systems With Predictive Modelling

Can we predict eventual reputation ratings of websites?

Lack of Coverage (e.g., < 36% of top 1-million pages have child-safety rating)
Perils in designing zero-effort deauthentication

How to break a zero-effort deauthentication scheme?

- Deauthentication must be
  - Zero-effort, reliable, fast, cheap
- ZEBRA (IEEE S&P 2014)
  - Bilateral re-authentication
  - Compare “actual” interactions with “inferred” interactions
- We show how to kill ZEBRA

Can still be useful in benign settings
Social Path Lengths of People Nearby

How to determine distance between two people in a social network without sacrificing privacy?

Distribute friendship tokens via social network
Fast Private Set Intersection using Bloom Filters
Private membership test with Bloom filters

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

• Server stores the database into an encrypted Bloom filter
• Cryptographic protocol allows client to check bits in the Bloom filter
  • Three different protocols – with various performance and privacy properties
  • Demonstrator for protocol based on Goldwasser-Micali cryptosystem
Secure deduplication of encrypted data

How to reconcile user privacy (client-side encryption) of cloud storage with server need of deduplication?

Oblivious Key Sharing

- Surprisingly efficient
- Alternative solution based on server-side trusted hardware

http://tinyurl.com/close-wp2
OmniShare

How to allow users to easily access encrypted cloud storage from multiple devices?

Key distribution channel discovered automatically (using capability info stored on cloud server)

Camera / Display: QR code
display / key board: passcode

https://se-sy.org/projects/omnishare/
Android Package Signing Key Analytics

What can we infer from Android package signing key usage patterns in the wild?

- Android packages are self-signed
- Can key usage patterns help detect malware?
Whispair: Silence Signatures for Securely Forming IOT Device Domains

How to automatically create groups associations for IoT devices using “silence signatures”

Effective, easy-to-use, privacy-preserving
Commitment-based device-pairing protocol with synchronized drawing

Can we replace passwords required in device pairing with … something else?

Pairing touch-screen and touch-surface devices by drawing almost the same picture on two devices with two fingers of the same hand

• Protocol
• Measuring the similarity of the drawings
• Evaluation
• And other remarkably interesting stuff!
Analysis of Topology Poisoning Attacks in Software-Defined Networks

What can attackers gain by poisoning topology of SDNs?

**Motivation**: Network-wide visibility is the key innovation of SDN but can be poisoned easily

**Goal**: To evaluate the significance of the topology poisoning attack in different kinds of networks

Example of two compromised switches with multiple tunnels scenario
Experimental Attacks on LTE Access Networks

How well do LTE implementations guarantee user privacy and availability?

• LTE deployments are progressing fast
• We identify privacy, availability issues in real LTE deployments
• May imply ambiguity in specifications
Thank you for coming!

We appreciate your feedback.