Aalto University
UNIVERSITY OF HELSINKI
ARCADA
F-Secure
NOKIA
ssh communications security
TRUSTONIC

Cloud-assisted Security Services (CloSer)

An overview

N. Asokan

Tekes
cloSer

Track record of CloSe (2014-2016)

2 journal papers, 12 conference papers

- Including at ACM CCS ’15, NDSS ’16 and Neurocomputing

Public demos

BlackHat EU ‘15, ACM S3 ‘15, ACM SIGCOMM ‘16, CeBIT ’16 (Grand Prize for OmniShare at MAPPING privacy-via-IT-security app competition)

Theses and dissertations

- PhD (1 completed, 1 submitted, 3 in progress)
- MSc (2 completed, 4 in progress)

Training

- 3 postdoc training; 8 research visits, 2 industry internships

All info at https://wiki.aalto.fi/display/CloSeProject/CloSe+Project+Public+Homepage

From CloSe to CloSer (2016-2018)

Tekes

CloSer refines/focuses work towards same objectives

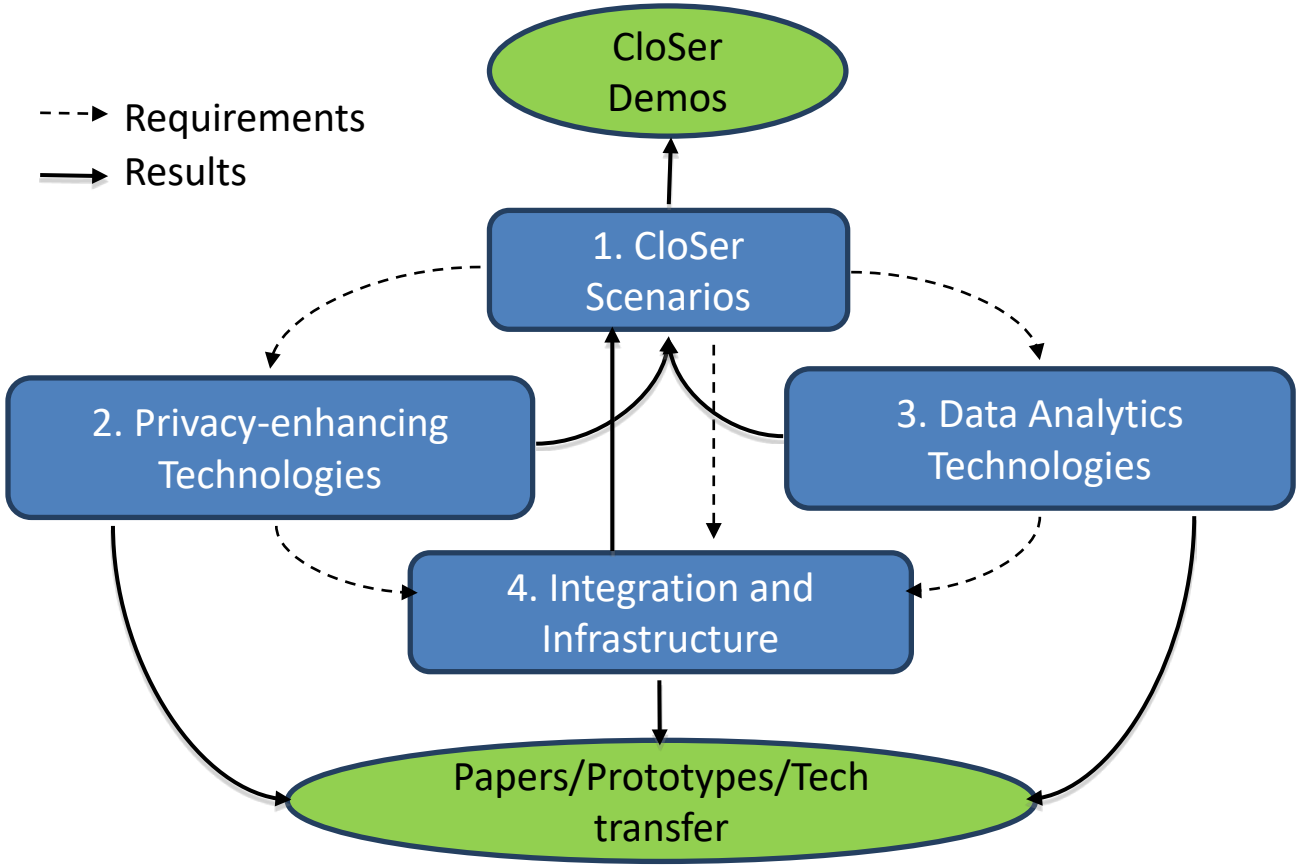
- informed by CloSe experience and SAB feedback

Cloud-assisted Security Services are interesting in their own right; Enabling technologies useful in other settings.

Objectives

- how to identify opportunities for utilizing assistance from cloud-deployed components for the purposes of security and privacy?
- how to address new security/privacy issues that arise when services move to a cloud-setting?

Structure of CloSer



WP1: CloSer scenarios

Cloud-assisted IoT Management (Trustonic)

- Scalable, privacy-preserving management schemes for constrained devices

Detection of user tracking (Nokia)

- e.g., fake base stations

Application and website reputation services, rapid attack detection (F-Secure)

- e.g., cloud-assisted content categorization and app reputation

Cloud-assisted trust relation database (SSH)

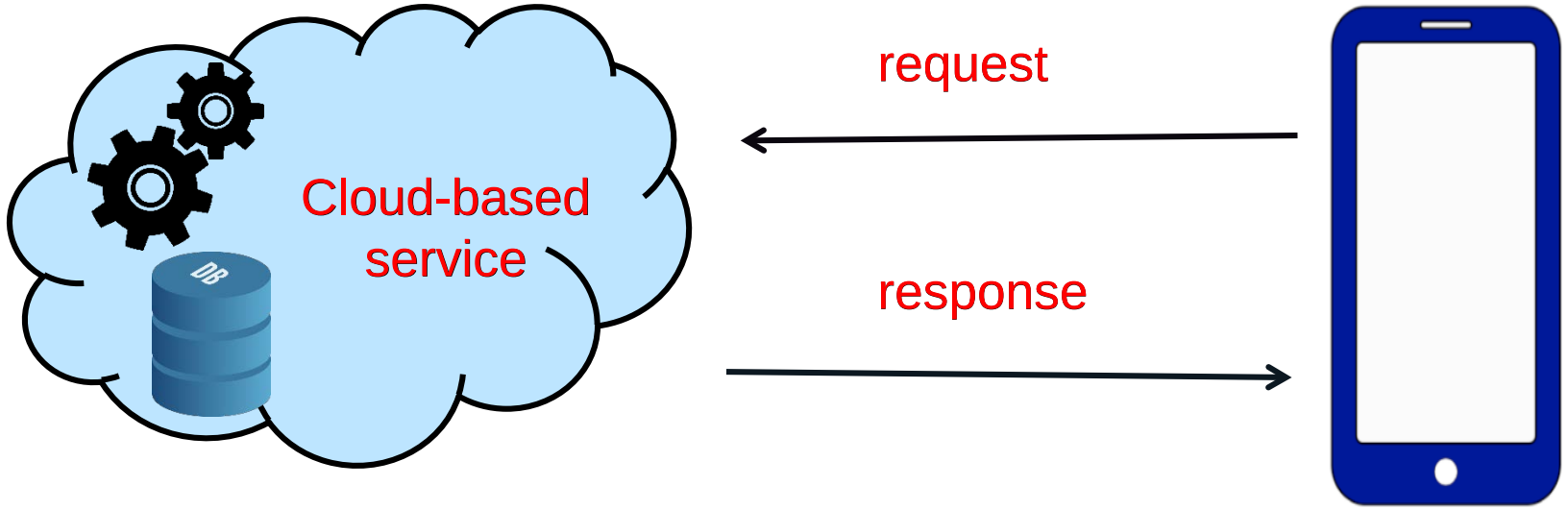
- e.g., privacy-preserving reachability queries

WP2: Privacy-enhancing Technologies

***Goal*:** suite of privacy-enhancing technologies (PETs) for ensuring privacy for various stakeholders in WP1 and other scenarios

***Approach*:** use cryptographic tools and/or hardware security support to design PETs

WP2: Privacy challenge in cloud-assisted settings



Cloud assistance is useful

- Cloud-resident databases (blacklists, whitelists, …)
- Machine-learning-as-a-service

but request and/or response may leak sensitive info

How can we make use of cloud-based services without compromising client privacy?

- using cryptographic techniques and/or
- using hardware security primitives

WP2: Privacy-enhancing Technologies

***Results so far*:**

Oblivious neural networks for privacy-preserving predictions

- poster / demo

Model privacy vs. query privacy

Two private membership test schemes for privacy-preserving malware checking

- Crypto based solution: poster / demo / paper (under submission)
- Hardware security based solution: poster / paper (AsiaCCS'17) (Honorable Mention)

Private graph search for cloud-assisted trust relation databases

WP3: Data Analytics Technologies

***Goal*:** Develop data analytics and machine learning solutions to enable WP1 services practically and efficiently

***Approach*:**

(a) Effective feature engineering to make the most of available data

(b) Adapt proven machine learning research to build models

(c) Careful evaluation strategies to ensure reliable operation

WP3: Data Analytics Technologies

***Results so far*:**

Image Analysis for Website Reputation Services

- Extracting features for image classification (poster and demo)
- Active learning to select samples for training (paper at ESANN 2017)

Android Malware Detection

- Feature extraction/engineering (paper at ICMLA 2016, poster)
- Pragmatic malware detector (paper under review, demo)
- Machine learning methods for large-scale sparse data (paper under review)

User and Traffic Profiling for Anomaly Detection

- Adaptive anomaly detection for SDN enabled networks (poster and demo)

WP4: Infrastructure for and Integration of CloSer

Goal*: *Develop an agent (to be deployed in edge networks) to support cloud services

***Approach*:**

- Extend Securebox model to develop Secure Intermediary (SI) with enhanced support for cloud services (to-be) developed in CloSer project.
- Develop lightweight components for cloud services to run on SI with small resource footprints and improve overall efficiency.

IoT lifecycle management

Results so far:

- IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT (Paper + Demo in ICDCS ’17 in collaboration with TU Darmstadt).
- IoTurva - Securing D2D communications in IoT Ecosystem (with TU Munich, in-progress).

WP4: Infrastructure for and Integration of CloSer

***Goal*:** enable live migration of virtual machines running apps with SGX enclaves

***Approach*:**

- cloud management VM that contains migration enclave to establish secure channel for transferring migrating enclave secrets
- a library built into the migrating enclave to provide migratable analogues of SGX non-migratable primitives (sealing, counters)

***Results so far*:**

- the protocol is designed and the library implementation has started.
- Poster: Live Migration of SGX enclaves

Virtual machines vs. attestation

CloSer Milestones

	Duration	Description
1	Y1M1-Y1M6	Selection & initial design of WP1 scenarios; Formulation of WP2-4 requirements
2	Y1M6-Y2M9	Iterative design and implementation WP2-4 technologies and WP1 scenarios
3	Y2M9-Y2M12	Refinement and wrapping up

Milestone 1 deliverables finalized in January

Annual Secure Systems Demo Day

Time: Tuesday, June 20 afternoon

Place: T-building (Konemiehentie 2)

Interested in getting an overview of the latest cutting edge information security research taking place in the Capital Area?

Please register.

Aalto University

UNIVERSITY OF HELSINKI

https://wiki.aalto.fi/x/xskDBw

Cloud-assisted Security Services

Objectives

- how to identify opportunities for utilizing assistance from cloud-deployed components for the purposes of security and privacy.
- how to address the new security/privacy issues that arise when security services are provided from a cloud-setting

Tekes

cloSer

https://goo.gl/JpMQ8s