Contextual Factors in Mobile Security and Privacy Policy Enforcement

Mobile Services and Edge Computing Workshop, Helsinki, 28.7.2016

Markus Miettinen

Technische Universität Darmstadt

About the Speaker

Alumnus of the University of Helsinki

13 years experience in industrial R&D at NOKIA Research Center Helsinki, Finland and Lausanne, Switzerland

Researcher at Fraunhofer Institute for Secure Information Technology, Darmstadt

Since 2013 Researcher at Technische Universität Darmstadt

Areas of interest include Mobile Security, Context-Awareness, Data analysis for security applications and IoT Security

Outline

Context-aware policy adaptation

- Utilizing profiled information about the context to make access control decisions

Context-based Proofs-of-Presence (PoP)

- Using context measurements to verify co-presence of two devices

What is Context?

In this presentation:

Any properties of the physical ambient environment that mobile devices can sense with their on-board sensors.

Context-Aware Policy Adaptation

TECHNISCHE UNIVERSITÄT DARMSTADT

Markus Miettinen, Stephan Heuser, Wiebke Kronz, N. Asokan and Ahmad-Reza Sadeghi "ConXsense - Automated Context Classification for Context-Aware Access Control", *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)* , June 2014.

CYSEC Cybersecurity TU Darmstadt

System Security Lab

Security and Context

Rich sensing capabilities

New context-aware apps and services

All of these features need to be managed!

Challenge: How to make security & privacy policy management

- User-friendly
- Personalized
- Context-aware

Challenge: Inflexible device lock

Many people feel device locks to be too difficult to use,
leaving their device unprotected

→ need for a better device locking mechanism

Goal: context-sensitive device locking:

- Quick locking in high-risk contexts
- Fewer passcode requests in low-risk contexts

Challenge: Sensory Malware

Mobile apps tend to ask for excessive permissions

- Users often grant permissions automatically

Adversary: Sensory Malware

- malicious software can use sensors to collect potentially sensitive information from user's context
  - e.g., audio, video, accelerometer, etc.

→ Need for more fine-grained, context-sensitive permission management

Goal: restrict apps' access to sensors in sensitive contexts

Legacy solution: user-specified, pre-defined policies

TECHNISCHE UNIVERSITÄT DARMSTADT

This has some Drawbacks:

- Difficult to understand
- Time-consuming
- Likelihood of erroneous policies is high

A quick remedy:

One preconfigured policy

- Inflexible
- Not personalized
- May surprise users

M. Covington, P. Fogla, Z. Zhan, and M. Ahamad. A context-aware security architecture for emerging applications. In Computer Security Applications Conference, 2002. Proceedings. 18th Annual, pages 249-258, 2002.

M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: A spatially aware RBAC. ACM Trans. Inf. Syst. Secur., 10(1), Feb. 2007.

M. Conti, V. Nguyen, and B. Crispo. CRePE: Context-Related Policy Enforcement for Android. In ISC 2011, volume 6531 of LNCS, pages 331-345. Springer, 2011.

User Perceptions

What security concerns do users have with regard to their smartphone?

Questionnaires and on-line survey
More than 150 participants

User Perceptions

Two main user concerns:

Concerns related to *privacy exposure*

- Intrusive apps exfiltrating sensitive user information to unauthorised parties

Risk of *device misuse*

- Someone stealing the user‘s device or using it without the user‘s permission

Main findings from the Survey

Perception of risk of ***device misuse*** depends on people present and their familiarity, not so much on the place

→ Estimate familiarity of people

Perception of ***privacy exposure*** depends on the place itself, not so much on the people present

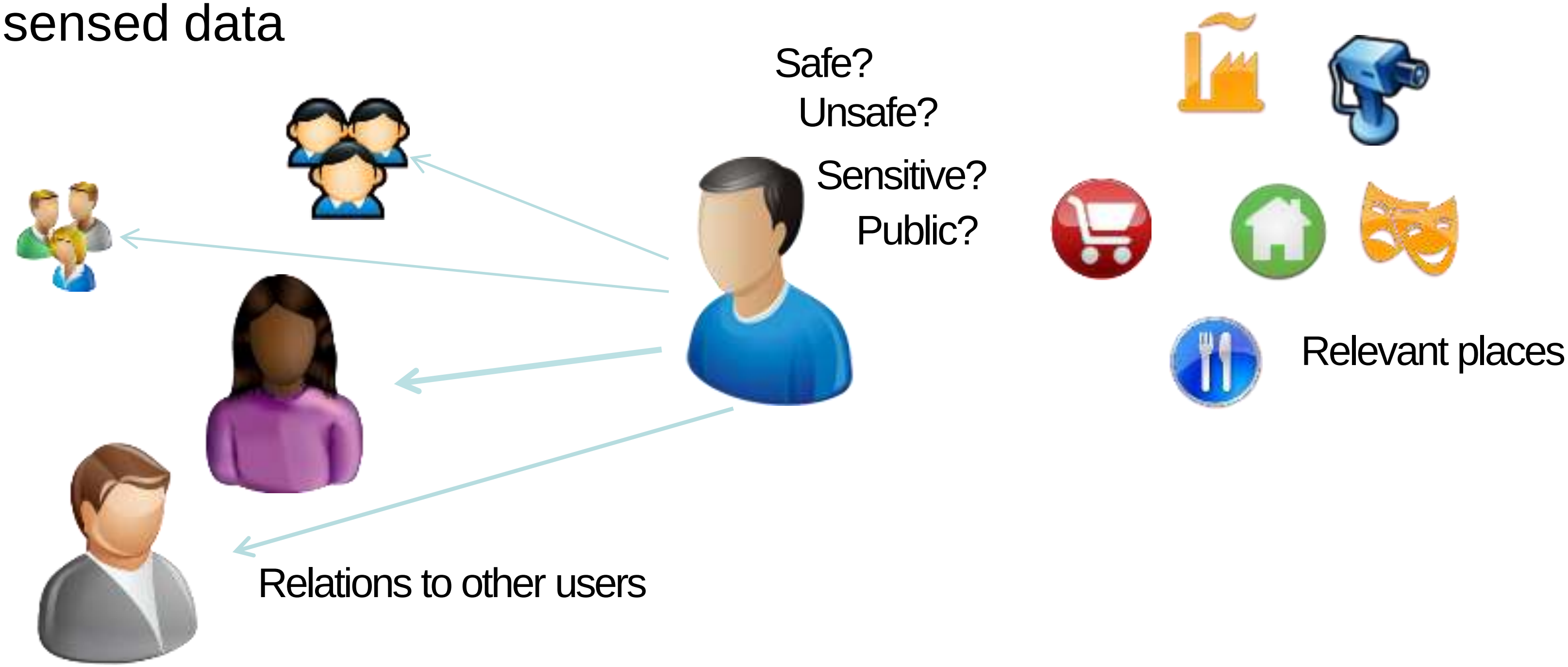
→ Estimate familiarity of places

Our approach

Profile user‘s relevant places (= "contexts")

Profile frequent social contacts (= devices)

Create prediction model for access control based on profiles and sensed data



Context Features

Familiarity of Context (identified through GPS and WiFi)

- Number of visits
- Time spent in context

Familiarity of devices in vicinity (identified thorough Bluetooth)

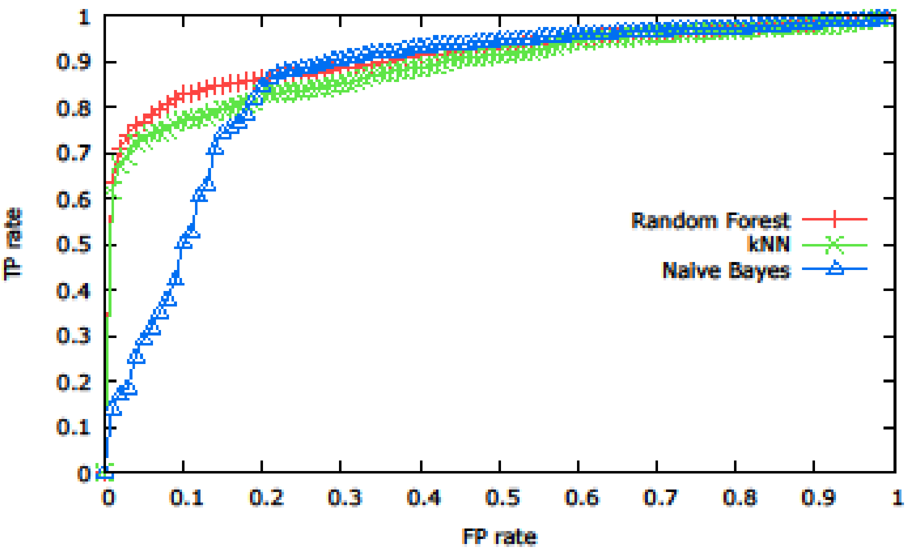
- Number of visible devices
- Number of visible familiar devices
- Average # of past encounters for familiar devices
- Average time spent with familiar devices

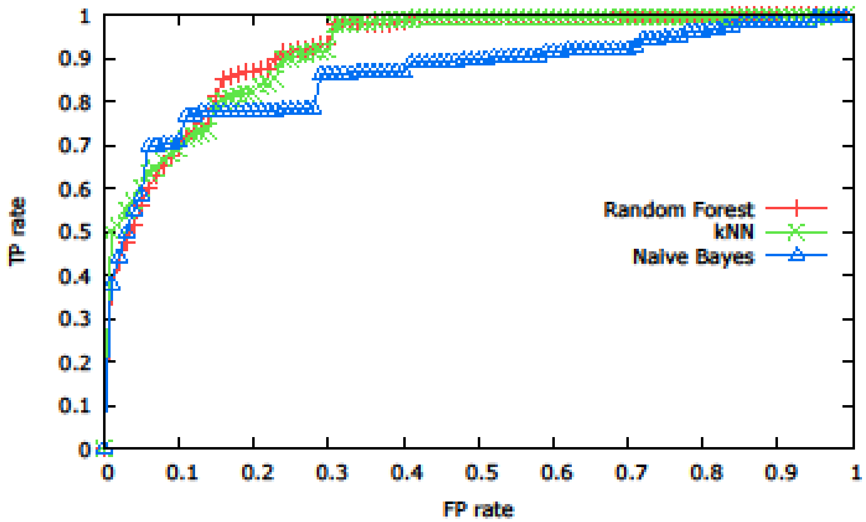
Results

Adaptive device lock:

70% TP rate at relatively moderate FP rate of 10%

Number of passcode queries reduced by 70%!





Sensory malware protection:

Random Forest and k-NN achieve 70% TP rate at very low FP rate of 2-3.5%

Context-based Proofs-of-Presence

Markus Miettinen, N. Asokan, Farinaz Koushanfar, Thien Duc Nguyen, Jon Rios, Ahmad-Reza Sadeghi, Majid Sobhani, Sudha Yellapantula, „I know where you are: Proofs of Presence resilient to malicious provers" *10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)*, April 2015.

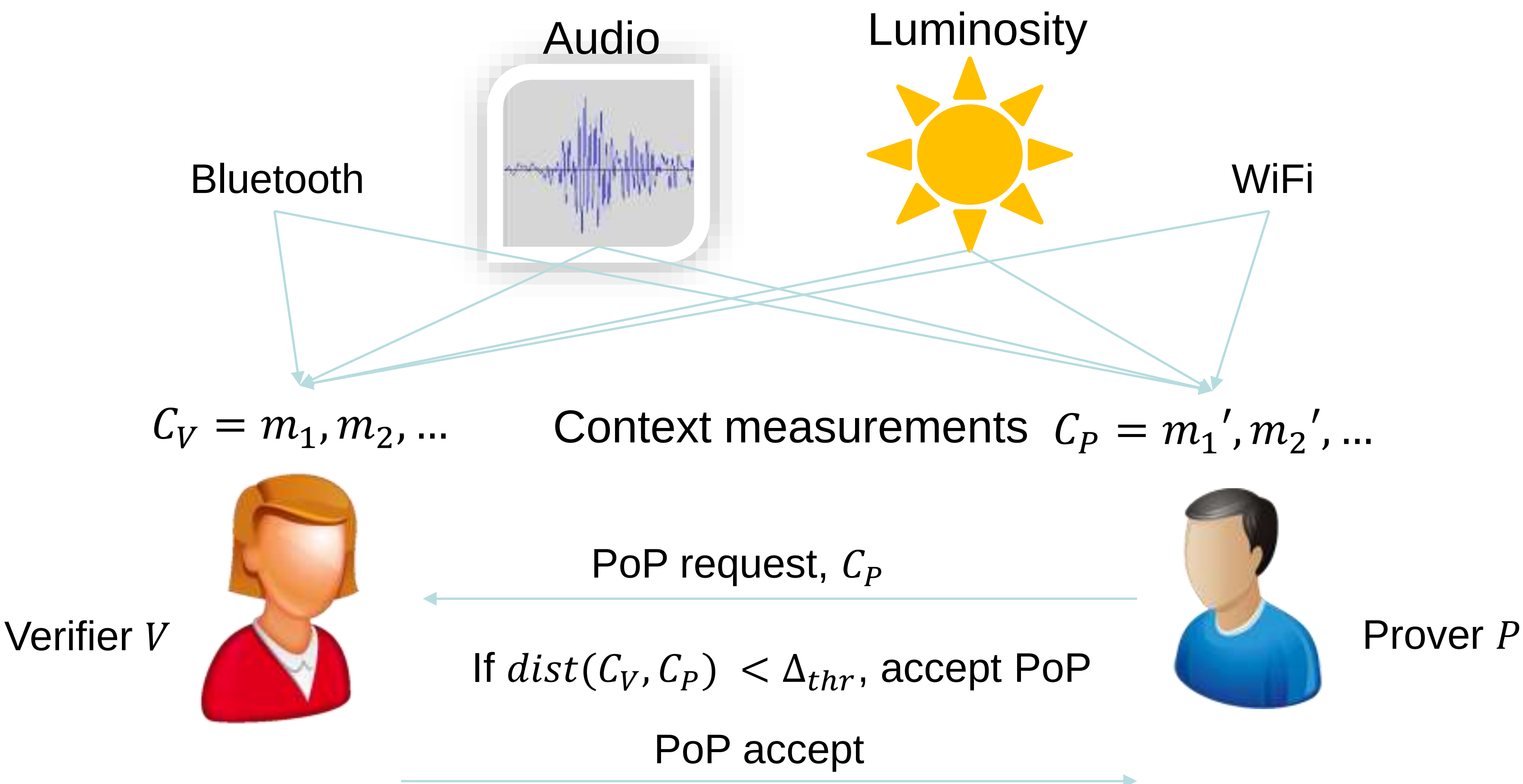
Venue check-ins in OSN:s

“check-in”

Location claim

Incentives for **location cheating**

Context-based Proofs-of-Presence



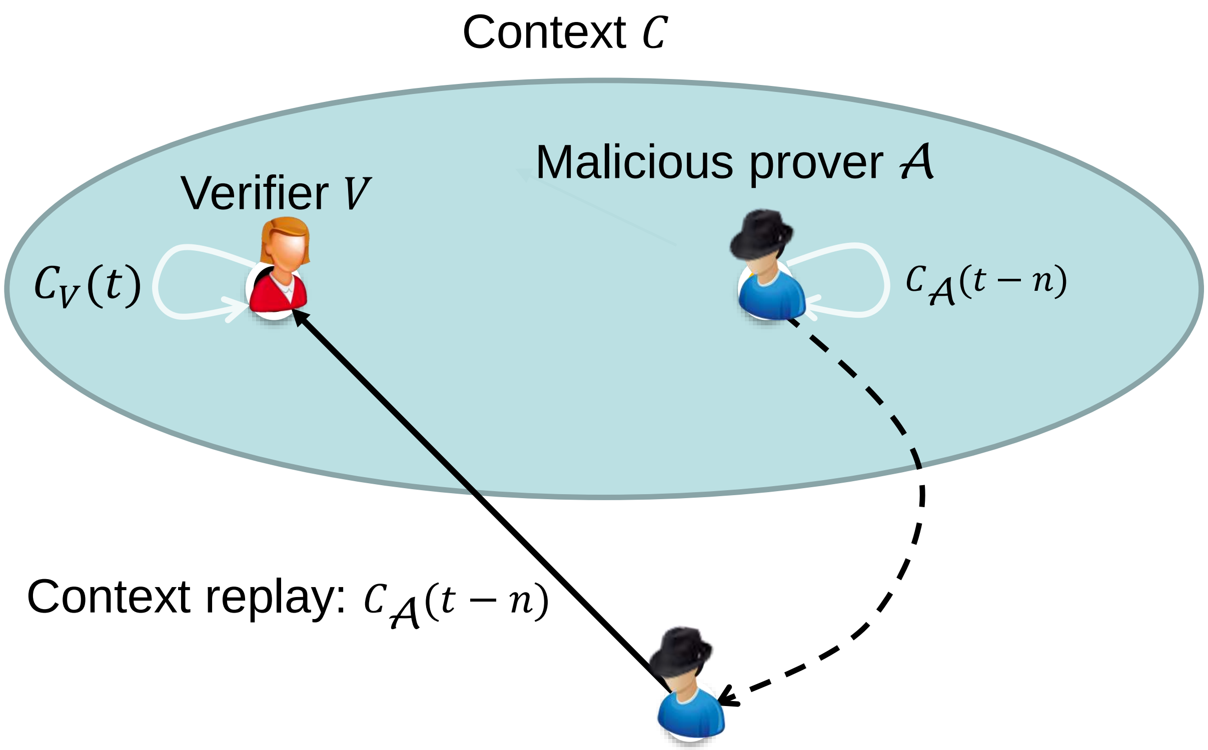
Location Claim Verification

Machine learning-based classification model

Trained with a set of annotated pairs of co-located and non-co-located measurements

Classifier used to determine whether two measurements originate from co-located devices or not

Context Guessing



Hardening of PoPs

Surprisal filtering

- Reject easy-to-guess PoPs

Longitudinal ambient context modalities

- Increase the inherent entropy of PoPs

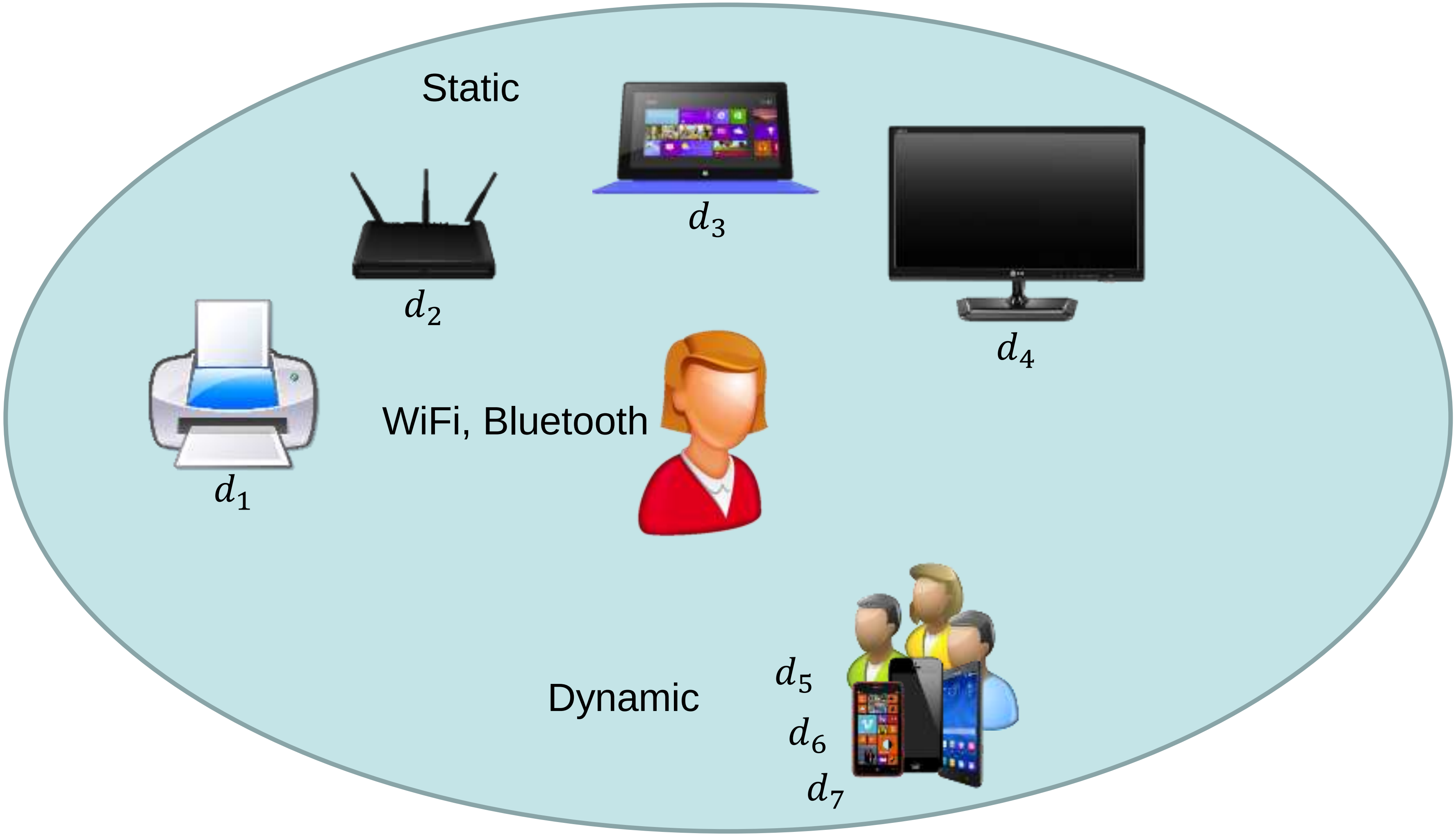
Surprisal of Context Measurements

We use *surprisal* to measure how easy it would be for a malicious prover to guess a valid context observation in a context. The higher the surprisal is, the more difficult it would be for the attacker to correctly guess such observations.

The surprisal of a context measurement C is defined as the self-information that measurement

$$I(O_X = C) = \log_2(\frac{1}{P(O_X = C)}) = -\log_2(P(O_X = C))$$

Types of Context Information



Surprisal Filtering

1. Profile the occurrence frequency of contextual elements (e.g. WiFi and BT devices) in the context
2. When receiving a PoP, evaluate the surprisal associated with the elements of the verifier's context measurement.
3. If surprisal is too below surprisal threshold I_{thr}, reject PoP.

Effectiveness of Surprisal Filtering

Surprisal filtering significantly reduces False Positive rate of PoPs

$I_{thr} = 4\ bits$	Unfiltered	Bluetooth	WiFi
Average	27.7 %	-16.7 %	-5.5 %
Rel. change		-60.4 %	-20.0 %

Longitudinal Ambient Context Modalities (Luminosity & Audio)

Goal: Increase entropy of PoP

Approach:

1. Measure ambient context modalities level and record snapshots

$$M = \{m_1, m_2, \ldots, m_n\}$$

Each measurement m_i has length w = 1 sec and n = 60

Trade-off

- Longer snapshot provides more entropy
- Shorter snapshot provides better usability
- Short measurements require accurate time synchronisation

Evaluation: Longitudinal Modalities

Attack Dataset	False Positive Rate
Luminosity	1.1 %
Audio	0.4 %
Luminosity + Audio	0.4 %
Bluetooth	21.9 %
WiFi	26.0 %
Bluetooth + WiFi	23.5 %
Luminosity + Audio + BT + WiFi	3.6 %

Conclusion

Use of context enables many novel applications and services but poses also challenges w.r.t. privacy and manageability

Utilizing context-profiling can help in tackling some of the manageability-related issues

Context fingerprinting-based approaches enable new possibilities for utilizing context to construct entirely new security functionalities like proofs-of-presence

Ongoing work

Utilizing deeper context-awareness to encounter sophisticated threats like relay attacks and context-manipulating adversaries

Extending the use of context into IoT domain through, e.g., context-based pairing

Thank You!

markus.miettinen@trust.tu-darmstadt.de

@mmietti

www.trust.informatik.tu-darmstadt.de/people/markus-miettinen