



# Secure Systems Group

N. Asokan



# “State of the Union”



# Who are we?

First group member recruited in March 2013

## Currently

- 2 postdocs
- 1 postdoc-in-waiting
- 5 MSc students
  
- 2 external doctoral students
  
- 2 summer interns



# How we are funded?

Dean's initiative on information security research

[Intel Collaborative Research Institute for Secure Computing](http://www.icri-sc.org)  
(<http://www.icri-sc.org>)

Internet of Things SHOK program (DIGILE/Tekes)

Gifts (Nokia for research; Intel for curriculum development)

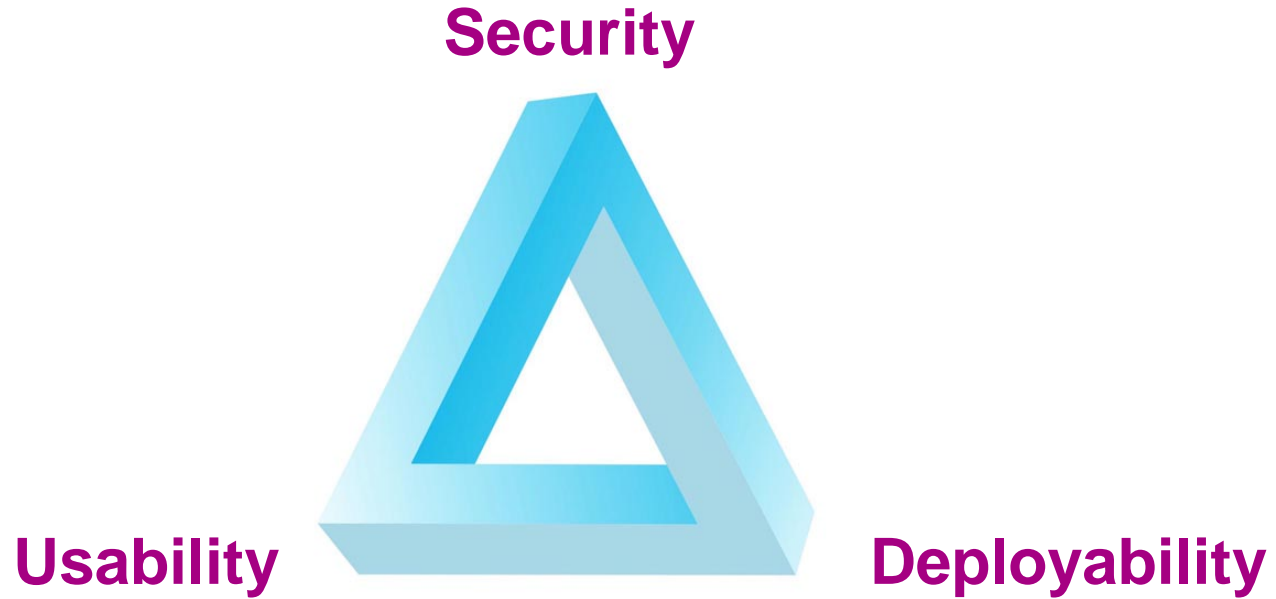


# What do we work on?

- Mobile (platform) security
  - Securing applications using OS security mechanisms
  - Trusted execution environments
  - Mobile malware
- Contextual security
  - Leveraging context information to balance security and usability
    - context perceived via on-board sensors
    - social relationships




# What do we work on?



# What have we achieved?

- Book on “Mobile Platform Security” (with ICRI-SC co-authors)
- Journals & Magazines
  - IEEE Security & Privacy – *trusted execution environments*
  - Proc. IEEE (conditional accept) – *mobile trusted computing*
- Conferences
  - WWW – *mobile malware infection*
  - ACSAC, ACNS – *privacy-preserving finding of common friends*
  - PerCom, Financial Crypto – *using context to decide co-presence*
  - ASIACCS – *using context for access control*
- Press coverage
  - ICRI-SC establishment, WWW paper (including in MIT Tech Review)



Self evaluation:  
Good but room  
to improve



# What do we teach?

- Mobile Platform Security:
  - Overview of mobile platform security and some current research
  - For students potentially interested in **research** in mobile security
- Software Security:
  - Introduction to software security, specifically threat modeling
  - For students heading to **software development** careers in industry
  - Taught by Antti Vähä-Sipilä

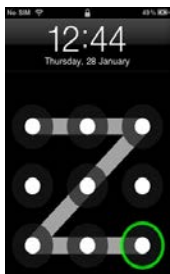
<http://www.cs.helsinki.fi/group/secureres/teaching.html>



# What do we teach? Course Content

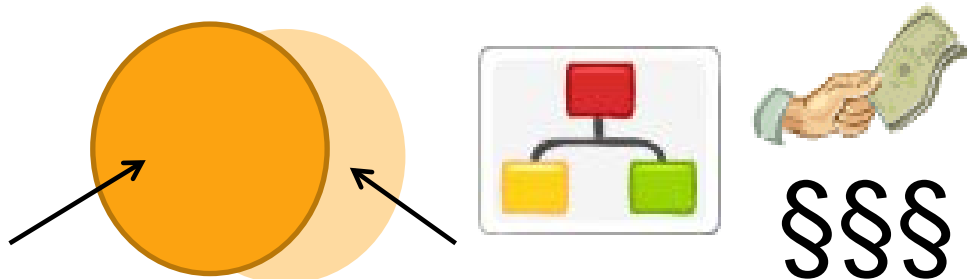
## Mobile Platform Security:

- Case study: **Android**
- **Software** platform security
  - General **model**
  - **Comparison** of platforms
- **Hardware** security enablers
- **Usability** of platform security
- Current research



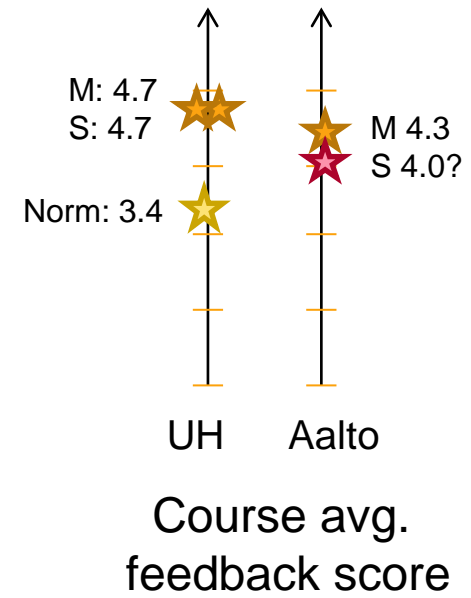
## Software Security:

- **How software breaks**
  - Native binaries
  - Web, incl. attack proxies
- Security activities in **projects**
- **Architectural risk analysis**
  - Privacy, sec. design patterns
- **Economics** and regulation



# What do we teach? Student Feedback

- Enthusiastic feedback from students
  - Aalto (compulsory,  $n_M=7$ ,  $n_S=9$ ), UH  $n_M=9$ ,  $n_S=7$
  - Evaluated at normal laboriousness
  - High voluntary attendance rates
- Nonexistent drop-out rate (!)



Course development supported by a gift from [Intel Security Curriculum Initiative](#)





# 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



# Nudging users away from unsafe content

## How to effectively signal risky content to ordinary users?

Crowdsourcing ratings: e.g., Web of Trust (<http://mywot.com>)

WOT WOT click to view details

vuupc.com

Trustworthiness Child safety

Download Size: 1mb. This  
n more.

- Malware or viruses
- Scam
- Suspicious

note access to ...

WOT WOT click to view details

play.google.com

Trustworthiness Child safety

Good site

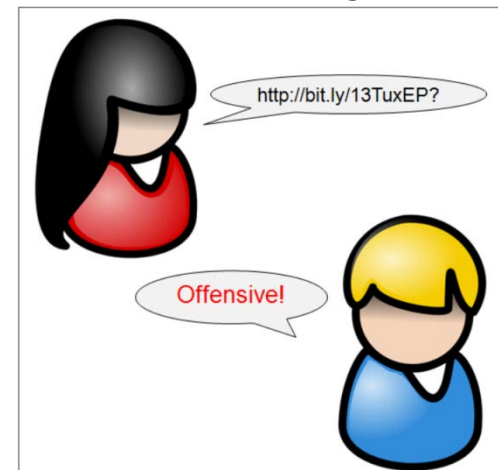
Online tracking

### Predicting rating from content

link	HTML.img.tags	JS.setTimeout	HOST.ns_ttl	...
vuupc.com	6	3	62320	...

➔

### “Groupsourcing”?





# On Mobile Malware Infection Rates

How prevalent is mobile malware?  
Can we predict vulnerability of a device?

time



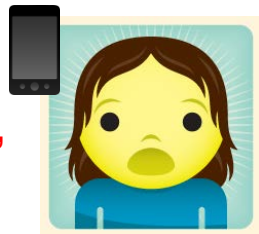
?



*Can the list of apps used on device detect susceptibility for infection?*



Device 1  
"infected"

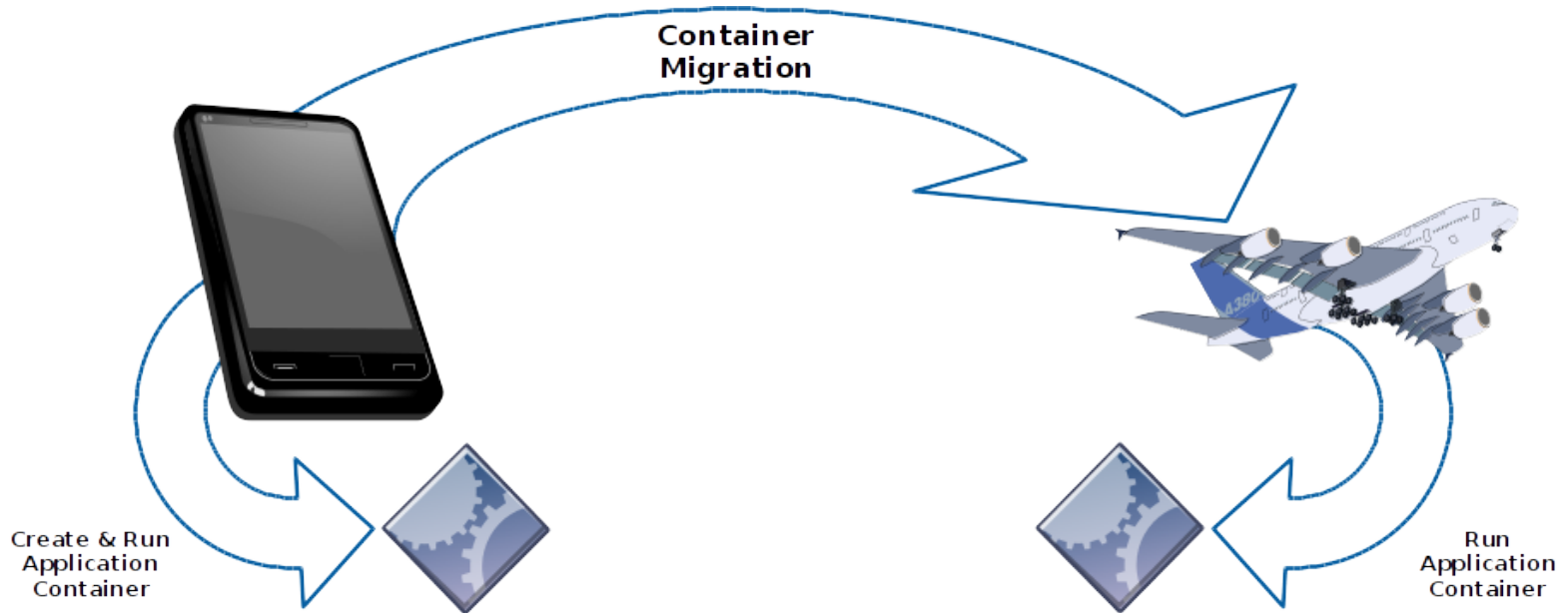


Device 2  
"clean"



# Dynamic Isolated Domains

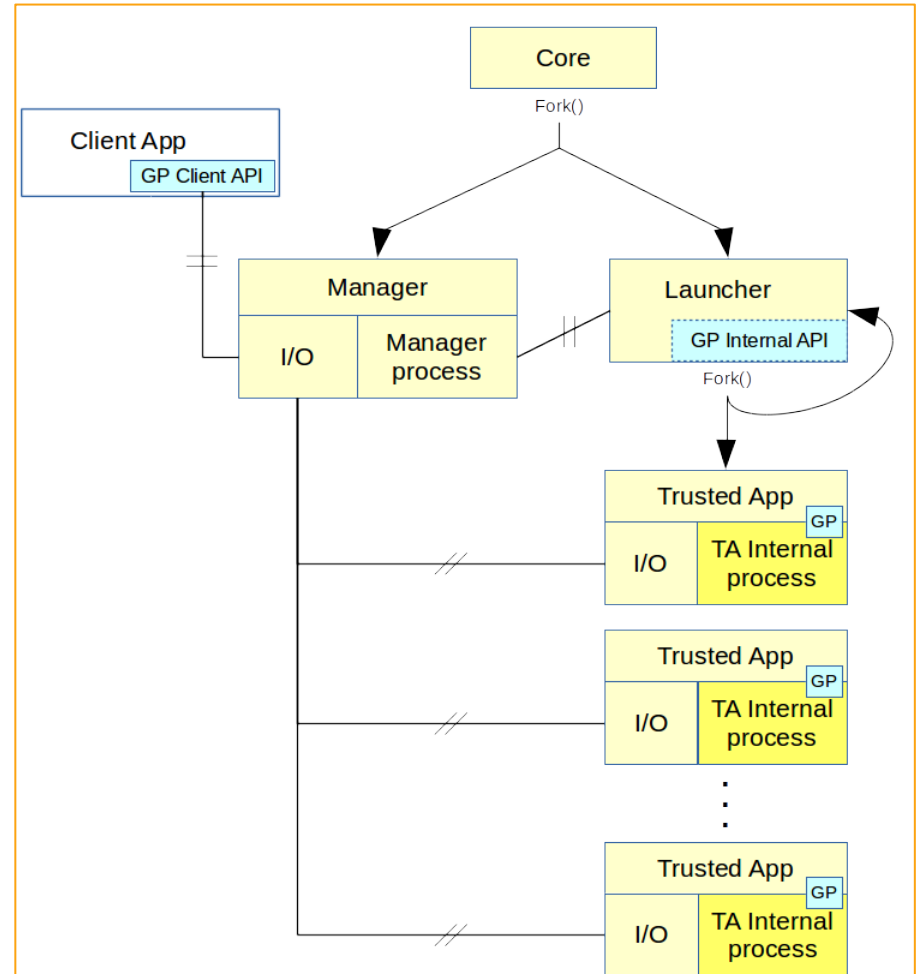
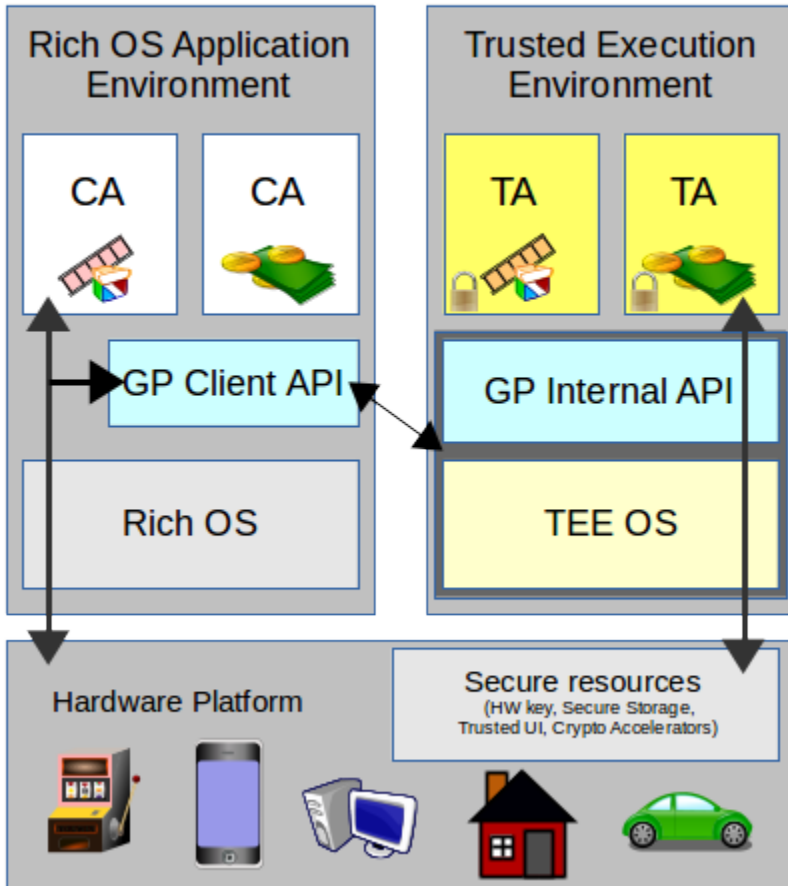
Can existing OS security mechanisms be used creatively to address security needs in new usage scenarios?





# Open Virtual TEE

## What is needed to enable app developers to use trusted hardware?

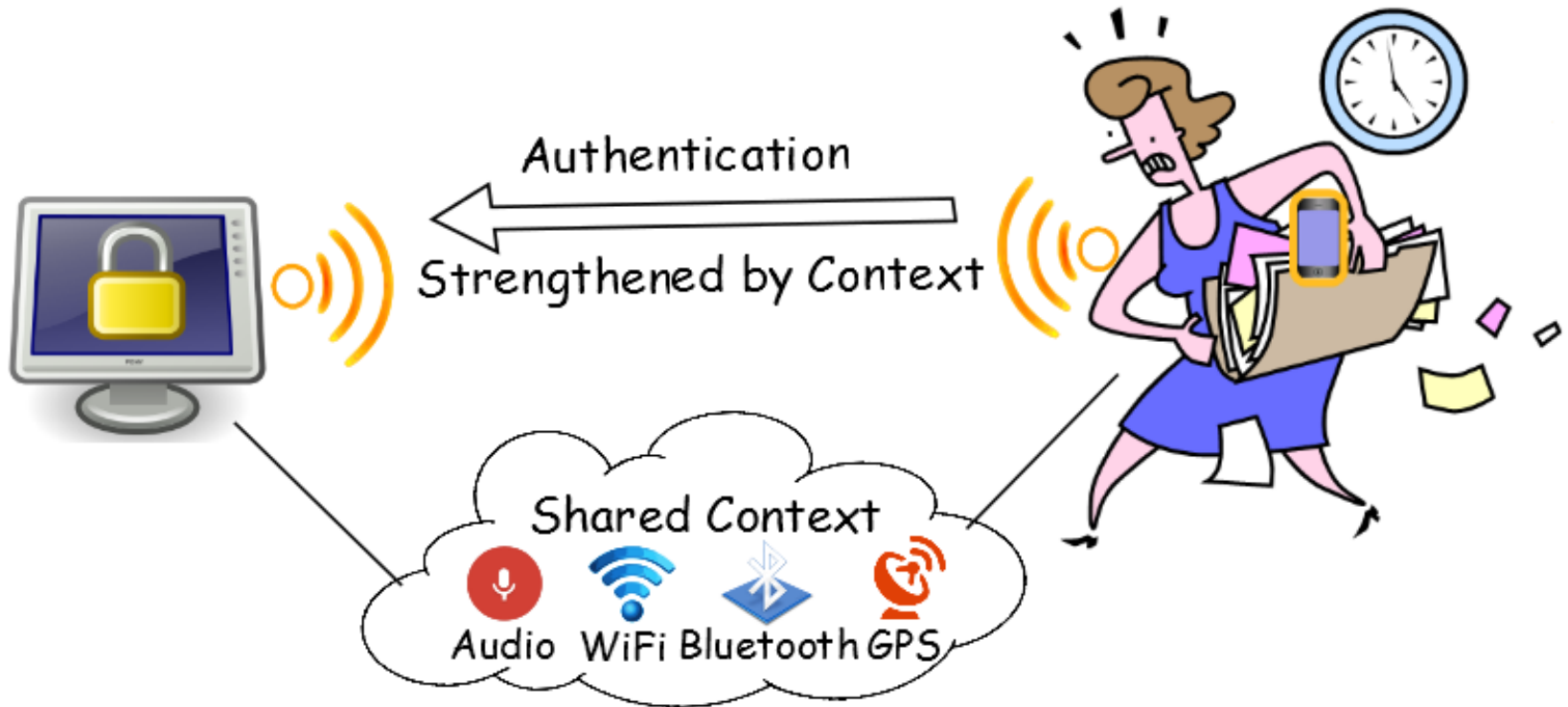






# Contextual Co-presence

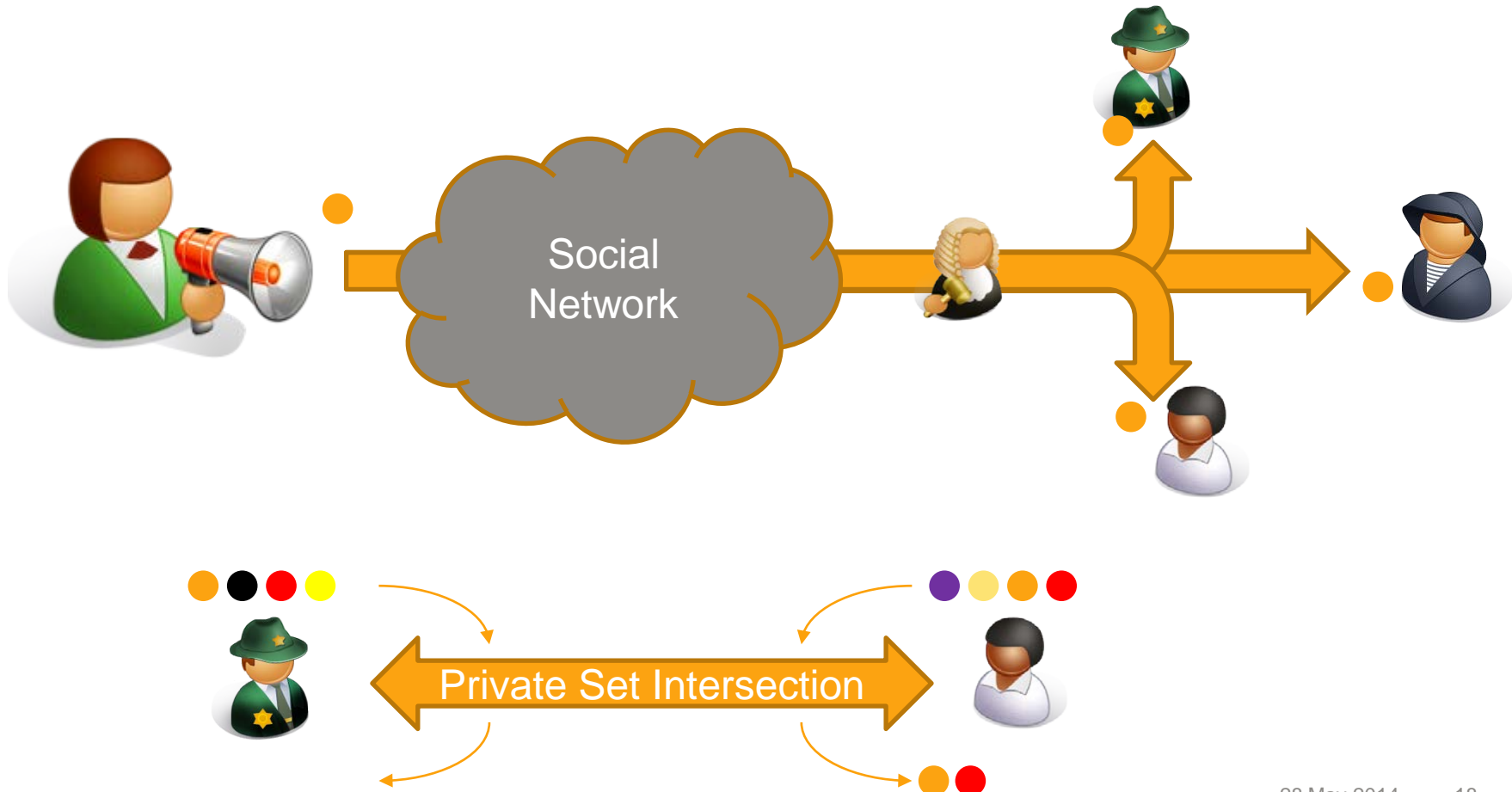
Can contextual cues be used to improve security and usability of systems?





# Proximity social interactions

Can existing social networks be used to improve security and usability of systems?





Thank you for coming!

We appreciate your feedback.