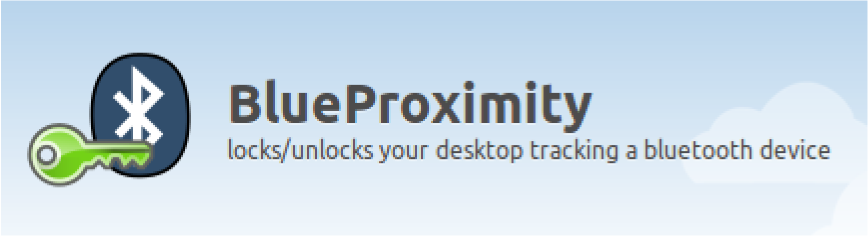
Exploiting Context for Security

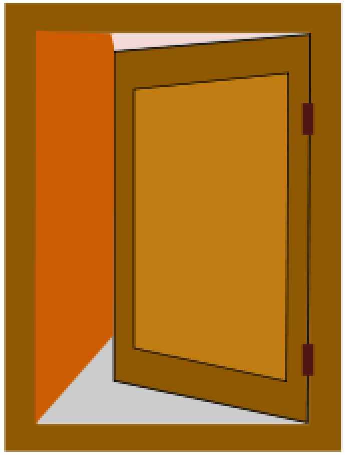
N. Asokan, University of Helsinki

Zero-interaction authentication

Easy-to-use security

Zero-interaction (de)authentication





Easy-to-use security

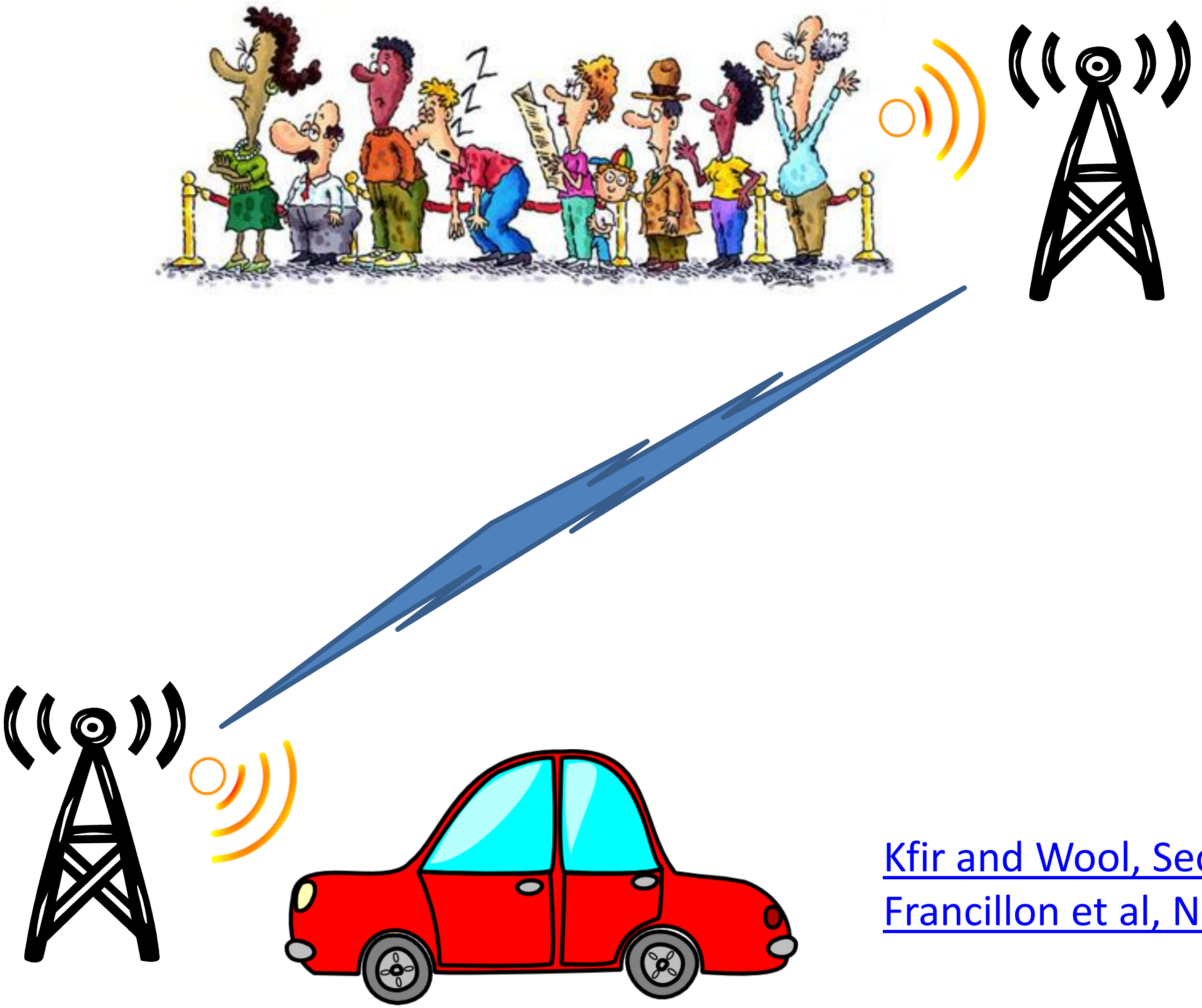
[BlueProximity project in SourceForge]

[Corner and Noble, MobiCom ‘02]

Does zero-interaction help crooks?

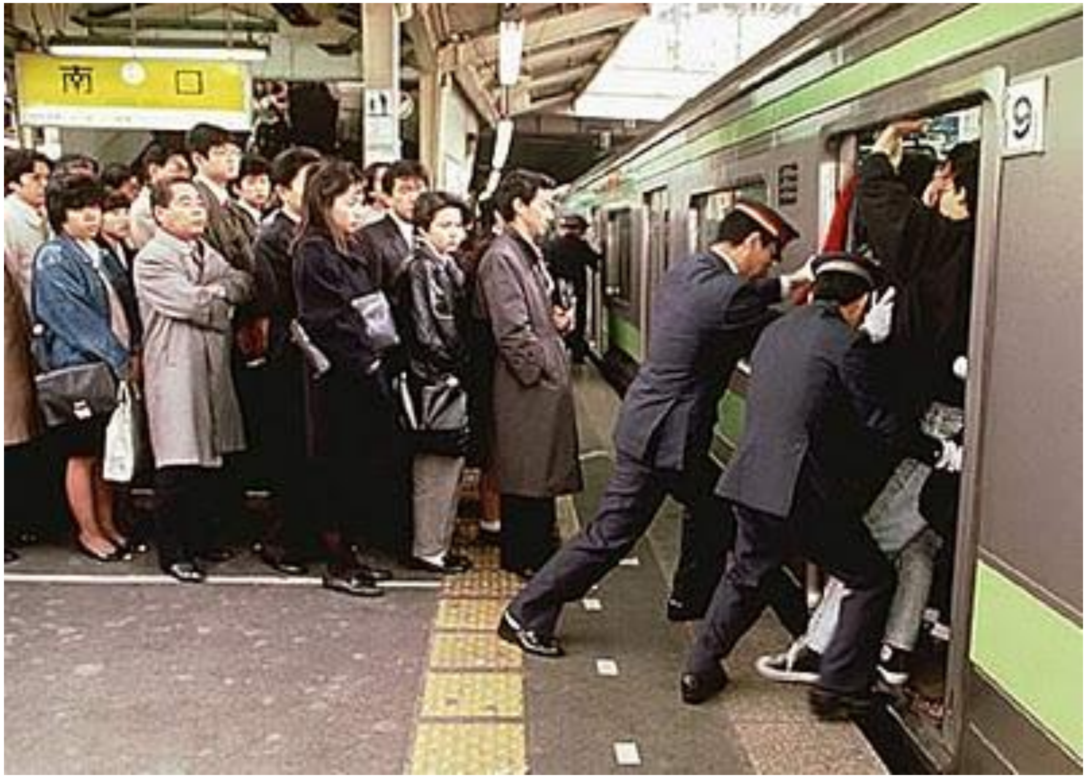
Easy-to-use security → Easy-to-use attacks?

Ghost-and-Leech attacks

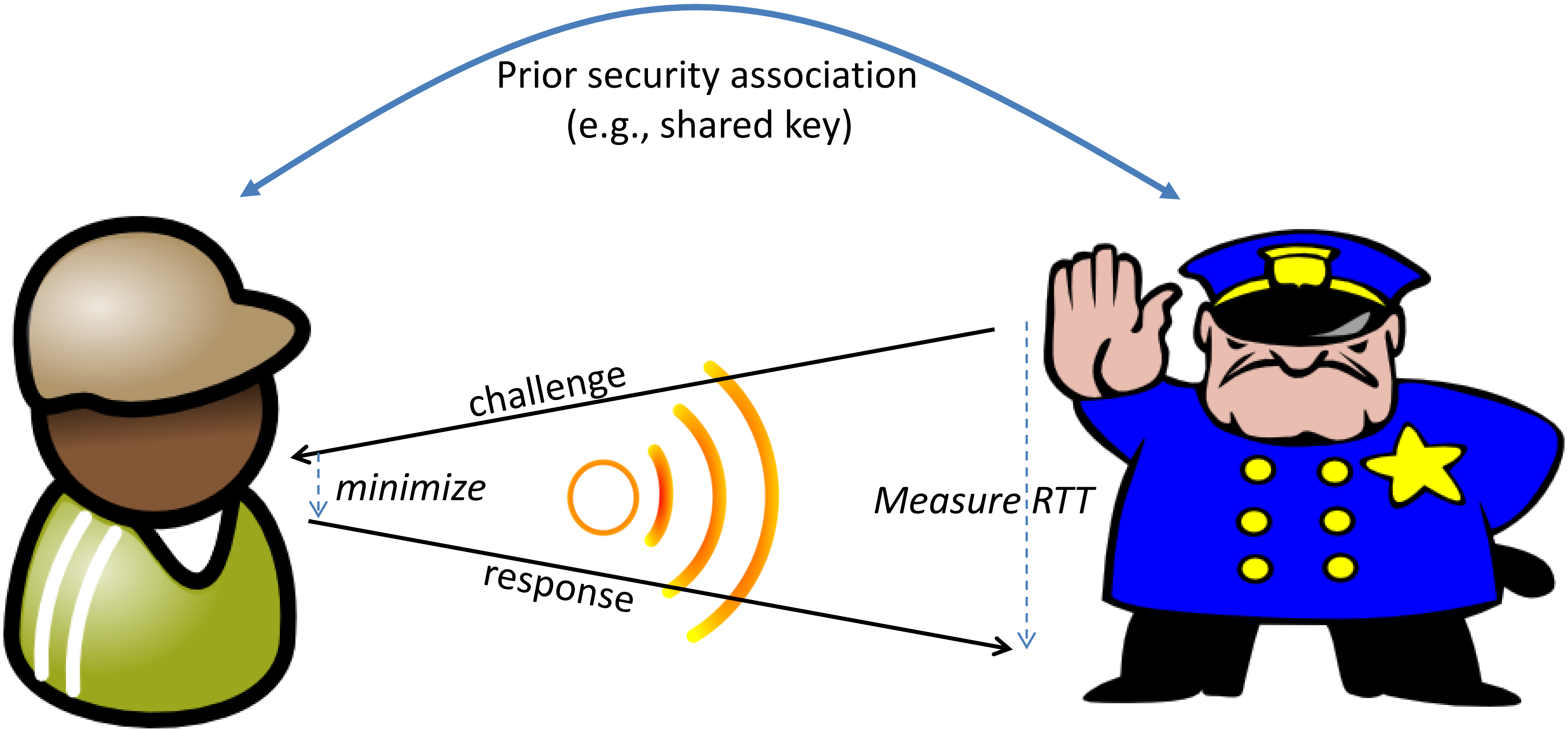


Kfir and Wool, SecureComm ’05
Francillon et al, NDSS ‘11

“Tokyo Metro Attack”



Defense: Distance bounding

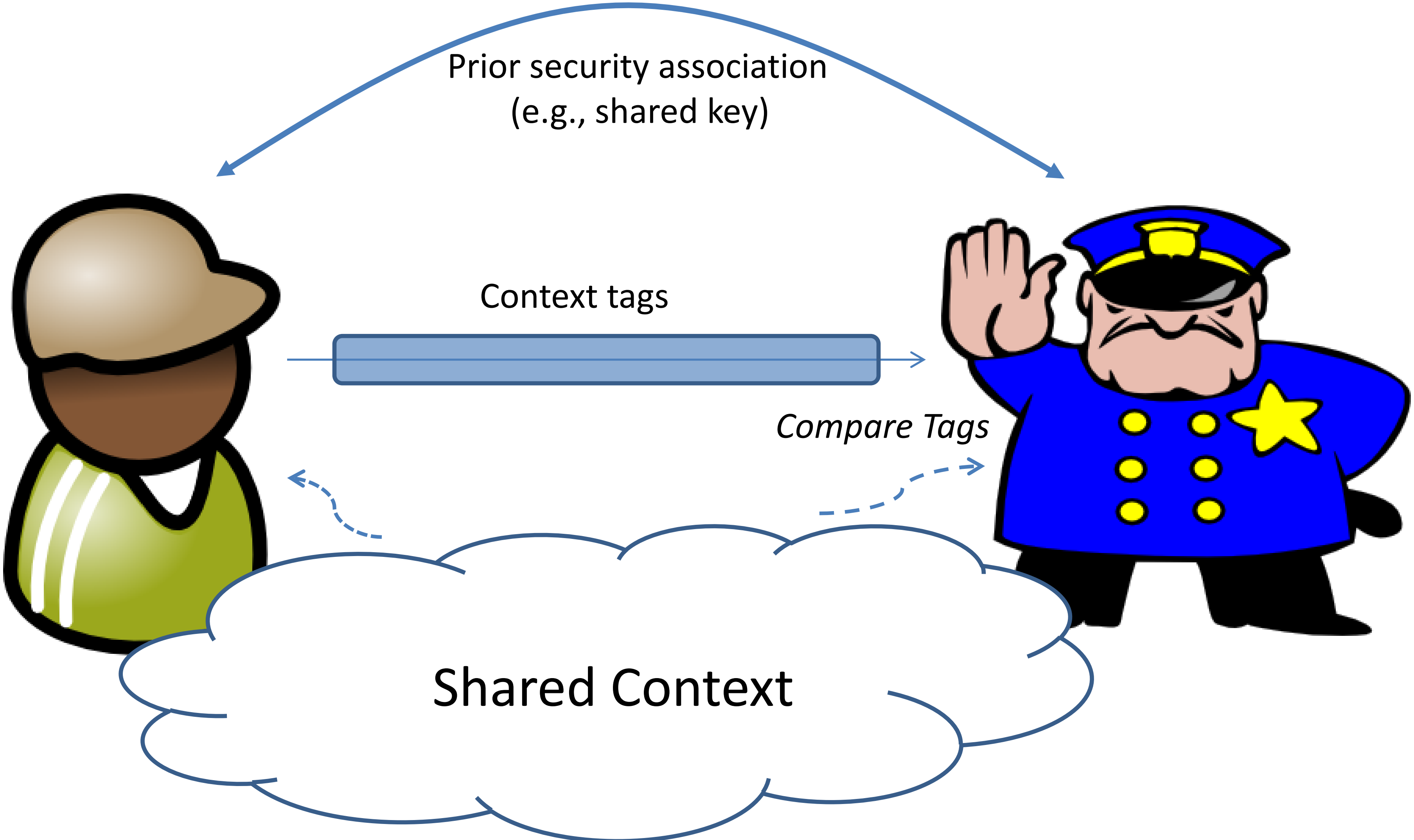


1 light nanosecond = 0.3m

Brands and Chaum, Eurocrypt '93

Rasmussen and Capkun, Usenix SEC '10

Defense: Contextual Co-presence



What kind of context tags?

- Easy to measure and compare
- Difficult to fake
  - *unpredictability not needed* (sensing by honest players)

- Location co-ordinates
- Ambient audio
- Observed wireless broadcast traffic
- Nearby devices
- …

Halevi et al, ESORICS ’12
Schurmann and Sigg, TMC ‘11
Narayanan et al, NDSS ‘12

Questions

- How to combine multiple tag types?
  - Availability of a tag type depends on context and capabilities of sensing device
- How to evaluate susceptibility of a tag type for faking?
- How to preserve context privacy when evaluation is done by a third party?
- …

Plan

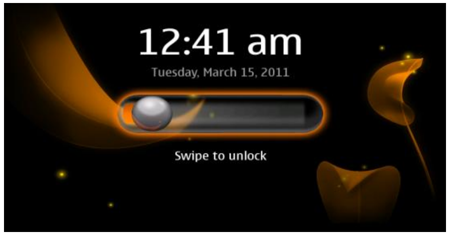
- Develop a general framework for **contextual co-presence detection**
  - Experiment with multiple tag types
  - Develop techniques for privacy-preserving context comparison
  - Show a ghost-and-leech attack against Blueproximity and prevent it using contextual co-presence detection
  - Joint work with Nitesh Saxena (Univ. Alabama) and his students
- **Potential MSc thesis: anyone interested**?

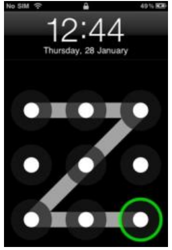
More generally: Contextual Security

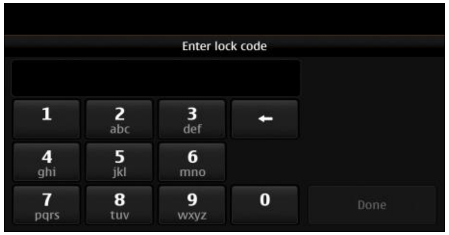
- Context Profiling
  - Keep track of context measurements over time

Better Dev. Lock via Context Profiling

Timeout and unlocking method adjusted based on estimated familiarity/safety of current context



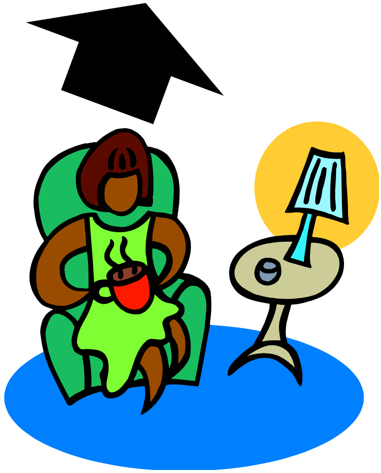




Long timeout

Medium timeout

Short timeout



Home

Work Cafeteria

Unknown

Gupta et al, SocialCom '12

More generally: Contextual Security

- Context Profiling
  - Configuring device lock
  - Configuring fine-grained access control (on-going joint work with Markus Miettinen et al, Fraunhofer SIT)
- Context-centric Security
  - Allow users to create dynamic isolated domains (“bubbles”) within a device based on “context”
  - Access granted to users, not apps

Tiwari et al, Usenix HotSec ‘12

Summary

- Contextual co-presence can thwart ghost-and-leech attacks
- An instance of “contextual security”
  - Personal devices sensing context (and keeping track of contexts) to make improve usability and security/privacy levels simultaneously.