

Security by Spatial Reference: Using Relative Positioning to Authenticate Devices for Spontaneous Interaction

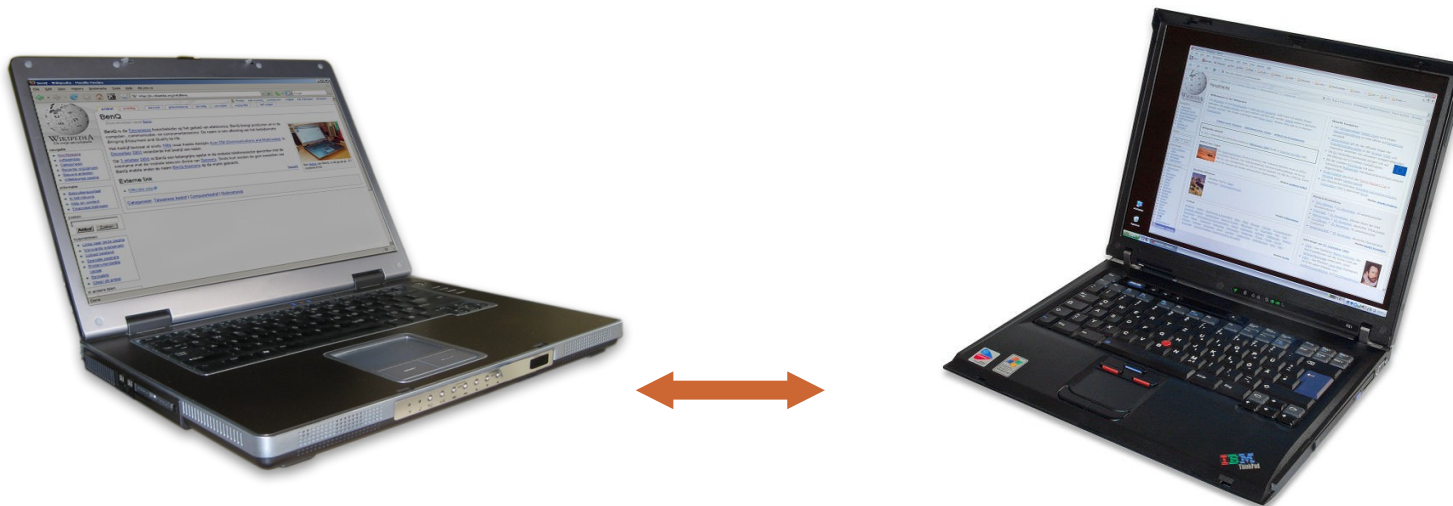
Ubicomp 2007, Session D
18. September 2007, 12:00

Rene Mayrhofer, Hans Gellersen, Mike Hazas
Lancaster University, UK

The problem

Wireless communication is insecure

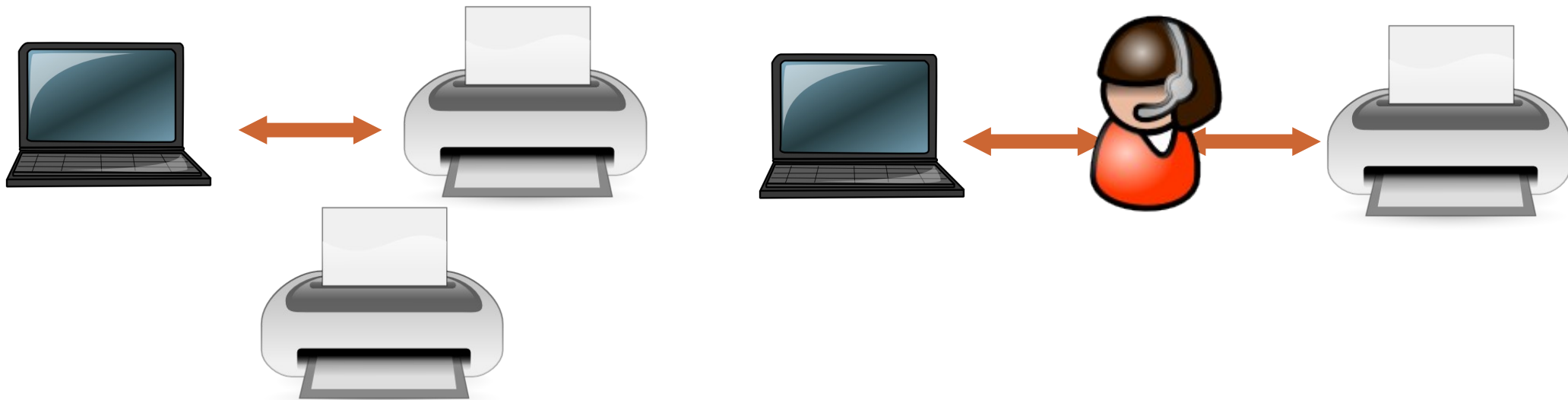
- Especially problematic for spontaneous interaction: **no a priori information** about communication partners available
- ⇒ User needs to establish **shared secret** between devices



Why is it a problem? (1)

Secret key exchange over wireless channels

- Can use Diffie-Hellman (DH) for key agreement
- Problem of Man-in-the-Middle (MITM) attacks



⇒ Secret keys need to be **authenticated**

Why is it a problem? (2)

Options for authentication

- Entering PINs (e.g. Bluetooth), passwords (e.g. WEP/WPA)
- Verifying hashes of public keys (e.g. web site certificates)

Need user interface for that!

- A printer/public display does not usually have capable input devices

Somebody needs to do it!

- Do you want to enter random passwords 10 – 100 times a day?

⇒ Problem of **scalability**

Human-verifiable spatial relationships

(Relative) Spatial relationships:

- Intuitive concept for most users: “**that device** over there”
- Network identities or names of involved devices no longer important
- Anonymous or pseudonymous interaction possible

Ultrasound can be used for authentication:

- transmitting messages with constraints ⇒ **implicitly**
- measuring spatial relationships ⇒ **explicitly**

How does spatial relationship help?

Spatial References:

verifiable by the user **and** the device – both can come to the same conclusions as to which device they are interacting with

1



[GSG 2007] D. Guinard, S. Streng, H. Gellersen: "Relategateways: A user interface for spontaneous mobile interaction with pervasive services", In: CHI 2007 Workshop

The “don't get in my way” principle

When selecting a device, the user

- **intends** to interact with it
- creates a **reference measurement**



2

Everything else should happen automatically

⇒ no steps “just for security”

Quantitative measurements with ultrasound

- Ultrasound signals travel comparatively slowly in air \Rightarrow possible to measure time of flight \Rightarrow distance estimation
- Angle-of-arrival estimation using multiple receivers difficult based on relative time of arrival
- Angle-of-arrival estimation based on relative signal strengths works in practice



Relate:

- <10 cm accuracy for distance measurements
- $\sim 33^\circ$ accuracy for local angle-of-arrival
- without infrastructure
- implemented as USB dongles + Java host software

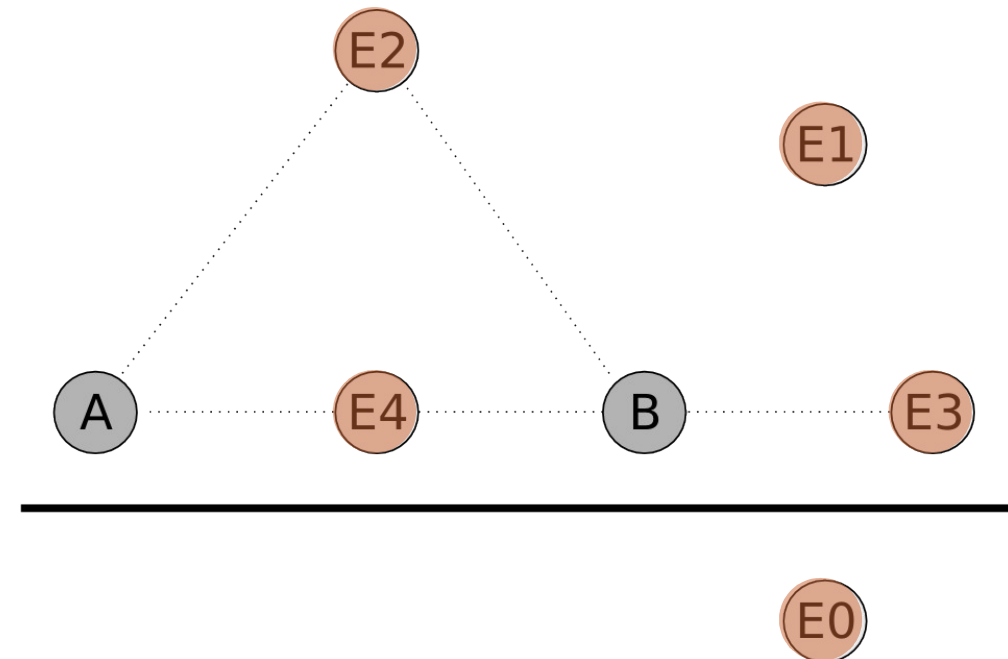
[HKG+ 2005] G. Kortuem, C. Kray, H. Gellersen: "Sensing and visualizing spatial relations of positioning system for co-located mobile devices", In: Proc. MobiSys 2005

Properties of ultrasound signals

- Reflected or absorbed by solid materials ⇒ **blocked** by walls, doors, windows, etc. ⇒ confined to rooms
- Sound forming seems infeasible with current technology
⇒ positions of senders can not be “virtualized”
- Anti-ultrasound has not yet been demonstrated to work
⇒ pulses can not be blocked after having been sent

Threats depending on attacker position

- General assumption: all wireless attacks possible
- **E0 outside room**: only RF, no US
- **E1 in room**: E0 + US eavesdropping, insert own messages
- **E2 equidistant positions**: E1 + US correct distance measurements
- **E3 in line**: E1 + US correct angle measurements from A
- **E4 in between**: R3 + US correct angle measurements from A and B



[MG 2007] R. Mayrhofer, H. Gellersen: "On the security of ultrasound as out-of-band channel", in Proc. IPDPS 2007

Threats depending on applications

- **Replacement**: DoS attack on B, E3 or E4 misrepresented as B no interaction between A and B
- **Asynchronous MITM**: replacement, then interaction between E and B application-level interaction between A and B with delay
- **Synchronous MITM**: full attack, only possible as E4

Difficult when:

- A and B are mobile
- B positioned so as to make E3 impossible

Remaining threat to address

Possible to address on sensing and application levels:

- Ultrasound distance estimation is not enough, but with **angle-of-arrival measurements** attacker positions are restricted to E3 and E4
- **Strategical placement** of infrastructure devices or mobility to prevent E3
- Introduce **application-level feedback** to rule out replacement and asynchronous MITM (e.g. LED)

Still open:

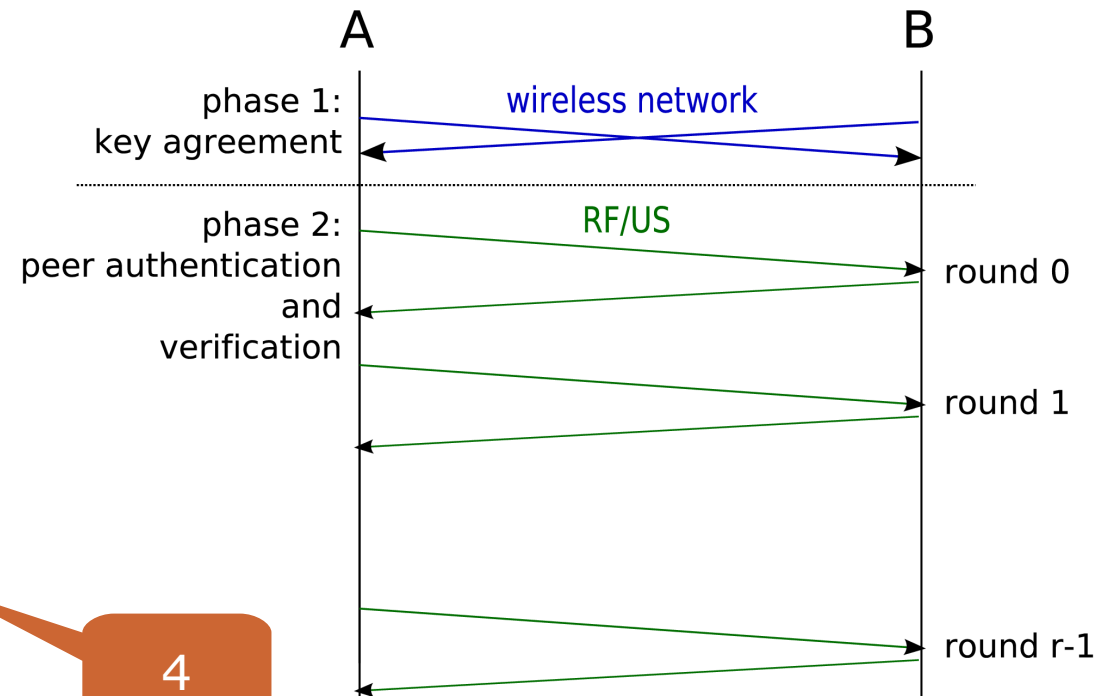
- Attacker E4 with RF-MITM, selective DoS on US to cancel and injecting own US signals

Spatial authentication protocol: concept

Main aspects of the protocol

- uses **2 (3) channels**: RF and US
- with 2 phases: **key agreement** and **peer authentication**
- **Diffie-Hellman** for key agreement in phase 1
- Exchange **random nonces** with **interlock protocol** in phase 2, both via RF (encrypted) and via US (plaintext)
- Interlock exchange tightly **coupled** with US measurements
- Both devices check **locally** that nonces received via RF and US match

3



4

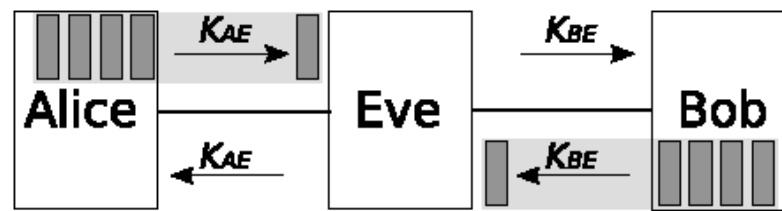
Spatial authentication protocol: interlock

Defending against MITM attacks

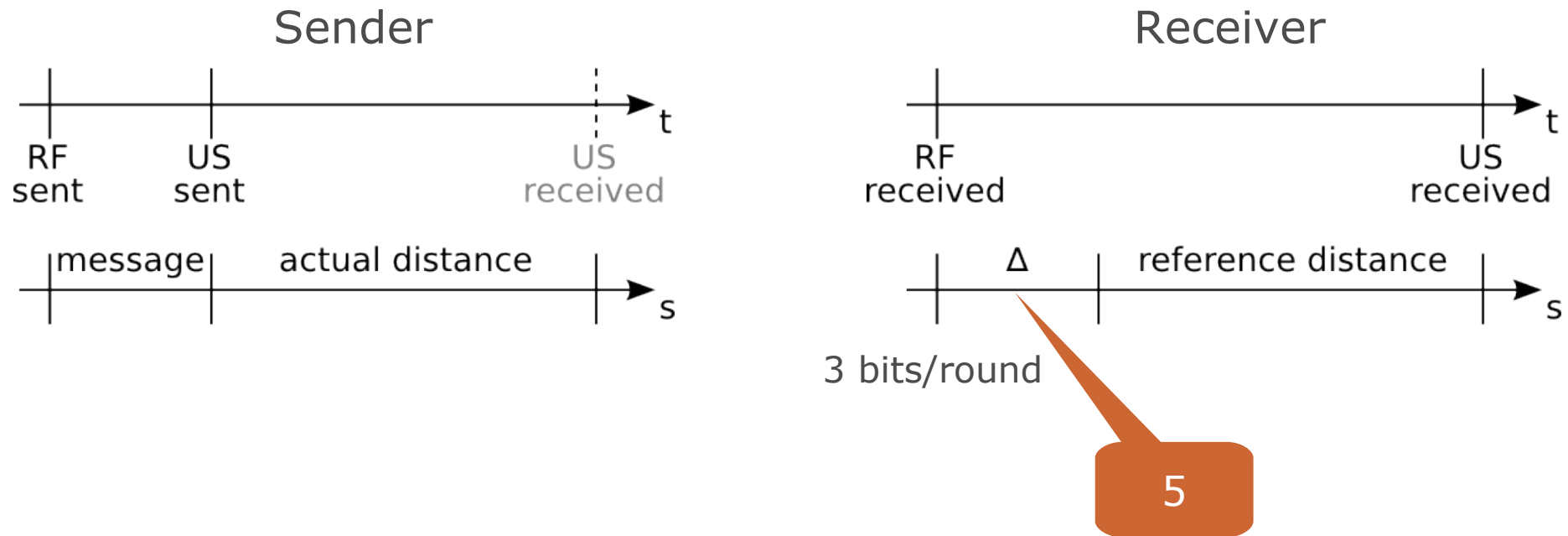
- MITM on RF channels possible by assumption
- Attacker could buffer, delay, re-order, delete, modify, or insert messages

One approach: **interlock** protocol

- RF transmission **encrypted with block cipher** and **split into multiple parts**
 - Peers adhere to **strict turn-taking**
- ⇒ effectively a size-efficient **commitment scheme**



Trick: mapping messages to distances



(Plaintext) message transmission over US channel depends implicitly on reference measurement

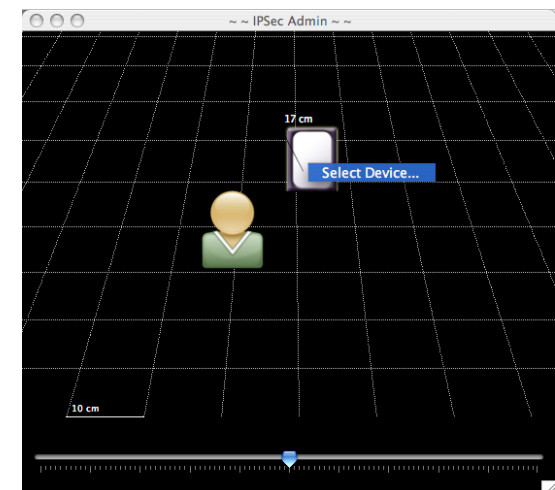
Spatial authentication protocol: security

- Reference measurement can be verified by the user
 - Message is (part of) nonce
 - Nonce is kept secret until ultrasonic transmission
 - Sender already committed to whole nonce transmitted also via RF
 - Just injecting new signals would be detectable
 - E could block signals **only if** it knew when the pulses were being sent in advance
- ⇒ Mapping message to delay/distance and random element make channel authentic using current technology

Implementation based on Relate

Current implementation of the method

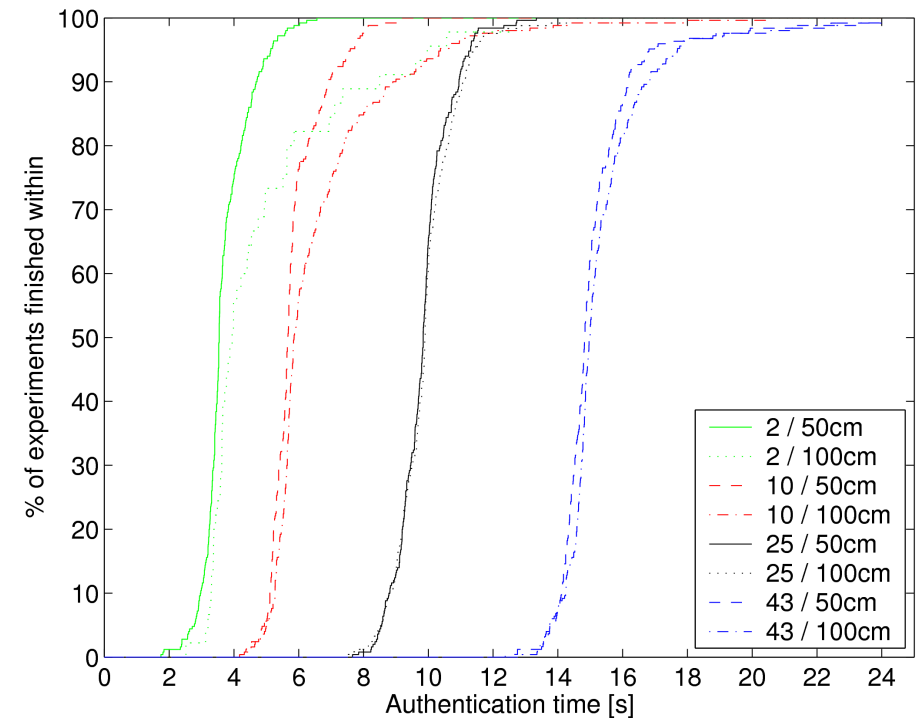
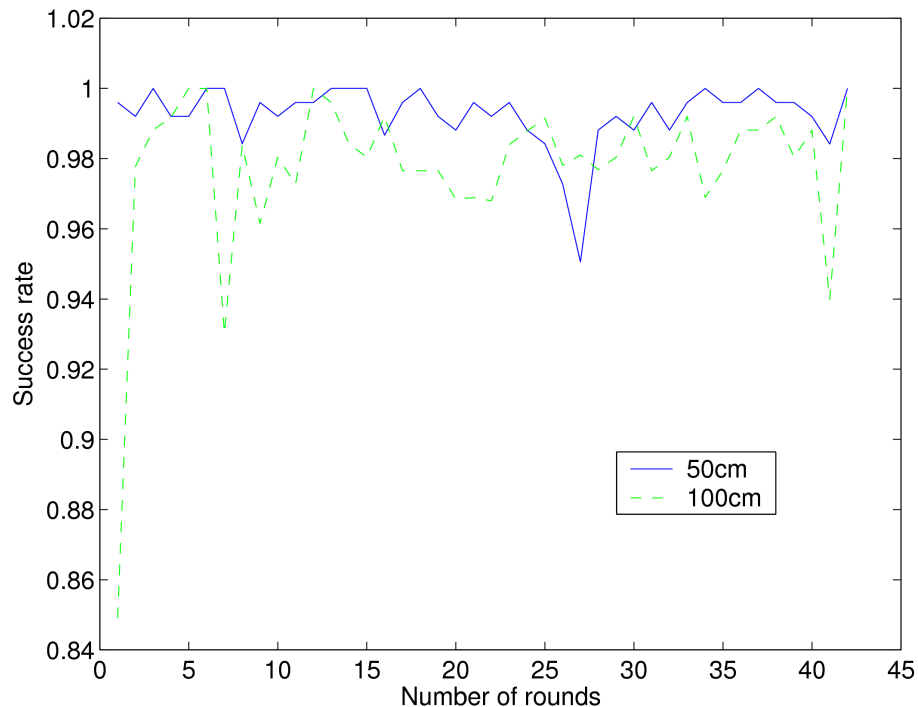
- Uses Relate "dongles" or "bricks" with enhanced firmware for interlock and sensing level verification
- Host implementation for Java 1.2 provides Diffie-Hellman, encryption/decryption, and distance/nonce verification
- GUI integration as simple as possible: one method call, callback with shared secret authenticated key



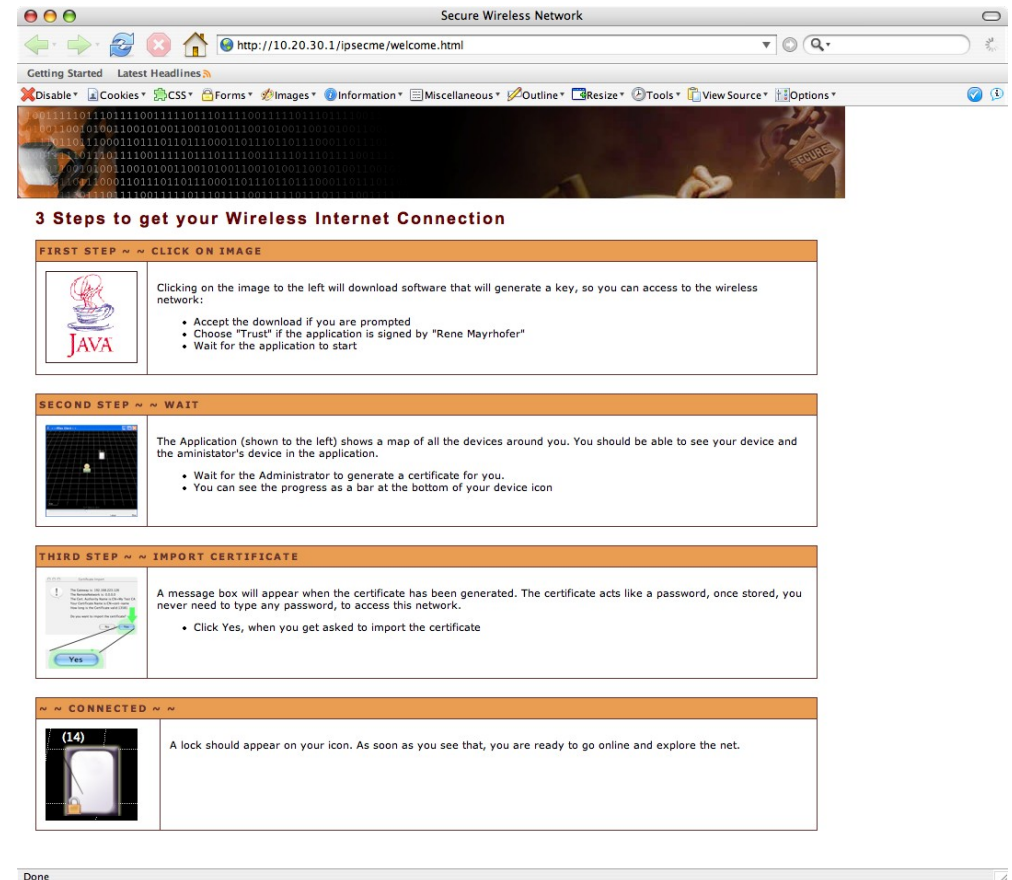
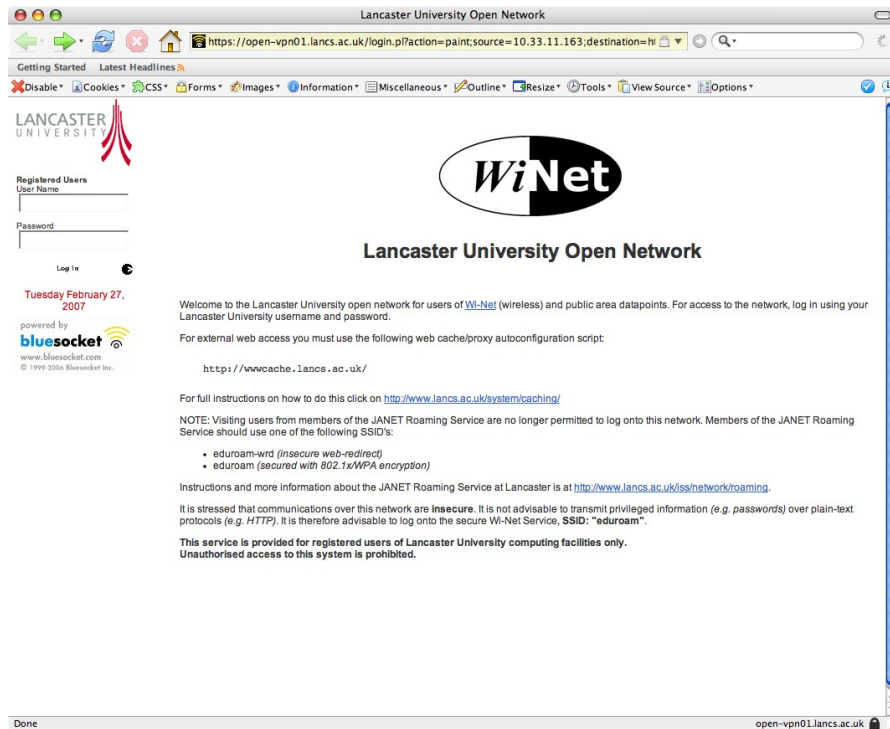
Quantitative evaluation

Noise in US measurements

- leads to authentication failures without attack (false negatives)
- can be improved with re-transmits



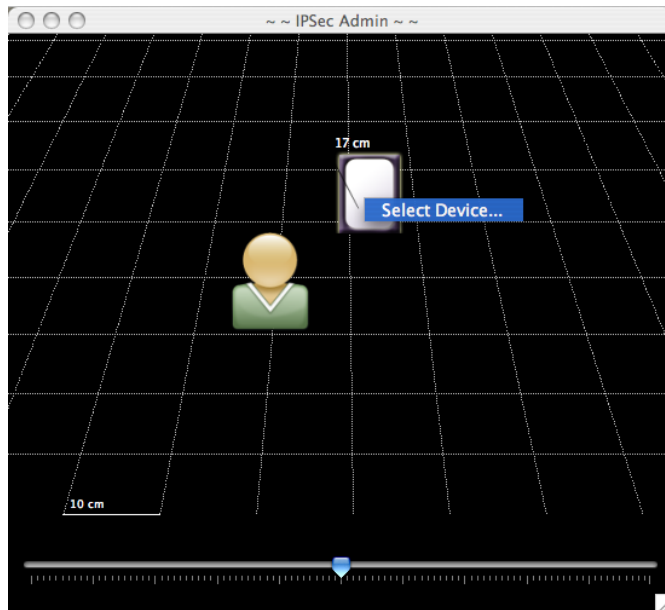
"IPSecME" for securing WLAN access



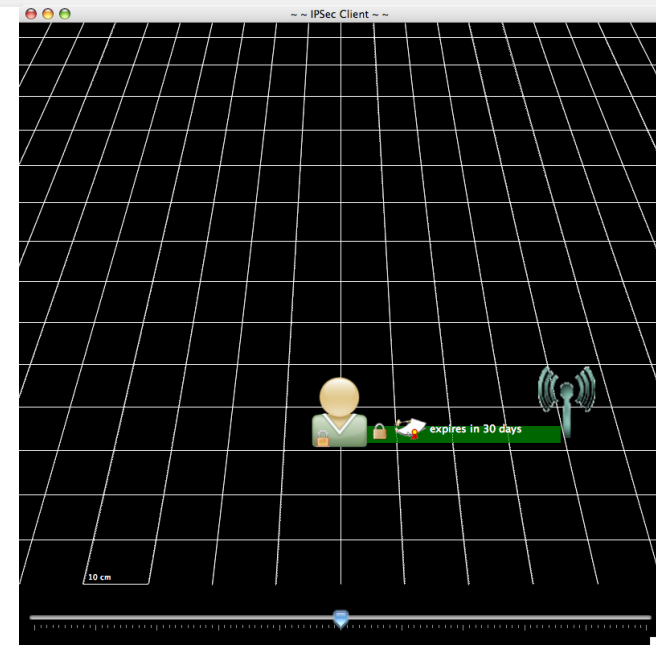
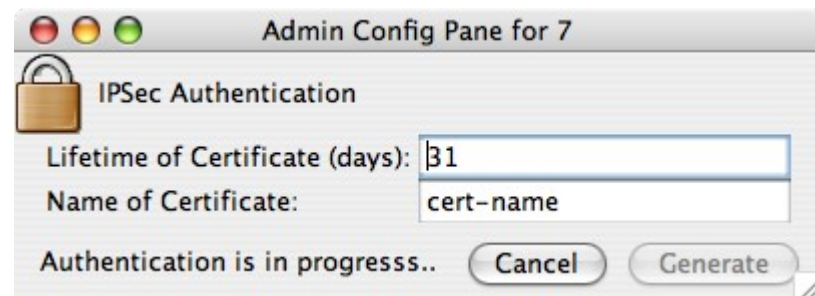
[MG 2007] R. Mayrhofer, R. Gostner: "Using a spatial context authentication proxy for establishing secure wireless connections", Journal of Mobile Multimedia, 2007

"IPSecME" for securing WLAN access

Admin

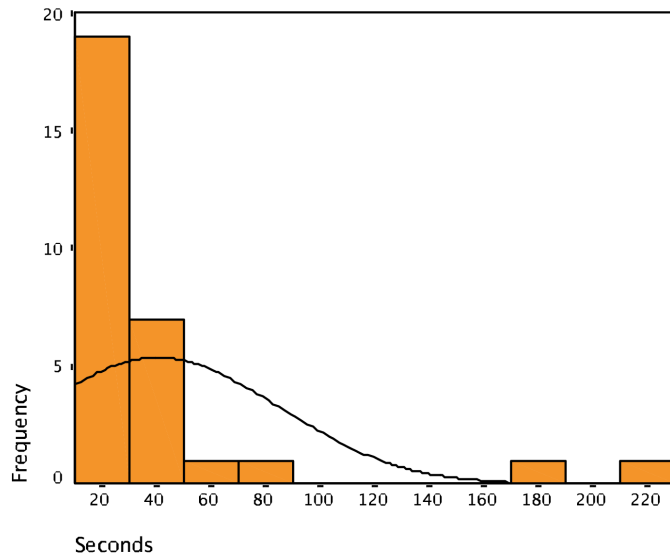


New client

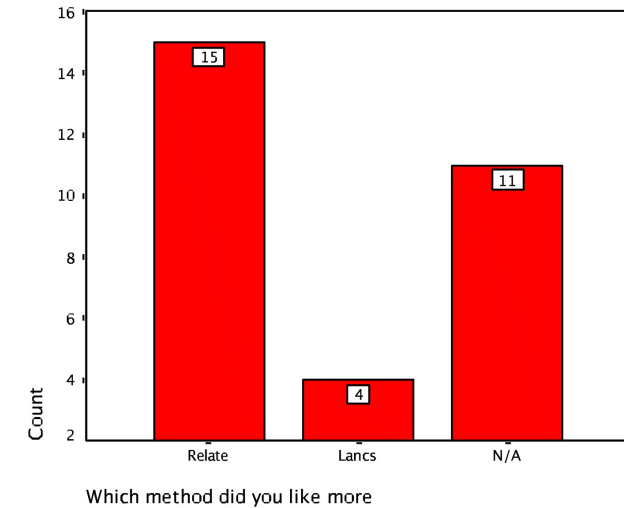
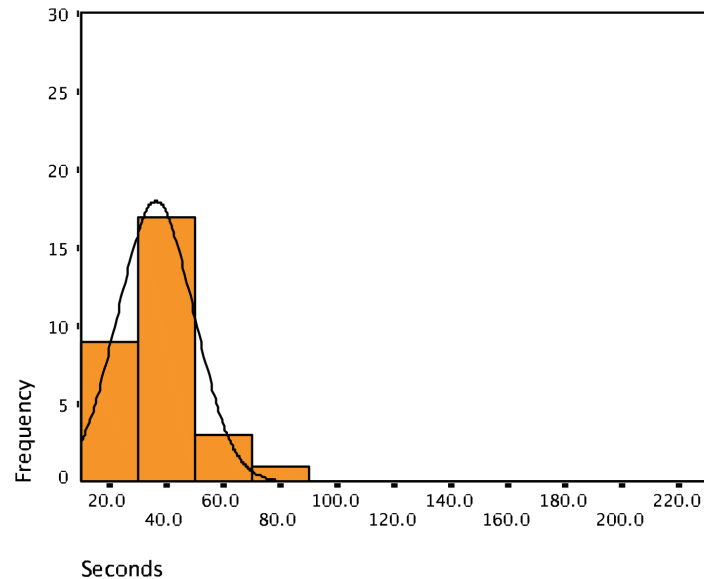


Captive portal password vs. IPsecME

Browser authentication

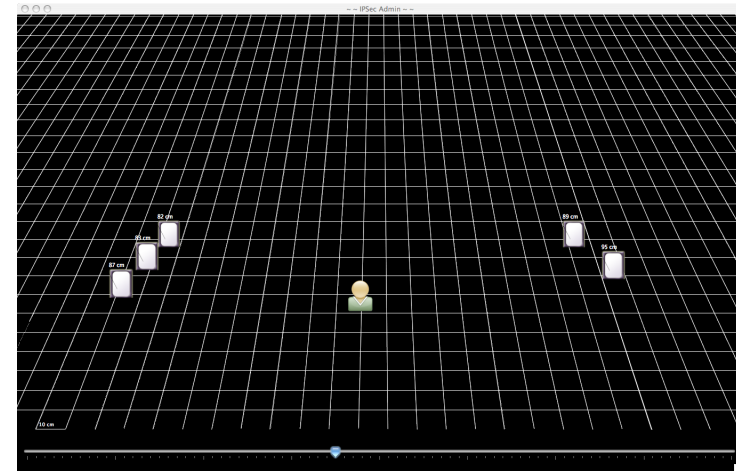
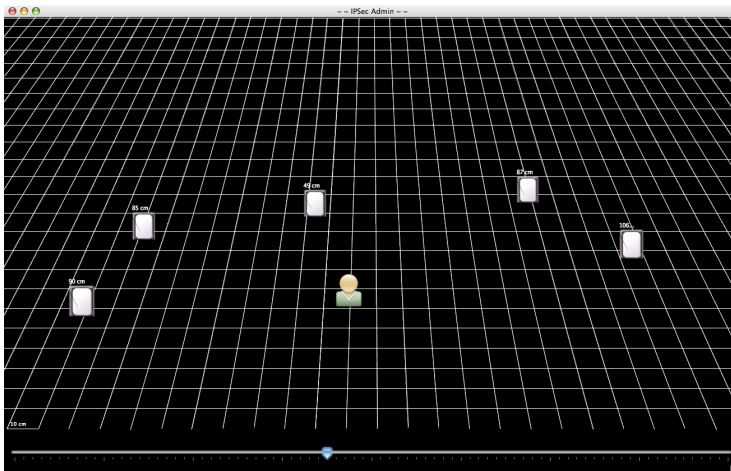
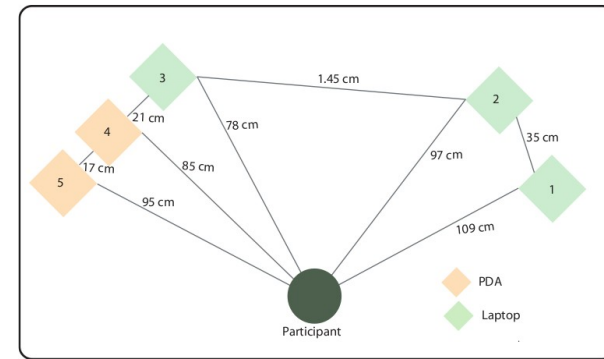
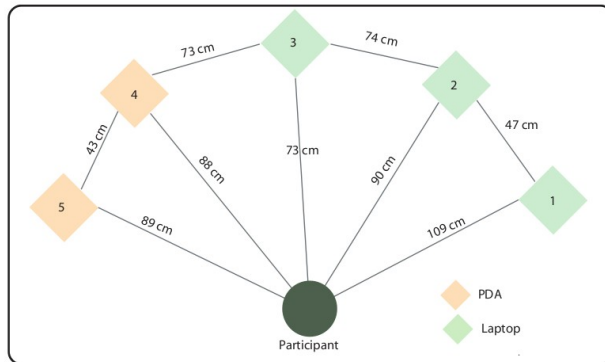


Spatial authentication



[MG 2007] R. Mayrhofer, R. Gostner: "Using a spatial context authentication proxy for establishing secure wireless connections", Journal of Mobile Multimedia, 2007

Spatial references and real world mapping



⇒ out of 30 subjects, only 4 made any error at all

[MG 2007] R. Mayrhofer, R. Gostner: "Using a spatial context authentication proxy for establishing secure wireless connections", Journal of Mobile Multimedia, 2007

What have we done?

- **Spatial references** can be verified both by users and their devices
- **Implicit** instead of explicit **authentication**
- Protocol uses
 - 2 phases: **key agreement** and **peer authentication**
 - Peer authentication done via **interlock**, tightly **coupled with spatial measurements**
 - Messages in US channel are **encoded as time/distance differences**

“The problem with passwords is that they are too easy to lose control of.”

Bruce Schneier, March 2005

Thank you for your attention!

Slides: <http://www.mayrhofer.eu.org/presentations>

Source code: <http://ubicomp.lancs.ac.uk/relate>

Later questions: rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE

7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE