

# On the Security of Ultrasound as Out-of-band Channel

SSN 2007, IPDPS 2007

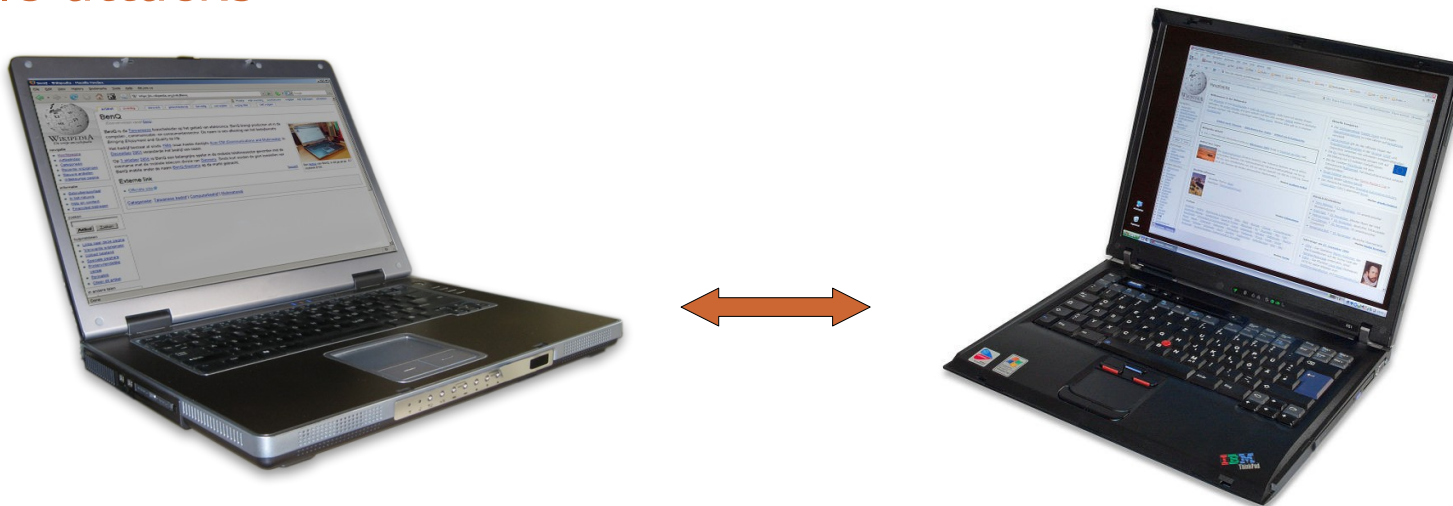
30. March 2007 11:00, Long Beach, CA, US

Rene Mayrhofer, Hans Gellersen  
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 and verify (authenticate) via some **out-of-band channel** to **prevent man-in-the-middle attacks**



# How does ultrasound help to solve it?

(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**

# 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

# 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

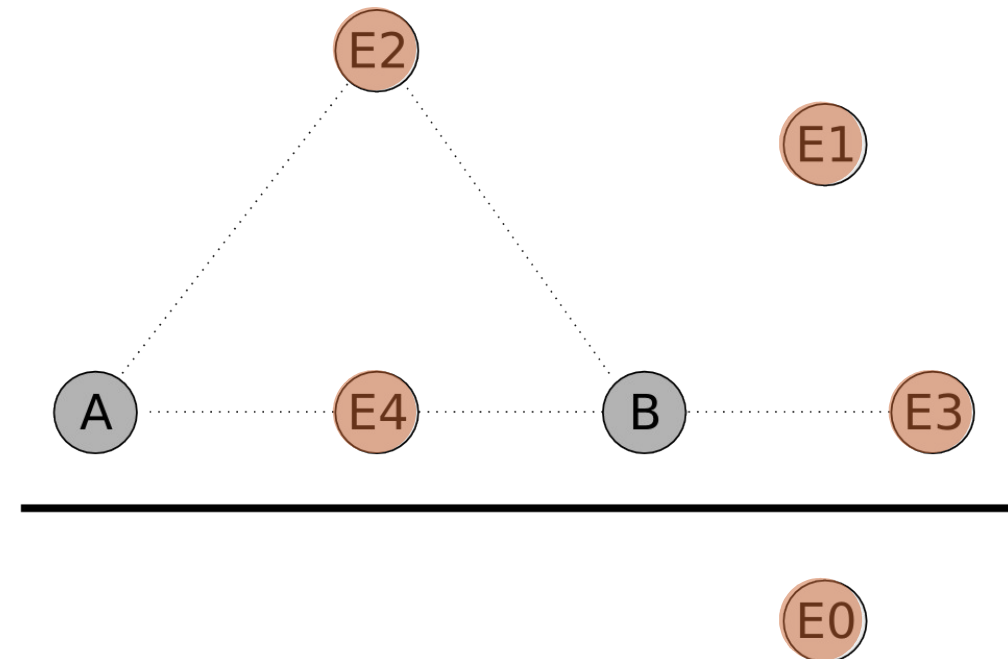


## Relate:

- $<10$  cm accuracy for distance measurements
- $\sim 33^\circ$  accuracy for local angle-of-arrival

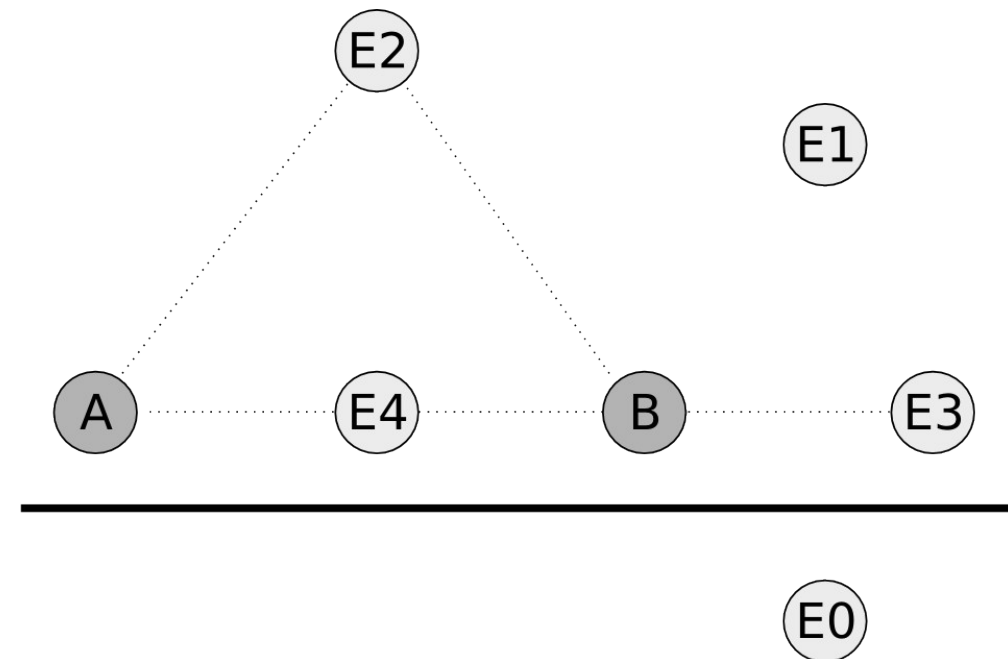
# Threats depending on attacker position

- 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



# Threats depending on attacker position

- **E0 outside room:**
  - a) DoS
  - b) cause erroneous distance measurements
  - c) modify shared measurements
- **E1 in room:**
  - d) eavesdrop on US
  - e) insert US pulses and messages
  - f) block US transmission
- **E2 equidistant positions:**
  - g) appear at same distance (also  $b + e$ )
- **E3 in line:**
  - h) appear from same angle as B to A
- **E4 in between:**
  - i) appear from same angle to both
  - j) cancel or modify US in transit



# 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:

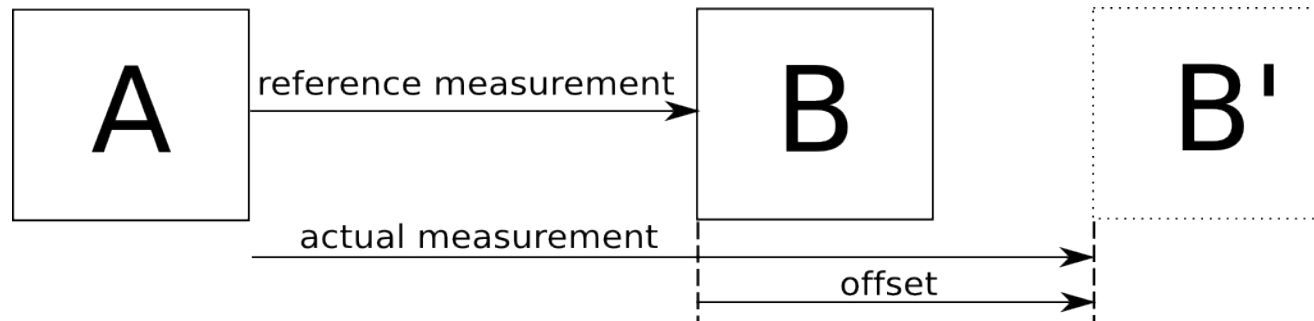
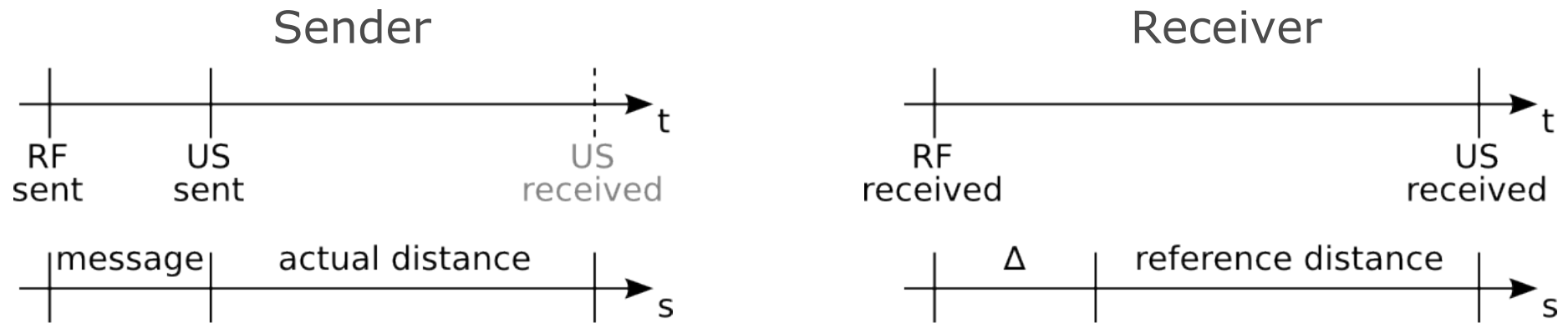
- Ultrasound distance estimation is not enough, but with **angle-of-arrival measurements** attacker positions are restricted to E3 and E4
- **Strategical placement** of infrastructure devices or mobility to prevent E3
- Introduce **application-level feedback** to rule out replacement and asynchronous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

Still open:

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

**Authentic communication over ultrasound**

# Trick: mapping messages to distances

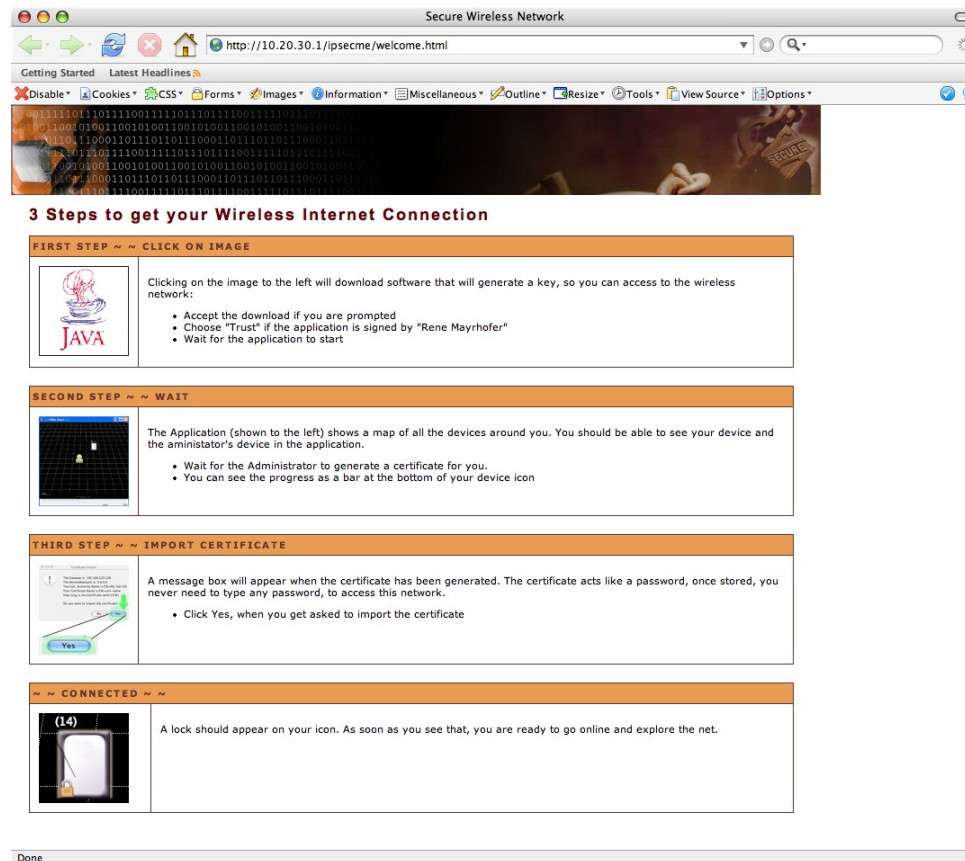


# Making ultrasonic messages authentic

- Reference measurement can be verified by the user
  - Message is (part of) nonce
  - Nonce is kept secret until ultrasonic transmission
  - Nonce can be used as part of higher-level authentication protocol
  - 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

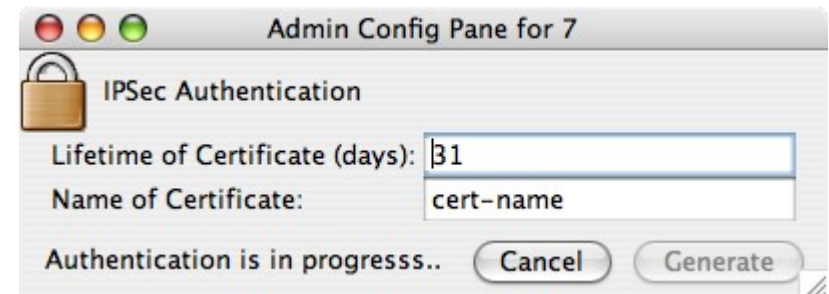
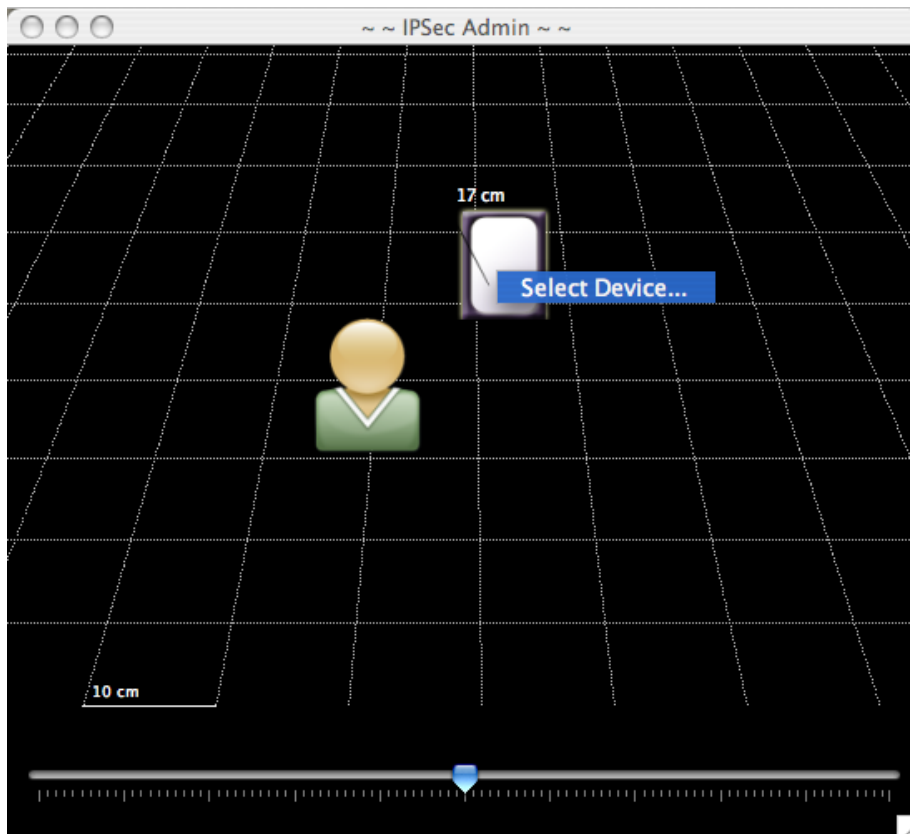
# Demonstration applications using OpenUAT

**IPSecME** (IPSec Made Easy): creating IPSec connections using a spatial authentication proxy



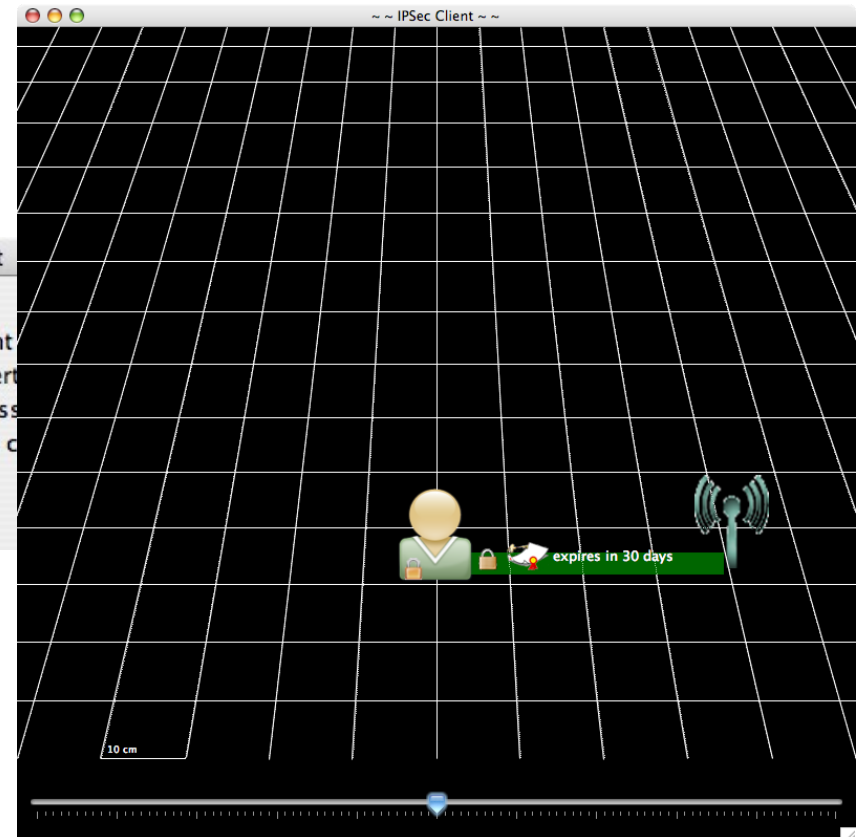
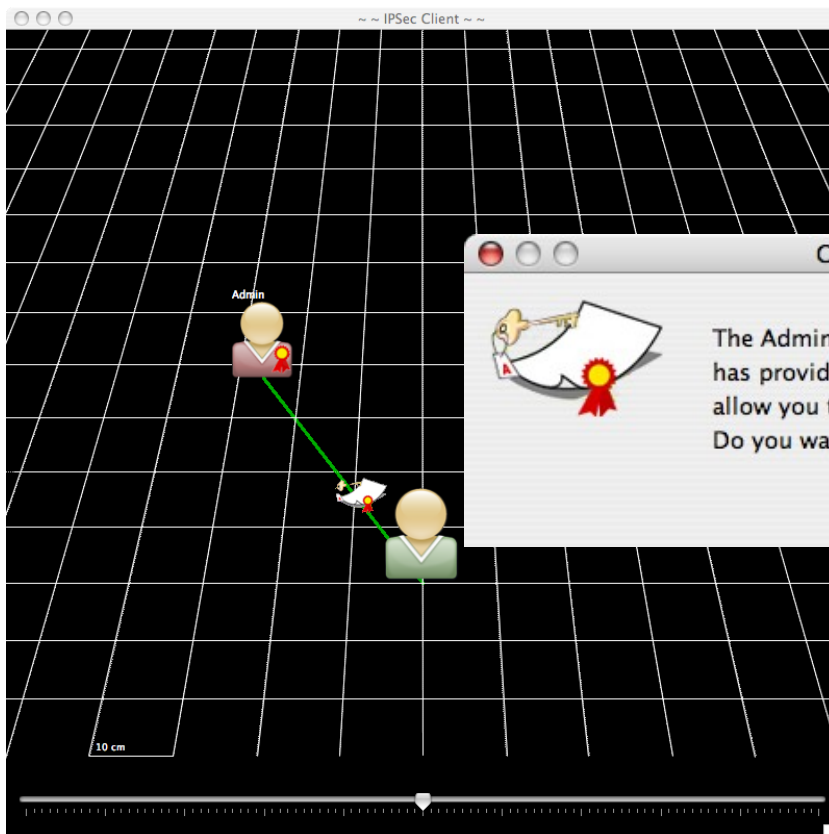
# Demonstration applications using OpenUAT

**IPSecME** (IPSec Made Easy): creating IPSec connections using a spatial authentication proxy



# Demonstration applications using OpenUAT

**IPSecME** (IPSec Made Easy): creating IPSec connections using a spatial authentication proxy



“Portability is for people who cannot write new programs.”

Linus Torvalds, 1992-01-29, comp.os.minix

# Thank you for your attention!

Slides: <http://www.mayrhofer.eu.org/presentations>  
Later questions: [rene@mayrhofer.eu.org](mailto:rene@mayrhofer.eu.org)

OpenPGP key: 0xC3C24BDE  
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE