



Context authentication: making secure communication more user-friendly

2. February 2006, Helsinki

Guest lecture 2

Rene Mayrhofer

Computing Department

Lancaster University, UK

rene@comp.lancs.ac.uk

Security in Ubiquitous Computing

Introduction

- Security is currently one of the largest problems in computer science (not the only one though...)
- Possible reason: often added as an **after-thought**
- Examples of large-scale security problems: Blaster (2003), Sasser (2004), Phishing/Pharming (2005ff)
- Security issues in server- and desktop-based computing already have a **large impact on real life**: ATM machines, UK coast guard, private online banking, ...

Why?

What?

How?

Current work

- Ubiquitous/pervasive computing aims to embed computer systems into objects of the real world, transparently, networked, and – most of the time – **invisible**
- In ubiquitous computing, many recent publications mention that „**security will be added in future research**“
- Security in ubiquitous computing has hardly been explored, some works even violate Kerckhoff's principle

Summary

Security vs. Privacy

Introduction

- Privacy is another major issue of many current ubiquitous computing systems/applications, but this lecture is not about privacy (cf. Marc Langheinrich)
- Security is a **necessary** building block for privacy, but is not **sufficient**

Why?

What?

How?

Current work

Summary

„When making public policy decisions about new technologies for the Government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the Government to deploy those technologies. This is simply a matter of good civic hygiene.“

(Phil Zimmerman, author of PGP, to the congress of the US)

Terminology

Introduction

Usual security requirements:

- **Secrecy** (prevent unauthorised reading)
- **Integrity** (prevent unrecognised modification)
- **Authenticity** (prevent impersonation)
- **Non-repudiability** (authenticity to third parties)



Why?

What?

How?

Current work

Summary

Additional terms:

- Identification
- Authentication
- Authorisation
- Availability

Basic methods from cryptography

Introduction

Encryption

- solves the issue of secrecy

Why?

What?

How?

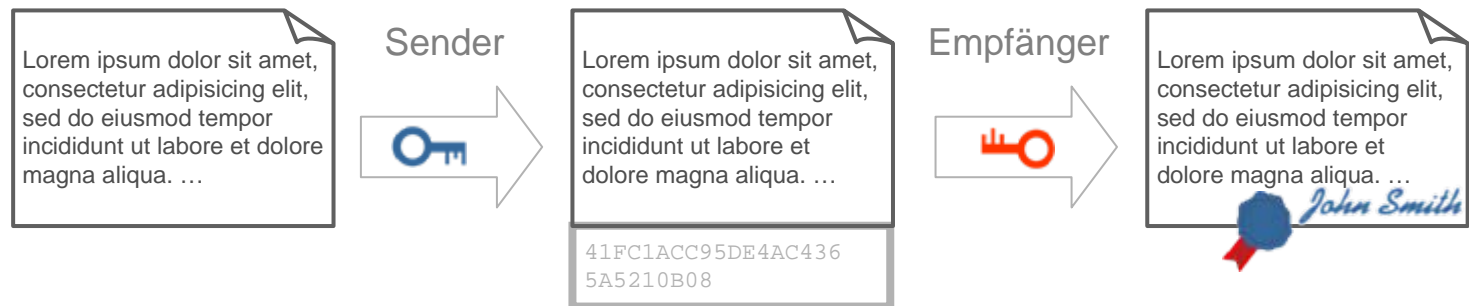


Current work

Digital signature

- Solves the issue of integrity

Summary



Cryptography can provide technical solutions to secrecy and integrity, but for authenticity (and non-repudiability), we need authentication

Remark: identification, authorisation, and availability can only be considered in conjunction with social, organisational, and legal aspects

Why authenticate?

Introduction

- To provide authenticity (and potentially non-repudiability)

Why?

- Authentication affirms the identity of the subject that was identified in a previous step

What?

- Well-known in conventional computer systems: log in at local computer, at web pages, SSH, SSL, ...

How?

- Authentication is necessary to prevent MÎTM attacks

Current work

- Remark: most of the time, authentication is mixed with identification

Summary

What to authenticate?

Introduction

- Which **subject** should be authenticated?

Why?

- **user**
- **device**
- **action**

What?

- Which **property**?

How?

⇒ depends on the subject

Current work

- Users

- **what I know** (password)
- **what I have** (token, smart card)
- **what I am** (fingerprint, iris)

Summary

- But: more difficult if no direct interface is available, i.e. no display, no keyboard, etc.



Context Authentication

Introduction

- Authentication is harder in ubiquitous computing because there is no conventional UI

Why?

- But: ubiquitous computing builds upon the notion of **context**
- ⇒ exploiting this context for authentication allows to build more intuitive methods of authenticating

What?

- Users

How?

- **what I know** (password)
- **what I have** (token, smart card)
- **what I am** (finger print, iris)
- **where I am**
- **what I am doing**
- **who is with me**
- **what I ate** (hopefully not...)
- **how I feel** (hopefully not...)
- ...

Current work

Summary

User vs. device authentication

Introduction

- User authentication works well for the “1:1” (one user, one device) and “n:1” (many users, one device) cases, i.e. for typical server- and desktop-computing

Why?

What?

- But: scales poorly for the “1:n” (one user, many devices) approach that ubiquitous computing is proclaiming

How?

- Intuitive alternative to direct user authentication: a **trusted personal device** that authenticates its user once (e.g. when being switched on) and is assumed to be owned and used by a **single user**:

Current work

- cf. conventional key chain
- PDA
- mobile phone

Advantage: **unobtrusive**, **scales** well to many devices

Challenges: this device must be **secure**



Summary

- Authentication is thus shifted from user-to-device to **device-to-device**

How not to touch the data devices?

Introduction

Frank Stajano: simple solution of direct electrical contact

Why?

What?

How?

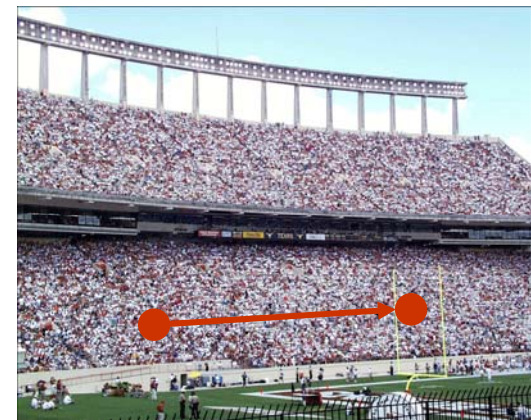


but: ...

Current work

- direct electrical contact is fragile and wears out
- is often infeasible because of distances

Summary



Context authentication between devices

Introduction

- We can define **context authentication** as:

A group of devices is authenticated with each other when certain aspects of their context match.

Why?

What?

- Therefore, use appropriate sensors to ensure that two or more devices have a common context

How?

- Tim Kindberg et al: Concept of “**constrained channel**”:
 - channels that are restricted by contextual constraints
 - either send- or receive-constrained

Current work

- Dirk Balfanz et.al: “**location-limited channel**”:
 - modelled after Frank Stajano’s work
 - requires “demonstrative identification”: identification based on physical context (i.e. location)
 - requires authenticity of the channel

Summary

Aspects of Context

Introduction

Context has a vast multitude of different aspects, e.g.

Why?

- time
- location
- physical (temperature, humidity, etc.)
- social (with colleagues / family etc.)

What?

Which aspects of context seem to be useful for authentication?

How?

Current work

Summary



⇒ Location is very **intuitive**, unobtrusive, and offered by a wide range of different sensors

How to authenticate: positioning techniques

Introduction

Conventional methods:

- **GPS**
- other **RF** time of flight/signal strength (e.g. GSM)
- **ultra sound**

Why?

What?

Methods depending more on qualitative than on quantitative factors:

How?

- **visible light** (laser, but also LED/display and camera)
- **infrared**
- **audio**
- **motion**

Current work

Summary

But never forget the users: we design for users, so be aware of their perception of how secure an authentication method seems to be.

Summing up: Taxonomy of ubiquitous authentication (v0.1)

Introduction

What?

- users
- devices
- actions

Why?

What?

How?

- user is **controlling** (passive) element (e.g. DH, then):
 - comparing keys by some visual representation of hashes (very bad: text, slightly better: image, but not tested in field)
 - „physical interlock“
 - Harmony protocol
- user is **acting** (active) element (key generated out of sensor data):
 - shaking, cf. Smart-Its friends
 - „Synchronous Gestures for Multiple Persons and Computers“
 - speaking (audio correlation)
 - „SyncTap“
 - one-button protocol (cf. Iwasaki „Touch-and-Connect“)
 - Human as electrical contact

How?

Current work

Summary

Authentication proxy

Introduction

Context authentication requires at least some sensors

Why?

- what if a device can not sensibly be equipped with such sensors?
- what if it would be simply inconvenient to share context with the device?

What?



How?

Current work

⇒ use an **authentication proxy**:

Summary

- associated with the real target by some pre-shared knowledge
- authenticate with this one instead
- Difference to e.g. laptop: is often shared temporarily, an authentication proxy should never be shared

Prototype 1: Spatial authentication using ultra sound (v0.8)

Introduction

Relate is a system for relative positioning

Why?

- based on ultra sound
- currently 2D, 3D is being worked on
- accuracy: <10cm, <30°

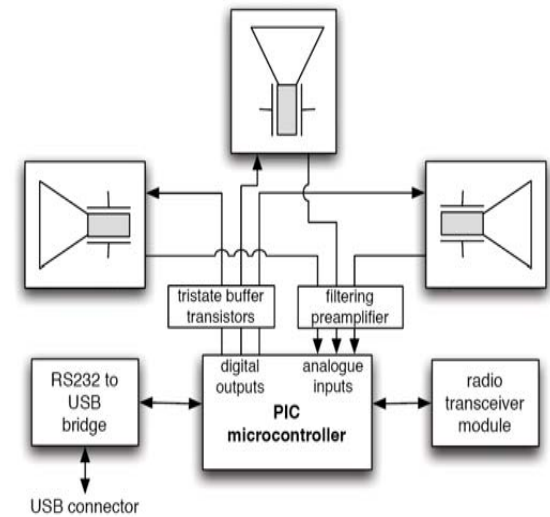
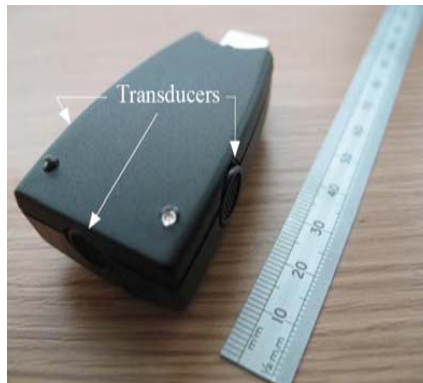
What?

- no infrastructure support required, but peer-to-peer
- currently implemented in the form of USB dongles (based on Smart-Its) and Java host software

How?

Current work

Summary



Security analysis

Introduction

Relate positioning based on:

- **RF** network for
 - managing network state
 - time-of-flight measurement triggering
- **Ultra sound** transducers for
 - sending ultra sound pulses synchronously with RF packets
 - receiving ultra sound pulses after receipt of an RF trigger packet

Why?

What?

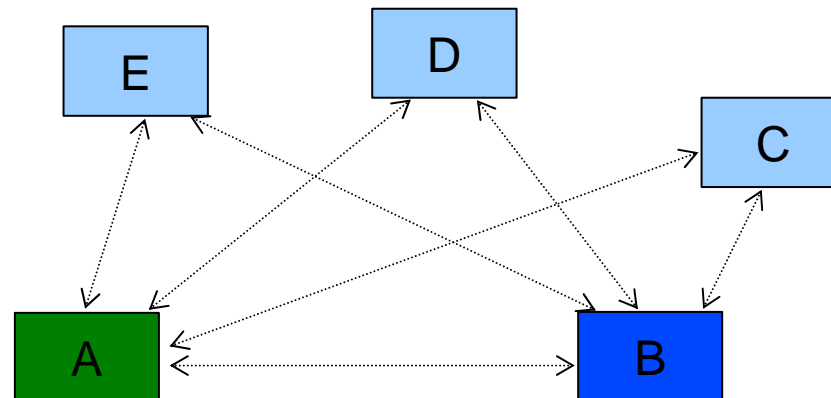
How?

Possible attacks:

Current work

- RF network completely open to passive and active attacks
- Ultra sound completely open to passive attacks, active attacks more difficult

Summary



At the moment **bilateral connections**, group authentication is planned

Spatial authentication protocol overview

Introduction

1. non-Relate RF channel (e.g. WLAN, BT) used for **zero-knowledge key-agreement** protocol (e.g. DH)

Why?

2. each host finds a random number used only for this authentication (**nonce**)
3. nonces are transmitted both over the RF and the ultra sound channels over **multiple rounds**:

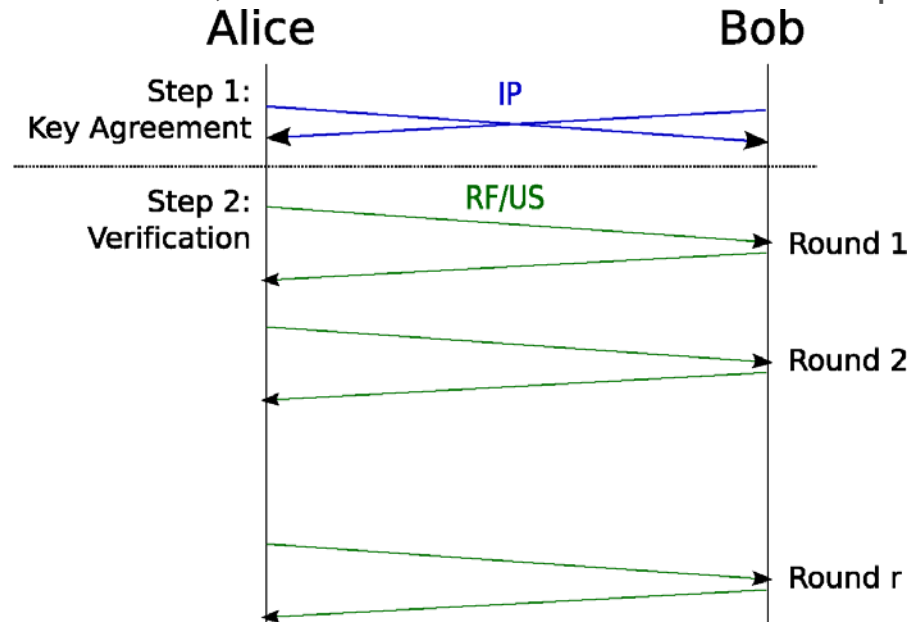
What?

- **encrypted** with the session key of step 1 over RF
- as **plaintext** over ultra sound

How?

4. both hosts compare the received RF packets with the data received within the ultra sound channel, authentication successful when equal

Current work



Summary

Interlock protocol against MiTM

Introduction

How can an attacker be prevented from:

Why?

1. Performing an active **MITM attack on the RF level** (possible by assumption)
⇒ shared key with Alice and shared key with Bob

What?

2. **Decrypting** the packets sent by Alice on th RF level

3. **Re-encrypting** them for and forwarding them to Bob (and vice versa)

How?

▪ Note: this attack could be performed purely on the RF level (no eavesdropping or active attacks necessary on ultra sound channels)

Current work

Solution: **interlock protocol**

▪ RF packets are **block-encrypted and split** over multiple rounds

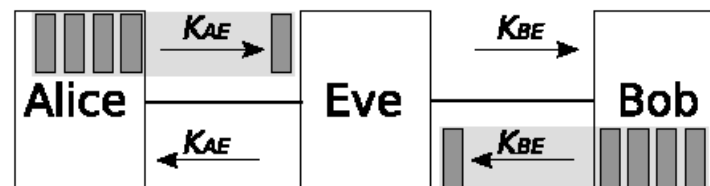
▪ Packet $i+1$ is only **sent after the receipt** of packet i from the other host

Summary

⇒ MITM can not decrypt packets before all rounds have been completed

⇒ MITM can not store packets and wait until all have been sent before forwarding *something* to the other host

⇒ Hosts effectively commit themselves to what they will be sending later



Spatial authentication protocol details

Introduction

Why?

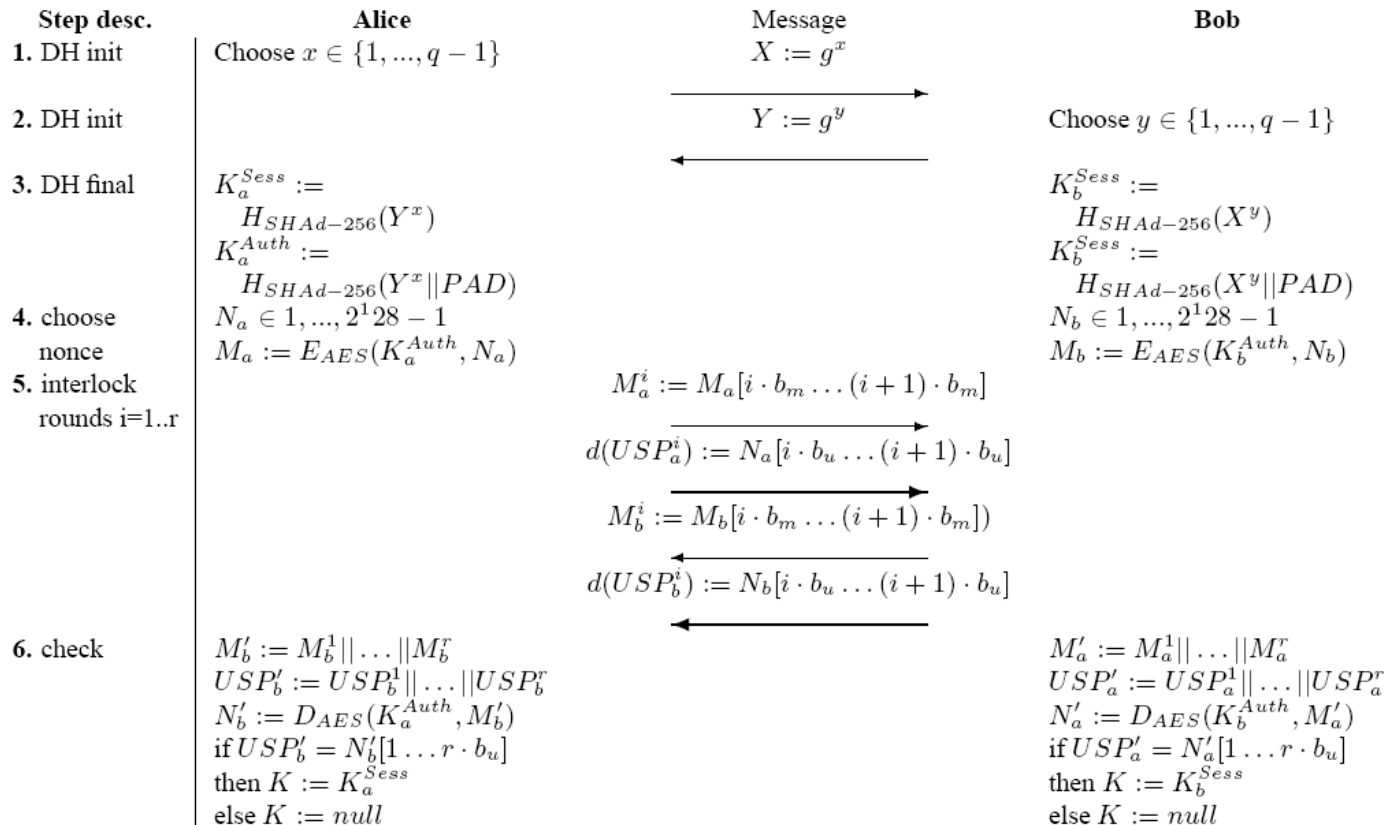
- Ultra sound transducers send only single, un-encoded pulses
 - Method to transmit information: delay pulses at sender and compute transmitted value at receiver by subtracting a reference measurement
- ⇒ Transmitted value **depends implicitly on reference measurement** (which has been used to select the device in the first place, i.e. for identification)

What?

How?

Current work

Summary



User interaction (alpha)

Introduction

Aims

- Intuitive
- Unobtrusive
- Simple

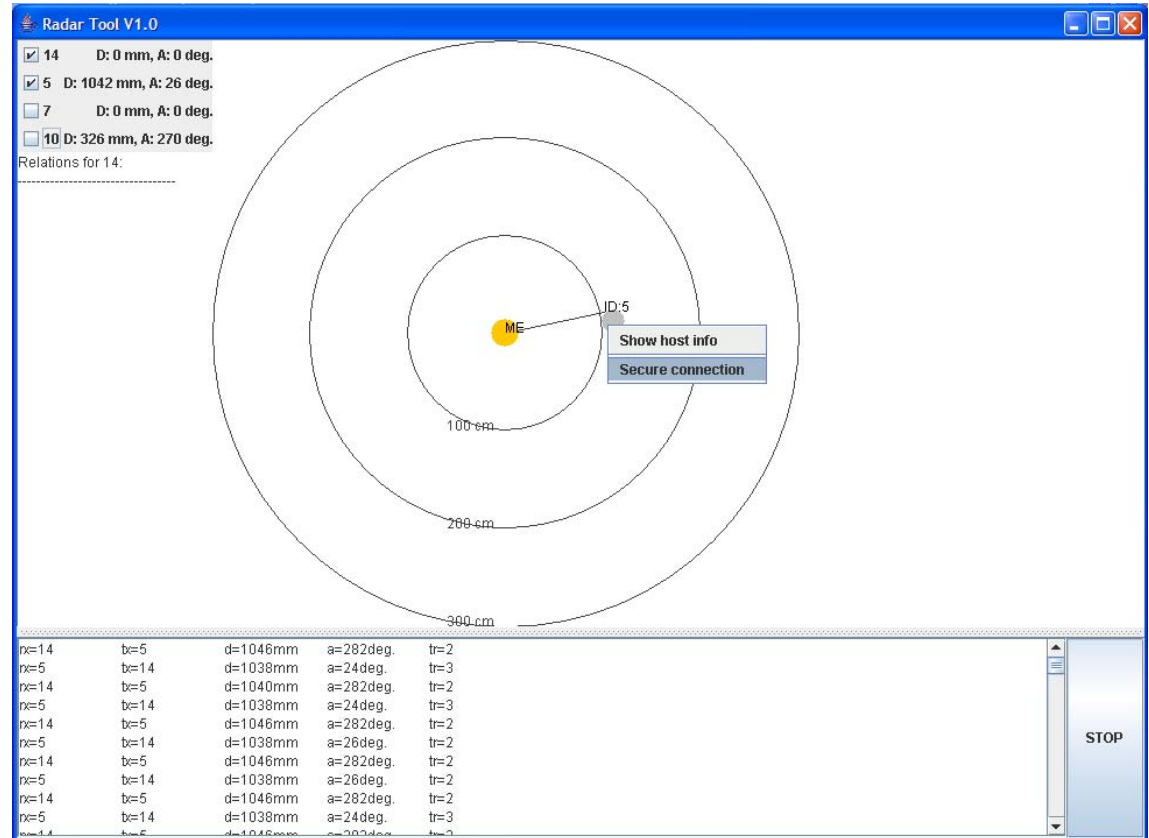
Why?

What?

How?

Current work

Summary



Threat scenarios and protocol security

Introduction

Threat scenarios

- **Passive Eavesdropping on RF and ultra sound:** if a zero-knowledge key-agreement protocol is used, should not reveal anything (no plaintext is transmitted other than nonce)
- **Active MITM on RF level:** could agree to a key K_a with A and a (different) key K_b to B and relay messages (but could not decrypt and re-encrypt parts of messages)
- **Active MITM on ultra sound level:** if combined with RF MITM, then attack will be successful – it would probably need two devices near hosts A and B that collaborated with each other
- **DoS on RF or ultra sound:** can currently not be dealt with, next hardware generation will allow better resistance against DoS
- **Attacks on the two devices themselves:** out of the scope of this research

Why?

What?

How?

Current work

Protocol security

- **Based on the following assumptions:**
 - it is very difficult for an attacker to fake the direction of ultrasonic pulses
⇒ all hosts should check that the receiving characteristic does not change during the authentication phase, the user should check that there is nothing between the devices and nothing close to them
 - the device we authenticate with is itself secure....
 - DH is secure, chosen symmetric block cipher is secure
 - random number generation on A and B is secure, i.e. it is **very** unlikely that $K_a = K_b$
- **Security comes from:**
 - the encrypted N_a/N_b can only be decrypted after **all** parts have been received, and then the peer has already committed itself to all the delays

Summary

Prototype 2: Motion authentication (v0)

Introduction

Smart-Its friends

- two Smart-Its: one master, one slave
 - master broadcasts its accelerometer data via RF
 - slave compares this stream with its own accelerometer data
 - association when “close enough”
- ⇒ **motion authentication**: shake two (or more) devices together to associate them with each other

How?

Current work

Secure implementation

- can not simply send accelerometer data, because then an attacker could replay it
- Two possibilities:
 - generate key material directly from sensor data: concepts from fuzzy cryptography/biometrics, can be extended easily to group authentication
 - zero-knowledge key agreement and authentication using interlock protocol (again to prevent simple replaying attacks after MITM on the key agreement)

Summary

Summary

Introduction

- Security in ubiquitous computing is still largely unexplored.

Why?

- Authentication is necessary to create secure connections.

What?

- Due to scalability issues, we expect direct user-to-device authentication to be replaced by device-to-device authentication.

How?

- Context authentication might be a scalable, intuitive, and unobtrusive way method device-to-device authentication.

Current work

- Location is a good choice due to its intuitiveness.

Summary

- Current work implements spatial authentication based on ultra sound sensing without infrastructure support by using zero-knowledge key agreement and the interlock protocol against MITM attacks.
- A Taxonomy of authentication methods for ubiquitous computing can help future applications to select appropriate ones.

“We must plan for freedom, and not only for security, if for no other reason than only freedom can make security more secure.”

Karl Popper

“Science may be described as the art of systematic over-simplification.”

Karl Popper



Thank you for your attention!

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

Later questions: rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE

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