

Security for Spontaneous Interaction: Problems and Examples

Rene Mayrhofer
University of Vienna
21. April 2008, 12:00 CET

Security in Pervasive Computing

- 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, ...
- Ubiquitous/pervasive computing aims to embed computer systems into objects of the real world, transparently, networked, and – most of the time – **invisible**
- Many projects mention that “**security will be added in future research**”

Most important aspect: Usability

If security and/or privacy and usability collide, then usability always wins!

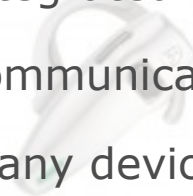
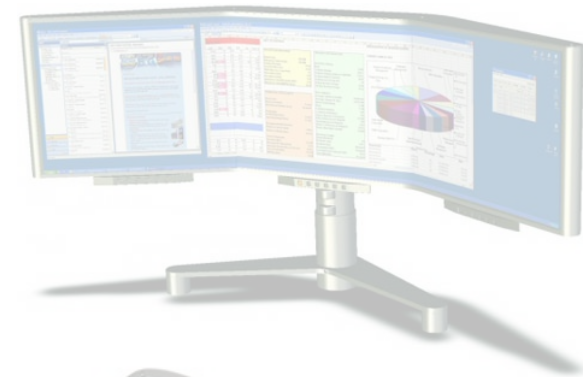
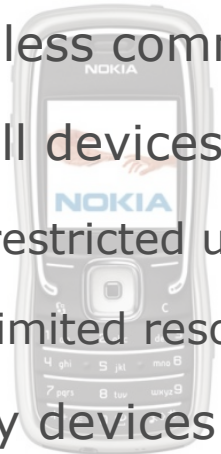
- When security methods or implications on users' privacy are not properly understood, systems will be used incorrectly
- Annoying and obtrusive security measures are simply deactivated so that users can get their jobs done
- For example:
 - sharing passwords, never logging out
 - writing PIN on back of card, most often used PINs "1234" and "0000"
 - "ALERT: The URL says www.mybank.com, but the certificate is for cracker.net, really continue?" - "Yeah, whatever, just let me enter my PIN and TAN codes now..."

Pervasive Computing: What is different?



Pervasive Computing: What is different?

- Wireless communication
 - Small devices
 - restricted user interfaces
 - limited resources (battery life!)
 - Many devices
 - integrated into physical objects
 - communicate among each other
 - many devices communicate with one user
 - Sensors
- ⇒ Devices and communication become **invisible**, **unverifiable**, and **uncontrollable**



Security for Ubiquitous Computing

- Security for whom?
 - User
 - mobile device
 - used service
- How much security?
- (One) real problem:
mobility (spontaneous interaction) + security + usability
- Specific issues of security for ubiquitous / mobile computing
 - wireless communication
 - user interfaces
 - scalability

Wireless communication

Main issue 1: **Wireless communication is insecure**

- Potential attacker can

- eavesdrop
- modify
- remove
- insert



- Especially problematic for spontaneous interaction: **no a priori information** about communication partners available

⇒ User needs to establish **shared secret** between devices

Why is wireless a problem?

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**

User interfaces

Options for authentication

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

Main issue 2: **Lack of powerful user interfaces**

- A headset doesn't have a classical user interface (display + keypad)

And somebody needs to do it...

Main issue 3: **User attention does not scale**

- Vision of ubiquitous computing: using **hundreds** of services each day, seamlessly embedded into daily live, **spontaneous** usage, different realms of control
- Who would like to enter passwords or biometric data into each of them?

General approach: using trusted personal devices

- A personal device for each user (2006: 478.4 million mobile ph in the EU, 108% mobile phones rate in Austria [DerStandard.at, 2007/03/30])
- Important: personal device device may be trusted, but wireless connections are not ⇒ **human-verifiable authentication**



What else is difficult?

- **Mobile devices**
 - attacker may have physical access to device
 - losing devices ⇒ losing keys/access/money? (revocation issues)
 - different security levels of environment
- **Privacy**
 - which sensors record what about whom, when, and who has access?
 - what can a personal, trusted, mobile device reveal about its owner?
- **Physical replacement**, matching physical with virtual entities
- Side-channel attacks
- Understanding how the whole system works (**mental models**)

What needs to be solved?



Issues

- wireless
- spontaneous interaction
- restricted user interfaces
- scalability

Approaches

- • authentication
- • peer-to-peer, context
- } → • human-verifiable authentication with personal mobile device

Wireless is not enough

Typical approach for secure channel setup:

- **Key agreement**: typically select peer device + Diffie-Hellman
- **Peer authentication**: various options
 - commitment schemes
 - interlock-based protocols
- Verification based on some **out-of-band channel**
 - verification of key hashes: display+user+yes/no
 - transmission over secret and/or authentic channel: display+user+keypad, infrared, ultrasound, laser, display+camera, audio, NFC, ...
 - shared secret: common data, possibly "fuzzy"

One out-of-band channel won't do either...

Different scenarios in which authentication is required, examples:

- Home environment
 - **pair** new TV set with existing universal remote control
 - **associate borrowed** Bluetooth headset with mobile phone for a single call
 - allow **guests** to **temporarily** access (parts of) music and video collection, and to use TV set to remotely access their own collection from their home
- Untrusted environment
 - use **public** printer or user interface terminal to **enhance personal mobile device capabilities** (think of building-size public displays)
 - use personal device as **electronic wallet**
 - **direct transfer** of data between two (or multiple) personal devices with different owners

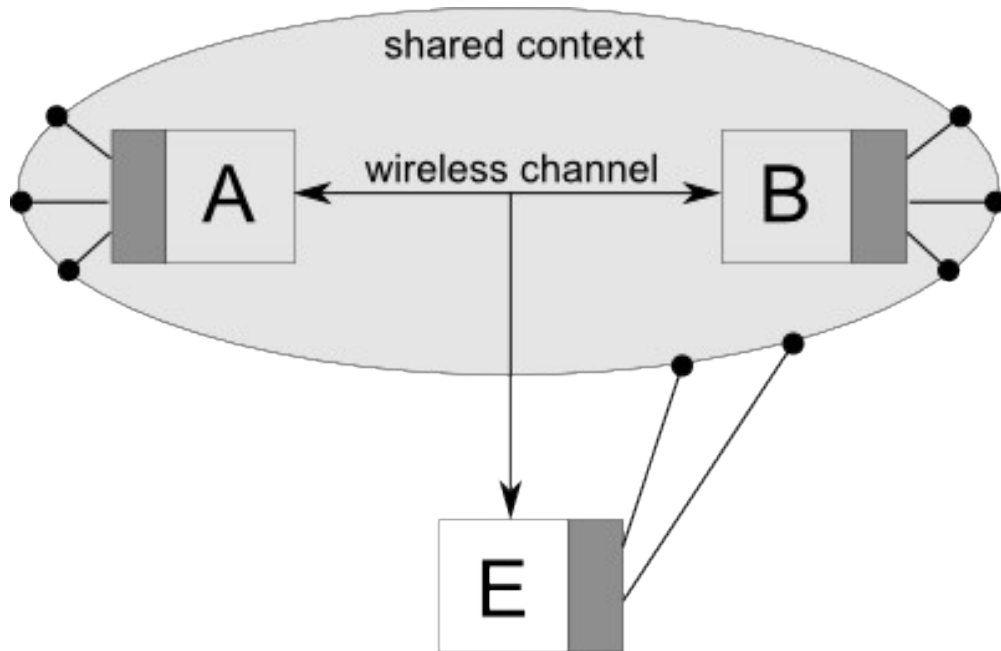
Recent protocol proposals

- “MANA I-III” (display/keypad)
[C. Gehrman, C. J. Mitchell, and K. Nyberg: “Manual authentication for wireless devices”, RSA Cryptobytes 7, 2004]
- Balfanz “pre-authentication”
[D. Balfanz, D. K. Smetters, P. Stewart, H. C. Wong: “Talking to Strangers: Authentication in Ad-Hoc Wireless Networks”, NDSS 2002]
- Hoepman “ephemeral key exchange ϕ KE”
[J.-H. Hoepman: “The Ephemeral Pairing Problem”, Financial Cryptography, 2004]
- Vaudenay “SAS”
[S. Vaudenay: “Secure Communications over Insecure Channels Based on Short Authenticated Strings”, CRYPTO 2005]
- **MANA IV** family of protocols
[S. Laur and K. Nyberg: “Efficient Mutual Data Authentication Using Manually Authenticated Strings”, CANS 2006]

Recent protocol proposals: standards

- Bluetooth pairing in current standard and WEP are completely broken
[Y. Shaked and A. Wool: "Cracking the Bluetooth PIN", Mobisys 2005]
[F.-L. Wong, F. Stajano, and J. Clulow: "Repairing the Bluetooth pairing protocol", Security Protocols 2005]
[E. Tews, R.-P. Weinmann, and A. Pyshkin: "Breaking 104 bit WEP in less than 60 seconds", Cryptology ePrint Archive 2007/120]
- **Bluetooth Simple Pairing** [Bluetooth SIG: Simple Pairing Whitepaper, 2006]
 - "just works" - insecure against MITM
 - "numeric comparison" of six digit number, yes/no on both devices
 - "out of band" e.g. with NFC
 - "passkey entry" with transferring a six digit number (human as out-of-band channel)
- **Wi-Fi Protected Setup**
 - "push button configuration" - insecure against MITM
 - "PIN" with four to eight digit number
 - "out-of-band" e.g. with NFC

Context-based authentication



- main threat scenario: MITM on wireless communication channel
 - intended communication partners A and B share some context
 - attacker E has inferior access to this context
 - respective aspect of context represented by sensor data streams
⇒ shared (**weakly**) secret information
- identification vs. authentication
 - anonymous/pseudonymous authentication possible
 - physical identities are more important than virtual ones

Context-based authentication

- We can define **context authentication** as:
 - A group of devices is authenticated with each other when certain aspects of their context match.
- Appropriate sensors to ensure that two or more devices are in common context
- Tim Kindberg et al: Concept of "**constrained channel**":
[T. Kindberg, K. Zhang, N. Shankar: "Context Authentication Using Constrained Channels", WMCSA 2002]
 - channels that are restricted by contextual constraints
 - either send- or receive-constrained
- Dirk Balfanz et al: "**location-limited channel**":
[D. Balfanz, D. K. Smetters, P. Stewart, H. C. Wong: "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks", NDSS 2002]
 - requires "demonstrative identification": identification based on physical context (i.e. location)
 - requires authenticity of channel

Authentication based on relative position

(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**

“Spatial Reference”

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



[R. Mayrhofer, H. Gellersen, M.Hazas: “Security by spatial reference: Using relative positioning to authenticate devices for spontaneous interaction”, Ubicomp 2007]

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:

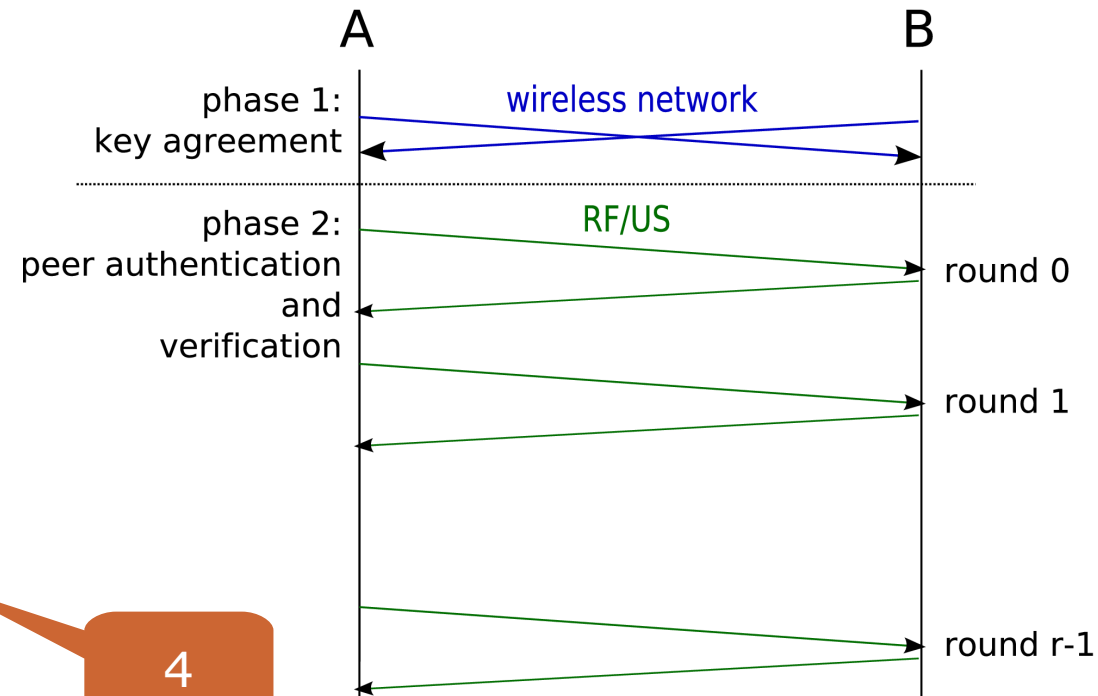
- <10 cm accuracy for distance measurements
- $\sim 33^\circ$ accuracy for local angle-of-arrival

Spatial authentication protocol: concept

Main aspects of the protocol

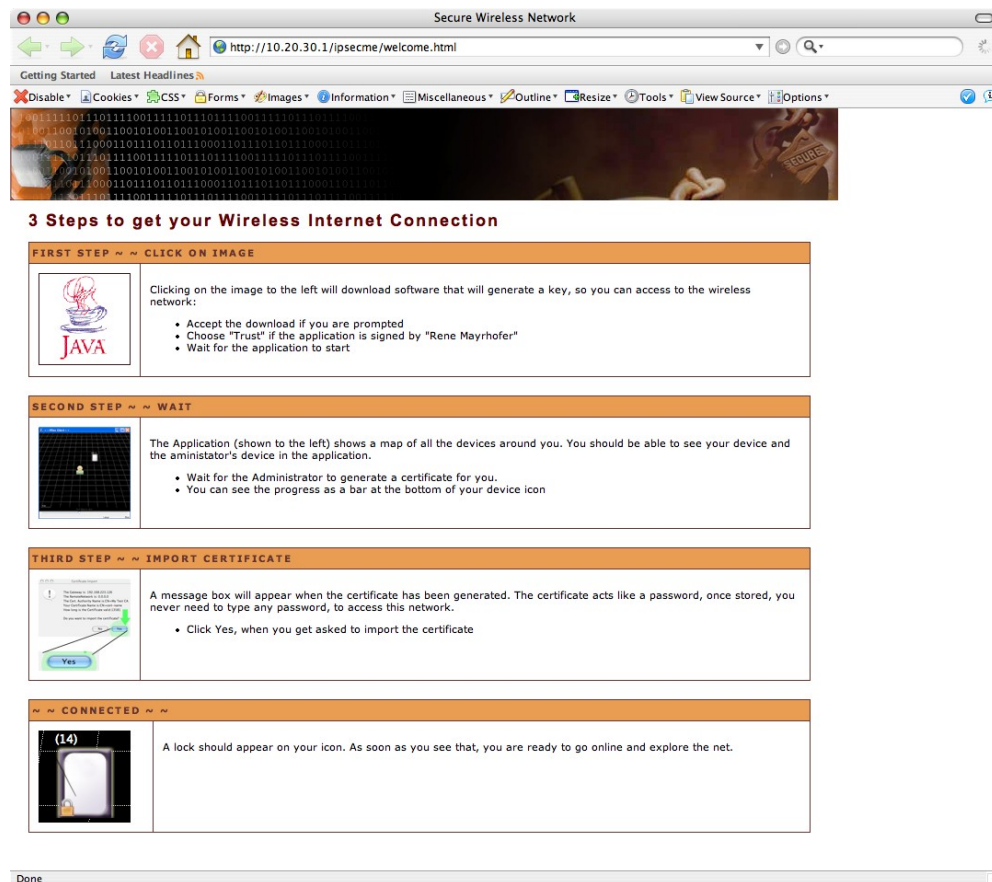
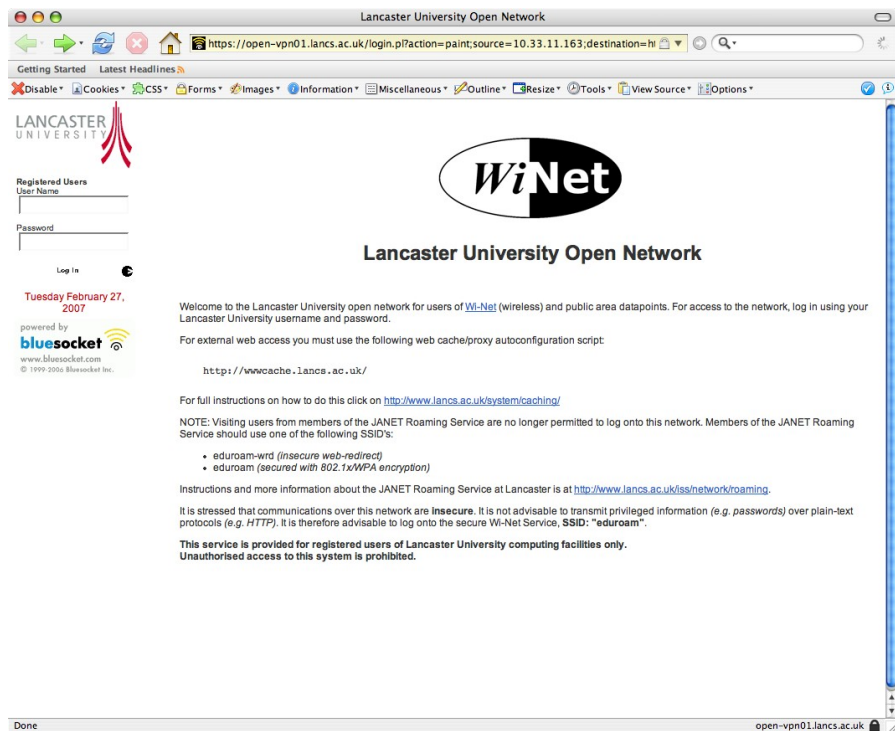
- uses **2 (3) channels**: RF and US
- with 2 phases: **key agreement** and **peer authentication**
- **Diffie-Hellman** for key agreement in phase 1
- Exchange **random nonces** with **interlock protocol** in phase 2, both via RF (encrypted) and via US (plaintext)
- Interlock exchange tightly **coupled**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

3



4

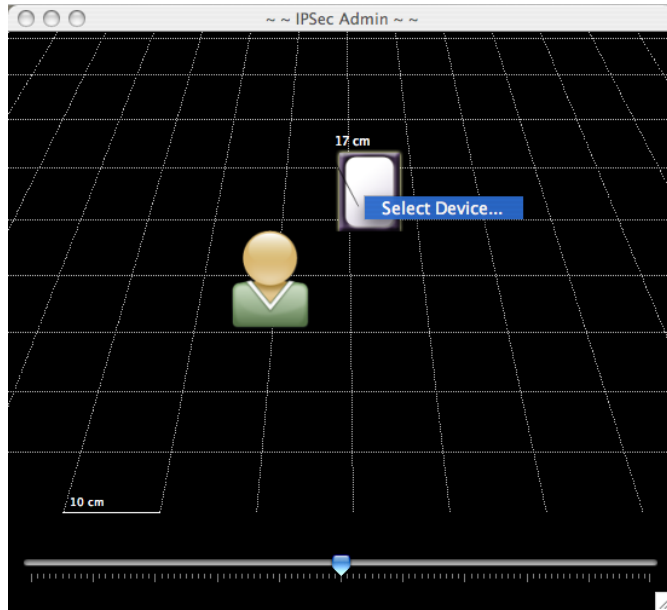
"IPSecME" for securing WLAN access



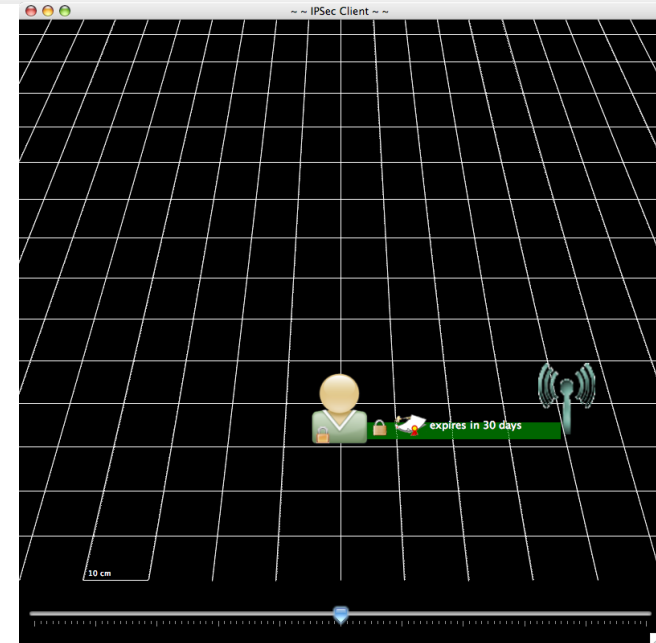
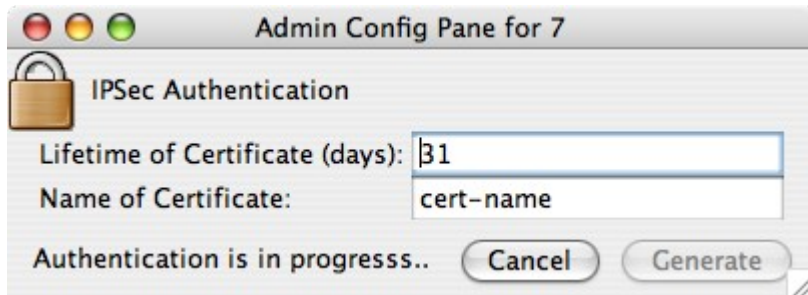
[MG 2007] R. Mayrhofer, R. Gostner: "Using a spatial context authentication proxy for establishing secure wireless connections", Journal of Mobile Multimedia, 2007

"IPSecME" for securing WLAN access

Admin



New client



Shaking as shared context

Shaking is common movement

- both (all) devices will experience very similar movement patterns
 - both (all) devices will experience very similar **accelerations**
- ⇒ not only use it as interaction technique, but also for generating keys

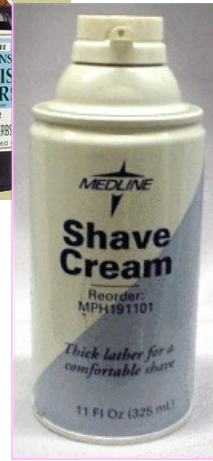
Acceleration is a **local** physical phenomenon

- ⇒ difficult for an attacker (MITM) to estimate or replicate
- Not used for identifying users, only as shared context!

Reasons for using shaking

Shaking is

- intuitive
- vigorous
- varying



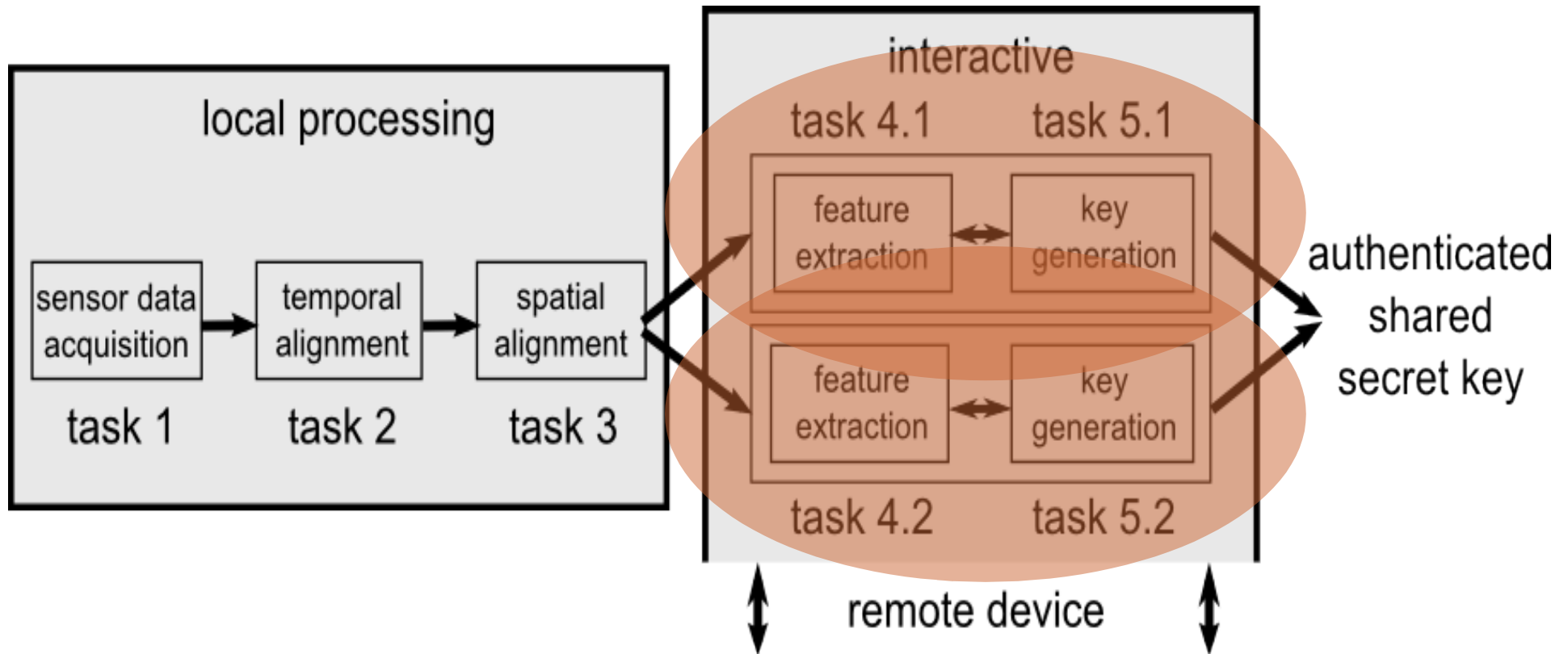
Accelerometers are

- small
- cheap
- (relatively) power-efficient



[R. Mayrhofer and H. Gellersen: "Shake well before use: Authentication based on accelerometer data", Pervasive 2007]

From sensor data to shared secret keys



Pre-processing

1. Sensor data acquisition

- Potential problem: side-channel attacks

2. Temporal alignment

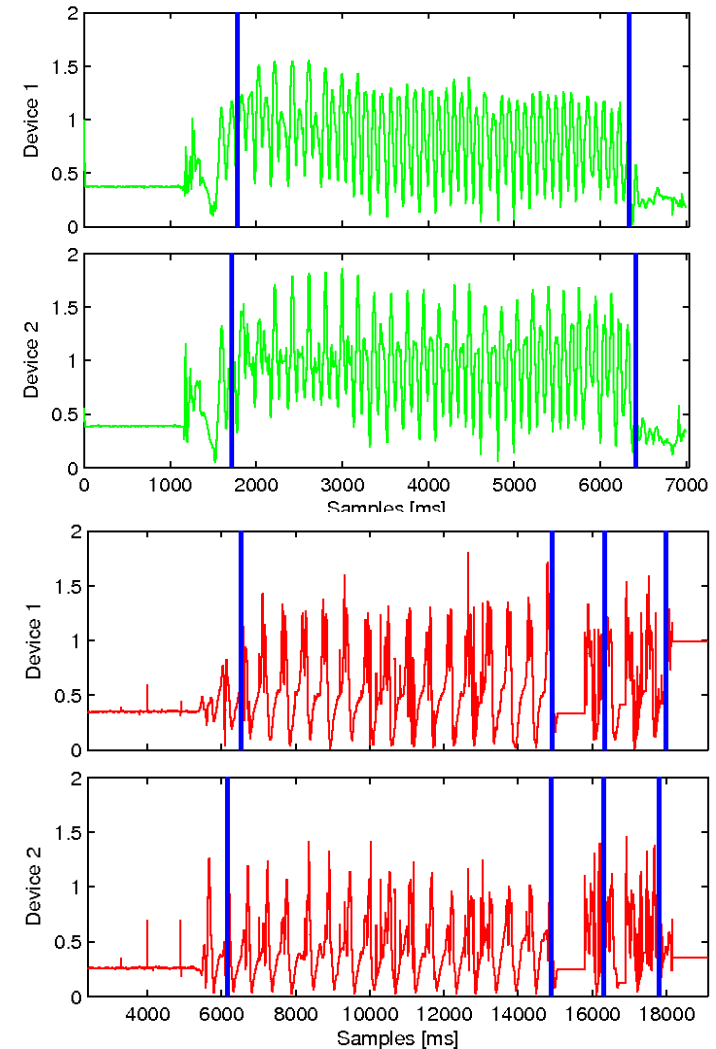
- Triggering
- Synchronization

⇒ use motion detection

3. Spatial alignment

- Devices arbitrarily aligned in 3D
- Alignment changes when picked up (between “silent” and “active”)

⇒ reduce to 1 dimension (magnitude)



Feature extraction

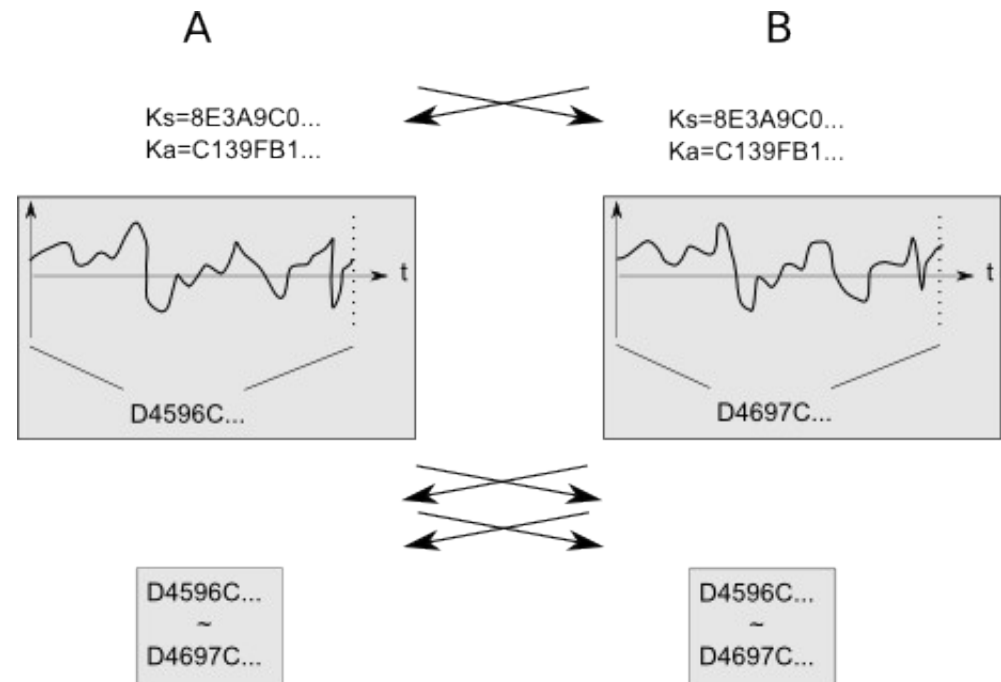
Features for shaking:

- Frequency domain
 - less accuracy required for synchronization
 - less sensitive to noise and alignment problems
- **Coherence**: measures power spectrum correlation between two signals split into overlapping slices, produces similarity value in $[0; 1]$
- **Quantized FFT coefficients**: pairwise added FFT coefficients quantized into exponential bands as feature vectors, compare equality

Cryptographic protocols (1)

Protocol 1:

- Uses **Diffie-Hellman** for key agreement
- Exchange sensor time series after pre-processing with **interlock*** protocol
- Both devices check similarity locally with **coherence**

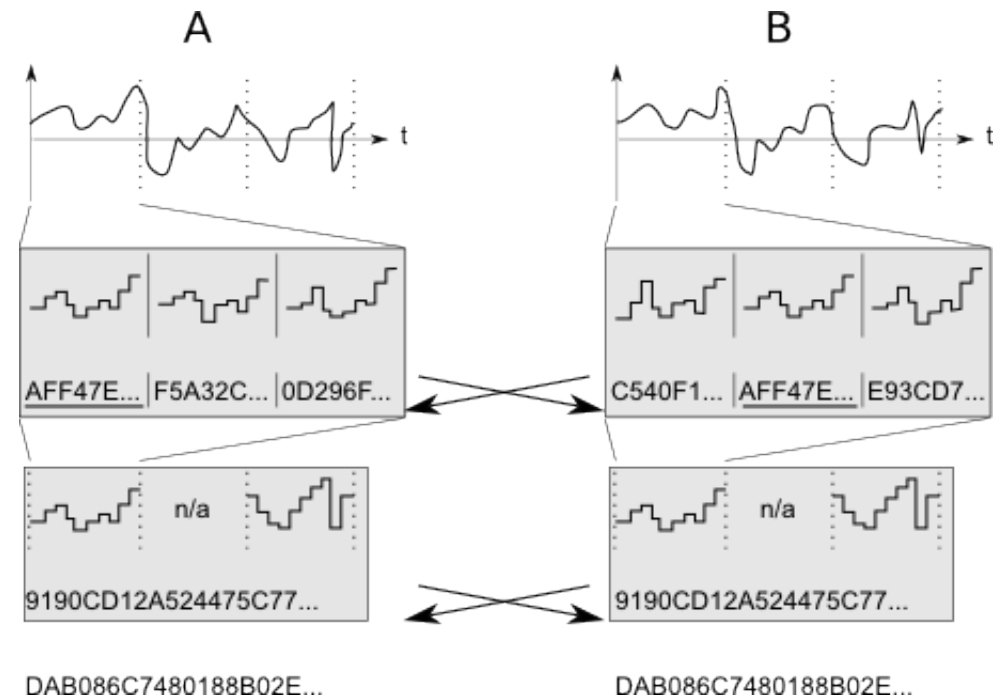


(4)

Cryptographic protocols (2)

Protocol 2:

- Generates secret shared keys directly from sensor data streams
- Computes feature vectors of **quantized FFT coefficients**
- Exchanges and compares hashes of feature vectors
⇒ **candidate key parts** (4)
- Matching vectors concatenated
⇒ **candidate keys**



[May 2007b] R. Mayrhofer: "The candidate key protocol for generating secret shared keys from similar sensor data streams". In Proc. ESAS 2007: 4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks. Springer-Verlag, July 2007

Protocol properties

Protocol 1

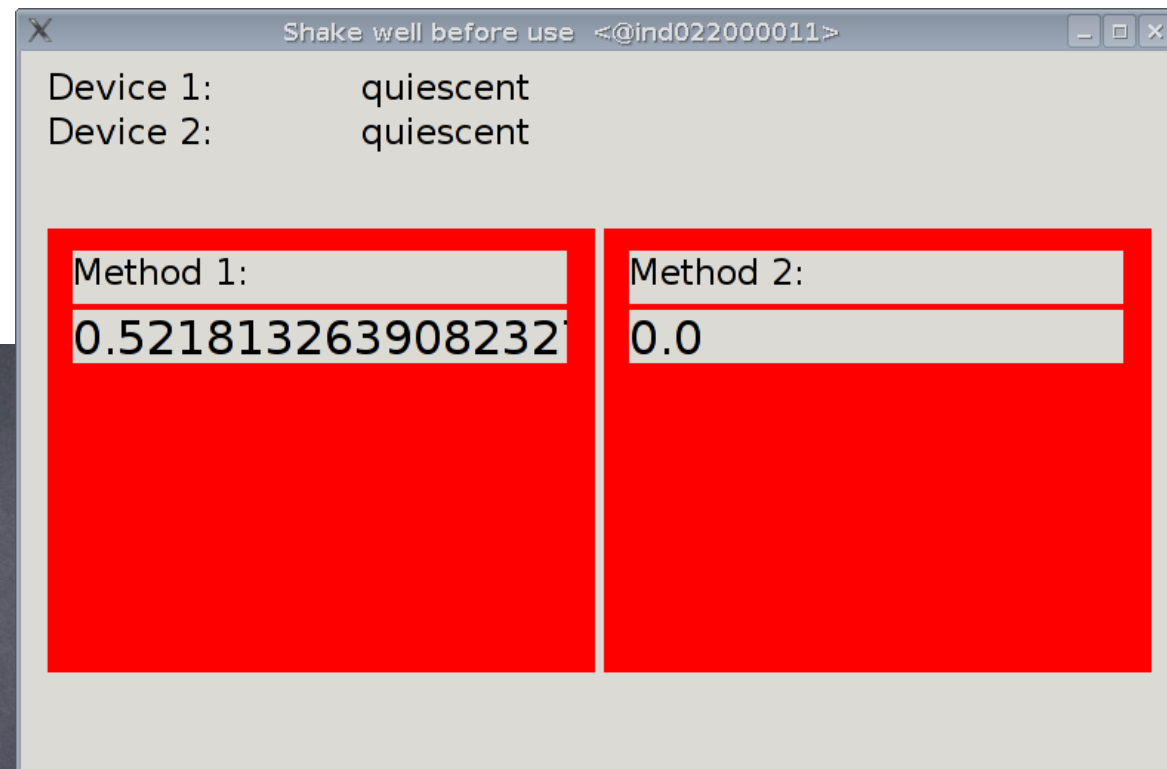
- Two phases:
 - Key agreement
 - Key verification
- Either with opportunistic key agreement or slight delay
- **Only one-off chance** for online attack
- Independent signal analysis

Protocol 2

- Single, continuous phase
- Devices **"tune into"** each other's key streams
- **Multi-device** authentication
- Offline lookup table attacks possible when feature vectors have insufficient entropy

"Shake well before use"

Shake well before use: Authentication based on Accelerometer Data



[R. Mayrhofer and H. Gellersen: "Shake well before use: Authentication based on accelerometer data", Pervasive 2007]

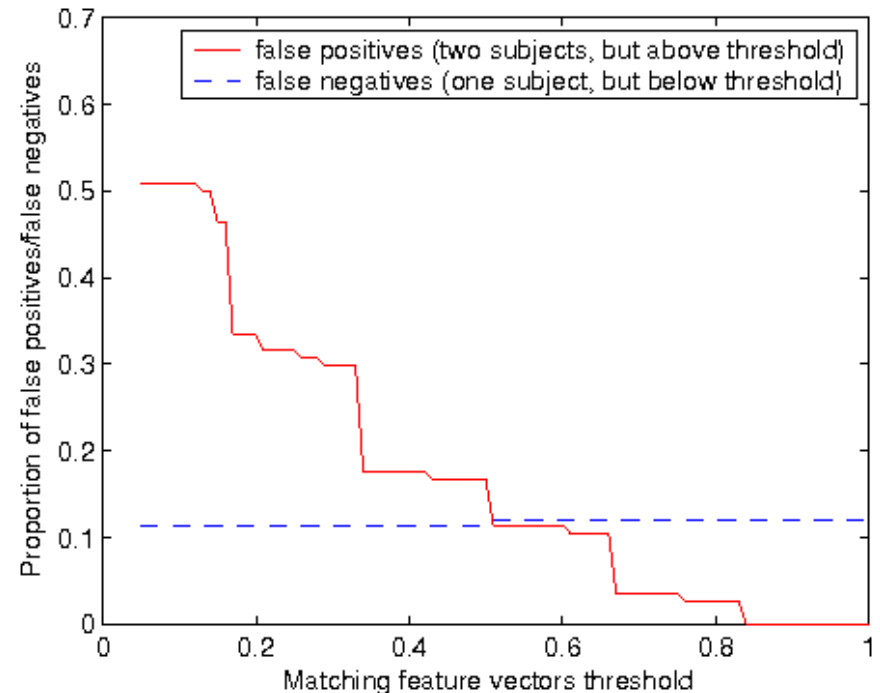
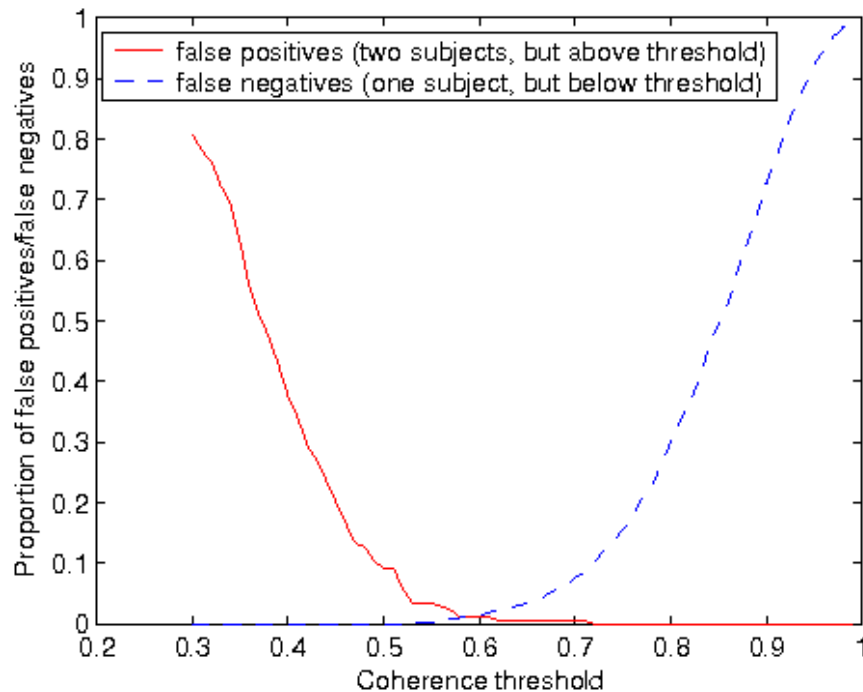
First experimental results

3 experiments:

- How do people shake?
- "Hacking" competition
- Live mode – does it work?

Results:

- Parameters for **no false positives**
- False negatives 10.24%, 11.96%
- 25/30 subjects successful

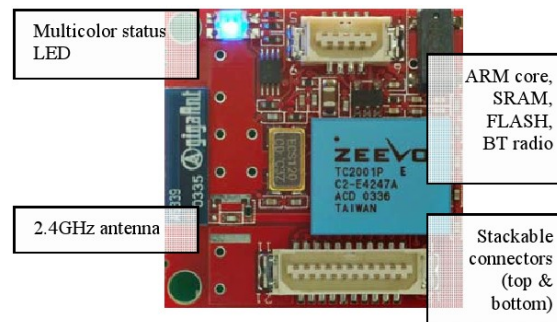


[R. Mayrhofer and H. Gellersen: "Shake well before use: Authentication based on accelerometer data", Pervasive 2007]

Scaling it down

Current developments:

- Implementing the method on embedded devices
 - “Nokia 5500 Sport” – includes 3D accelerometer with API
 - Intel iMote 1 with TinyOS – to emulate headset
- Bluetooth instead of TCP and UDP
 - different way of communication setup
 - no broadcast
- Improving classification accuracy



[R. Mayrhofer and H. Gellersen: “Shake well before use: Authentication based on accelerometer data”, Pervasive 2007]

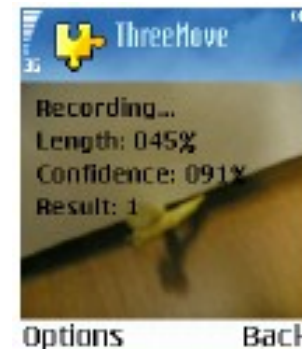
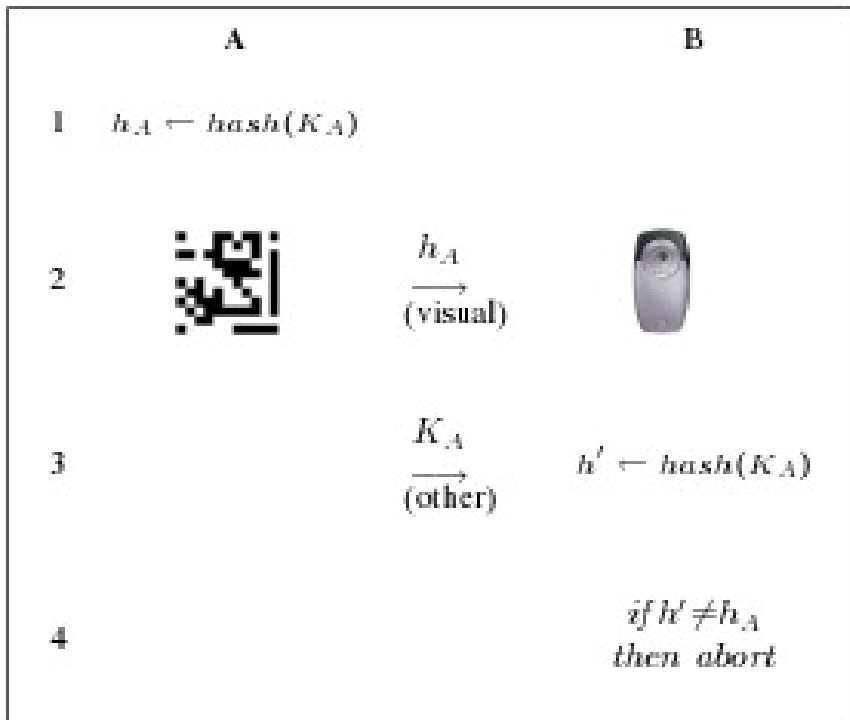
"Seeing-is-Believing"

Visual out-of-band channel

[J. M. McCune, A. Perrig, and M. K. Reiter: "Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication", IEEE Symp. on Security and Privacy 2005]

extended to use blinking patterns

[N. Saxena, J.-E. Ekberg, K. Kostianen, and N. Asokan: "Secure Device Pairing based on a Visual Channel", Cryptology ePrint Archive 2006/050]



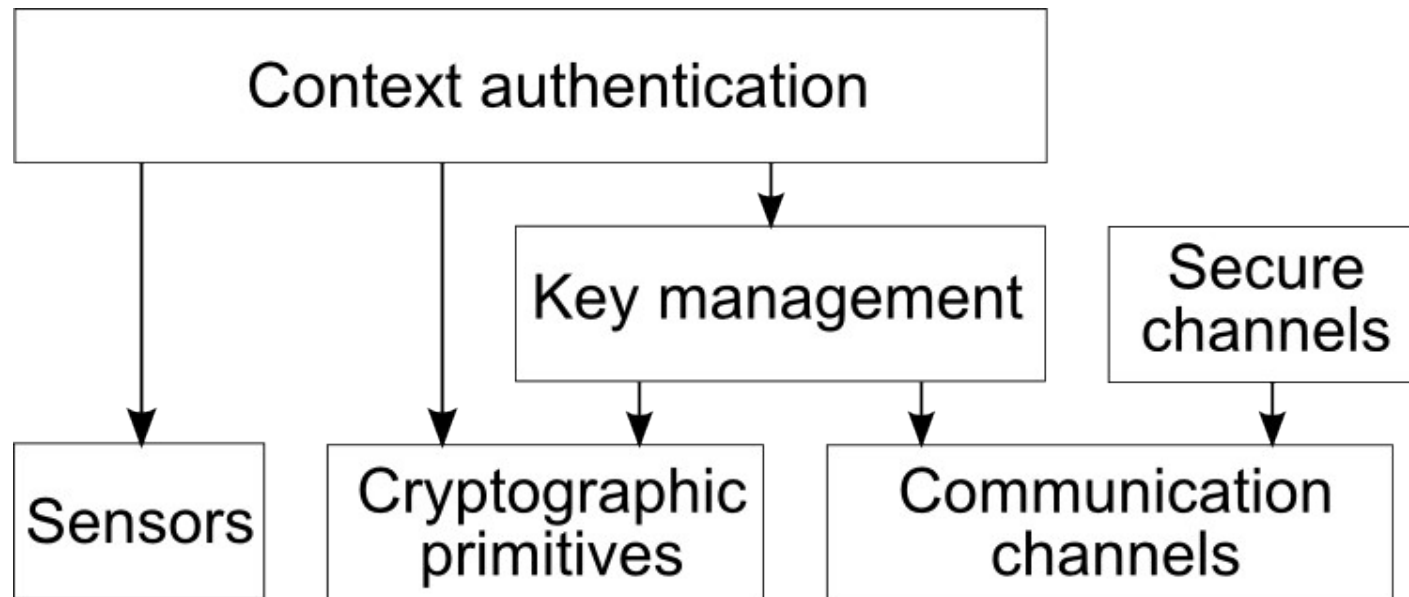
Other suggested approaches

- **“LoKey”**: use SMS as out-of-band channel, integration with applications
[A. J. Nicholson, I. E. Smith, J. Hughes, and B. D. Noble: “LoKey: Leveraging the SMS Network in Decentralized, End-to-End Trust Establishment”, Pervasive 2006]
- **“Loud and Clear”**: comparing non-sensical English sentences, **“HAPADEP”** extension
[M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun: “Loud And Clear: Human Verifiable Authentication Based on Audio”, ICDCS 2006]
[C. Soriente, G. Tsudik, and E. Uzun: “HAPADEP: Human Asisted Pure Audio Device Pairing”, Cryptology ePrint Archive 2007/093]
- **“Personal Pen”** coupled with RFID for seamless, transparent user login
[Jakob E. Bardram, Rasmus E. Kjær, and Michael Ø. Pedersen: “Context-Aware User Authentication - Supporting Proximity-Based Login in Pervasive Computing”, Ubicomp 2003]
- **Location-based WLAN authentication**
[D. B. Faria and D. R. Cheriton: “No Long-term Secrets: Location-based Security in Overprovisioned Wireless LANs”, HotNets-III, 2004]
- **“Harmony”** protocol for comparing interlocked media streams
[T. Kindberg, K. Zhang, and S. H. Im: “Evidently secure device associations”, HP Labs Techreport HPL-2005-40, 2005]
- **“Amigo”** using RF environment as common context
[A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara: “Amigo: Proximity-based Authentication of Mobile Devices”, Ubicomp 2007]
- **“BEDA”**: synchronized button presses
[Claudio Soriente, Gene Tsudik, and Ersin Uzun: “BEDA: Button-Enabled Device Pairing”, IWSSI 2007]
- **“Shake them Up”**: moving devices to achieve source indistinguishability
[C. Castelluccia and P. Mutaf: “Shake Them Up!”, Mobisys 2005]
- Elena Vildjiounaite, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, Heikki Ailisto (Technical Research Centre of Finland): Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices, Pervasive 2006

OpenUAT

Documentation, demo applications, data sets: <http://www.openuat.org>

Source code, mailing list, bug tracker:
<http://sourceforge.net/projects/openuat>



[R. Mayrhofer: "Towards an open source toolkit for ubiquitous device authentication", PerSec/PerCom 2007]

Components in the current release

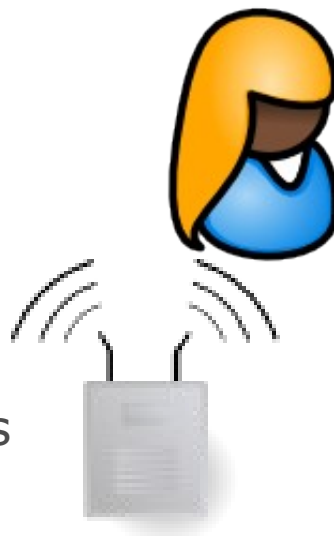
- **Cryptographic primitives**: ciphers, hashes (JCE and Bouncycastle with wrappers), DH with default parameters and utility methods, interlock*, on-the-fly creation of X.509 CAs and certificates
- **Communication channels**: threaded TCP and Bluetooth RFCOMM servers using same interface (transparently interchangeable), UDP multicast, Bluetooth background discovery and peer management (opportunistic authentication)
- **Key management protocols**: DH-over-streams (TCP or RFCOMM), Candidate Key Protocol
- **Sensors and feature extractors**: ASCII line reader with various implementations for accelerometers, simple statistics, time series aggregation, activity detection/segmentation, FFT, quantizer
- **Context authentication protocols**: spatial references, shared motion (shaking)
- **Secure channels**: IPSec tunnel and transport (Linux, MacOS/X, Windows)

Utilizing Log4j, JUnit, Ant build system including J2ME builds

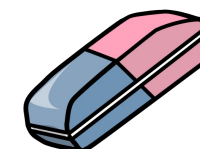
[R. Mayrhofer: "Towards an open source toolkit for ubiquitous device authentication", PerSec/PerCom 2007]

Security needs users!

- Unobtrusive, but not invisible
- Supporting spontaneous interaction
 - mobile devices with direct contact
 - mobile device with remote gateways
 - integrating with web services, client-less authentication approaches



- Re-use of existing metaphors
 - passing on keys
- New metaphors
 - „Shake well before use“



Summary

- Issues in security for spontaneous interaction
 - Wireless communication
 - Lack of user interfaces
 - Scalability of user attention
- Potential solution: **context-based device authentication**
 - Out-of-band channels in addition to (in-band) wireless communication
- Principles for security for spontaneous interaction
 - (1) references must be verifiable by the user and their device
 - (2) security – “don't get in my way”
 - (3) key agreement is not enough, but needs peer authentication
 - (4) verification needs to be tightly coupled with communication/interaction
- Many possible approaches, no one-size-fits all (application specific!)
- Need library/toolkit of potential methods for application designers

Thank you for your attention!

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

Sources: <http://www.openuat.org/>

Later questions: rene@mayrhofer.eu.org

OpenPGP key: 0xC3C24BDE

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