Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts

Written by: Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl and Hans-W. Gellersen

Presented by: Ueli Etter

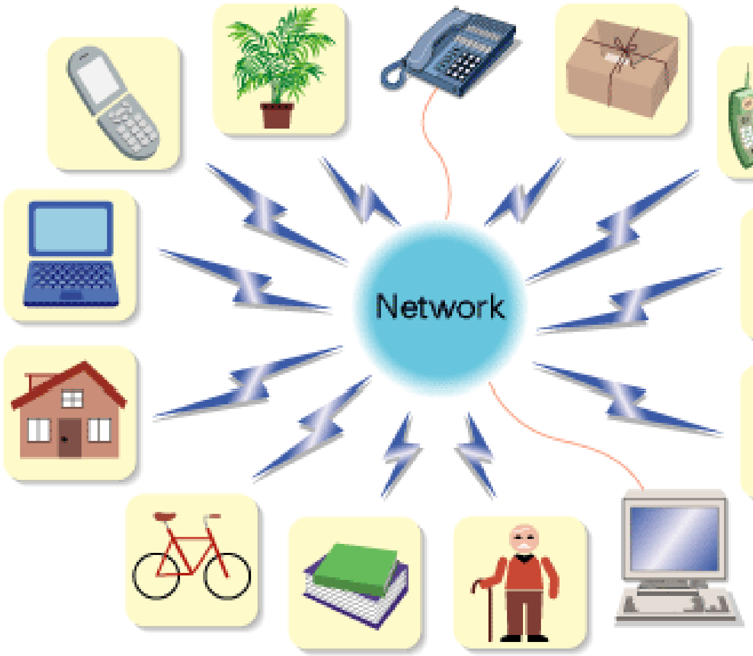
Seminar in Distributed Computing, ETHZ
November 12th 2008

Video: http://www.youtube.com/watch?v=TIVXxmxX-eg

Overview

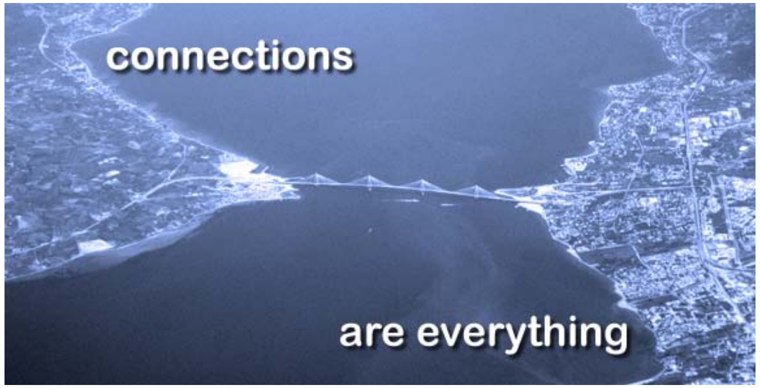
- Part 1
  - What is the Association Problem?
  - The concept of Smart-Its Friends
    - Idea
    - Application Examples
    - Assessment
- Part 2
  - The impact of Smart-Its Friends
    - iPhone application „Friend Book“
    - Alternative device association techniques
    - Device-to-device Authentication
    - Implicit Interaction
- Summary

Association Problem



- Ubiquitous Computing: smart objects linked wirelessly
- How to associate 2 objects with each other?
- How can you tell 2 devices that they „belong together“?

Association Problem (II)



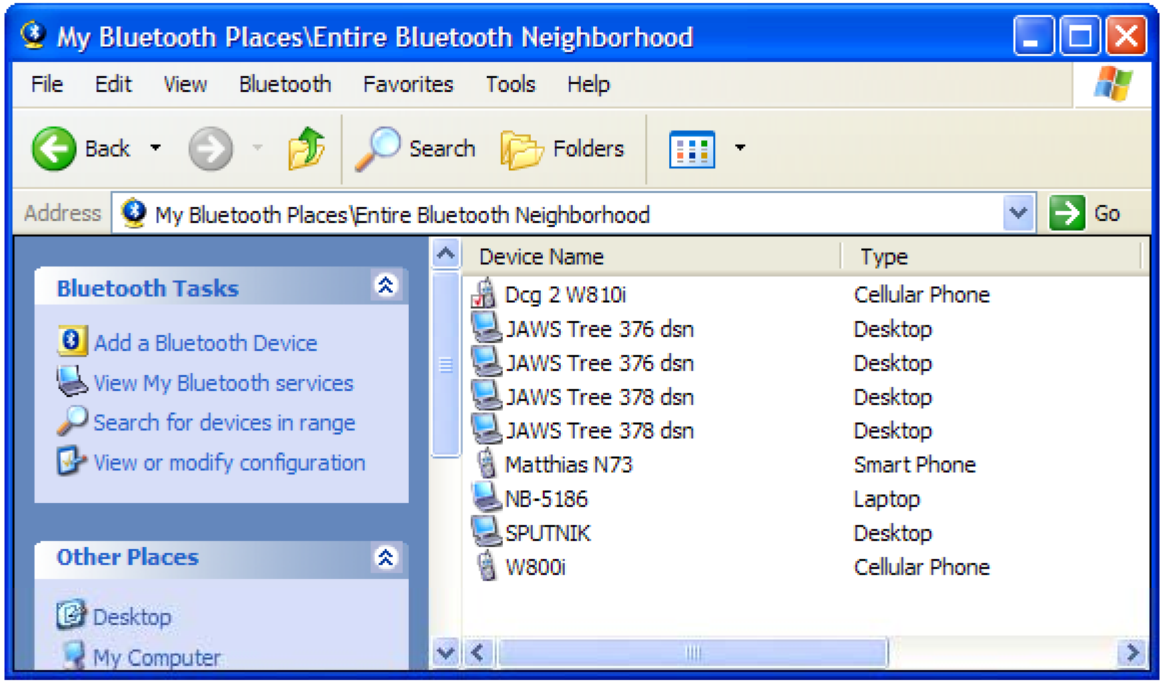
- Examples:
  - Pairing of a mobile phone with a headset
  - Data exchange between mobile users
- Challenges:
  - Restricted User Interfaces
  - User Attention Scalability: many short-lived interactions
  - Security

Conventional Solutions

- Enter address of target device
  - What is its address?
  - Requires input device (e.g. keyboard)
  - Tedious for user (who wants to enter dozens of addresses per day?)

Conventional Solutions (II)

- Select device from a list
  - Which list item corresponds to the target device?!
  - Requires output device (e.g. display)
  - Annoying for the user (especially if the list is long)


My Bluetooth Places\Entire Bluetooth Neighborhood
File
Edit
View
Bluetooth
Favorites
Tools
Help
Back
Search
Folders
Go
Bluetooth Tasks
Add a Bluetooth Device
View My Bluetooth services
Search for devices in range
View or modify configuration
Other Places
Desktop
My Computer

Address: My Bluetooth Places\Entire Bluetooth Neighborhood

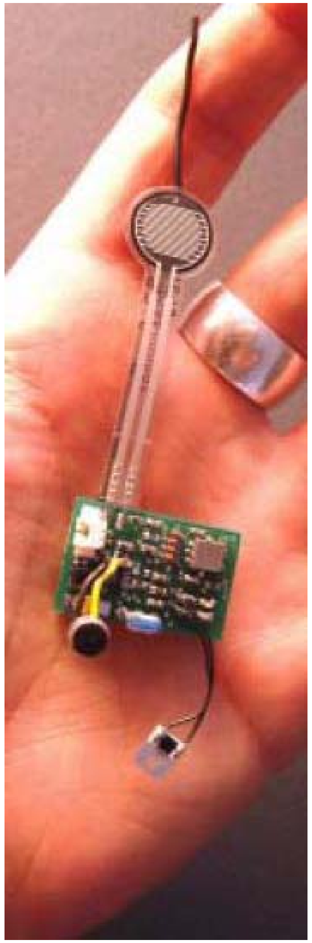
Device Name	Type
Dcg 2 W810i	Cellular Phone
JAWS Tree 376 dsn	Desktop
JAWS Tree 376 dsn	Desktop
JAWS Tree 378 dsn	Desktop
JAWS Tree 378 dsn	Desktop
Matthias N73	Smart Phone
NB-5186	Laptop
SPUTNIK	Desktop
W800i	Cellular Phone

Solution by Holmquist, Mattern et al.

- Shake well before use!
- Idea: **Context Proximity**
  - Devices that experience same context should be connected
- More specific: Context Proximity through **Shaking**
  - Shake two artefacts together to impose same context on them

Smart-Its

- Small-scale embedded devices
- Can be attached to everyday objects (just like a Post-It note…)
- Augment objects with
  - Sensing (Temperature, Light, Pressure, Movement, …)
  - Computation
  - Communication
- Prototyping platform for evaluating UbiComp applications



Smart-Its Friends

equipped with accelerometers

- User holds 2 Smart-Its together and shakes them
- Smart-Its broadcast their shaking pattern
- A Smart-It receiving a shaking pattern from another Smart-It compares it to its own movement data
- If the shaking patterns are „close enough“ the Smart-Its become friends, i.e. get connected

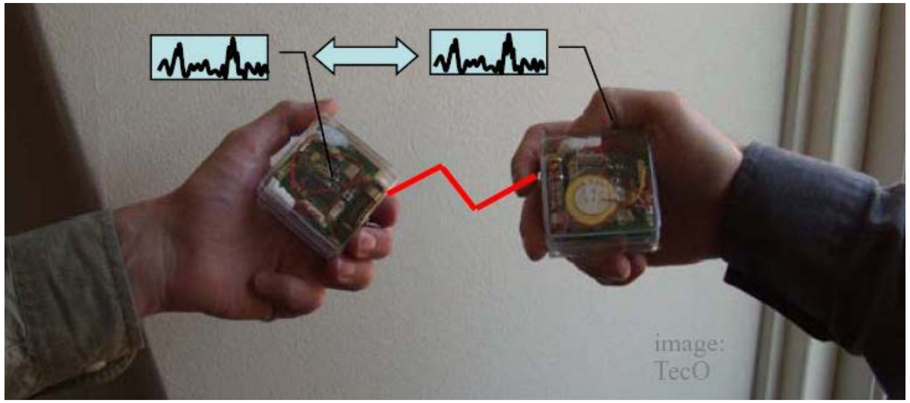


image: TecO

Smart-Its Friends – Application Examples

- Establishing a communication channel
  - Pairing of a mobile phone with a headset
  - Information exchange between mobile users
- Telling 2 objects to keep track of each other
  - Wrist-watch beeps whenever you leave your cell-phone behind you
  - Credit card that only works when a „friend“ is around
  - Child monitor
- Modifying the behaviour of a smart artefact
  - „modifier objects“ to set a parameter
  - Use a „magic stick“ with a slider to parameterise the distance a child is allowed to be away from its parents

Smart-Its Friends - Assessment

Pros

- Intuitive
- Unobtrusive
- More than 2 objects
- No input devices necessary
- Accelerometers are
  - small
  - cheap
  - power-efficient

Contras

- Not all objects can be shaken…

- Insecure
- Explicit user interaction

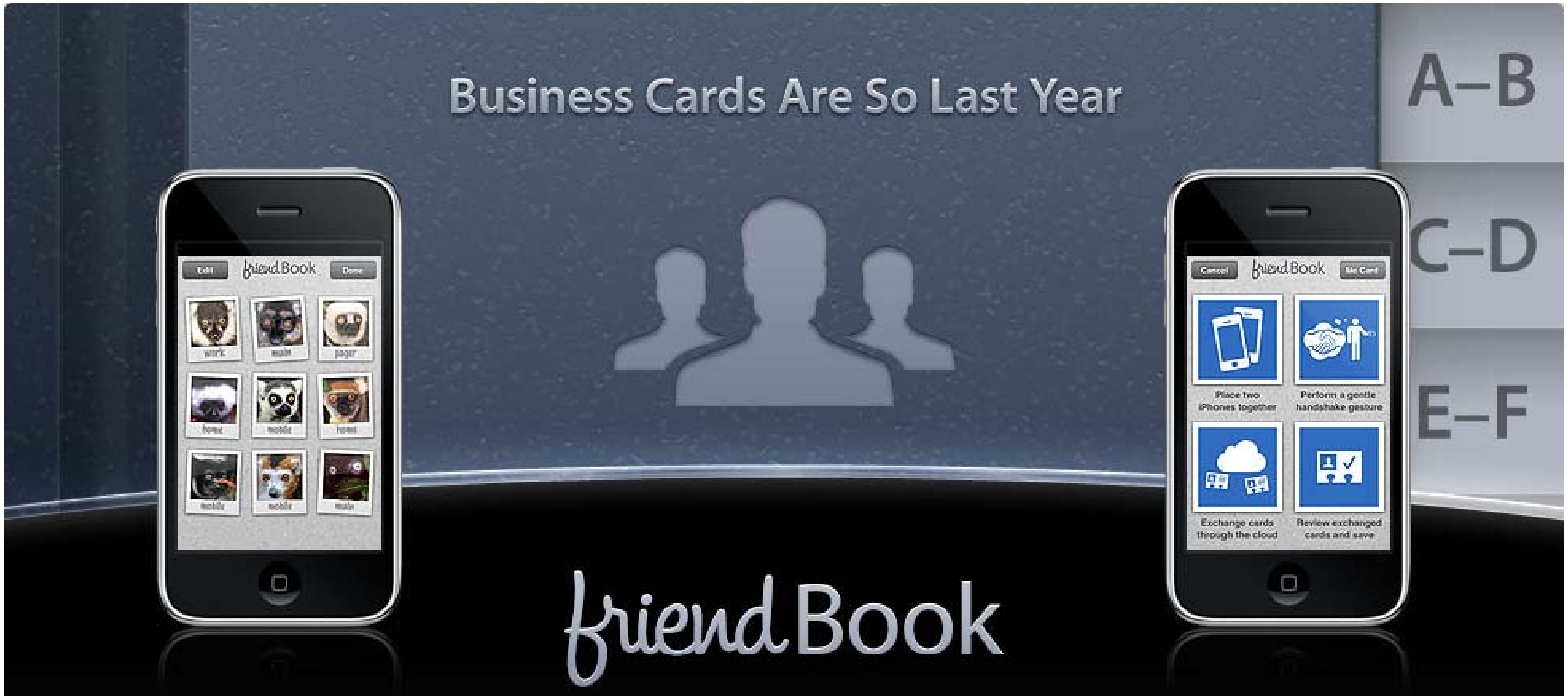
Smart-Its Friends – Assessment (II)

- Does the idea work in practice?
  - Paper doesn‘t show any experimental results
- Paper implicitly assumes that 2 devices don‘t experience the same shaking pattern unintentionally
  - Is this realistic?
  - What if two devices are on the same bumpy bus?
  - Will all phones be connected after the next earthquake?
- Does it scale?
  - n devices → n^2 potential connections
  - Network/CPU overload?
  - Probability of false positives?

  ⟶ Some way to restrict the number of potential „friends“ necessary
    - E.g. location

iPhone Application: Friend Book [2]

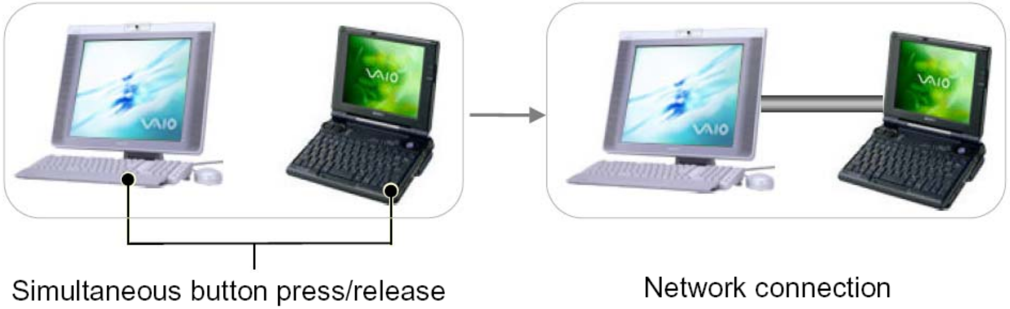
- Shake 2 iPhones together to exchange contact information
- Video: http://www.youtube.com/watch?v=DFOozO0390g


Business Cards Are So Last Year
A–B
C–D
E–F
Edit
friendBook
Done
work
mobile
pager
home
mobile
home
mobile
mobile
main
Cancel
friendBook
Me Card
Place two iPhones together
Perform a gentle handshake gesture
Exchange cards through the cloud
Review exchanged cards and save
friendBook

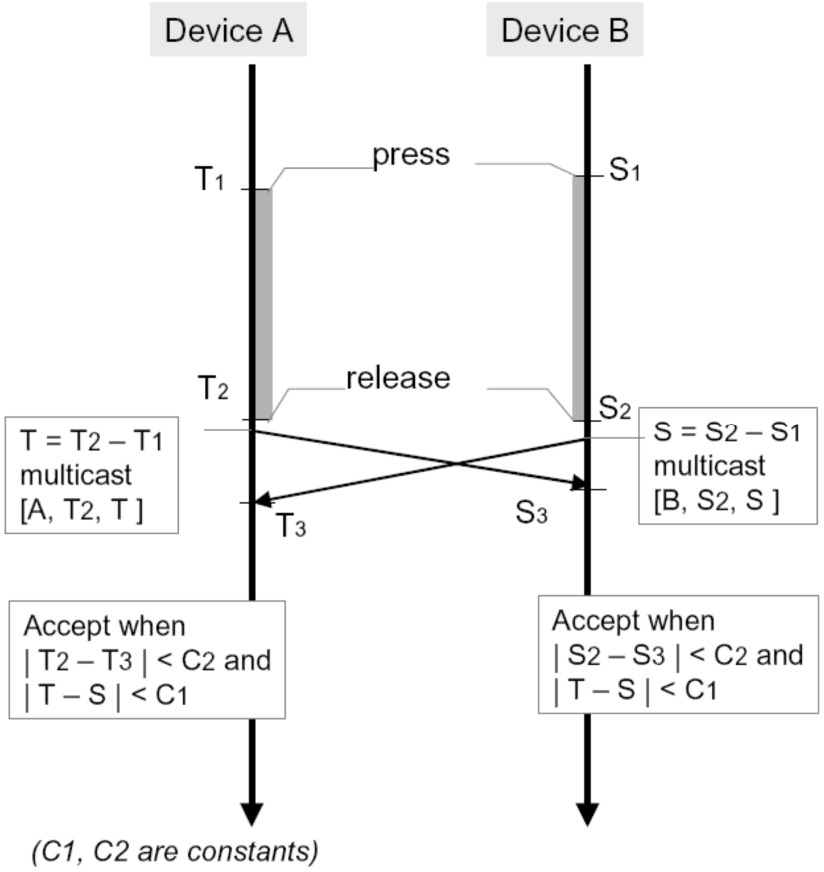
iPhone Application: Friend Book (II)

- Got removed from App Store after users had complained that their contact information had been sent to random people
- Explanation by the developers:
  - “The algorithm for matching of address cards was overly relaxed, meaning that matches were made that should not have been made. We did not discover this issue prior to the release because we were unable to test the feature with more than a dozen users (pre-AppStore launch, it was impossible to let outsiders test the app).”
- Implementation issue or concept wrong?!

SyncTap [3]

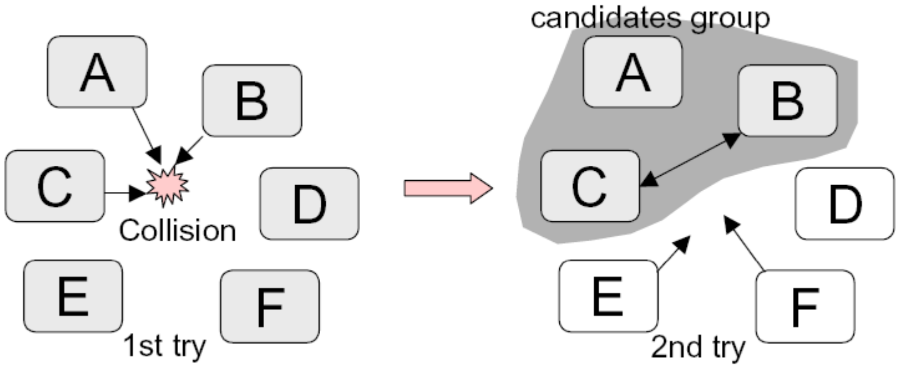


- Why so complicated?
- Rekimoto suggests a much simpler protocol that doesn‘t require any sensors:
  - User presses buttons on both devices simultaneously
  - Devices multicast time interval between press and release
  - By comparing received time intervals with locally recorded ones connections can be established



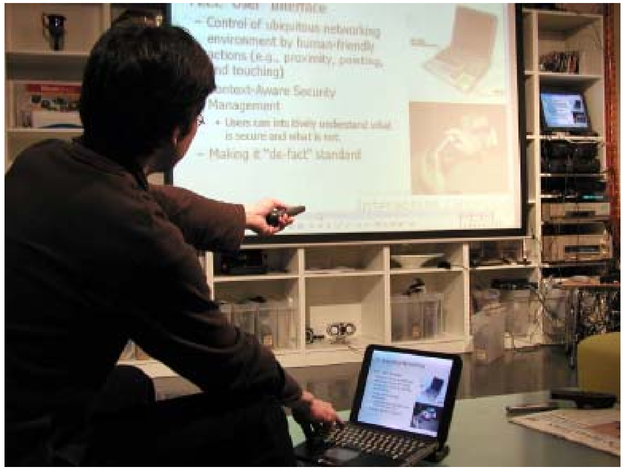
SyncTap (II)

- Protocol is collision resistant and scalable
  - If 2 or more requests arrive at the same time, the device asks the user to press the SyncTap buttons again
  - In the 2. round the device accepts no new candidates



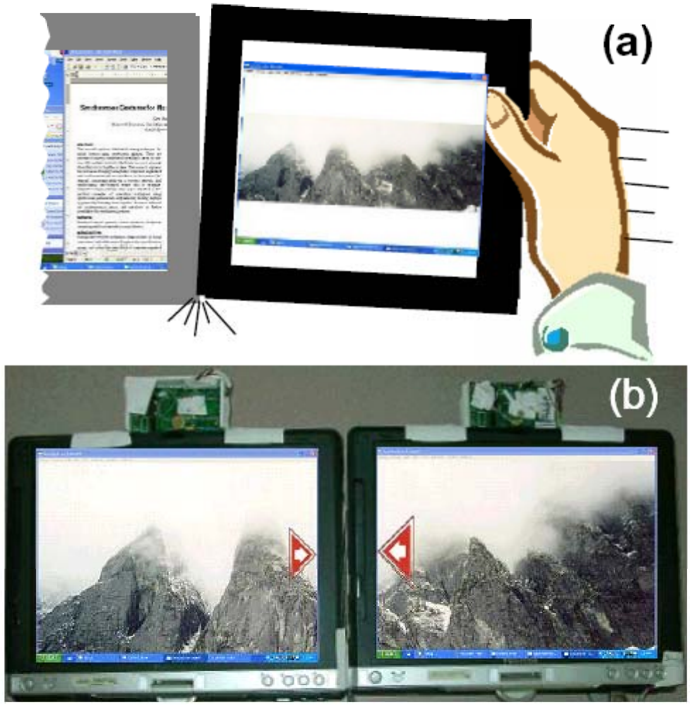
- Public keys can be exchanged for making the connection secure
- Works for any kind of devices that have at least one button (not only for handheld devices)!

SyncTap (III)


– Control of ubiquitous networking environment by human-friendly actions (e.g., proximity, pointing, nd touching)
ontext-Aware Security Management
• Users can intuitively understand what is secure and what is not
– Making it "de-fact" standard

Device association through bumping [4]

- Hinckley suggests device association by **bumping** devices together
- Example application: tablet PCs equipped with accelerometers and touch sensors
  - Dynamic display tiling
  - Information exchange

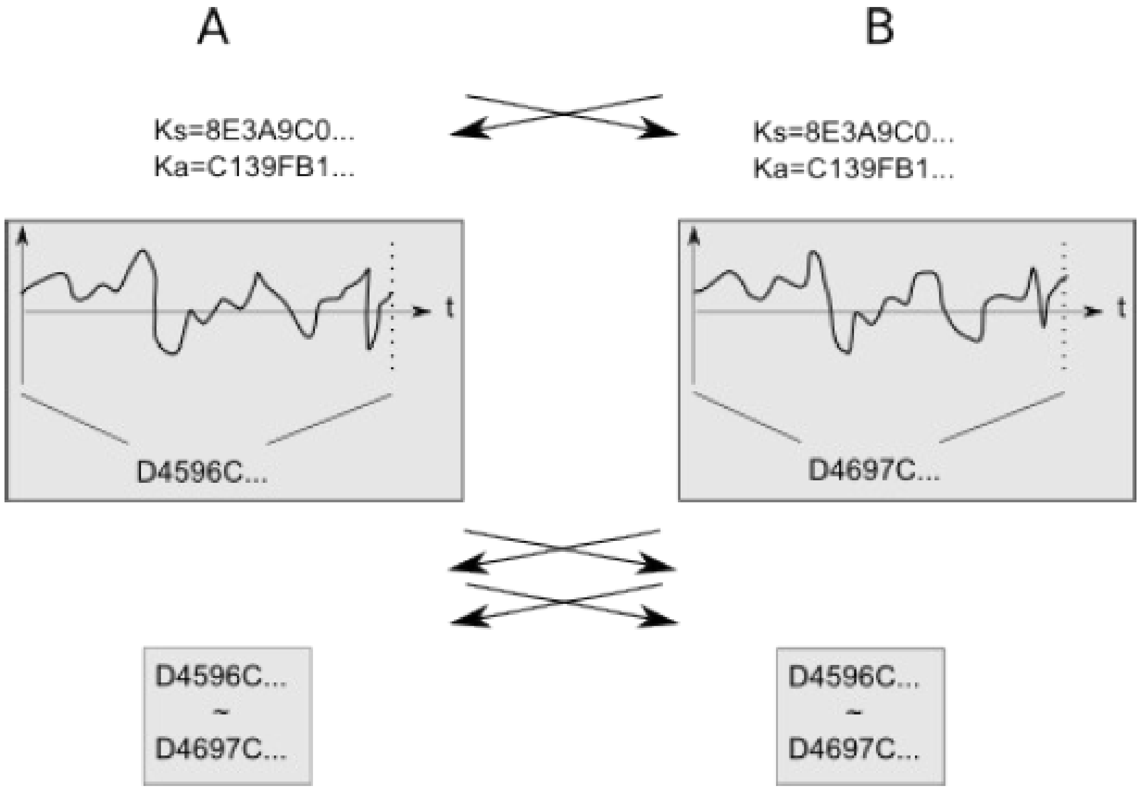


Video: http://www.acm.org/uist/archive/html/proceedings/2003.html#p149-hinckley

Generating authenticated secret keys by shaking [5]

- Protocols are vulnerable to man-in-the-middle attacks
- To prevent this, devices need to be authenticated
- Many protocols for device-to-device authentication exist
- Mayrhofer and Gellersen propose a protocol to generate authenticated shared secret keys using acceleration data
- Shaking pattern: shared secret
- Protocol: Diffie-Hellman and Interlock
  - Key agreement with Diffie-Hellman
  - Key verification using acceleration data

Generating authenticated secret keys by shaking (II)



1. Key Generation with Diffie-Hellman

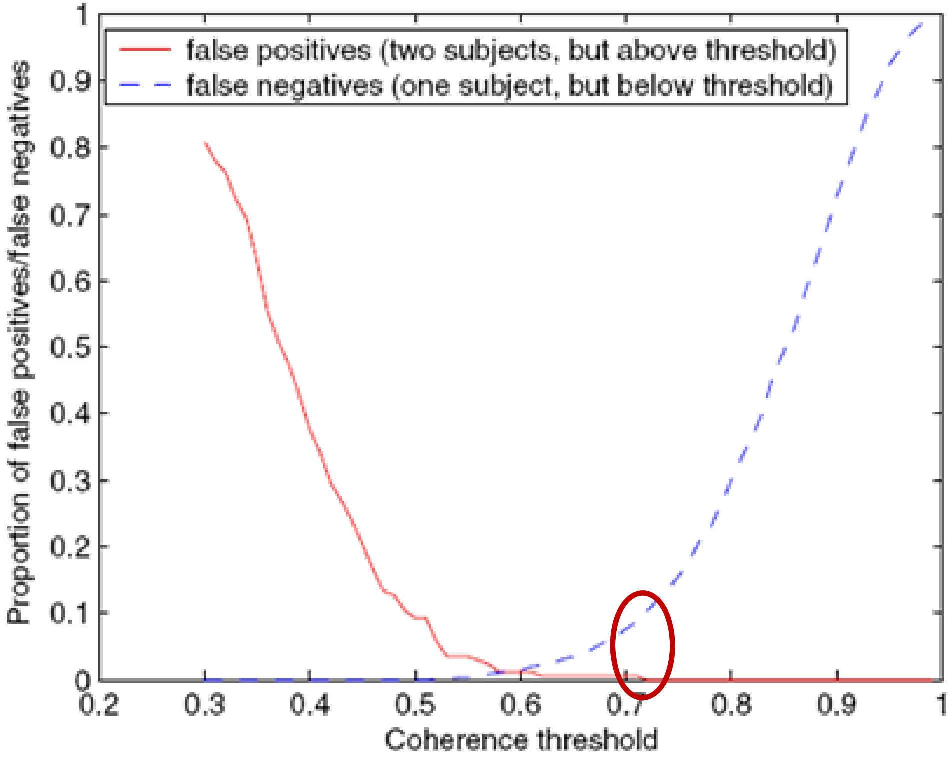
2. Pattern exchange with Interlock

3. Local comparison of patterns

- Keys get accepted iff $\text{pattern}_A \approx \text{pattern}_B$

Generating authenticated secret keys by shaking (III)

- Experimental results of „hacking“ competition:
  - No false positives when accepting false negatives rate of 10.24%



Video: http://www.youtube.com/watch?v=ktJC0S4_X58

Implicit Interaction

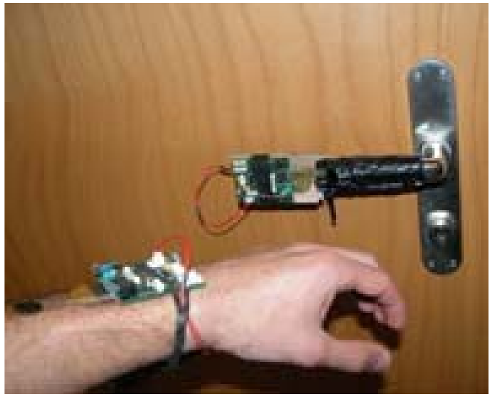
- So far: explicit interaction (shaking, bumping, button pressing)
- Implicit Interaction: „an action, performed by the user that is not primarily aimed to interact with a computerized system but which such a system understands as input"
- Example:
  - Decrease song rating when you skip a track on your music player
  - Setting the computer to standby when you close the lid of your laptop

Using Accelerometers to Determine if Two Devices are Carried by the Same Person [6]

- Oberservation:
  - Devices carried by the same person experience same shaking pattern
- Idea
  - Use this to form a body network
- Implicit Interaction
  - Existing natural action exploited: walking
- Results so far:
  - Determine reliably if 2 devices are being carried by the same person using 8 seconds of walking data (devices have to be worn in a fanny pack)
- Potential applications of a body network:
  - Borrowable cameras that can keep track of what other devices (and what persons) they were being carried by when a picture was taken
  - Automatic Synchronization of data between PDAs, laptops and wrist-watches
  - Automatic connection between music player and earphones

Implicit access control when opening a door [7]

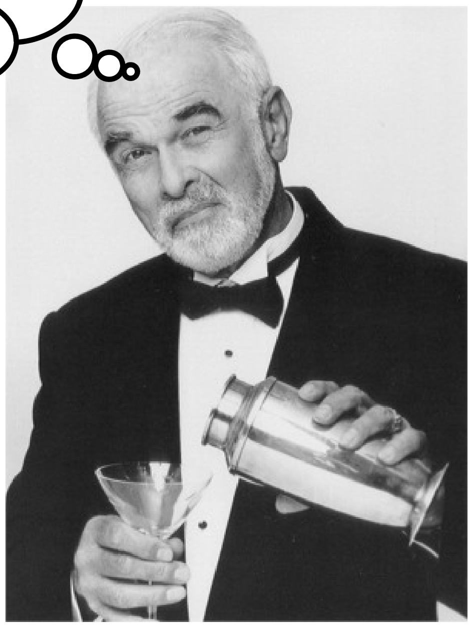
- Explicit Interaction:
  - Swipe Identification Badge
  - Enter PIN
  - …
- Implicit Interaction:
  - Press door handle normally (existing natural action)
  - Accelerometers at your wrist and at door handle experience same movement
  - Door can identify you
  - Door unlocks if you have access rights
  - No special user actions are necessary!



iBand [8]

- iBand: bracelet that can store, display, and exchange information about its user and his relationships.
- Augments the handshake gesture
- By shaking hands with somebody you implicitly exchange contact information
- Combines wearable computing with social networking
- Handshake detection:
  - Infrared Transceivers: to detect when 2 hands are in alignment
  - Accelerometers: to detect a synchronized up-and-down motion

Summary



- Shaking: technique for associating devices
  - General Concept: Context Proximity
- Does it work?
  - „Counterexample“: Friend Book
- Other device assocation techniques
  - SyncTap
  - Bumping
- Device association combined with secure authentication
  - Generating authenticated secret keys using sensor data
  - Real advantage of shaking technique
- Explicit vs. Implicit Interaction
  - Explicit: shaking, bumping, pressing buttons
  - Implicit: walking, pressing a door handle, handshaking

Questions?

References

1. **Smart-Its Friends: A technique for users to easily establish connections between smart artefacts**
(Holmquist, Mattern, Schiele, Alahuhta, Beigl, Gellersen; 2001)
2. http://tapulous.com/friendbook/
3. **SyncTap: synchronous user operation for spontaneous network connection**
(Rekimoto; 2004)
4. **Synchronous Gestures for Multiple Persons and Computers**
(Hinckley; 2003)
5. **Shake Well Before Use: Authentication Based on Accelerometer Data**
(Mayrhofer, Gellersen; 2007)
6. **"Are You With Me?" – Using Accelerometers to Determine if Two Devices are Carried by the Same Person** (Lester, Hannaford, Borriello; 2004)
7. **Grouping Mechanisms for Smart Objects Based On Implicit Interaction and Context Proximity** (Antifakos, Schiele, Holmquist; 2003)
8. **iBand: a wearable device for handshake-augmented interpersonal information exchange** (Kanis, Winters, Agamanolis, Cullinan, Gavin; 2004)