HAPADEP: Human-Assisted Pure Audio Device Pairing

Claudio Soriente, Gene Tsudik, **Ersin Uzun**

University Of California, Irvine

Outline

- What is secure pairing and why is it hard to secure?
- Current methods and related work
- HAPADEP protocol and operation
- Usability analysis
- Limitations, advantages of HAPADEP

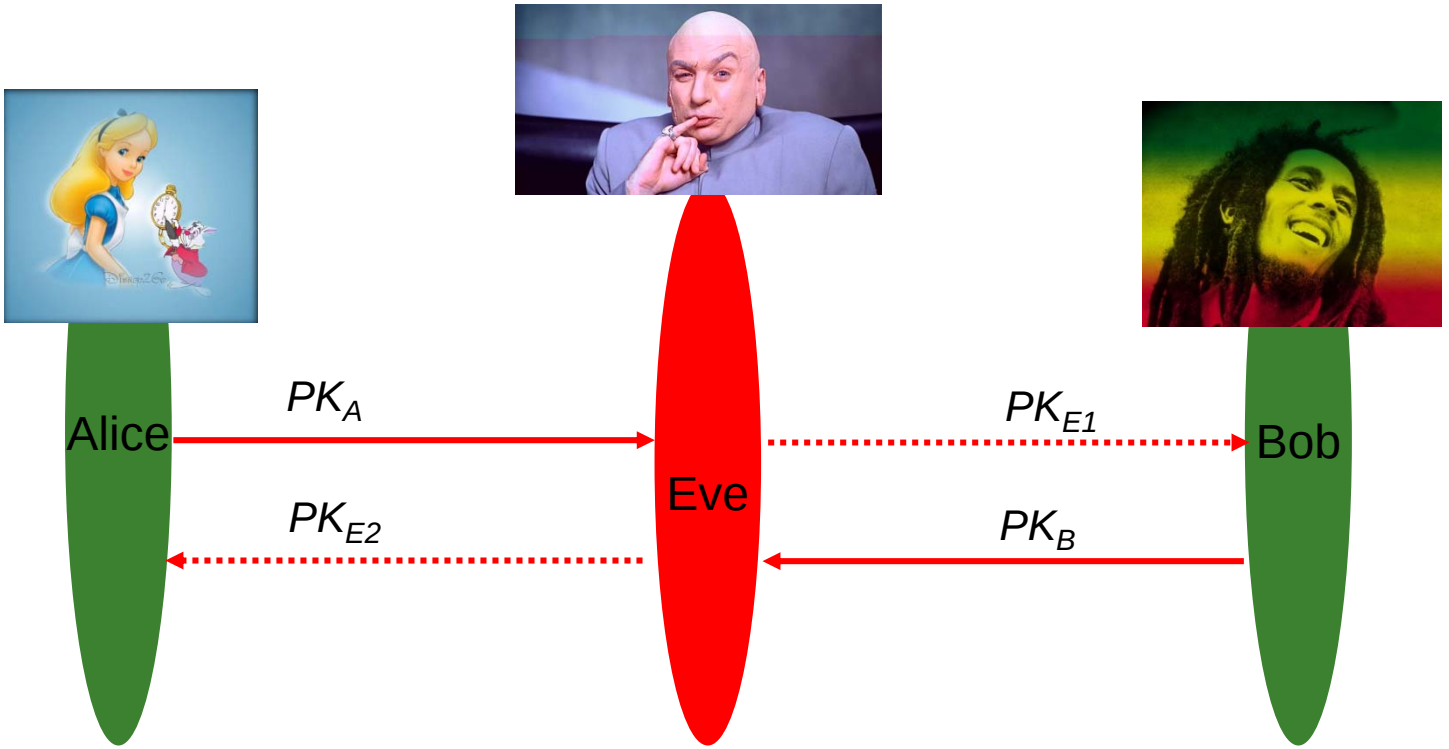
Secure pairing of personal devices

- **Pairing**: setup of association and security contexts for subsequent communication.
  e.g.:
  - Pairing a bluetooth phone and a headset
  - MP3 player and a PDA
  - Enrolling a phone or PC into a home WLAN
  - More instances to come: Wireless USB, WiMedia

Problem

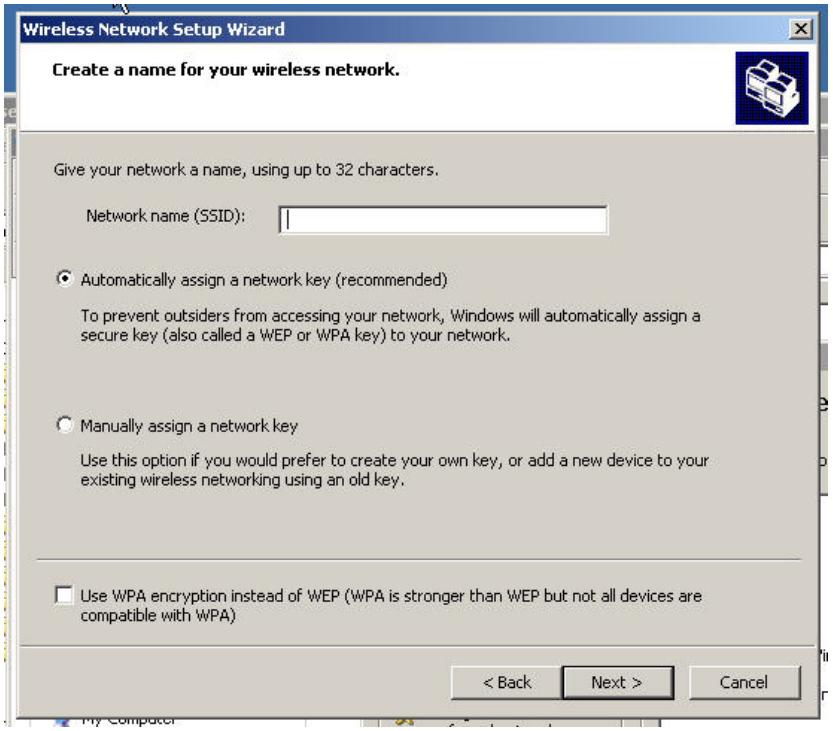
- Setting up a security association where:
- No prior context exists (no PKI, common TTPs, key servers, shared secrets, etc.)
- Ordinary non-expert users
- Cost-sensitive commodity devices

Biggest Security Threat



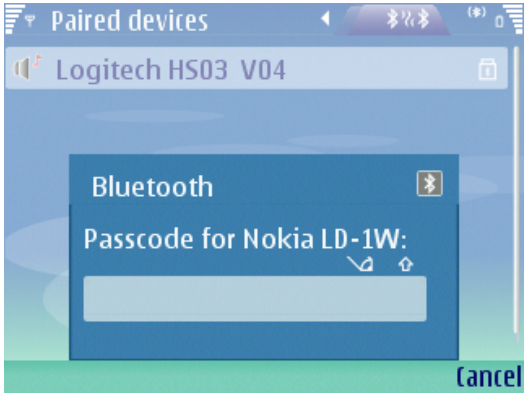
Man in the middle attack

Current mechanisms are not intuitive



SSID? WPA?
Passcode!

Which E61?



... not for all devices!

… and some are not even secure!

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP

August 6, 2001

Adam Stubblefield
Rice University
astubble@cs.rice.edu

John Ioannic
AT&T Lab
{ji,r

Cracking the Bluetooth PIN*

Yaniv Shaked and Avishai Wool

School of Electrical E
Tel Aviv University, Ram
shakedy@eng.tau.ac.il,

IEEE P802.11
Wireless LANs

Unsafe at any key size; An analysis of the WEP encapsulation

Date: Oct 27, 2000

Author: Jesse R. Walker
Intel Corporation
2211 NE 25th Avenue
Hillsboro, Oregon 97124
Phone: +1 503 712 1849
Fax: +1 503 264 4843
e-Mail: jesse.walker@intel.com

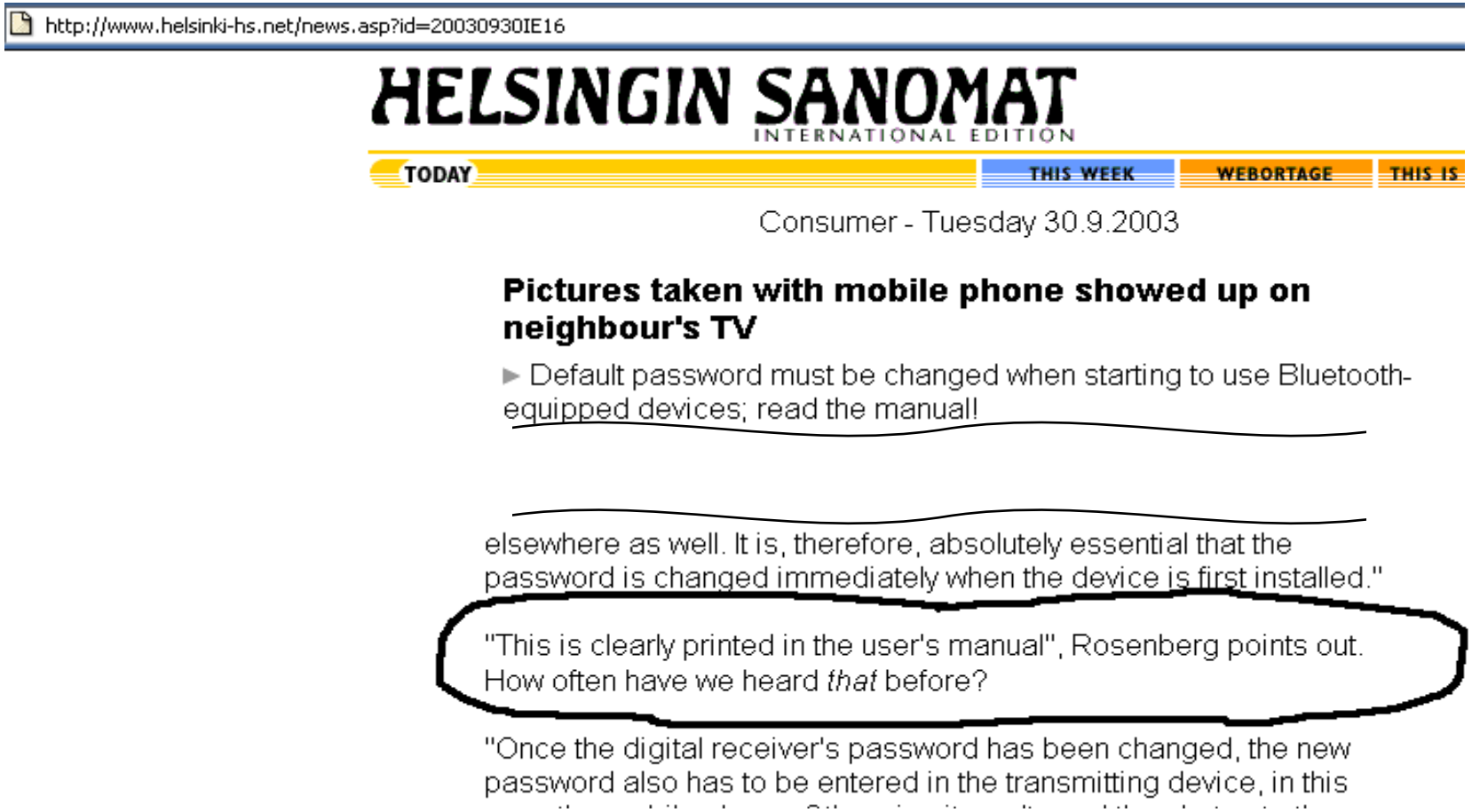
Security Weaknesses in Bluetooth

Markus Jakobsson and Susanne Wetzel

Lucent Technologies - Bell Labs
Information Sciences Research Center
Murray Hill, NJ 07974
USA
{markusj,sgwetzel}@research.bell-labs.com

Abstract. We point to three types of potential vulnerabilities in the Bluetooth standard, version 1.0B. The first vulnerability opens up the system to an attack in which an adversary under certain circumstances is able to determine the key exchanged by two victim devices, making

Naïve usability measures damage security



http://www.helsinki-hs.net/news.asp?id=20030930IE16

HELSINGIN SANOMAT
INTERNATIONAL EDITION

TODAY | THIS WEEK | WEBORTAGE | THIS IS

Consumer - Tuesday 30.9.2003

Pictures taken with mobile phone showed up on neighbour's TV

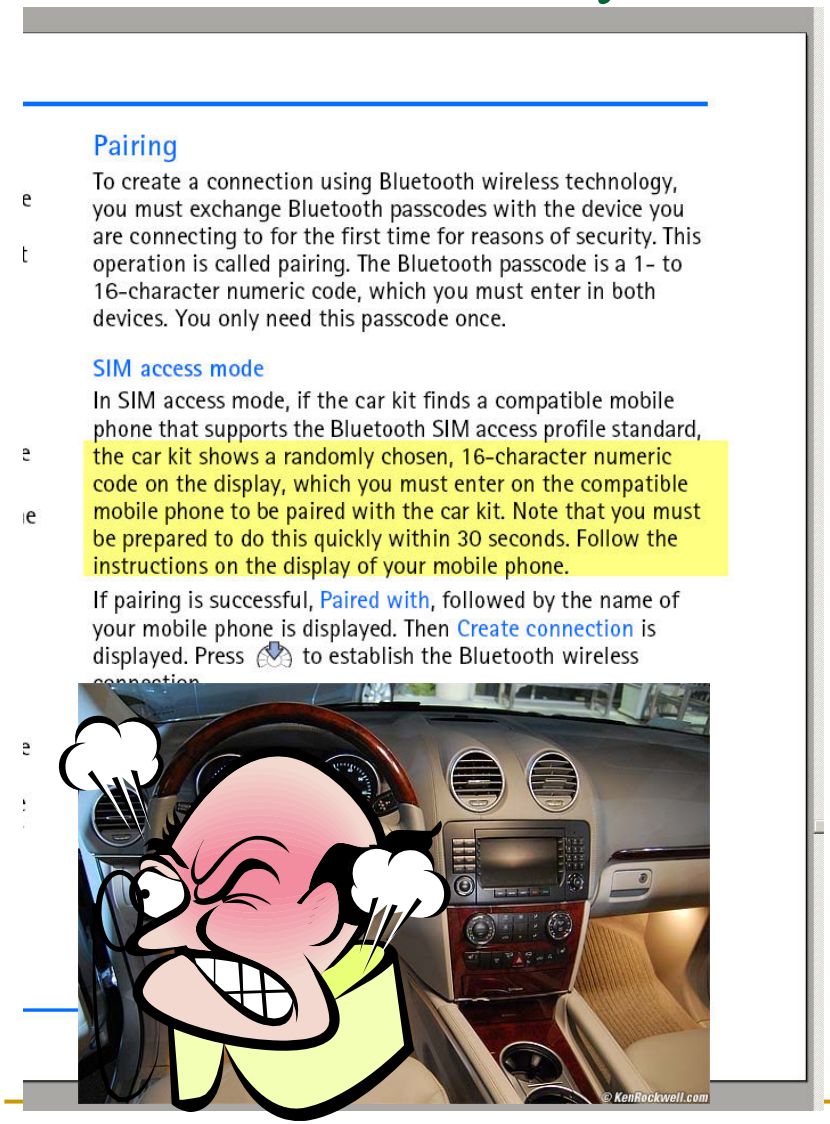
▶ Default password must be changed when starting to use Bluetooth-equipped devices; read the manual!

elsewhere as well. It is, therefore, absolutely essential that the password is changed immediately when the device is first installed."

"This is clearly printed in the user's manual", Rosenberg points out. How often have we heard *that* before?

"Once the digital receiver's password has been changed, the new password also has to be entered in the transmitting device, in this

Naïve security measures damage usability



Pairing

To create a connection using Bluetooth wireless technology, you must exchange Bluetooth passcodes with the device you are connecting to for the first time for reasons of security. This operation is called pairing. The Bluetooth passcode is a 1- to 16-character numeric code, which you must enter in both devices. You only need this passcode once.

SIM access mode

In SIM access mode, if the car kit finds a compatible mobile phone that supports the Bluetooth SIM access profile standard, the car kit shows a randomly chosen, 16-character numeric code on the display, which you must enter on the compatible mobile phone to be paired with the car kit. Note that you must be prepared to do this quickly within 30 seconds. Follow the instructions on the display of your mobile phone.

If pairing is successful, Paired with, followed by the name of your mobile phone is displayed. Then Create connection is displayed. Press to establish the Bluetooth wireless

- Bluetooth pairing was designed with moderate security in mind
- Car kits allow a car phone to retrieve and use session keys from a simcard
- Car kit requires higher level of security
  - users have to enter 16-character passcodes

More secure = Harder to use?

Goal: Secure, intuitive & inexpensive methods for device pairing

- Two (initial) problems to solve
  - Discovery: finding the other device and establishing an insecure channel.
  - Authenticated key agreement: setting up cryptographic keys for subsequent communication
- Assumption: Peer devices are physically identifiable
- Idea: Use a human-perceivable (out-of-band) channel to transport authenticated information.

Some proposals

- For better security and usability, solutions suggested the use of
  - Cables
    - Resurrecting Duckling, [Stanajo, et al. IWSP'99]
  - IrDA, Camera and barcodes/LEDs, speakers
    - Talking to Strangers, [Balfanz, et al. NDSS'02]
    - Seeing-is-believing, [McCune, et al. S&P'05]
    - SIB revisited, [Saxena, et al. S&P'06]
    - Loud and Clear, [Goodrich, et al. ICDCS'06]
  - More Exotic hardware
    - Accelerometers → "Shake well before use", [Mayrhofer, et al. Pervasive'07]
    - Ultrasound, laser transceivers and many others....
  - Recently also
    - "BEDA: Button Enabled Device Association", [Soriente, et al. IWSSI'07]
    - "Simple and effective defenses against evil twin access points" [Roth, et al. WiSec'08]

Recent Standardization Activities

- WiFi
  - WiFi Protected Setup (P1, P2, P3, P6, P8), Jan 2007
    - Announcement: http://www.wi-fi.org/news/pressrelease-081606-WiFiProtectedSetup/
  - Windows Connect Now (P1, P6)
    - Specifications: http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc
    - similar to WiFi Protected Setup
- Bluetooth Secure Simple Pairing, Feb 2007
  - White paper: http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf
- Wireless USB Association Models Supplement, 2006
  - http://www.usb.org/developers/wusb/wusb_2006_0302.zip (P1, P4)
- Others are in the works

Problems with previous approaches

- Using 2-channels during pairing
  - In-band channel (Bluetooth, 802.11, etc.) to transfer PKs
    - May not be available during the pairing.
    - Needs discovery and set-up
    - Vulnerable to DoS (e.g., jamming) attacks
  - Out-of-band channel (e.g., user typing a PIN) to authenticate the exchanged PKs.
- Exotic hardware or interfaces
  - not available on all devices (e.g., laser transceiver)
  - hard to expect from the future ones (cost, space, esthetic)
- Asking too much from an ordinary user
  - Less than handful have been evaluated for usability.

Why is HAPADEP different?

- Audio as the sole communication channel
  - Audio is
    - perceptible (Authentication, DoS protection, attacker identification)
    - broadcast in nature (no configuration, discovery etc.)
    - capable of relatively higher bandwidths
  - Speakers and microphones are
    - relatively ubiquitous
    - inexpensive to add
- Tested and optimized for usability

HAPADEP Operation

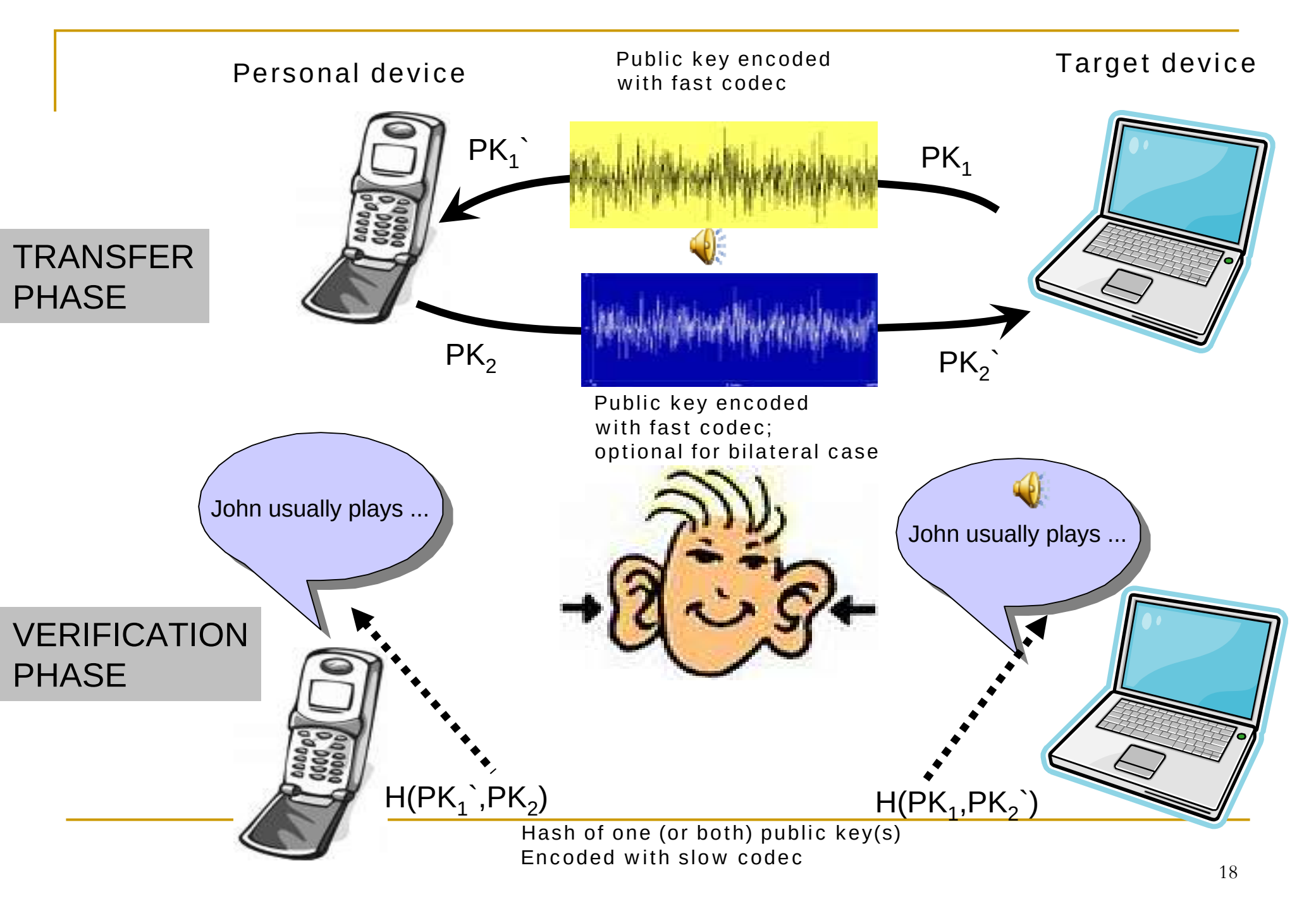
- Consist of two phases:
  - **Transfer Phase:** Devices exchange their public keys over audio.
    - Public keys are encoded into audio using a *fast* codec.
    - Each device plays its encoded public key while the other is recording.
  - **Verification Phase:** User is involved to verify secure completion.
    - Digest of the exchanged keys are calculated and encoded into audio using a *slow* codec.
    - Both devices play the encoded digest.
    - User listens them both and decide if they match.

Fast Codec in transfer phase

- PKs are big
  - Higher bit-rate (faster transmission) is needed
- We used Digital Voices codec (UCI and PARC collaboration). 
  - Quite tolerant to
    - Background noise
    - Transmission errors
  - Transmits 240-bits in about 3 seconds
- Any codec that is reasonably fast and error tolerant can be used here.

Slow codec in verification phase

- Digests are smaller so lower bit-rate (slower) is OK.
- Output is compared by a human
  - Must be pleasant to hear and easy to compare.
- We tried
  - Digital Voices codec: Sounds like a child playing a toy piano 
    - Created on the fly
      - For each byte: 4-bit selects the chord, previous & present byte selects the octave
  - Grammatically correct non-sensical English sentences 
    - Uses stored catalogues, one for each part of speech (verb, noun,…)
    - Each 10-bit is used to choose a word from the corresponding catalogue.


Personal device
Public key encoded
with fast codec
Target device
TRANSFER
PHASE
PK1`
PK1
PK2
PK2`
Public key encoded
with fast codec;
optional for bilateral case
VERIFICATION
PHASE
John usually plays ...
John usually plays ...
H(PK1`,PK2)
H(PK1,PK2`)
Hash of one (or both) public key(s)
Encoded with slow codec

Usability Testing

- 20 subjects were recruited
- Each participant paired the devices in total of 4 times:
  - Each variant is tested twice: once with matching and once with non-matching values (in random order).
- Timing and number of trials are automatically logged by the software
- User experience is gathered through structured interviewing and questionnaires.

Test Results (1/4)

- When there is no attack, users can complete the pairing in roughly a minute on their first use.

Method	Completion Time (sec.)
Melody (No Attack)	62.15
Melody (Under Attack)	74.5
Sentences (No Attack)	56.95
Sentences (Under Attack)	80.5

Test Results (2/4)

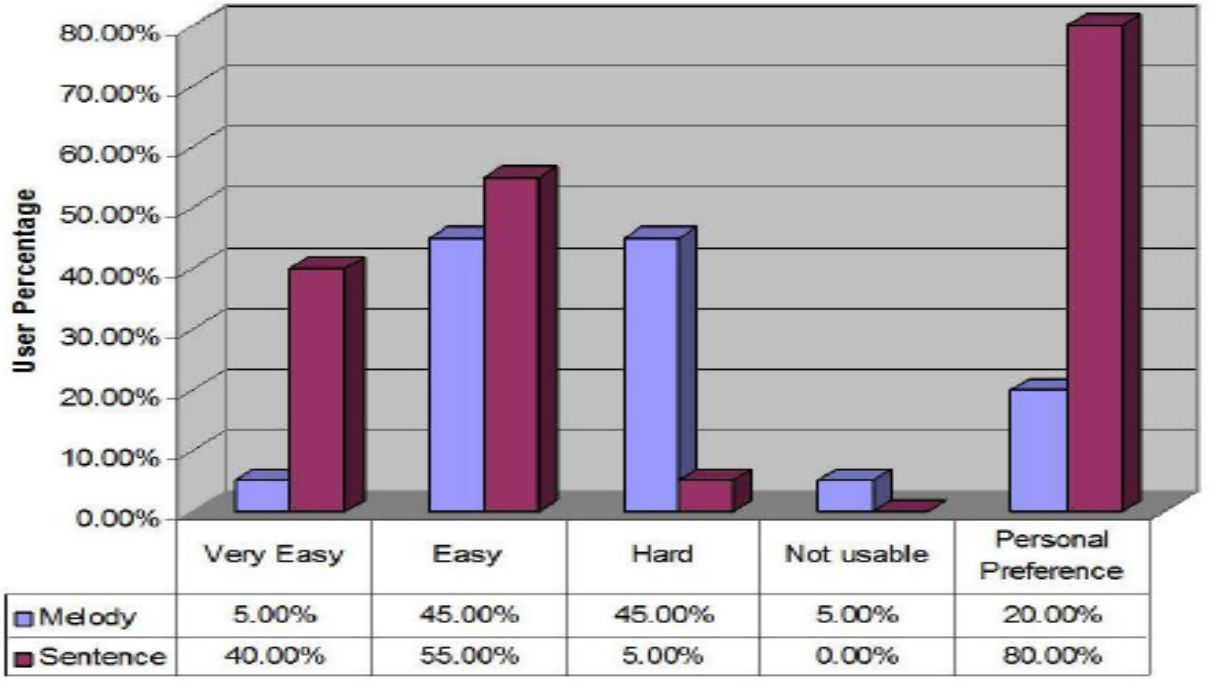
- Melody variant is not mature enough (high error rate)

Method	Fatal Error Rate	Safe Error Rate
Melody (No Attack)	N/A	10%
Melody (Under Attack)	15%	N/A
Sentences (No Attack)	N/A	0%
Sentences (Under Attack)	5%	N/A

- Sentences provide good usability and low error.
  - Only 1 person accidentally pressed match on non-matching values.

Test Results (3/4)

- Subjects also liked sentences better



	Very Easy	Easy	Hard	Not usable	Personal Preference
Melody	5.00%	45.00%	45.00%	5.00%	20.00%
Sentence	40.00%	55.00%	5.00%	0.00%	80.00%

Test Results (4/4)

- Comparison to their previous experience
  - All that have Wi-Fi pairing experience (70%)
    - Found HAPADEP easier.
    - Prefer HAPADEP instead.
  - Only %22 of those with Bluetooth pairing experience
    - Prefer original Bluetooth pairing to HAPADEP
      - Biggest concern was noise.
- HAPADEP is simple and fun to use!

Limitations

- HAPADEP
  - Needs
    - speaker and a microphone on device(s)
    - sufficient proximity between devices
  - Not suitable for
    - Hearing impaired
    - Noisy environments (e.g., factories, stadiums)
    - Silence required (e.g., library, classroom)
  - Takes longer than some other techniques

Strengths

- HAPADEP
  - Uses pure audio for communication
    - No other common wireless interface is needed for pairing.
      - May not be available at the time of pairing.
      - May be troublesome to configure and initialize.
    - Audio communication does not need any complicated set-up.
    - Provides better protection against MiTM and DoS attacks
  - Can help to automate the configuration for subsequent communication
    - e.g., sending the Bluetooth MAC and configuration during transfer phase adds less than 1 second to the protocol.
  - Very usable and inexpensive to deploy

Thanks!

- Questions?