**Mobile Device and Wireless Network Security**

# Pervasive Computing Security: Secure Pairing

Motivation;

Device pairing schemes for various devices

Di Ma

# Lecture outline

- Motivation
- Device Paring Schemes
  - Resurrecting Duckling
  - Talking to Strangers
  - Visual Out-of-Band Channels
    - Seeing-is-believing
  - Audio Out-of-Band Channels
  - Proximity-Based Approaches
  - Accelerometer-Based Approaches
  - Biometrics-Based Approaches

# What is Pervasive Computing?

- A.k.a. ubiquitous computing

- Technology View
  - Computers everywhere – embedded into fridges, washing machines, door locks, cars, furniture, people

  →intelligent environment
  - Mobile portable computing devices
  - Wireless communication – seamless mobile/fixed
- User View
  - Invisible – implicit interaction with your environment
  - Augmenting human abilities in context of tasks
- Ubiquitous = mobile computing + intelligent environment

# Ubiquitous Electronics

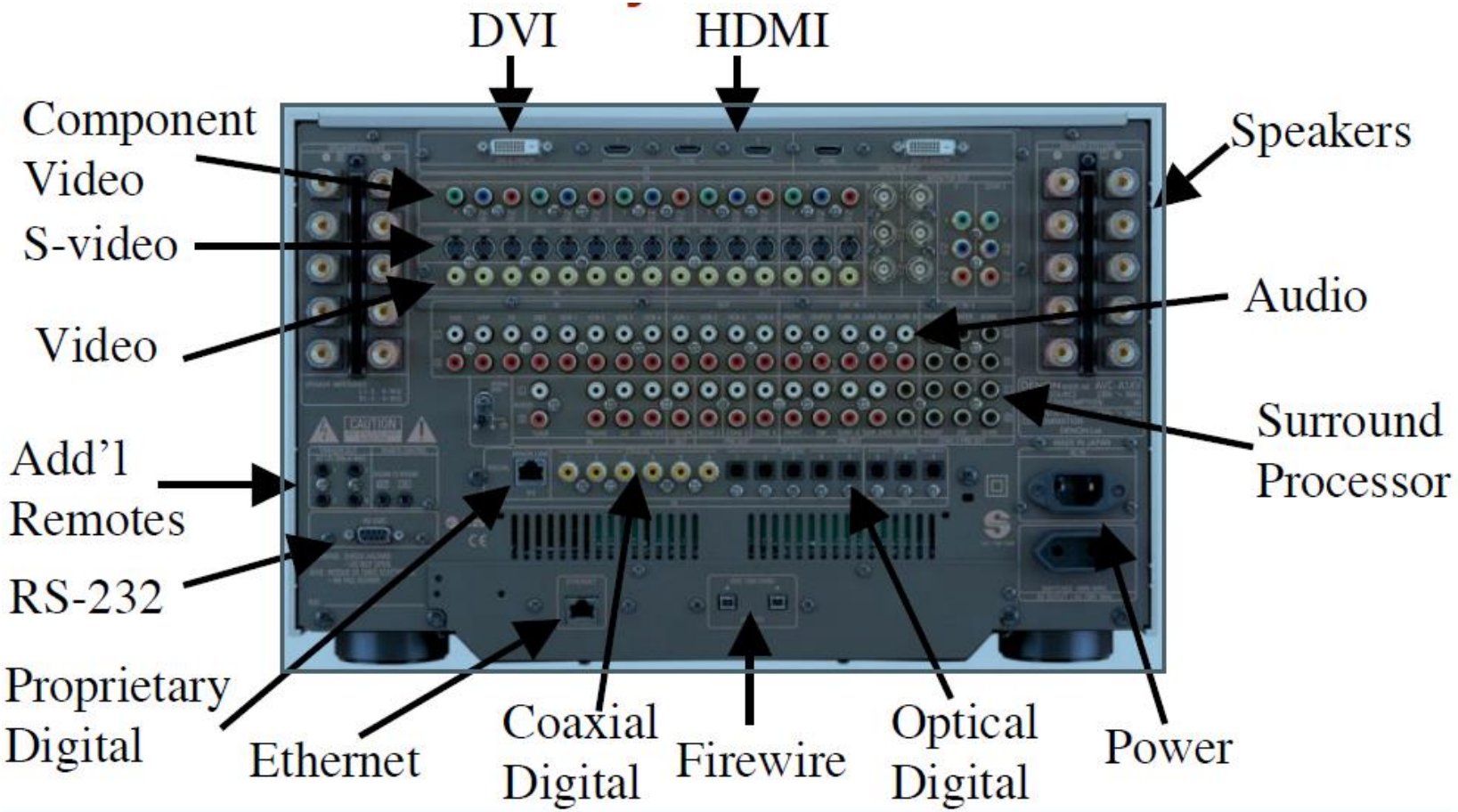


# Ubiquitous Electronics

- More and more devices every day
  - Varying size and capabilities
  - Varying connection methods (e.g. Cable, Bluetooth, etc)
  - Varying user interface (rich, moderate and poor)
- Spontaneous method of interaction
- Increasing Mobility in devices
- Frequent associations and disassociations
  - e.g. pairing of Bluetooth enable headset with mobile phone or MP3 player, pairing IR remote with laptop, etc.

# Ubiquitous Electronics

- More devices every day
- More device interaction
- → Too many connections!



# Go Wireless!

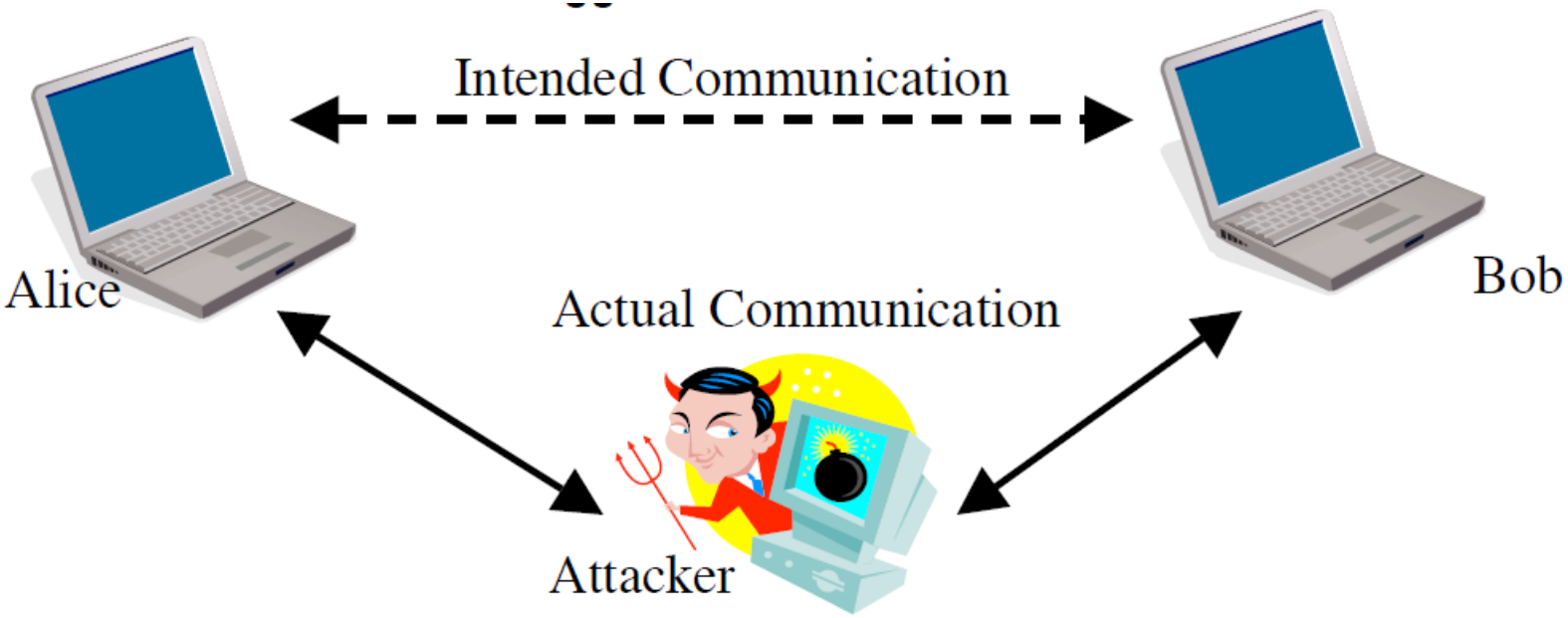
- 802.11, Bluetooth, infrared, Zigbee, 3G, …


- Cable replacement
  - Computer to printer
  - MP3 player to computer
  - Cell phone to laptop
  - Etc…

- Introduces a problem

# Man in the Middle!

- Attacker can easily control communication between wireless devices
- More devices == bigger threat



# Solution?

- Communication must be authenticated
  - To rule out man-in-the-middle
  - Need to bootstrap secret  in order to have private communication
  - Reduced problem: **key setup** between communicating devices or device paring

# Secure pairing of personal devices

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

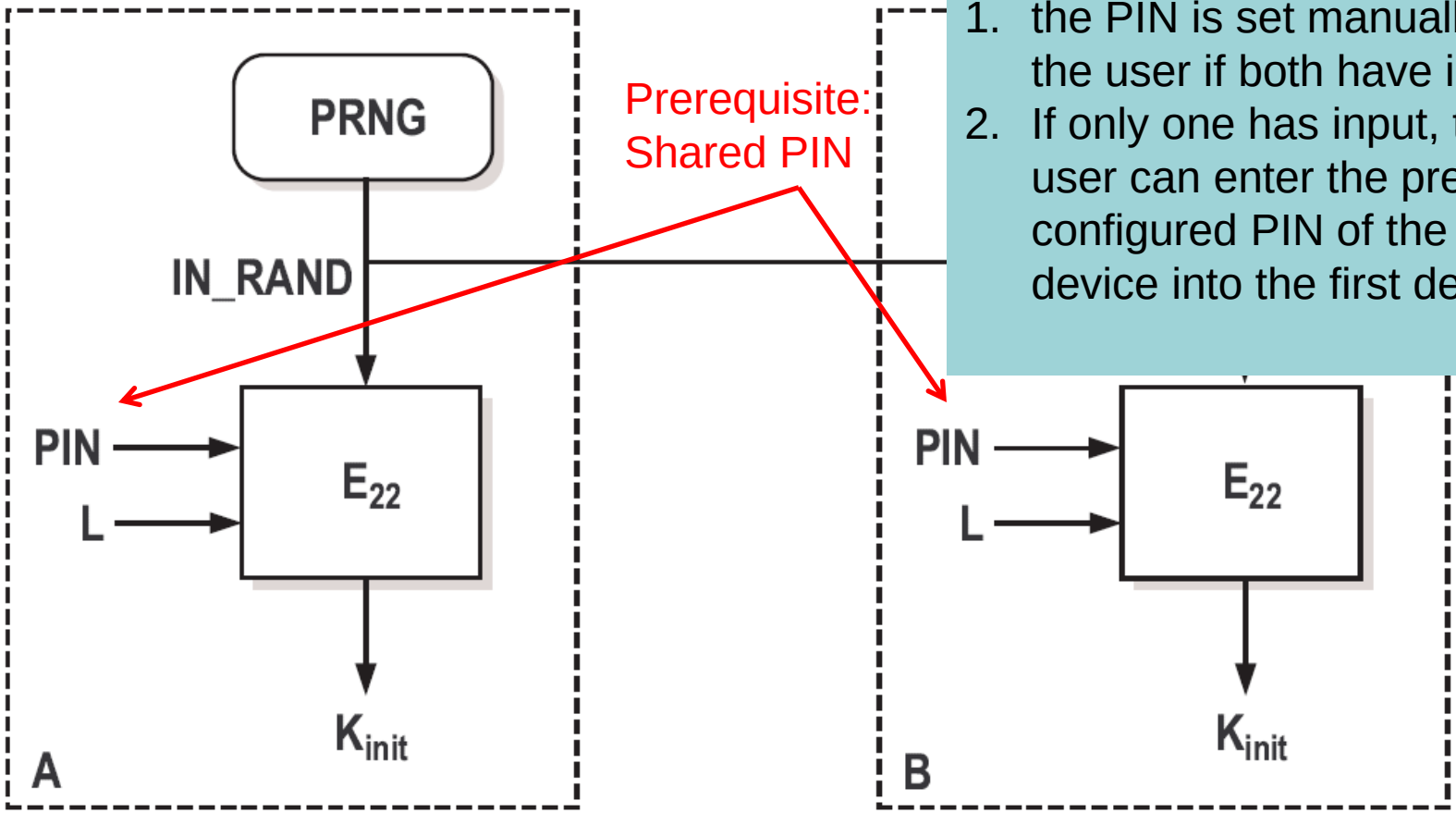

Recall in "Lecture 3: the Security of Existing Wireless Networks" how Bluetooth users initiate secure communication?

# Bluetooth

- Short-range communications between nearby devices
  - A mobile phone and a head set, a laptop and a mouse, or a computer and a printer, etc.
  - Only wireless stations
- Master-slave principle
  - One master, up to 7 slaves
- Security issues:
  - Authentication of the devices to each other
  - Confidential channel

# Bluetooth – initialization key setup

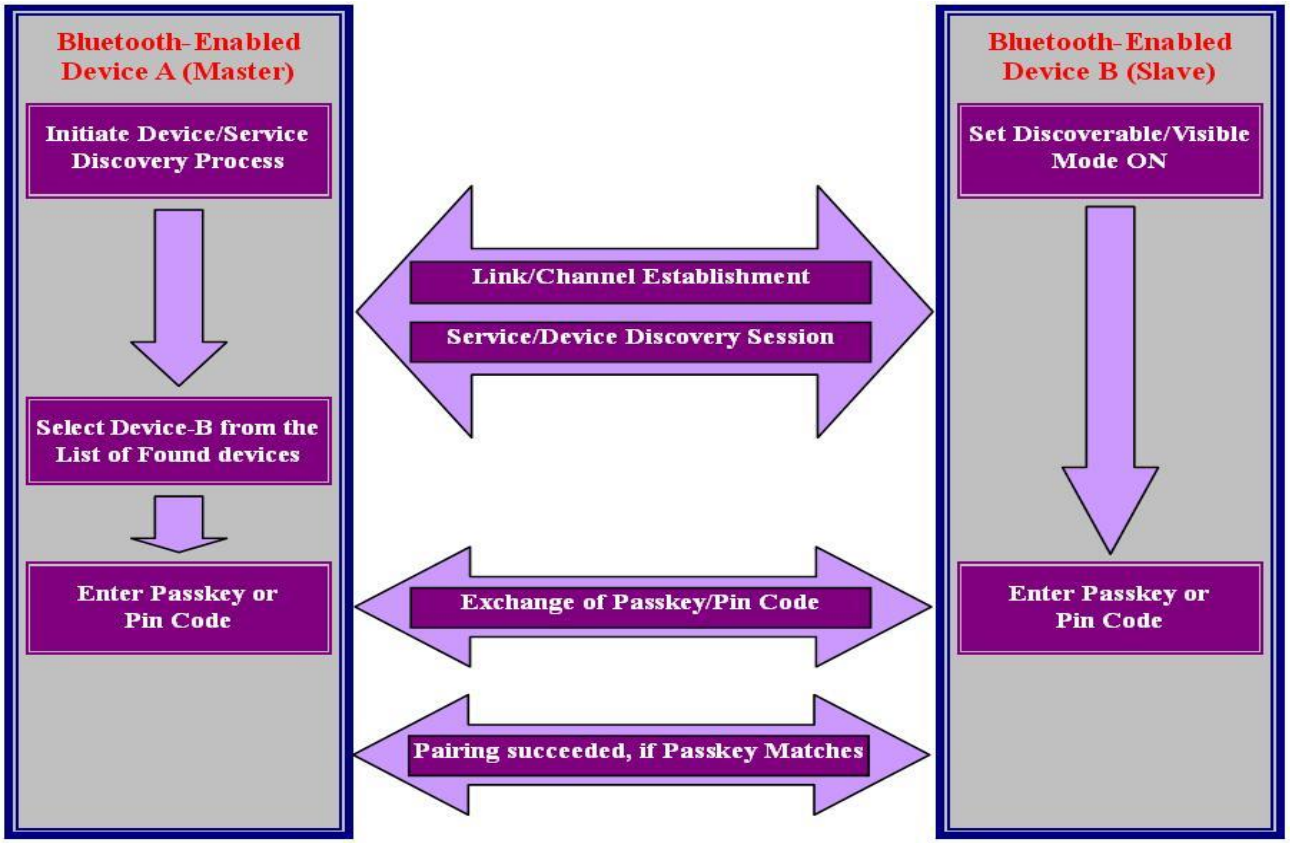
- When two devices communicate for the first time:
  - Set up the temporary initialization key.

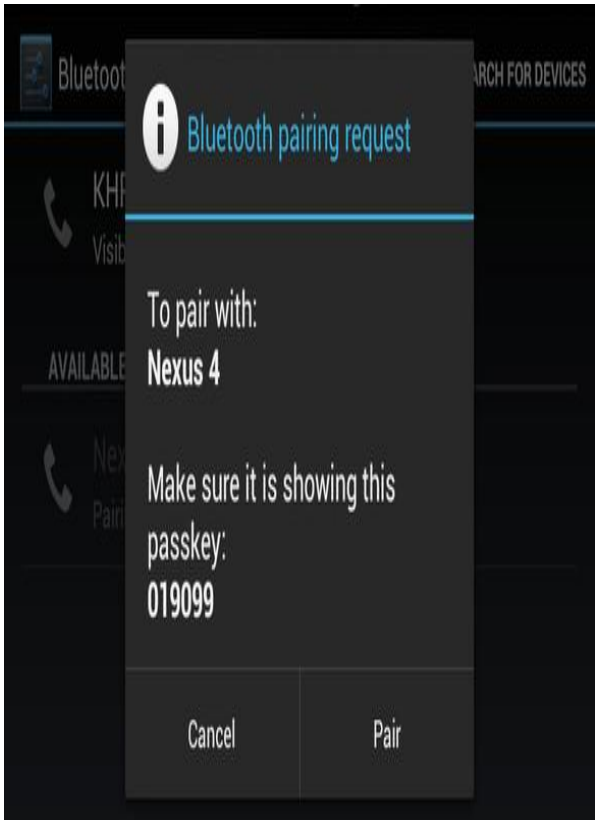



PIN can be shared in several ways:

1. the PIN is set manually by the user if both have inputs.
2. If only one has input, the user can enter the pre-configured PIN of the other device into the first device.

# Bluetooth Pairing



# Problem we are going to tackle today …

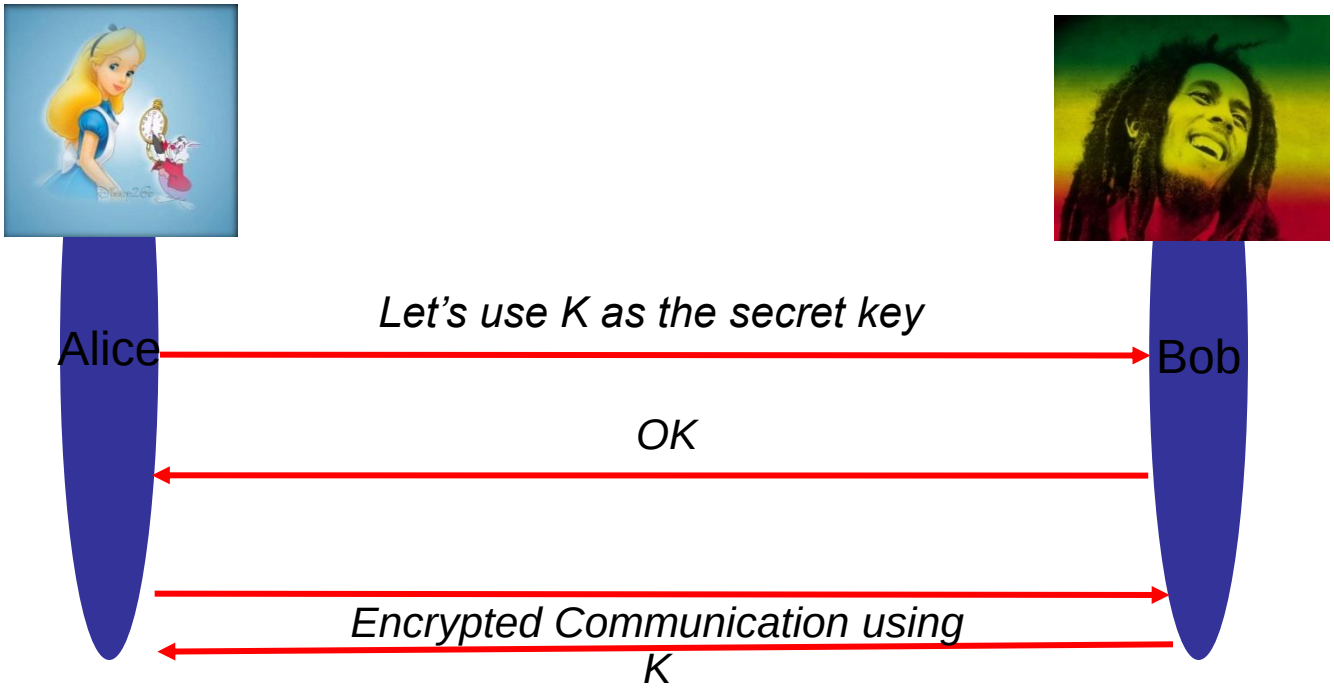
- Setting up a security association (authenticated secure communication) where:
  - No prior context exists (no PKI, common TTPs, key servers, shared secrets, etc.)
  - Ordinary non-expert users
  - Cost-sensitive commodity devices varying in device capabilities
    - Communication channels
    - User-interfaces
    - Power and computational resources
    - Sensing technology, etc.



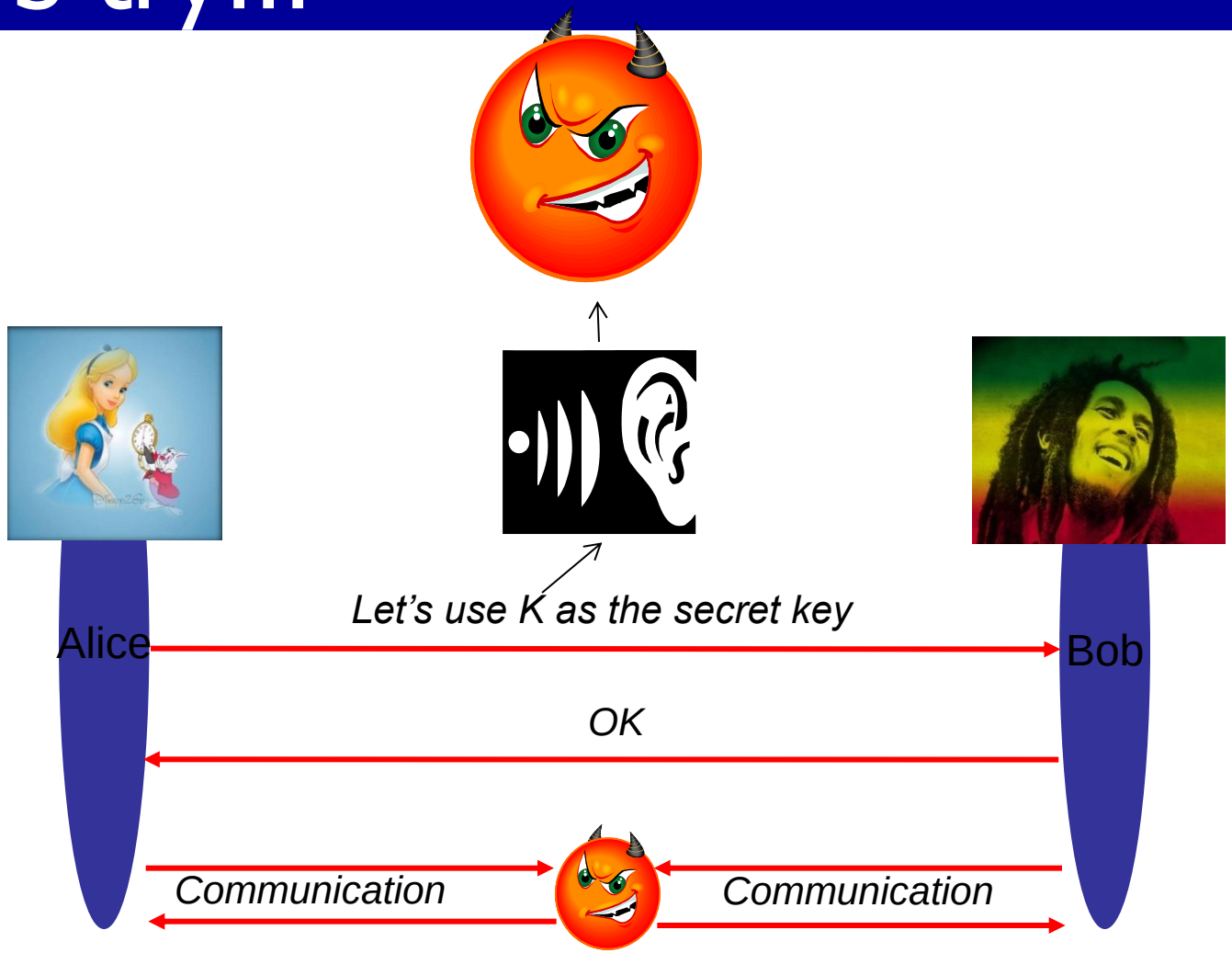

Today's tasks:

1. To study multiple schemes
2. To explore more possibilities, if possible

# Let's try…


Alice
Bob
Let's use K as the secret key
OK
Encrypted Communication using K

# Let's try...




Eve can decrypt the communication!
Eve can impersonate either party!

# Diffie-Hellman Key Agreement

- Shows how to agree on a secret where none existed…

Public values: large prime p, generator g
Alice has secret value a, Bob has secret b

1. A → B: $g^a \bmod p$
2. B → A: $g^b \bmod p$
3. Bob does: $(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$
4. Alice does: $(g^b \bmod p)^a \bmod p = g^{ab} \bmod p$

- Eve cannot compute $\mathbf{g^{ab} \bmod p}$

So, are we done yet?

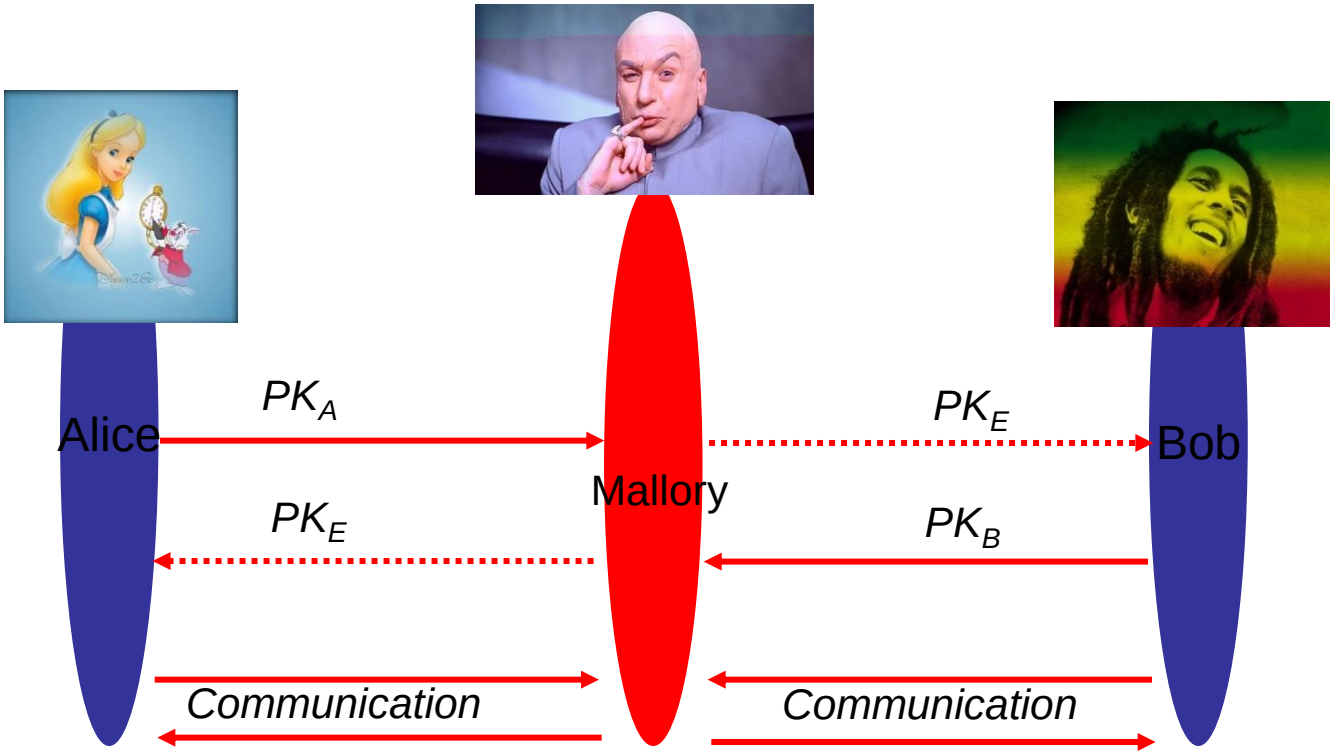
# Problem: Man-in-the-Middle (MitM) Attacks

Mallory (M) can impersonate Alice to Bob, and Bob to Alice!

1. A → B/M: $g^a \bmod p$
2. M → A: $g^m \bmod p$
3. M/A → B: $g^m \bmod p$
4. B → A/M: $g^b \bmod p$
5. Bob does: $(g^m \bmod p)^b \bmod p = \mathbf{g^{bm} \bmod p}$
6. Alice does: $(g^m \bmod p)^a \bmod p = \mathbf{g^{am} \bmod p}$

Why? No authentication…

# Man-in-the-Middle (MitM) Attacks

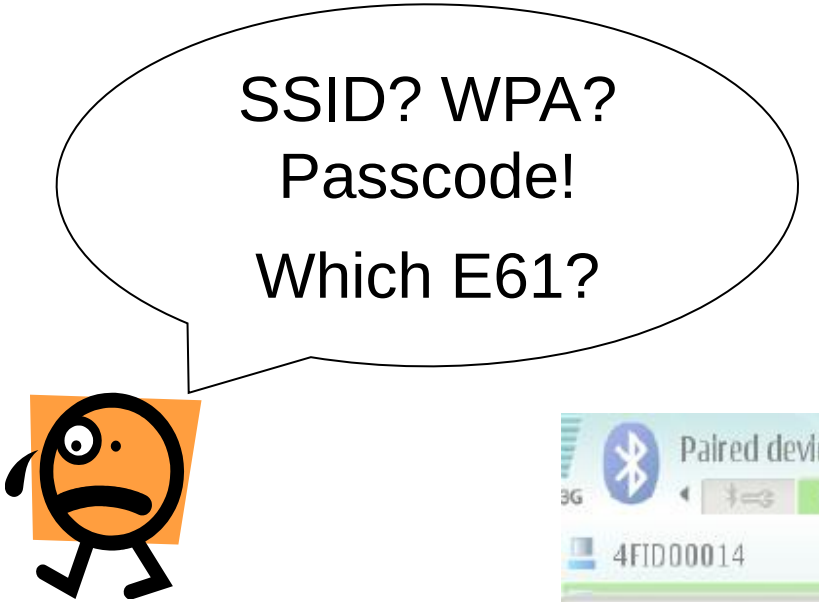



Mallory controls the communication!

# How Serious are MitM Attacks?

- Wireless communication is "*invisible*" or human-imperceptible
  - People can't tell which devices are "talking"
  - A rogue device might not be "visible" or identifiable as such
- A neighbor can easily execute an MitM attack
  - If neighbor has a faster computer, it can easily respond faster than the legitimate device(s)
  - Meanwhile, legitimate device(s) may also be "silenced" by DoS
- **Easy to mount with high success rate!**

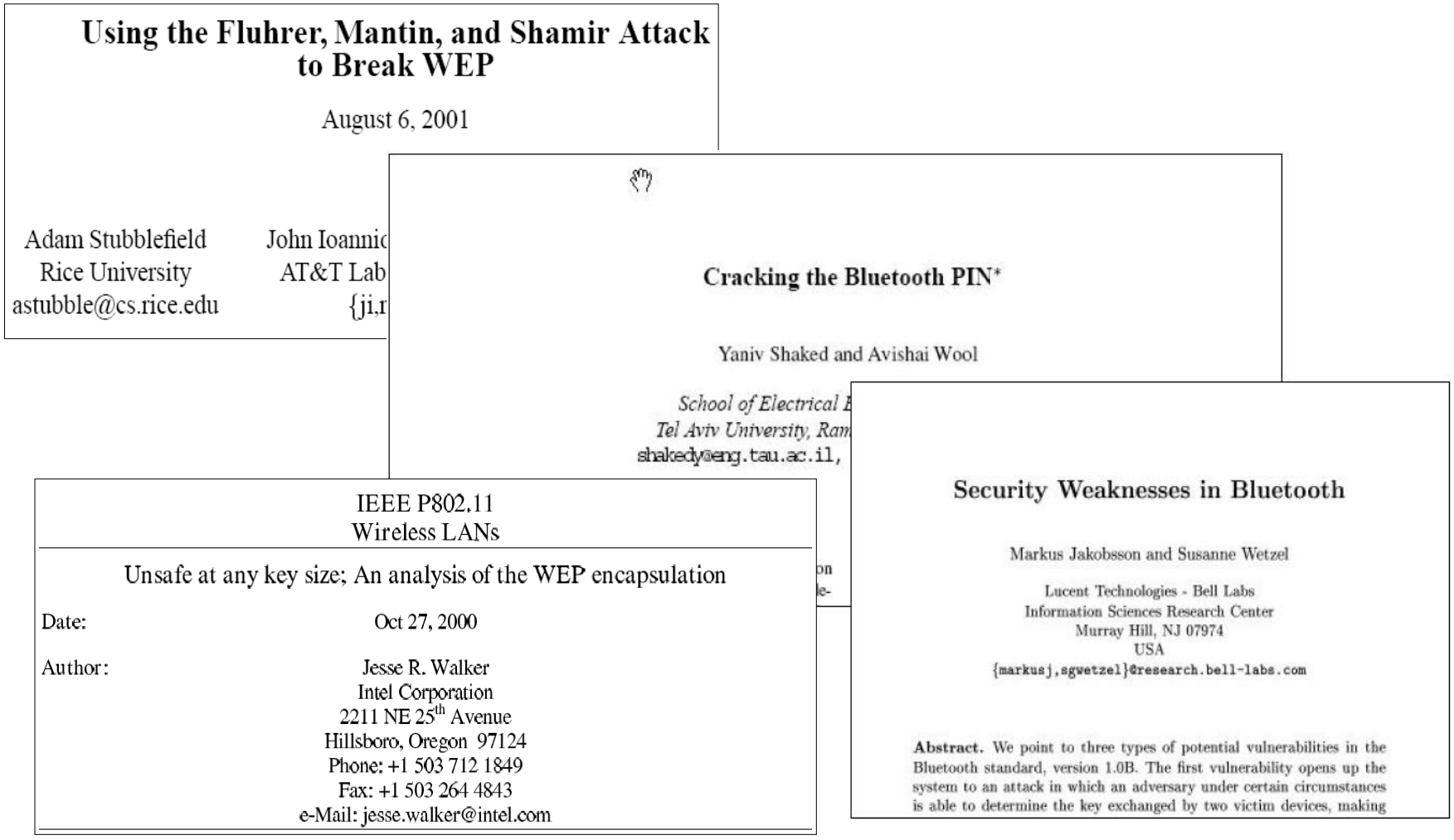
# Mechanisms should be intuitive




... They are not for all devices as well!

# … and 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

# Goal: Secure, intuitive, inexpensive methods for device pairing

- Two (initial) problems to solve
  - Discovery: finding the other device and likely to establish an insecure channel.
  - Authenticated key agreement: setting up cryptographic keys for subsequent communication
- Assumption: Peer devices are physically identifiable
- Idea:
  1. Use a human-perceivable (**out-of-band or OOB**) channel to transport authenticated information (e.g. checksum of the public keys, or public key itself)

# Lecture outline

- Motivation
- Device Paring Schemes
  - Resurrecting Duckling
  - Talking to Strangers
  - Visual Out-of-Band Channels
    - Seeing-is-believing
  - Audio Out-of-Band Channels
  - Accelerometer-Based Approaches
  - Biometrics-Based Approaches
  - Others

We want to explore a spectrum of solutions targeting embedded devices with varied capabilities.

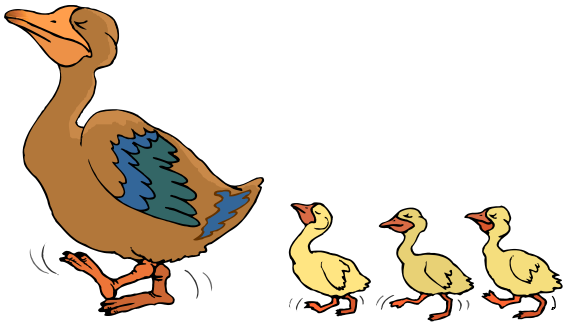
# Resurrecting Duckling

## F. Stajano and R. Anderson, IWSP '99

- Problem: how to set up keys in a ubiquitous computing environment?
  - Devices use wireless communication
- Target scenarios
  - modern home with multiple remotely controlled devices
    - DVD, VHS, HiFi, doors, air condition, lights, alarm, …
  - modern hospital
    - mobile personal assistants and medical devices, such as thermometers, blood pressure meters, …
- Common in these scenarios
  - transient associations between devices
  - physical contact is possible for initialization purposes

# Resurrecting Duckling

**imprinting**



Konrad Lorenz(1903-1989)
The Nobel-winning investigator of animal behavior
Described how a goose hatchling assumes that the first moving object it sees must be its mother.

# The Resurrecting Duckling

- **Solution:** set up keys using **trusted communication channel**
  - No cryptographic keys to setup this channel
  - Physical contact establishes a secure channel
  - E.g., a simple wire

# The *resurrecting duckling* Security Policy

- At the beginning, each device has an empty *soul*
- Each empty device accepts the first device to which it is physically connected as its master (imprinting)
- During the physical contact, a device key is established
- The master uses the device key to execute commands on the device, including the *suicide* command
- After suicide, the device returns to its empty state and it is ready to be imprinted again
- A new imprinting by another mother is possible*: reverse metempsychosis*

# Summary – Resurrecting Duckling

- Two state device (duckling)
- Can be "imprinted" multiple times (device ownership)
- Mother gives "life" via **physical contact**
  - Establishes shared secret
  - Rules out man-in-the-middle
  - Very convenient for user

Caveats:

- Interface unavailable in commodity devices
- Awkward cables

# Lecture outline

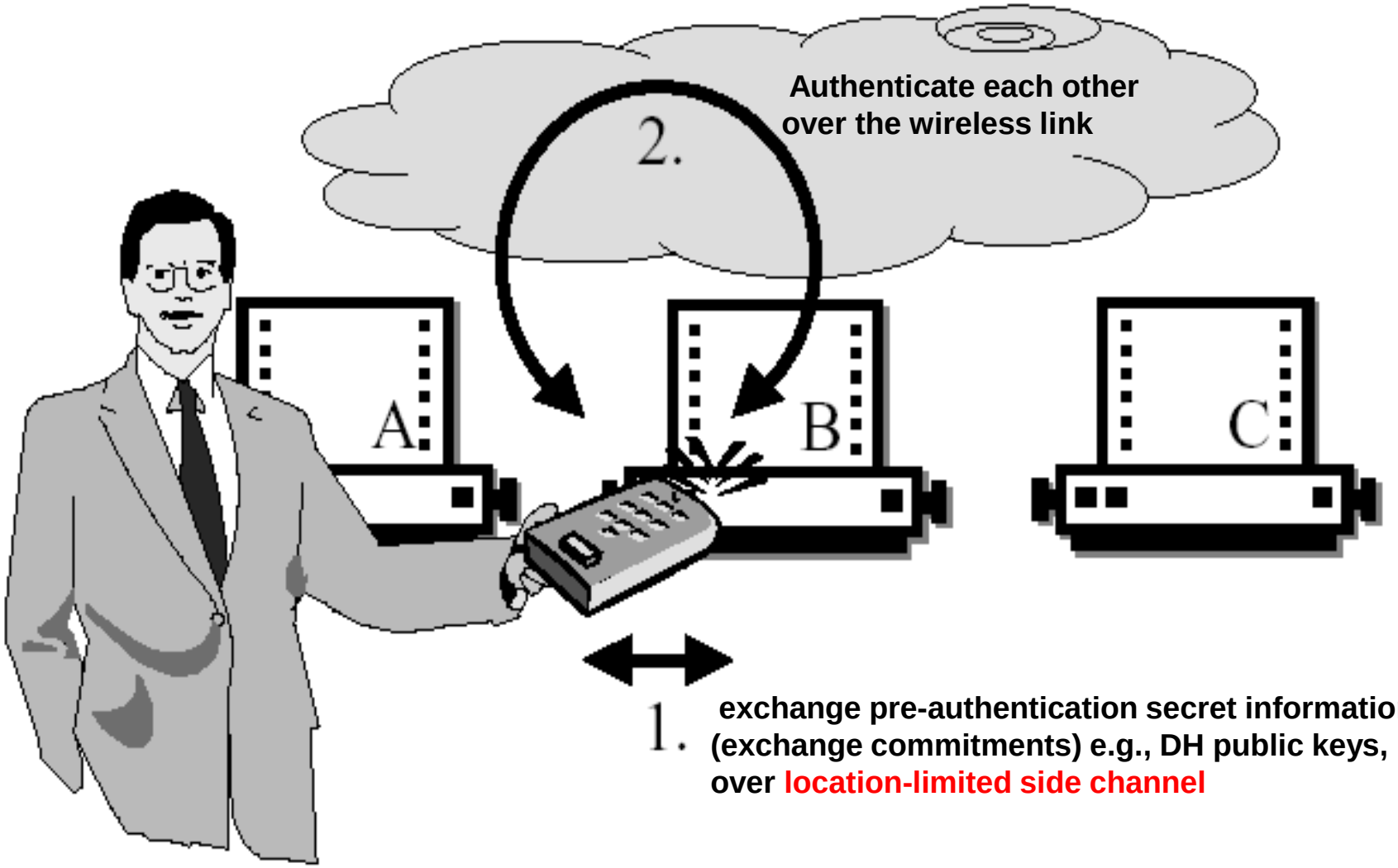
- Motivation
- Device Paring Schemes
  - Resurrecting Duckling
  - Talking to Strangers
  - Visual Out-of-Band Channels
    - Seeing-is-believing
  - Audio Out-of-Band Channels
  - Proximity-Based Approaches
  - Accelerometer-Based Approaches
  - Biometrics-Based Approaches

# "Talking to Strangers"

Balfanz, et al. NDSS '02

- Addresses practical shortcomings of Duckling
  - Devices have no interfaces for physical contact
  - Cables are cumbersome
- Propose Infra-red as a "**Location-Limited Side Channel"**
  - Which human operators can precisely control which devices are talking with each other
    - Impossible for an attacker to transmit in that channel
  - Assumed to be immune to MitM attack
  - Many of today's (yesterday's) devices equipped with IR

# Talking to Strangers



# Talking to Strangers

- Pros
  - Works(-ed) on many commodity devices
  - Eliminate physical contact
  - Location-limited side channel
    - Restricts location of attacker
- Cons
  - Most users do not know where their IR port is
  - Most devices require IR to be explicitly turned on
  - IR is invisible, attacker may still be able to mount MitM attack
  - Infrared not available in all devices

# Lecture outline

- Motivation
- Device Paring Schemes
  - Resurrecting Duckling
  - Talking to Strangers
  - Visual Out-of-Band Channels
    - Seeing-is-believing
  - Audio Out-of-Band Channels
  - Proximity-Based Approaches
  - Accelerometer-Based Approaches
  - Biometrics-Based Approaches

# Seeing-is-Believing (SiB)

McCune, et al. IEEE Security &Privacy '05

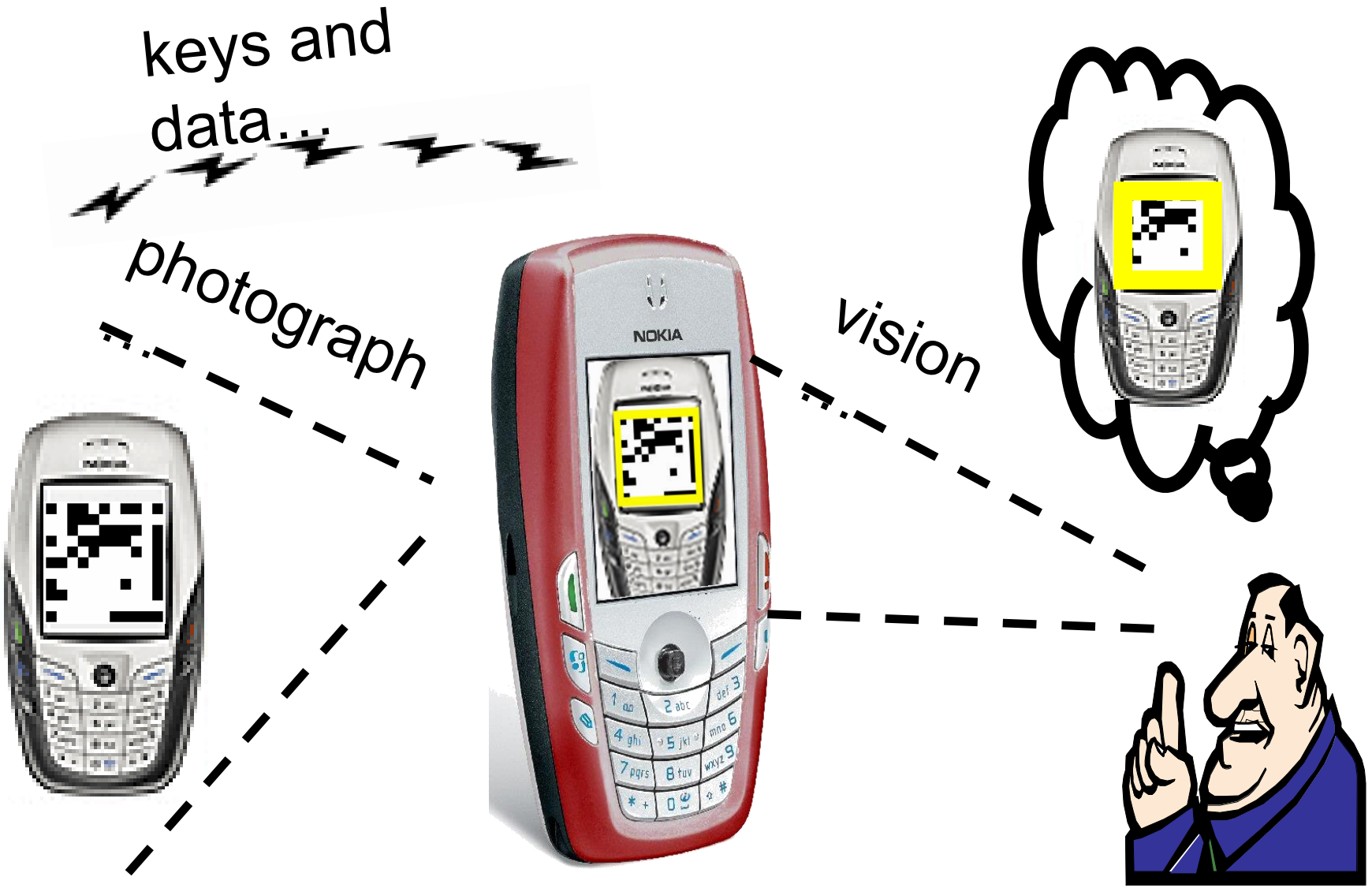
- Difficult to achieve **demonstrative identification** of devices communicating wirelessly with no prior context
- Prior work proposes the use of a **location-limited side-channel** to authenticate devices
  - Infrared, ultrasound, physical contact
- Proposals to-date too cumbersome for non-expert users
  - None of them convince the user that they are really communicating with ***the target*** device

# Seeing-Is-Believing

- Camera phones have sufficient resources to scan 2D barcodes
- Some have high-quality screens which can display freshly-generated barcodes
- Using them together yields a ***visual***, location-limited channel
- Visual channel ***can*** provide **demonstrative identification** of communicating parties to the user

- Enables strong human-assisted authentication

# Basic SiB Protocol



# Basic SiB Protocol

| | A | | B |
|---|---|---|---|
| 1 | $h_A \leftarrow Hash(PK_A)$ | | |
| 2 |  | $h_A \xrightarrow[\text{(visual)}]{}$ |  |
| 3 | | $PK_A \xrightarrow[\text{(other)}]{}$ | $h' \leftarrow Hash(PK_A)$ |
| 4 | | | $if\, h' \neq h_A\ then\ abort$ |

# SiB Caveats

- Not all devices have big enough displays to show two-dimensional bar codes
- Not all devices have good-enough cameras
- Sometimes devices cannot be placed sufficiently near
- There might not be enough light for pictures

# SiB Summary

- 2D barcodes to authenticate devices with camera phones
  - Involve the user, but a way that is intuitive
  - Taking pictures of desired communication endpoints is one way to achieve this property

- Disadvantages
  - Many devices lack a camera or barcode scanner
  - Need graphical display or sticker
  - Visually-impaired users
  - Poor visibility scenarios (e.g., smoke, darkness)
  - Requires sufficiently clear picture

# More visual out-of-band channels

- "Snowflake" , "Random Arts Visual Hash" and "Colorful Flag"
  - OOB data encoded in images, users are asked to compare them on two devices. Require both devices to have displays with sufficiently high resolution

- Secure Device Pairing Based on Visual Channel by Saxena et al.
  - Proposed as an improvement to SiB through the use of LED and extracting information based on inter-blink gaps
  - One device blinks
  - The other takes a video clip
  - Video clip parsed to extract an authentication string

# Lecture outline

- Motivation
- Device Paring Schemes
  - Resurrecting Duckling
  - Talking to Strangers
  - Visual Out-of-Band Channels
    - Seeing-is-believing
  - Audio Out-of-Band Channels
  - Proximity-Based Approaches
  - Accelerometer-Based Approaches
  - Biometrics-Based Approaches

# Audio out-of-band channel

- Loud and Clear (L&C) by Goodrich et al.,
  - Use audio as OOB channel for human-assisted authentication
  - Derive auditory-robust, syntactically correct, but nonsensical (MadLib) sentence from hash of a public key
    - E.g., Donald the fortunate blue-jay fraudulently crushed over the creepy arctic-tern.
  - Compare the vocalized sentences

- Human-Assisted Pure Audio Device Pairing (HAPADEP) by Soriente et al.,
  - Pairing two devices that have no common standard wireless channel at the time of pairing
  - Use audio to exchange both cryptographic material and protocol messages

# Audio out-of-band channel caveat

- Not applicable to pairing scenarios where one of the devices does not have a display and/or a speaker (or microphone in case of HAPADEP)
- Not suitable for hearing-impaired users
- Not feasible in noisy environments
- Places burden on user to compare the two Madlib sentences or Melodies

# Current research…

- Group pairing scenarios for >2 devices.
- Pairing  with interface-less devices e.g. RFID, some sensors
- …

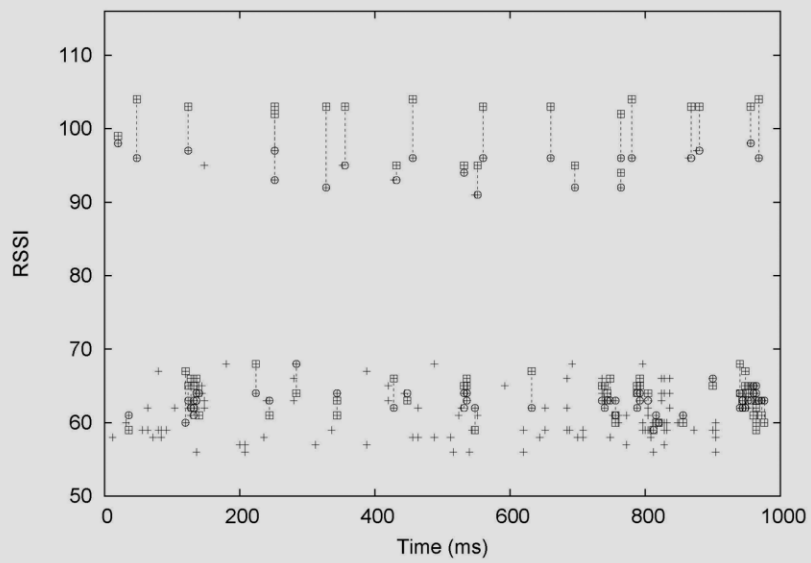
# OOB is not the only way …

- Amigo: Proximity-Based Authentication of Mobile Devices [Varshavsky et.al. UbiComp 2007]
  - Secure pairing requires a shared secret
  - Devices in close proximity perceive a similar radio environment
  - Derive shared secret from common radio environment
    - Listen to traffic of ambient radio sources
  - **Use knowledge of common radio environment as proof of proximity**

# Requirements on Radio Environment

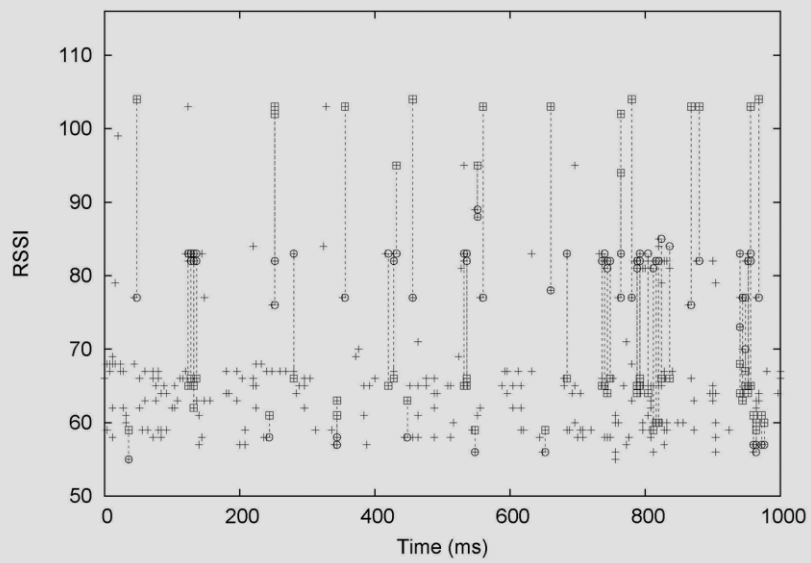
Devices in proximity should perceive similar environment

5 cm




85% common pkts

10 m



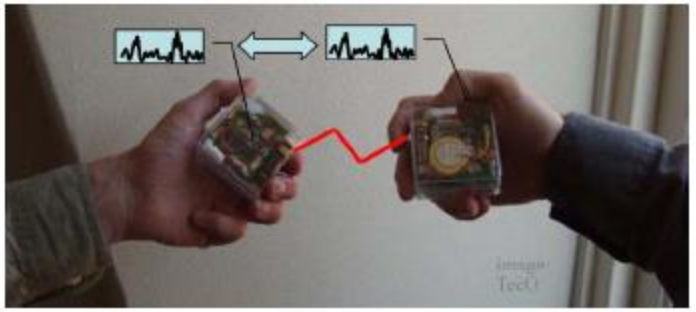

40% common pkts

# Amigo: advantages & disadvantages

- Advantages
  - No extra hardware
    - Leverage radio already available on device
  - No user involvement to verify pairing
  - Not subject to eavesdropping
    - Secret derived by listening to ambient sources
- Disadvantages
  - Robustness is an issue
    - Different antennas, imperfect synchronization and other differences between devices may prevent pairing.
  - Only security guarantee is that the devices are close to each other.
  - Security is not really provable or quantifiably in a traditional way

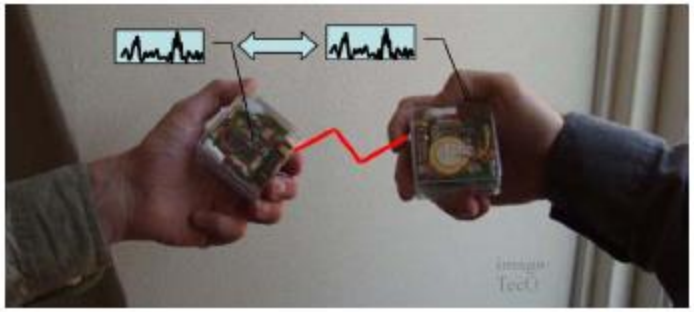
# Accelerometer-Based Approaches

- Smart-its-Friend by Holmquist et al.
  - Use common readings from the embedded accelerometers in the devices
  - Security has not been the major concern
- Are You With ME by Lester et al.
  - Use accelerometers' data to show that a set of devices is being carried by the same person
- Shake-Well-Before-Use by Mayrhofer et al.
  - Combine cryptographic primitives with accelerometer data analysis for secure device-to-device authentication



# Accelerometer-Based Approaches

- Require accelerometer in each device
- Large variety of devices can not be shaken together



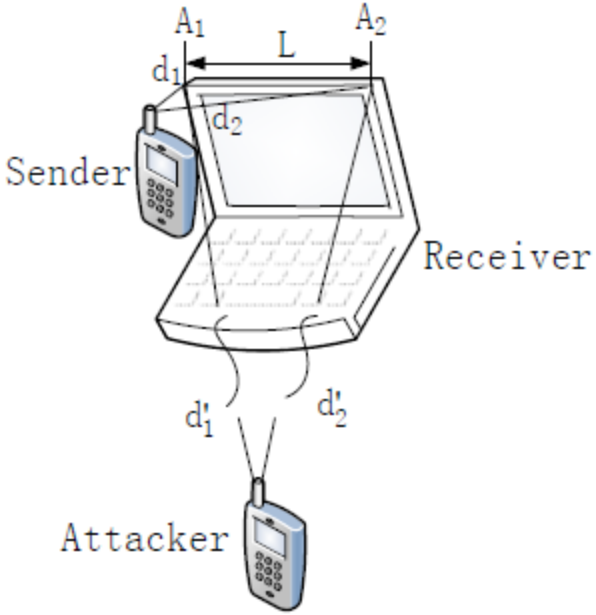
# Biometrics-Based Approaches

- Biometrics are a common technique for identifying human beings
- Feeling-is-Believing (FiB) by Buhan et al.
  - Keys derived from grip pattern biometrics for smart guns
- Secure Ad-hoc Pairing with Biometrics (SAfE) by Buhan et al.
  - Keys derived from face recognition result

- Logic and calculations to accurately recognize the biometric-patterns are a heavy burden on its applications
- Issue regarding the accuracy of recognition techniques still need more research and improvement
- Require biometrics reader in both of the devices

# More Pairing Example

- Good Neighbor: Ad-Hoc Pairing of Nearby Wireless Devices by Multiple Antennas
  - No OOB channel
  - Require multiple antennas
  - utilizing the characteristics of wireless signal that the power of the received signal is inversely proportional to some exponent of the distance between the sender and receiver



# Comparison of OOB Channels

| | Device/Equipment Requirements | | User Actions | | | |
|---|---|---|---|---|---|---|
| **Pairing Method** | **Sending Device** | **Receiving Device** | **Phase I: Setup** | **Phase II: Exchange** | **Phase III: Outcome** | **OOB Channels** |
| Resurrecting Duckling* | Hardware port (e.g., USB) on both and extra cable | | Connect cable to both devices | **NONE** | **NONE** | Cable |
| Talking to Strangers* | IR port on both | | Activate IR on both & find /align IR ports | **NONE** | **NONE** | IR |
| Visual Comparison: Image, Number or Phrase | Display + user-input on both | | **NONE** | Compare two images, or two numbers, or two phrases | Abort or accept on both devices | Visual |
| Seeing is Believing (SiB)* | Display + user-input | Photo camera + user-output | Activate photo mode on receiving device | Align camera on receiving device with displayed barcode on sending device, take picture | Abort or accept on sending device based receiving device decision | Visual |
| Blinking Lights* | LED + user-input | User-output + Light detector or video camera | Activate light detector or set video mode on receiving device | Initiate transmittal of OOB data by sending device | Abort or accept on sending device based receiving device decision | Visual |
| Loud & Clear<br>▪Display-Speaker<br>▪Speaker-Speaker | User-input on both +<br>▪display on one & speaker on other, or<br>▪speaker on both | | **NONE** | Compare: two vocalizations, or display with vocalization | Abort or accept on both devices | ▪Audio, or<br>▪audio + visual |

# Contd.

| | | | | | | |
|---|---|---|---|---|---|---|
| Button-Enabled (BEDA)<br>▪Vibrate-Button*<br>▪LED-Button*<br>▪Beep-Button* | User input +<br>▪vibration , or<br>▪LED, or<br>▪beeper | User output +<br>One button + | Touch or hold both devices | For each signal (display, sound or vibration) by sending device, press a button on receiving device | Abort or accept on sending device based receiving device decision | ▪Tactile, or<br>▪Visual + tactile, or<br>▪Audio + tactile |
| Button-Enabled (BEDA)<br>▪Button-Button* | One button on both + user-output on one | | Touch or hold both devices | Simultaneously press buttons on both devices; wait a short time, repeat, until output signal | **NONE (unless synch. error)** | Tactile |
| Copy–and-Confirm* | Display + user-input | Keypad + user-output | **NONE** | Enter value displayed by sending device into receiving device | Abort or accept on sending device based on receiving device decision | Visual |
| Choose-and-Enter* | User input on both devices | | **NONE** | Select "random" value and enter it into each device | **NONE (unless synch. Error)** | Tactile |
| Audio Pairing*<br>(HAPADEP variant) | Speaker + user-input | Microphone + user-output | **NONE** | Wait for signal from receiving device. | Abort or accept on sending device | Audio |
| Audio/Visual Synch.<br>▪Beep-Beep<br>▪Blink-Blink<br>▪Blink-Beep | User-input on both +<br>▪Beeper on each , or,<br>▪LED on each, or<br>▪Beeper on one & LED on other | | **NONE** | Monitor synchronized:<br>▪beeping, or<br>▪blinking, or<br>▪Beeping & blinking | Abort on both devices if no synchrony | ▪Visual, or<br>▪ Audio, or<br>▪Audio + visual |
| Smart-its-Friends*,<br>Shake-Well-Before-Use* | 2-axis accelerometers on both + user-output on one | | Hold both devices | Shake/twirl devices together, until output signal | **NONE (unless synch. error)** | Tactile + motion |

# Conclusions

- Secure Device Pairing problem has 3 dimensions: security, usability and practicality
- If the user is involved, it should be intuitive, resistant to user errors and not burdensome
  - Taking pictures/videos is one way
  - Listening is another
  - Reading is yet another
  - And there other others like shaking too…
- Exotic hardware assumptions (laser transceiver, etc.) or protocols like Amigo and Distance-Bounding doesn't help to solve the problem in real-life, at least not today.

# Conclusions (cont.)

- Pairing protocols vary in the:
  - Strength of their security
  - The level of required user intervention
  - Their susceptibility to environmental conditions
  - Required physical capabilities of the devices
  - Required proximity between the devices
- Majority of the users are non-technical
- Difficult to remember the different kinds of steps for establishing secure channel in varying situations and scenarios

# Conclusions (cont.)

- We need to:
  - Investigate ways of integrating different pairing protocols within a general architecture for providing secure and usable pairing mechanisms for a large set of ad hoc scenarios
  - Integrate discovery mechanism into pairing schemes

Emerging scenarios are even more challenging

- Group pairing
- Home sensor networks
- Pairing with personal RFID tags