'Usable Security: The Case of Pairing of Wireless Personal Devices'

Cor Wit Lecture - Prof. dr. G. Tsudik

February 23, 2011
Usable & Secure Device Pairing

Gene Tsudik
SPROUT: Security & Privacy Research Outfit
University of California, Irvine
http://sprout.ics.uci.edu

Joint work with:
Ersin Uzun (UCI)
Alfred Kobsa (UCI)
Yang Wang (UCI)
Nitesh Saxena (NYU Polytechnic)


My Current Research

http://sprout.ics.uci.edu
- Privacy-Preserving Techniques
  - PSI, Secret Handshakes, Private DB Querying, etc.
  - Location Privacy in MANETs/VANETs
  - Private WSN Querying
- Security of Personal and Embedded Devices
  - Unattended WSNs
  - Security for Embedded Devices (e.g., Attestation)
  - Distance Bounding
  - Usable Security (wireless device pairing)
- Internet Security
  - Privacy-agile Name Service
  - Phishing and Typo-squatting Countermeasures
  - DTN security
  - Future Internet Architecture (Named Data Networking)
Outline

- What is device pairing (aka “first connect”)?
- Why is it hard?
- Usability vs. security
- Overview of notable methods
- Studying pairing methods
  - Security-centric
  - Usability-centric
- Group device pairing (opt)
- Pairing with passive devices (opt)
- Open issues / future research

Secure pairing of personal devices

- **Pairing**: initial security context setup between un-familiar devices for subsequent wireless communication

- Between, e.g.:
  - Two cell phones
  - A cell phone and a BT headset
  - An MP3 player and a PDA
  - Enrolling a phone or a PDA into a home WLAN
### What kinds of devices?

- Desktops
- Laptops
- PDAs
- Phones
- MP3 Players
- Wireless Headsets
- Navigators
- Cameras
- Appliance (e.g., TV) remote control units
- Wireless Access Points
- FAX-s/Copiers/Printers
- Sensors
- RFID tags (high-end)
- Medical devices, e.g., pacemakers

### What kind of pairing?

- Casual / temporary
- Long-term

### How many devices?

- Two (one or two owners?)
- Many (one or two owners?)

### Input? Output?

#### INPUT

- Keyboard, keypad, touch-screen
- Microphone (audio-in)
- Photo camera
- Video camera
- Vibration detector
- Infrared
- WLAN
- Cellular
- Bluetooth
- Ultrasound
- Accelerometer
- Scanner
- etc., etc.,

#### OUTPUT

- Screen
- LED
- Speaker (audio-out)
- Beeper
- Vibration ability
- Printing
- Infrared
- WLAN
- Cellular
- Bluetooth
- Ultrasound
- Printing
- etc., etc.,
Why is it hard?

Need to set up a security association with:

- Unfamiliar devices
- No global or common security infrastructure, i.e., no PKI or TTPs
- Ordinary non-expert users, from: to:
- Cost-sensitivity

Why isn’t it easy?

- Let’s assume each device has an (uncertified) public key and there is a common wireless channel
- Devices exchange public keys over the wireless channel and confirm successful exchange
  - Could use standard crypto protocols...
  - No user involvement
  - Low cost
Security Threats (1)

Man in the middle (MitM) attack

Security Threats (2)

"Evil Twin" attack

So, user involvement is not an option
So, why don’t we just:

- Let Homer pick and enter a password (or PIN) into each device, and

Alternatively:

- Unauthenticated Key Exchange

Each device communicates to Homer some short function of the exchange (or new key), e.g., via display. Homer accepts in case of a match; rejects otherwise.
Not just security at stake

- Usability is very important!
- Personal wireless devices are everywhere
- Everyone has them and everyone needs security
- Wide range of users; most are not tech-savvy

Usability in current mechanisms?

SSID? WPA? Passcode!
Which E61?

How would your grandmother or daft uncle fare?
... and (in)security of some

Challenge: Security vs. Usability

- Trivial techniques are unusable and/or insecure
- Tradeoff between security and usability is unavoidable
- Security and usability can coexist via careful design and usability assessment
Naïve usability is harmful to security

Naïve security is harmful to usability

Bluetooth pairing was designed with moderate security in mind

- Bluetooth pairing was designed with moderate security in mind
- Car kit allows a car phone to retrieve and use session keys from a simcard of the cellphone
- Car kit requires higher level of security
  - User must enter a 16-character passcode within 30 seconds
  - More secure = Harder to use?

• Bluetooth pairing was designed with moderate security in mind
• Car kit allows a car phone to retrieve and use session keys from a simcard of the cellphone
• Car kit requires higher level of security
  • User must enter a 16-character passcode within 30 seconds
  • More secure = Harder to use?
Ultimate Goal (a dream)

• Secure, burden- & error-free, intuitive, and inexpensive universal pairing method

• Two initial problems:
  • Discovery: how to find/identify the other device?
  • Secure Channel Establishment (via authenticated key agreement): how to set up key(s) for subsequent communication?

One Sensible Approach

• Assumption: Peer devices are physically identifiable by their human user/owner

• Basic approach:
  • Use a human-imperceptible (e.g., wireless) unauthenticated channel to transfer device-specific cryptographic material (e.g., public keys) and other protocol messages/data
  • Use a human-perceivable (out-of-band =OOB ) channel to transport a small amount of authenticated information (e.g. checksum of the public keys)
A typical protocol (one of many)

Choose long random \( R_A \)

\[ h_A = h(A, R_A) \]

\[ v_A \leftarrow H(A, B, PK_A|PK'_B, R_A, R'_B) \]

User accepts if \( v_A \) and \( v_B \) match

\( h() \) is a hiding commitment; e.g., SHA-256

\( H() \) is a mixing function; e.g., SHA-256, truncated to 4-6 digits

Some notable proposals

- Cables:
  - "Resurrecting Duckling", [Stanajo, et al. IWSP '99]
- IrDA, cameras and barcodes/LEDs
  - 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]
- Speakers, Microphones
  - Loud and Clear, [Goodrich, et al. ICDCS '06]
  - HAPADEP, [Soriente, et al. ISC' 08]
- Displays, keyboards, whiteboards
  - Hash Visualization, [Perrig et. al. CRYPTEC' 99]
  - Colorful Flags, [Ellison et al. TISSEC' 03]
  - Bluetooth 2.1, Windows Connect Now, WUSB standards
- Other (uncommon) hardware
  - Accelerometers → "Shake well before use", [Mayrhofer, et al. Pervasive' 07]
  - Ultrasound, laser transceivers and many others....
Resurrecting Duckling

- F. Stajano and R. Anderson, IWSP ’99

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

Caveats:
  - homogeneous physical interfaces
  - awkward cables

Talking to Strangers

- [Balfanz, et al., NDSS ’02]

Infrared (IR) as a “Location-Limited Side Channel”
  - Assumed to be immune to MitM attack
  - Many (yesterday’s) devices equipped with IR
  - Pre-authentication over IR: exchange commitments, e.g., to respective public keys

Problems:
  - Finding and turning on IR ports
  - IR is invisible to humans, MitM is still possible
Key Agreement in Wireless Networks


- Uses Diffie-Hellman to establish keys
- Three techniques to combat MitM:
  - Visual comparison of short strings
    - Requires displays
  - Distance bounding
    - Hard to implement (need ultra-wideband radio)
    - Poor usability, i.e., users are lousy at correctly judging distances with required accuracy.
  - Integrity codes on radio signals
    - Hard to implement & make it work, e.g., radio interference, noise, incompatibility with current wireless technologies,

Ad Hoc Group Device Pairing


- Group of devices need to establish a secure common channel (e.g., conference)
  - Group leader identified
  - Chooses fresh password/PIN and shared among devices, e.g., written it on a blackboard and entered (by each user) into devices
  - Password used to derive a strong shared session key using group DH
- Bluetooth 2.0 and earlier used a similar user interaction but a different cryptographic protocol.
- Problems:
  - Devices must have a keyboard/keypad
  - Humans are not good random number/string generators
Seeing-is-Believing (SiB)


- Demonstrative identification of devices using cameras and 2-D barcodes
  - One device shows a 2-D barcode encoding the hash of its public key; the other snaps a photo, parses & decodes the hash
  - Repeat in the opposite direction
  - Public keys exchanged over the wireless channel and checked against barcode-extracted hashes

Basic SiB Protocol

keys and data

photo

Visual channel
Caveats

- Not all devices have big enough displays to show two-dimensional bar codes
- Not all devices have good-enough cameras
- Placing devices sufficiently near and aligning the camera may not always be possible

Visual Auth-n w/Integrity Checking


  Basic idea:
  - Device A blinks
  - Device B takes a video clip of the blinking pattern
  - B parses clip to extract authentication string and decides to continue/abort.
  - User conveys B’s decision to A

  Relaxes display requirements of SiB but needs video camera on one device
Loud & Clear & HAPADEP

  • Exchange PKs over the wireless channel
  • Create a grammatically correct (MADLIB) sentence from hash of exchanged keys
  • User confirms displayed/spoken sentences match

• “HAPADEP: Human-Assisted Pure Audio Device Pairing”, [Soriente, et al. ISC’08]
  • Each device encodes its public key into audio and plays it while the other records
  • User verifies that sound is coming from intended devices
  • Optional second verification (similar to L&C) for better assurance
  • Requires microphones but solves the device discovery problem

Other comparison based methods

• Using Display
  • Hash Visualization [Perrig, et. al. CRYPTEC’99]
  • Colorful Flags [Ellison, et. al. TISSEC’03]
  • Numeric Compare [Bluetooth 2.1 & WUSB]

• Using LED
  • Blink-Blink [Saxena, et. al. ACNS’08]
  • Simple defense against evil twin APs [Roth, et. al. WISEC’08]

• Using beeper
  • Beep-Beep [Saxena, et. al. ACNS’08]

• Using beeper+LED
  • Beep-Blink [Saxena, et. al. ACNS’08]
Other methods

• Button-Enables Device Association (BEDA) protocol suite for interface-constrained devices
  • LED-Button
  • Vibrate-Button
  • Beep-Button
  • Button-Button
• BTW: BEDA emulates the “ideal” pairing method:
• Some new standards
  • Windows connect now: user transfers a number or a USB stick
  • HomePlugAV: user transfers a number

More exotic methods

• Accelerometers:
  • “Shake well before use”, [Mayrhofer, et al. Pervasive’07]
  • “Smart-its-friends”, [Holmquist, et al., UbiComp’01]
• Ultrasound
  • [Kindberg, et al. ISC’03]
• Laser
  • [Mayrhofer, et al. ARES’07]
• NFC
  • OOB mode of Bluetooth 2.1
Methods with different security assumptions

- Mainly based on proximity, distance-bounding or location-limited channels
  - No user-aided authentication of exchanged data
  - But, assures that MitM not launched from far away

- Some examples;
  - Distance bounding protocols
    - Compute communication distance from transmission time. Practical accuracy is about 1’ (one foot) with UWB radio technology.
  - Amigo [Varshavsky, et al. Ubicomp’07]
    - Compares environmental radio noise sensed by devices to verify their respective proximity within a couple of meters.

So what?

- Many methods using various OOB channels: audio, visual, tactile, etc.
- All designed by well-meaning geeks 😊
- Typically:
  - Security/crypto people don’t understand USABILITY
  - HCI/usability people don’t understand SECURITY
  - Industry/standards folks often understand NEITHER

- What’s the winning recipe?
  - Team up with HCI experts
  - Ask real-world users!
Security-Centric Usability Study of notable pairing methods

• “Caveat Emptor: A Comparative Study of Secure Device Pairing Methods” [Kumar, et. al. PerCom’09]
  • Compares / evaluates 13 notable pairing methods
  • 20 young & geeky participants (enough to start!)
  • Observations and post-test questionnaires
  • Measures:
    • Fatal (security critical) error rate
    • Safe (non-critical) error rates
    • Completion time
    • Ease-of-use rating
    • Personal preference

Caveat Emptor: Summary of methods

<table>
<thead>
<tr>
<th>Pairing Method</th>
<th>Device/Equipment Requirements</th>
<th>User Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending Device</td>
<td>Receiving Device</td>
<td>Phase I: Setup</td>
</tr>
<tr>
<td>Visual Comparison, Image, Number or Phrase</td>
<td>Display + user-input on both</td>
<td>NONE</td>
</tr>
<tr>
<td>Seeing &amp; Believing (SB)</td>
<td>Display + user-input</td>
<td>Photo camera + user-output</td>
</tr>
<tr>
<td>Blinking Lights</td>
<td>LED + user-input</td>
<td>User-output + Light detector or video camera</td>
</tr>
<tr>
<td>Loud &amp; Clear Display-Speaker, Speaker-Speaker</td>
<td>User-input on both + display on one &amp; speaker on other, or keypad on both</td>
<td>NONE</td>
</tr>
<tr>
<td>Button-Enabled (BEDA) Vibrate-Button</td>
<td>User input + vibration</td>
<td>LED</td>
</tr>
<tr>
<td>Button-Enabled (BEDA) LED-Button</td>
<td>User input + LED</td>
<td>User output + One button</td>
</tr>
<tr>
<td>Audio Pairing (HAPADEP)</td>
<td>Speaker + user-input</td>
<td>Microphone + user-output</td>
</tr>
<tr>
<td>Audio/Visual Synch. Enable-Disable, Audio-Visual</td>
<td>User-input on both + KLED on each device or on one &amp; KLED on other</td>
<td>NONE</td>
</tr>
</tbody>
</table>
## Error rates

<table>
<thead>
<tr>
<th>Method name</th>
<th>Specific test case</th>
<th>Avg. completion time (seconds)</th>
<th>Avg. fatal error rate</th>
<th>Avg. safe error rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Comparison</td>
<td>Matching Images</td>
<td>12.7 (sd=4.0)</td>
<td>N/A</td>
<td>15%</td>
</tr>
<tr>
<td>Number Comparison</td>
<td>First Digit Mismatch</td>
<td>4.5 (sd=1.6)</td>
<td>10%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Middle Digit Mismatch</td>
<td>7.1 (sd=5.2)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Phrase Comparison</td>
<td>Matching Phrases</td>
<td>12.7 (sd=4.0)</td>
<td>N/A</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>2-Word Mismatch</td>
<td>6.7 (sd=3.4)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Middle Word Mismatch</td>
<td>7.2 (sd=4.4)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Loud &amp; Clear (Display/Speaker)</td>
<td>First Word Mismatch</td>
<td>11.7 (sd=3.7)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Loud &amp; Clear (Speaker/Speaker)</td>
<td>2-Word Mismatch</td>
<td>18.5 (sd=4.8)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>First Word Mismatch</td>
<td>18.6 (sd=4.2)</td>
<td>10%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Last Word Mismatch</td>
<td>20.0 (sd=8.3)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Seeing Is Believing</td>
<td>Accepting Receiving Device</td>
<td>26.9 (sd=7.5)</td>
<td>N/A</td>
<td>5%</td>
</tr>
<tr>
<td>Audio/Visual (Beep/Blink)</td>
<td>Matching Patterns</td>
<td>26.3 (sd=5.3)</td>
<td>N/A</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>First Bit Mismatch</td>
<td>28.9 (sd=4.0)</td>
<td>20%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Middle Bit Mismatch</td>
<td>27.6 (sd=3.5)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>Audio/Visual (Blink/Blink)</td>
<td>4-Bit Mismatch</td>
<td>24.9 (sd=5.1)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>First Bit Mismatch</td>
<td>25.0 (sd=5.1)</td>
<td>30%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Synchrony Bit Mismatch</td>
<td>25.5 (sd=8.0)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Middle Bit Mismatch</td>
<td>24.8 (sd=5.3)</td>
<td>5%</td>
<td>N/A</td>
</tr>
<tr>
<td>HAPADEP Variant</td>
<td>Accepting Receiving Device</td>
<td>10.8 (sd=2.8)</td>
<td>N/A</td>
<td>5%</td>
</tr>
</tbody>
</table>

*Estimated Standard Deviation from sample

## Method completion times

![Method completion times chart](chart.png)

TU Delft
Method ease-of-use ratings

Take-away

• Best overall choices:
  • When both devices have a display
    • Number Comparison
  • When at least one device has no display but has an audio interface
    • HAPADEP (if microphone is available on one, and speaker on the other)
    • L&C Display-Speaker (if one has a display and the other has a speaker.
  • For interface-constrained devices
    • BEDA Vibrate-Button, if possible
    • BEDA LED-Button otherwise
Impact of research results

- New industry standards improve both usability and security.
- But they fail to:
  - Provide security when devices don’t have displays/keyboards or USB/NFC interfaces, e.g., Bluetooth headsets, wireless access points, cameras, media players, etc.
  - Systematically consider appropriate user interface design choices, thus opening the door for usability and security problems.
- More tools are becoming available from the open-source community to test or integrate different pairing solutions. E.g.,
  - Usability testing framework [Kostiainen, et. al.]
  - Ubiquitous Authentication Toolkit [Mayrhofer, et. al.]

Usability-Centric Study of notable pairing methods


- Motivation:
  - Many pairing methods
  - Insufficient evaluation
    - Usability Analysis of Secure Pairing Methods [Uzun et al. USEC’07]
    - Caveat Emptor: A Comparative Study of Secure Device Pairing Methods [Kumar, et al. PerCom’09]

- Methodology
  - Experimental study with a mix of real users to compare and evaluate the usability of various methods.
Criteria for selecting methods

- Excluded methods that:
  - require uncommon or inconvenient hardware (e.g., laser transceiver, cable)
  - shown to have poor usability/security (e.g., choose-and-enter a pin number)
  - don’t provide explicit demonstrative authentication (e.g., distance bounding protocols)

Tested methods (1/4)

- Number Comparison (PIN-Compare)
  “65473” =? “65473”

- Sentence Comparison (Sentence-Compare)
  “Alice eats jackets” =? “Alice eats jackets”

- Image Comparison (Image-Compare)
  =?
Tested methods (2/4)

- Button enabled (BEDA) methods
  - LED-Press
  - Vibrate-Press
  - Beep-Press

Tested methods (3/4)

- Loud and Clear (L&C) variants
  - Listen-Listen
  - Listen-Look
Tested Methods (4/4)

- Seeing is Believing (See-Believe)
- Visual Integrity Code (Video)
- HAPADEP Audio Pairing (Over-Audio)

Implementation

- Common software platform and GUI design principles
- Same level of security for all methods
- Ubiquitous test devices (cell phones)
Test design (1/2)

- Subjects
  - 22 subjects balanced by age group and gender
  - Mainly UC Irvine students and staff
- Procedures
  - Background questionnaire
  - Scenario Presentation
  - Experiment with pairing methods (sequence of methods in Latin Square design)
  - Subjective Perceptions by System Usability Scale (SUS) questionnaire
  - Observable usability indicators by automatic logging
  - Qualitative evaluation via post-test questionnaire and interviews

Test design (2/2)

- Within-subjects usability measures:
  - Task performance time
  - SUS score
  - Perceived security
  - Task completion (a categorical variable)
- Between-subjects factors:
  - Age group
  - Gender
  - Prior experience with device pairing
RESULTS: EFFECT OF METHOD

- Task performance time
  - PIN-Compare < Image-Compare < Listen-Look < See-Believe < Video
  - PIN-Compare < Sentence-Compare < Over-Audio < Listen-Listen
  - Listen-Look < Listen-Listen < LED-Press
  - Video < LED-Press < Beep-Press

- SUS Score
  - PIN-Compare > Sentence-Compare > Over-Audio
  - Sentence-Compare > Image-Compare > See-Believe
  - Over-Audio > Listen-Look > Listen-Listen
  - Listen-Look > LED-Press, Vibrate-Press
  - See-Believe > Video > Beep-Press

- Perceived Security: G1 > G2 > G3
  - G1 = PIN-Compare
  - G2 = (Sentence-Compare, Over-Audio, Listen-Look)
  - G3 = (See-Believe, LED-Press, Vibrate-Press, Beep-Press, Listen-Listen, Video)

NOTE: “>” or “<” denotes %5, and “<” or “>” denotes %1 level of statistical significance

RESULTS: EFFECT OF METHOD (OVERVIEW)
Results: effect of age

- Task performance time
  - 18-25: front plane
  - 41+: middle plane
  - 26-40: rear plane

- Task completion rate
  - 18-25 > 41+

- Perceived security
  - 26-40 > 41+

Results: effect of gender

- On task performance time
- Perceived Security
  - Males > Females

- Assigned SUS Scores
  - Males > Females
Results: cluster analysis based on principal components

Summary

- Ease-of-use is by far the most important reason in favoring a method.
- Guidelines for choosing the best pairing method:
  - Both devices have a display
    - Use PIN-Compare (stands out as the most usable method)
    - Sentence-Compare and Image-Compare are the next choices in the order of preference
  - One has a display and the other only audio output
    - Listen-Look is the best choice
  - One has audio output (i.e., speaker) and the other has audio input (i.e., microphone)
    - Over-Audio is the recommended method.
Open issues & future directions

- Mass pairing, e.g., one master & many slave devices (e.g., WSN deployment)
- Pairing groups of devices, e.g., for an ad hoc conference or a long-term association
- Pairing involving passive devices, e.g., RFID tags, e.g., a cell phone with an e-passport

- Secure device pairing is one of the few topics involving: cryptography, security and usability (HCI)
  - Offers many opportunities for collaboration among experts in these fields

Conclusions

- Secure Device Pairing has THREE equally important dimensions:
  - security, usability and practicality

- If a human user is involved, the pairing process must be: fast, simple, intuitive, attack- and error-resistant
- Many methods have been proposed
- Most are either impractical or unusable
  - Simplicity is very important
  - Usability can only be assessed via thorough experiments/studies
QUESTIONS?