

Carnegie Mellon  
**CyLab**  
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab  
 4800 UNIVERSITY STREET  
 PITTSBURGH, PA 15260  
 PH: 412.246.7100  
 FX: 412.246.7100  
 WWW.CYLAB.CMU.EDU

---

Low-cost Manufacturing, Usability, and Security:  
 An Analysis of Bluetooth Simple Pairing and  
 Wi-Fi Protected Setup

Cynthia Kuo    Carnegie Mellon University  
 Jesse Walker    Intel Corporation  
 Adrian Perrig    Carnegie Mellon University

CyLab www.cylab.cmu.edu Carnegie Mellon

## Device Introduction


- Goal: Establish authentication credentials between two devices that have not yet done so
- Terminology
  - Introduction = setup = pairing

2

CyLab www.cylab.cmu.edu Carnegie Mellon


## Device Introduction

**Bluetooth**



Pair two devices in a master/slave relationship

**Wi-Fi**



Enroll one device into an existing network, assuming initial network setup completed

3

CyLab www.cylab.cmu.edu Carnegie Mellon

## Overview

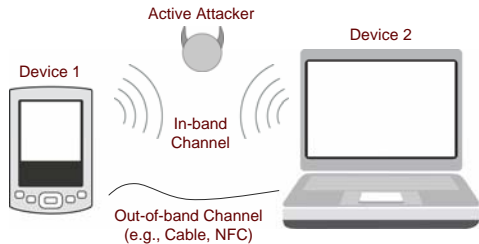
- Define secure and usable device introduction
- Summarize setup methods in Bluetooth Simple Pairing and Wi-Fi Protected Setup
- Discuss potential causes of poor security and usability
- Recommend improvements

4

CyLab www.cylab.cmu.edu Carnegie Mellon

## Secure Introduction Criteria

1. Conforms to standard model



5

CyLab www.cylab.cmu.edu Carnegie Mellon

## Secure Introduction Criteria

1. Conforms to standard model
  - Accepted by cryptographers
2. Provides high level of security
  - No more than  $2^{-30}$  probability of success
    - $2^{80}$  cryptographic operations required through 2010
    - Assume attackers can perform  $2^{50}$  operations
3. Preserves simplicity
  - Easier to find and correct vulnerabilities in simpler systems

6

CyLab Carnegie Mellon

## Usable Introduction Criteria

1. Verifies in-band connection between devices
2. Handles errors
  - User experience interoperability → better application design and better support
3. Maintains a consistent user experience across devices
  - Learning

7

CyLab Carnegie Mellon

## Overview

- Define secure and usable device introduction
- Summarize setup methods in Bluetooth Simple Pairing and Wi-Fi Protected Setup
- Discuss potential causes of poor security and usability
- Recommend improvements

8

CyLab Carnegie Mellon

## Setup Methods

	Bluetooth	Wi-Fi
<b>Copy</b>	Passkey Entry	PIN
<b>Compare</b>	Numeric Comparison	-
<b>Auto</b>	Just Works	Push Button Configuration
<b>Out-of-band</b>	Out-of-band	Out-of-band

9

CyLab Carnegie Mellon

## Evaluating Each Setup Model

- **Secure**
  1. Standard model
  2. Security
  3. Simplicity
- **Usable**
  1. Connection verification
  2. Error handling
  3. Consistent UX

Out-of-band channel  
Probability of attack success  
[Overall]

Connection verification  
Error handling  
[Overall]

10

CyLab Carnegie Mellon

## “Copy” Setup Methods

Out-of-band channel	Visual & Human
Probability of attack success	$> 2^{-20}$ (6) / $> 2^{-7}$ (4*); $> 2^{-14}$ (8*)
Connection verification	? (Implementation issue)
Error handling	Start over / ?

\*WPS

11

CyLab Carnegie Mellon

## “Compare” Setup Method

- Bluetooth only

Out-of-band channel	Visual & Human
Probability of attack success	$> 2^{-20}$
Connection verification	?
Error handling	Start over

12

CyLab Carnegie Mellon

## "Auto" Setup Methods

Out-of-band channel	None
Probability of attack success	Very likely ☹
Connection verification	?
Error handling	Start over / ?

13

CyLab Carnegie Mellon

## Out-of-Band Setup Method

Out-of-band channel	Out-of-band channel
Probability of attack success	Depends on channel
Connection verification	?
Error handling	Start over / ?

14

CyLab Carnegie Mellon

## Overview

- Define secure and usable device introduction
- Summarize setup methods in Bluetooth Simple Pairing and Wi-Fi Protected Setup
- Discuss causes of poor security and usability
- Recommend improvements

15

CyLab Carnegie Mellon

## Evaluating Each Setup Model

- **Secure**

1. Standard model	Out-of-band channel
2. Security	Probability of attack success
3. Simplicity	[Overall]
- **Usable**

1. Connection verification	Connection verification
2. Error handling	Error handling
3. Consistent UX	[Overall]

16

CyLab Carnegie Mellon

## Preserving Simplicity

- Complex systems harder to fully analyze for vulnerabilities
- Each setup mode has its own issues
- Multiple setup modes per device leads to many possible setup combinations

17

CyLab Carnegie Mellon

## Combinations of Setup Methods

<b>Bluetooth</b>	<b>Wi-Fi</b>
<b>4</b> Pairing models	<b>3</b> Pairing models
<b>15</b> Possible combinations per device	<b>7</b> Possible combinations per device
<b>120</b> Possible combinations between any two devices	<b>28</b> Possible combinations between any two devices

18

CyLab Carnegie Mellon

## Interactive Complexity

- Difficult to consider all the potential system states during design, implementation, and evaluation
- Difficult to handle so many different possible situations (especially a rare situation or error)

19

CyLab Carnegie Mellon

## Reducing Complexity


- Reduce number of combinations by prioritizing setup models
- Reduce number of setup models

20

CyLab Carnegie Mellon

## Auto Setup Methods

Bluetooth Just Works and Wi-Fi Push Button Configuration supported for low-cost manufacturing



Devices with no screens

- Works if
  - No other devices in setup mode in wireless range
  - No errors
- Never secure against malicious device within range
  - Active attacker must be physically present

21

CyLab Carnegie Mellon

## Combinations of Setup Methods

<b>Bluetooth</b>	<b>Wi-Fi</b>
<b>3</b> Pairing models	<b>2</b> Pairing models
<b>7</b> Possible combinations per device	<b>3</b> Possible combinations per device
<b>28</b> Possible combinations between any two devices	<b>6</b> Possible combinations between any two devices

22

CyLab Carnegie Mellon

## Evaluating Each Setup Model

- Secure
 

1. Standard model	Out-of-band channel
2. Security	Probability of attack success
3. Simplicity	[Overall]
- Usable
 

1. Connection verification	Connection verification
2. Error handling	Error handling
3. Consistent UX	[Overall]

23

CyLab Carnegie Mellon

## Issues in UX Consistency

Absent from specifications:

<ul style="list-style-type: none"> <li>• Prioritization of setup methods</li> <li>• Connection verification</li> <li>• Error handling               <ul style="list-style-type: none"> <li>– Recovery</li> <li>– Messages</li> <li>– Technical support</li> <li>– Documentation</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Wording</li> <li>• User interaction flow</li> <li>• Setup initiation               <ul style="list-style-type: none"> <li>– Device or user?</li> </ul> </li> <li>• Entering and exiting setup mode</li> <li>• Basic checks               <ul style="list-style-type: none"> <li>– Wireless enabled?</li> </ul> </li> <li>• Timeout values for PINs</li> </ul>
--	--

24

CyLab Carnegie Mellon

## Importance of Consistency

- Fewer setup methods improves consistency
  - Rewards learning
  - Raises quality of error handling, documentation, and technical support
    - Cross-vendor, cross-product
  - Reduces confusion about level of security assurance
  - Minimizes implementation work

25

CyLab Carnegie Mellon

## Overview

- Define secure and usable device introduction
- Summarize setup methods in Bluetooth Simple Pairing and Wi-Fi Protected Setup
- Discuss causes of poor security and usability
- Recommend improvements

26

CyLab Carnegie Mellon

## In-band Setup

- Copy:** Bluetooth Passkey Entry or Wi-Fi PIN
- Static Copy:** PIN entry using a PIN on a sticker
- Compare:** Bluetooth Numeric Comparison
- Auto:** Bluetooth Just Works or Wi-Fi Push Button Configuration

	Copy or Compare	Copy or Compare	Copy or Compare	Copy	Static Copy	Static Copy
		Compare	Compare	Copy	Auto	Auto
			Auto	Copy	Auto	Auto
				Static Copy	Static Copy	Static Copy
					Auto	Auto
						Auto

27

CyLab Carnegie Mellon

## P(Attack Success): In-band

- $2^{14} - 2^{27}$
- First time only ( $2^{20} - 2^{27}$ )
- No real security (no out-of-band channel)

Out-of-band capability (visual & human)

28

CyLab Carnegie Mellon

## P(Attack Success): Out-of-band

- Only mode capable of attack success probability  $\sim 2^{-30}$ 
  - Assumes that selected out-of-band method is a good one
  - Assumes same setup mode can be used for all devices

29

CyLab Carnegie Mellon

## Recommendations

- Common denominator of hardware features
  - At least 2 buttons
  - Out-of-band capability

30

CyLab Carnegie Mellon

## Usability: Feedback Capability

- Good
- Passable
- None

- Screens used to confirm setup or display error messages
- Applies to in-band and out-of-band

31

CyLab Carnegie Mellon

## Example: LED / One Button

MULTIPLE USES OF A LONG PRESS ON THE CALL CONTROL BUTTON

HEADSET FUNCTION	STATE OF THE BLUETOOTH DEVICE	RESULT
Turn on power	Power off	Turns the power on
Re-link to Bluetooth device	Power on Link dropped	Re-links the device
Reject call	Power on Linked Incoming call	Disconnects the call or sends the call to voice mail depending on your device
Transfer a call between Headset and Bluetooth device	Power on Linked On a call	Transfers the call from one device to another
Voice activated dialing	Power on Linked No call	Activates the voice recognition feature

Plantronics Discovery 640 Bluetooth Headset User Guide

32

CyLab Carnegie Mellon

## Recommendations

- Common denominator of hardware features
  - At least 2 buttons
  - Out-of-band capability
  - Screen on at least one device (both preferable)
- Common user experience
  - Common menu options, wording, user interaction flow, error logging
  - Promotes
    - Consistency across devices and protocols
    - Interoperability of user interfaces
    - Error handling and recovery

33

CyLab Carnegie Mellon

## Selected Related Work

- Usability evaluation of different pairing schemes (Uzun et al.)
- Setup in HomePlug (Newman et al.)
- Interactive complexity (Leveson)
- Importance of consistency (Endsley et al.)
- Schemes for exchanging authentication credentials using demonstrative identification
  - Resurrecting Duckling (Stajano et al.)
  - Talking to Strangers (Balfanz et al.)
  - Seeing-Is-Believing (McCune et al.)

34

CyLab Carnegie Mellon

## Conclusion

- Networking relies on interoperability
- For security applications, UI should not be product differentiator
- Standardization of certain UX aspects can benefit technology in the same way as protocol standardization

35

CyLab Carnegie Mellon

Thank you!

Questions? Comments?

[cykuo@cmu.edu](mailto:cykuo@cmu.edu)

36