Multi-Model Security Associations
in Personal Networks

Jani Suomalainen

Research Seminar on Authentication and Key Establishment
Helsinki University of Technology
27th October 2006
Introduction

- “The first generation’s” mechanisms for the first connection between personal devices have thought some security lessons
- Current standardization efforts for personal networks address these vulnerabilities as well as provide easiness and alternatives for association
- This presentation presents four new standards, all supporting multiple association models, and discusses how to attack against them
Association Models

Out-of-band

In-band

Static ID
Temp ID

Static ID
Temp ID

Static ID
Temp ID
Bluetooth Simple Pairing

- Public key crypto (Diffie-Hellman) for correcting vulnerabilities of current (symmetric) pairing

1. Numeric comparison model
   - 6 digit temporary value displayed by both devices

2. Passkey entry model
   - E.g. for keyboards

3. ‘Just works’ model
   - No MitM protection

4. Out-of-band model
   - Enables e.g. use of Near Field Communication
   - Two directional channels change public keys
   - One directional channels change secret
Wi-Fi Protected Setup

- Easy-to-use mechanisms for configuring WLANs
- Microsoft’s implementation Windows Connect Now

1. USB flash drive model
   - Network encryption key is copied to USB stick and copied to every new device

2. Network model
   - E.g. 4 or 8 digit values, which the user must compare
   - A value may be either temporary (displayed) or static (printed to a label)
   - Diffie-Hellman prevents passive eavesdropping
WUSB Association Models

- High-speed wireless standard on top of ultra-wideband channel
  1. Cable model
    - Implicit association (in addition to plugging the wired USB cable, no other user actions are needed)
  2. Numeric model
    - Both host and device display temporary number
    - Temporary values to be compared are at least 2 digits long
    - Diffie-Hellman prevents passive eavesdropping
HomePlugAV Protection Modes

1. Simple connect mode
   - The user sets a control device into a state where it is waiting for association requests
   - The user connects a new device to powerline network -> device sends a nonce, which is a hashed to get AES key
   - Eavesdropping hard due to bad signal-to-noise ratio
   - MitM can be detected

2. Secure mode
   - Users must type 12 alphanumeric passwords

3. Optional modes for out-of-band NEK distribution
Standards for association can be evaluated from the following points of view, each affecting others:

- Exploring Security
- Extensibility
- Threats/trust assumptions
- Usability
- Hardware requirements
Examples of Unaddressed Threats

- Portable memory devices (e.g. USB flash drives) must be physically secure (cryptography cannot provide integrity or confidentiality protection)
- WPS USB model does not support authentication of individual devices (since same copy of NEK is delivered to every device)
  - Insider threats cannot be addressed
- New HomePlugAV devices may be associated with attacker's control device (users reassociate when devices do not work as expected)
  - A threat that attacker’s control device e.g. installs Trojans to new devices is not addressed
Ignoring Security

- To ease comparison / typing, short-checksums / passwords (from 2 to 8 digit) have been adopted to BT, WUSB and WPS numeric comparison models
  - MitM guessing attacks have 1 in 100 to 1 in 1000 000 changes to succeed
- How to assure that the user really compares two displayed numbers?
- Models where user is forced to type identifiers are alternatives in BT and HomePlugAV
Users’ Mistakes

Are users required too much? How can users’ mistakes enable intrusions?

E.g. in HomePlugAV Simple Connect:

1. If a control device is set to wait for associations but a new device is not powered up, an attacker may associate with the control device.

2. If a control device is set to wait for associations only after a new device has been powered, the new device may have been associated with a MitM attacker which then associates with the control device.
An Attack Fooling Users: MitM between Numeric Comparison and ’Just Works’ Models

- In BT ’just works’ model compared value is not displayed
- MitM between **BT** numeric comparison and **BT** ’just works’ models or between **WUSB** numeric and **BT** ’just works’ models
- Control devices should anyhow display values?
Jamming a More Secure Model to Get the User to Switch into a Less Secure Model

- Jamming BT comparison model to get the user to switch into 'just works' model or HomePlugAV secure mode to get the user to switch into simple connect
- Simple ‘IDS’ as a protection?: warning if weak association succeeds after recent unsuccessful secure associations
Requesting Explicit Association while the User Makes Implicit WUSB Association

- In implicit association (e.g. plugging USB cable) there are no explicit user dialogs
- However, BT or WUSB access request may not be suspicious
- Requires attackers to know when a cable is plugged
- Preventing explicit requests when implicit association is made?

Diagram:

- New device
- Control Device
- Attacker

Associations:
- Associate (cable_model)
- Associate (num_mod, rand_number)

Display:
- 123456
- Accept?
Conclusions

- New emerging standards utilize different association models to provide:
  - better usability
  - alternatives for manufacturers and users
  - better security by correcting found vulnerabilities

- However, additional complexity and new technology may introduce new vulnerabilities
  - Few new vulnerabilities enabling users to be fooled to associate attack devices were presented
The End

- Thank you!

- Comments? Discussion?