Multi-Model Security Associations in Personal Networks

Jani Suomalainen
Jani.Suomalainen@iki.fi

October 18, 2006

Abstract

The first connect between unknown devices is one of the most security critical phases of the communication in personal networks Many existing security configuration mechanisms have been vulnerable against passive eavesdropping or active man-in-the-middle attacks or have been ignored by users as too cumbersome. Consequently, attackers have been able to gain access to users' network and devices. To address these problems, different association models, aiming to be both easy-to-use and secure, have been proposed and, in recent standardization work, adopted. This paper provides comparative survey on association models in current specification efforts. Particularly, the paper will evaluate Bluetooth Simple Connect, Wi-Fi Protected Setup, HomePlugAV protection modes and Wireless USB association models. Evaluation criteria includes adopted threat models, hardware assumptions, usability and extendibility. The paper presents some new attack scenarios, where attackers take advantage of devices' support for multiple association models and fool users to associate attack devices. Further, the paper discusses how implementations can address these threats.

Keywords: Personal networks, secure association, comparative evaluation, attacks

1 Introduction

Short-range broadband communication standards have brought large amount of new services to the reach of common users. For instance, standards for personal networks such as Bluetooth, Wi-Fi, Wireless USB and HomePlugAV enable users to easily introduce, access and control services and devices both in home and mobile environments. However, in the side of new opportunities also new security threats have emerged enabling malicious users and devices to gain access to resources and sensitive information in users' devices and networks.

A particular problem is how to control that new devices, e.g. appliances and terminals which the user wants to use with other devices, can be treated as trusted and that connection requests from attackers' and neighbors' devices blocked. This is challenging since new devices can be introduced dynamically at any time and since typical users should not be demanded to perform complex configuration operations. Also, in personal networks there are no trusted third parties, which would know the old and new devices and which would be able to introduce devices to each others. To address the problem, different association (also called as pairing,

bonding, bootstrapping) models, where the user introduces devices to each others, have been developed. For instance, association in personal wireless LANs, particularly between WEP, WPA and WPA2 secured devices, has been based on shared password, which the user must type to wireless devices as well as to access points. Another example is Bluetooth pairing where users are required to enter a short PIN to associate two devices. However, these mechanisms have been problmatic. Long, at most 64 hexadecimal characters, WLAN pre-shared keys are cumbersome for end-users whereas short keys are vulnerable to attacks. Bluetooth has been vulnerable to passive eavesdropping attacks, since secrecy has been based on weak symmetric cryptographic algorithm and typically short PINs, as well as man-in-the-middle (MitM) attacks, when attackers are assumed to be able to intercept and tamper communication in wireless channel.

To address these usability and security worries, various new association models have been developed. For instance, schemes utilizing short passwords and out-of-band channels, such as short-range wireless and wired media as well as cameras and portable memories, have been proposed. Security of these individual association models has been studied quite much. However, when several models are supported in standards simultaneously, new kinds of threats and attacks may emerge. Support for multiple models makes the systems more complex, which means that end-users must to learn several mechanism in order to understand all potential security incidents. Further, since some models may be weaker than others, attackers may, for instance, prevent use of stronger association models in order to force users to associate through vulnerable models. Also, in some cases, it may be possible that a MitM attacker changes an association model or that at the same time as authorized association is made also an unauthorized association is made, without the end-user noticing.

This paper explores security of association models in different standards from the practical point of view. Section 2 will provide an overview of different association models. Section 3 surveys how and which association models are used in standards for personal networks. Section 4 presents a framework for evaluating these standards and compares presented standards using the framework. Section 5 will contribute by presenting novel attack scenarios where attackers utilize availability of different association models. Section 6 provides discussion on potential countermeasures against the identified new threats.

2 Association Models

Secure association of new devices is possible with different models, which are used to change authentication information between devices. Association models may require some kind of user-mediated assurance that a device, which is authenticated to a network, is really the new device and not attacker's device, and that a network to which a device is connected is the correct one. Various models have been proposed with different usability, security and hardware assumptions. These models include:

- **User's comparison** of authentication identifiers is a model where the end-user checks that the identifier displayed by a control device belongs to the new device. The new device may either display the same random secret number or it may have an unique identification code, which is e.g. displayed or which is available in printed paper format. Visual comparison models assume that the users will always make comparison.

Another threat is that, if identification numbers are static and unique for devices, an attacker may gains access to them e.g. with phishing attacks. If numbers are random, weaknesses in random number generation may expose association for attacks.

- **Keyboard** can be used to type authentication identifiers. This model enhances the previous visual comparison models as the user cannot avoid making the check. Also, it is suitable for devices without display but with input capabilities, such as keyboard. Downsides are that typing a code, which is long enough to protect against MitM attacks, takes time and is not highly usable.

- **Short-range radio connections** may be used to transmit authentication information as presented by Balfanz et al. [7]. This requires that both the new device and controller device support some short-range communication technology like Near Field Communication. Since the communication is wireless, an attacker, managing to get close enough, may be able to eavesdrop communication.

- **Physical connections** may be used to transmit authentication information. For instance, devices may be connected using cables. The solution is difficult to attack as short cables cannot be intercepted without the end-user noticing. Also, end-user cannot easily connect wrong devices together. A downside is the effects to the usability as a wireless solution turns out to be a wired one.

- **Portable memory devices** such as USB flash drives can be used to carry authentication information from one device to another. This channel can be considered secure against attacks, particularly if memory devices are assumed to be trustworthy and if an association model addresses the threat that an attacker later on gains access to memory device, which the user has e.g. lost. However, if an attacker gains access memory devices even for a short time, it may be tampered or network keys may be easily copied without the user noticing anything.

- **Visual or audio channel** can be used to transmit authentication information. For example, a camera can be used to capture a secret from a display of a device to be associated [10]. These models assume that attacker does not have audiovisual access to display e.g. through surveillance cameras.

- **Push button and timing** may be utilized in protection when transmitted authentication information in the same channel with the rest of traffic. In push button method, the user can e.g. initiate short time periods by pressing button in a control device. During this time new devices can be attached to the network by powering them up. This model is vulnerable to eavesdropping and MitM attacks. However, getting into the middle of devices may cause delays to communication as well as additional signalling enabling attacks to be detected.

3 Association Models in Standards for Personal Networks

3.1 Bluetooth Simple Pairing

Two individual Bluetooth devices are associated with pairing mechanisms. Initial pairing mechanism, based on based on symmetric cryptography, has been vulnerable both against

passive eavesdropping and active (MitM) attacks. To correct identified vulnerabilities Bluetooth Special Interest Group has developed Simple Pairing [3] specification. Simple pairing is based on Elliptic Curve Diffie-Helman protocol and supports the following association models:

1. **Numeric comparison model** where the user must manually compare that a random number displayed by both devices is identical. The compared key, preventing MitM attacks, is six digit long.
2. **'Just works' model** is similar to numeric comparison model. However, devices do not display key, which the user would be required to compare. Hence, the model protects against passive eavesdropping but does not provide any protection against MitM attacks.
3. **Passkey entry model** is targeted for devices without a display but with a keyboard. The user is required to type a number, which another device displays.
4. **Out-of-band model** has been specified to enable use of different out-of-band channels. A particular out-of-band channel discussed by Bluetooth documentation is Near Field Communication technology. Two directional out-of-band channels are used to change public keys. One directional out-of-band channels are used to transmit a secret random number, which a receiving device uses to prove that there are no MitM attackers.

3.2 Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) [9] - previously named as simple configuration - is Wi-Fi alliance's specification for secure association of wireless LAN devices. WPS implementations include Microsoft's Windows Connect Now (WCN) [4, 5]. The purpose of the technology is associate devices as well as to ease configuration. WCN supports the following association models:

1. **USB flash drive** can be used to copy configuration information including network encryption keys (e.g. 64 HEX character WPA pre-shared keys) from a control device to portable memory device. This device can then be used to distribute keys to new devices. Validity time of keys can be limited.
2. **Network model** enables association over Ethernet or wireless networks. The user is required to enter a PIN of new device to a control device. This PIN may be temporary (and displayed by the new device) or static (and printed to a label). The length of PIN may vary. For instance, Windows Vista supports both 4- and 8-digit PINs. Devices use PINs to generate hashes, which prove that both parties know the same secret and thus prevent MitM attacks. During association, devices change Diffie-Hellman public keys, which enable network encryption keys to be delivered securely for the new device.

3.3 Wireless USB Association Models

Wireless USB (WUSB) is a short-range wireless communication technology for high speed data transmission. WUSB Association Models Supplement 1.0 specification [6] supports two

association models for creating trust relationships between WUSB hosts and devices:

1. **Cable model** utilizes wired USB connection to associate devices. Connecting two WUSB devices together is considered as an implicit decision and, hence, the standard does require users to perform additional actions like clicking user interface dialogs.
2. **Numeric model** requires that the user makes visual comparison between random numbers, which both host and device displays. After the user has verified that both numbers are the same, association must be explicitly authorized.

3.4 HomePlugAV

HomePlugAV [1, 2] is a power-line communication standard for broadband data transmission inside home and building networks. HomePlugAV supports the following association models [11]:

1. **Simple connect mode** utilizes timing when associating new devices. The end-user initiates short time periods by pressing button in a control device. During this time, the user switches power to new device, which connects to a controller device and requests symmetric network encryption keys. This key is protected with a temporary key, which is a hash from a nonce that the new device sent. When a device is started, it may connect to a wrong subnetwork in powerline network. The user notices this, when a device does not work as expected, and must retry.
2. **Secure mode** requires the user to type 12 alpha numeric characters. Each device has an own unique identification number, which is typically printed to the label in equipment and which the user must manually entry to a control device. A network membership key is then encrypted using this identifier and broadcasted to the new device. A control device distributes network encryption keys periodically to devices with network membership key. Devices in the secure mode have an own network encryption keys. Hence, e.g. devices connected with simple connect are not in the same network as devices of secure mode.
3. **Optional modes** enables alternative use of alternative models for distributing the network encryption key between devices. For instance, manufacturer's could support the following models: manufacturer keying, where a group of devices have factory installed shared secret, and external keying, where trust is bootstrapped from other layers such as Bluetooth, UWB or Windows Connect Now.

MitM attacks are prevented, in simple connect mode, by utilizing characteristics of powerline medium. Before two nodes can communicate, they must negotiate tone maps, which enable devices to compensate disturbances caused by powerline channel and to receive communication signal. This negotiation is done in a narrow band channel, where all communication is heard. Thus, MitMs and other attackers, trying to invade network during association time, can be detected.

Passive eavesdropping in broadcast channel is difficult since eavesdropper, who hasn't negotiated tone maps is not be able to extract signal from the channel. Particularly, when an

attacker is outside a building signal-to-noise is poorer than inside buidling. Also, licensees of HomePlugAV technology do not provide devices, which are able to extract signal without negotiating tone maps. Hence, attackers must be able to build expensive devices for eavesdropping.

4 Evaluating Association Models in Standards for Personal Networks

This section presents a framework for evaluating association models and compares standardization proposals using the framework. The following subsections present four different points of view to the security of association models for personal networks. After presenting evaluation criteria, a comparison between four standard proposals is presented.

4.1 Threat Model

4.1.1 Evaluation Criteria

Association models should be able to prevent attackers from gaining access to users existing devices as well as to prevent existing devices from connecting attackers devices, which might e.g. collect confidential information with bogus services. However, they may not address all threats nor be able to defend against all kinds of attacks. For instance, in some cases, deliberate security compromises are made, for example, due to usability or costs. In some cases, a communication environment, for instance physical medium, may be assumed to be secure enough for some threats. In some cases, a treat may be unknown for the designers.

The main attack categories against association models have been illustrated in Figure 1. They include fooling the users to associate attackers devices, passive eavesdropping and active MitM attacks. In order for these attacks to succeed attackers must be able to succeed in various attack phases as whose relationships are illustrated.

Attacks against associations require that the user is able to find some, e.g. algorithmic or protocol, vulnerability in association model. If there are no known vulnerabilities in the used model, an attacker may be able to switch into a model, which is has vulnerabilities. Consequently, standards, which support multiple association models, must be able to withstand attacks where an attacker tries to force the user to use less secure model or where an MitM attacker communicates with one model to one direction and with another model to another direction.

In passive eavesdropping and MitM attacks, the attacker must be able to eavesdrop communication when association are made. An attacker who cannot listen initial associations may force new associations. For example, original Bluetooth pairing has been shown to be vulnerable for attackers forcing devices to perform re-pairing [13].

Since the communication medium for personal networks is typically available also for attackers, some association models utilize out-of-band channels for transmitting security information such as network encryption keys, public keys or identifiers preventing MitM attacks. Different out-of-band channels have different security assumptions. These assump-

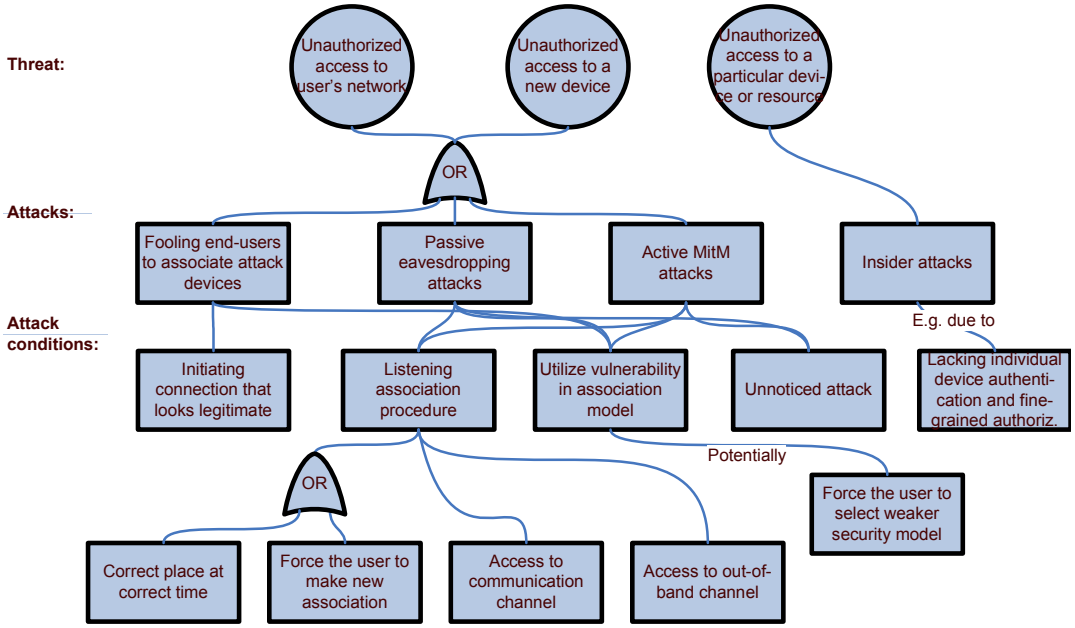

Figure 1: Attack phases and conditions

tions where presented in Section 2. An attacker may, for instance, be assumed so that visual 'over the shoulder' eavesdropping and listening very-short range communication are not possible. Also, the user may be assumed to protect portable memory devices.

Attacks must also be made so that the user cannot detect them. This is a problem particularly for MitM attackers, who must be able to prevent legitimate connections and forward traffic fluently without noticeable delays.

Fooling the users to associate attack devices category relates to the usability and has been further discussed in Subsection 4.3 and in Section 5.

Some association models do not enable individual devices to be authenticated. Consequently, these models consider only external threats. However, protection schemes against insider threats, e.g. fine-grained access control architectures neutralizing malicious software attacks, require that individual devices can be authenticated.

4.1.2 Comparison between Personal Networks

To address passive eavesdropping attacks, public key cryptography - particularly Diffie-Helman, have been adopted to every association standard using in-band models except to the HomePlugAV, which utilizes medium specific characteristics for protection against passive eavesdropping as well as MitM attacks. Summary of selected protection mechanisms has been presented in Table 1.

MitM protection in HomePlugAV simple connect mode works, if any additional traffic in the narrowband channel at the time when association button is pressed causes association to fail. If an attacker is able to prevent new device and control device from hearing other

Association model	Passive eavesdropping	Man-in-the-middle attacks
BTSP Numeric Comparison model	Public key crypto (DH)	Comparison model
BTSP Just works model	Public key crypto (DH)	-
BTSP Passkey Entry model	Public key crypto (DH)	Typing a key, which another has device displayed
WPS Network model	Public key crypto (DH)	Comparison model
WPS USB model	Secure out-of-band channel	Secure out-of-band channel
WUSB Numeric model	Public key crypto (DH)	Comparison model
WUSB Cable model	Secure physical channel	Secure physical channel
HomePlugAV Simple Mode	Signal-to-noise ratio makes eavesdropping difficult	All connection setups in narrowband channel including MitM can be detected
HomePlugAV Secure Mode	Symmetric crypto (AES CBC with 72 bit key)	Typing a identification key of new device

Table 1: Defence against attacks

connections, MitM attacks may occur. For instance, an attacker may physically separate networks. Also, it might be possible that an attacker is able interfere with powerline channel so that all connections will not be detected by other nodes in the network.

All other models except the WPS USB model provide support for authentication of individual devices. In WPS USB model, the same network encryption key is distributed to every device to which USB flash drive is inserted. In the other models, association is done between two devices and the control device will learn either devices' public keys or device specific shared secrets.

4.2 Hardware Requirements

4.2.1 Evaluation Criteria

Association requires devices to support cryptographic functions and use of out-of-band channels may require that additional hardware is supported. These features are expensive and often security association alone is not enough to justify extra costs. Therefore, these requirements may limit types of devices to which different association models can be applied.

Hardware requirements for user interface of association and for out-of-band channel may include buttons, keyboard, display, camera, speakers, audio recorder, cabling, portable memory devices and readers as well as radio receivers and transmitters. For some association models, mutual association (i.e. authenticating a new device for a network and the network for the new device) may require that both parties (a new device and a control device) must provide the same equipment. However, in some schemes it is enough that only one device has hardware supporting association. For example, Wong and Stajano [15] proposed a scheme for mutual association by making verification only in one direction and Saxena et al. [12] described a

protocol for associating when only one device has a camera.

Processing requirements depend on utilized cryptographic algorithms. Typically, use of asymmetric algorithms have been considered to be significantly more demanding than symmetric and thus less suitable for devices with restricted battery and computing capacities.

4.2.2 Comparison between Personal Networks

Summary of required UI capabilities has been presented in Table 2.

Association model	**New device**	**Control device**
BTSP Numeric Comparison model	Display (6 PINs) and button	Display (6 PINs) and button
BTSP Just works model	-	Display and button
BTSP Passkey Entry model	Keyboard	Display
WPS Network model	Display (or printed label)	Display
WPS USB model	USB port	USB port and flash drive
WUSB Numeric Model	Display (2 PINs) and button	Display (4 PINs) and button
WUSB Cable Model	USB port	USB port and cable
HomePlugAV Simple Mode	-	Button
HomePlugAV Secure Mode	- (printed label)	Keyboard

Table 2: UI capability requirements

Public key cryptography, particularly Diffie-Helman, must be supported in Bluetooth, WUSB and Wi-Fi devices. Furthermore, Bluetooth requires SHA-1 algorithm and WUSB and Wi-Fi require SHA-256 support. HomePlugAV does not require public key cryptography. Required algorithm for association is SHA-256, which is used to generate device access keys from secure mode passwords or from simple connect nonces, as well as AES, which is used in secure mode to encrypt network membership keys using device access keys.

4.3 Usability

4.3.1 Evaluation Criteria

Usability sets constraints for security mechanisms in personal devices. Too difficult association mechanisms will not be used as the user either ignores security altogether or, if this is not possible, selects alternative devices. Also, the user may by mistake configure security wrongly and, hence, enable attacks. Consequently, secure standards minize users' ability to make mistakes, which will compromize security.

Generic attributes affecting to the usability of individual association models include the amount efforts required from users, easiness of learning as well as sensitivity for users' mistakes. Particular questions, which association models must address when requiring the end-user actions and decisions, include:

1. How to minimize configuration time and interaction amounts, which individual users are required to give for association? These factors affect to how easy it is to learn and how willing users are to use association model.
2. Can users ignore security or avoid making some security critical step?
3. How unique association model is? This affects to easiness use security mechanisms. The less devices and technologies, which support similar models, there are, the more things there are for users to learn.
4. How to make it clear and unambiguous which devices are associated? How can the model be attacked against? Is it possible for attackers to initiate associations, which look authentic? For instance, can there be multiple simultaneous associations?

Particular association models have own usability characteristics. For instance, usability of password-based association models depends on lengths of passwords. To address the difficulty of using passwords, recent work e.g by Vaudenau [14] has demonstrated how to use short passwords in secure association. These schemes use short passwords e.g. 5 PINs to prevent MitM attacks when asymmetric cryptography such as Diffie-Helman protocol is used. Models, where portable memory devices are used, may require more user actions when information is copied to portable memory. For instance, the user is required to acguire portable memory, plug it into a control device, launching an application for editing and copying association information and potentially configuring this information. After that a large amount of new devices can be easily associated. Camera and audio based models may require users to learn more complex tasks

Standards and devices supporting multi-model security associations have some special usability related security characteristics. Particularly, if disabling security altogether or selecting a less secure model is possible and easier than configuring a secure model, many users will do so and ignore security threats. Furthermore, attackers may try to get users to select less secure models by preventing use of more secure models with different denial of service attacks. Therefore, the easiness of switching between modes and disabling security, affects to the security of personal networks.

4.3.2 Comparison between Personal Networks

Models where the user cannot ignore security, not even by ignoring advises to compare to values, have been included to every standard. Particularly, WPS USB, BT passkey entry, WUSB cable and HomePlugAV's secure and simple connect modes all require users to explicitly do correct actions before security association is created.

None of the standards discusses on alternatives where users could ignore security altogether. Only one model, Bluetooth 'just works', ignores the threat of MitM attacks. Users may be negligent against MitM attacks in numeric comparison models. Since in this model users

may by mistake enable attacks, it is important that comparing displayed short keys becomes a routine. This model is supported in Bluetooth, Wi-Fi and WUSB. Also, it has been part of devices already in earlier Bluetooth devices. Therefore, many users will be using regularly this model and some are already familiar with it.

Short passwords have been adopted to every association standard, which require users to type or compare displayed numbers, except to the HomePlugAV, which utilizes symmetric cryptography for MitM protection. Short passwords-based models make compromises between usability and security when preventing MitM attacks. For instance, in Bluetooth Simple Connect with 6 digit PINs, a MitM attacker has a 1 in 1 000 000 change to guess number correctly. Table 3 summarizes how standards use identifiers, which the user must compare or type, by presenting their length and protection they bring against MitM attacks, which are based on password guessing.

Association model	**Compared value**	**Success ratio for MitM guesses**
BTSP Comparison and Passkey Entry models	6 digit PIN	1 in 1 000 000
WPS Network model	4 or 8 digit PIN in Windows Vista	1 in 10 000 or 1 in 100 000 000
WUSB Numeric model	2 (or more) digit PIN	1 in 100(+)
HomePlugAV Secure Mode	12 alpha numeric characters	1 in 2^{72}

Table 3: Length and MitM resistance of device identifiers

Completely unique association models, requiring users to learn novel skills are at least WPS USB flash drive model as well as HomePlugAV simple connect.

Vulnerabilities utilizing devices support for multi-model security associations are discussed in Section 5.

4.4 Extendibility

4.4.1 Evaluation Criteria

Some security models may be found vulnerable, existing models may be unsuitable for hardware capabilities of forthcoming devices and new models with better usability characteristics may emerge and gain popularity. Therefore, there is a need to allow manufacturers to extended their devices by implementing new association models. Of course, the purpose of standards is to dictate mechanisms enabling devices to be compatible. However, standards may enable and support manufacturers to implement optional or custom association model, which complement devices.

Standards may support extendibility by provide some common mechanisms for association so that manufacturers do not need to design and implement all the phases of association themselves.

Extendibility may open doors also for security vulnerabilities. When new models are adopted

to devices, implementers should consider both the security of individual model as well as the security of whole device with several supported association models.

4.4.2 Comparison between Personal Networks

Extendibility is supported only in Bluetooth Simple Pairing. Wi-Fi Protected Setup and WUSB Association Models do not support alternative models. However, forthcoming releases of the WUSB specification may support alternative models. For instance, Near Field Communication is currently being investigated. [8] HomePlugAV's optional mode enables manufacturers to implement alternative models to distribute network encryption keys. However, the standard does not provide any particular support for alternative models.

Out-of-band model of Bluetooth supports alternative association models with two different ways. Two directional out-of-band channels, such as NFC, are used to change public keys. One directional channels are used to transmit random secret, which protects against MitM attacks. Other phases of association, including generation of authentication information, agreeing on use of alternative models and changing other required association information, are part of the specification.

5 Vulnerabilities due to Multi-Model Associations

Finding vulnerabilities, which can be used to fool users to associate attacking devices, is easier when systems are complex and haven't faced thorough inspections. Typically, the newer and the more complex a system is, the more vulnerable for attacks it is. New multi-model standards for association are one source of complexity and unfound vulnerabilities. This is demonstrated by the attacks presented below:

5.1 Man-in-the-middle between the numeric comparison and 'just works' models to hide a compared value

In this attack, which is illustrated in Figure 2, MitM intercepts a connection request, which is send using Bluetooth numeric comparison model. Then MitM responds with a message encrypted with its own private key and sends to another direction Bluetooth 'just works' connection request. In 'just works' model the receiving device does not display number, instead the user is only requested to accept the connection [3]. The user is educated to detect attacks where displayed numbers are different. However, now, when only another device displays a number, the user may easily accept association without noticing any attack.

The attack is not limited to Bluetooth. The MitM attack might be implementable also between different technologies. For instance, an attacker with a gateway device supporting both WUSB and Bluetooth may implement MitM between WUSB numeric model and Bluetooth 'just works' model. This attack requires that an MitM has a working gateway so that user does not notice anything when using the connection. A user interface may in some cases may inform that Bluetooth connection is made, however, this may not be enough to raise users suspicions.

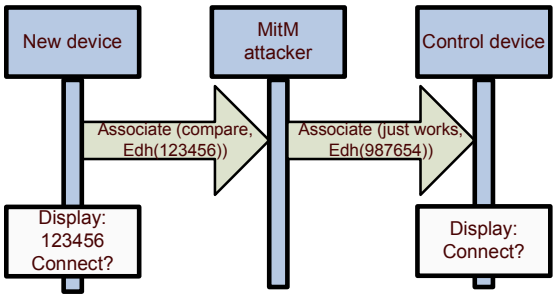

Figure 2: MitM between comparison and 'just works' models

5.2 Jamming the numeric comparison model to get the user to switch into the 'just works' model

This attack scenario, illustrated in Figure 3, is an example of cases where attacker prevents the user from making association until the frustrated user decides to try the alternative 'just works' model. When detecting that the 'just works' model is used, an attacker may perform MitM attack without being detected. This attack requires that the attacker is able to determine when comparison model connections are made and disturb communication when this occurs. The attack is more likely get the user to try alternative model when the user considers a manual and user interface for association to be difficult and, hence, blames a device, instead of an invisible MitM attacker.

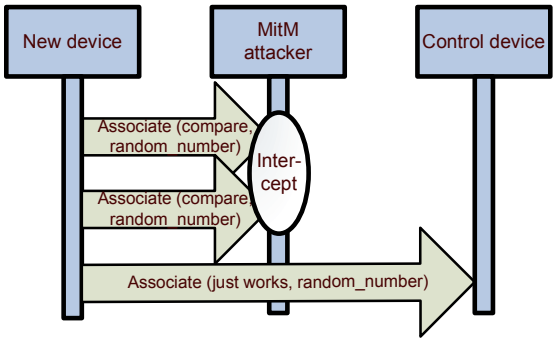

Figure 3: Jamming the BT comparison model to get the user to switch into the 'just works' model

In addition to Bluetooth, the jamming attack is possible also in HomePlugAV where attacker may try to get user to use simple connect mode instead of secure mode. The attacker must able to determine when secure mode associations are made as well as to disturb this communication. For instance, an attacker who is able to eavesdrop broadband communication may detect when secure mode associations are made and also able to extract keys for simple connect mode.

5.3 Requesting explicit association while the user makes implicit WUSB association

In this attack, which is illustrated in Figure 4, an attack device initiates numeric model association at the same time when the user has connected two devices with a USB cable. In cable model, association may implicit, i.e. happens automatically without any user prompts. If a user prompt anyhow emerges in this situation, the user may not consider this to be suspicious. Consequently, the user may explicitly accept the attacker. The fact that only one device displays number to be compared may not be enough to raise users suspicions. In order to attack succeed, the attacker must be able to determine when cable associations are made. This may be possible e.g. trough surveillance cameras or if an attacker has a direct visual access.

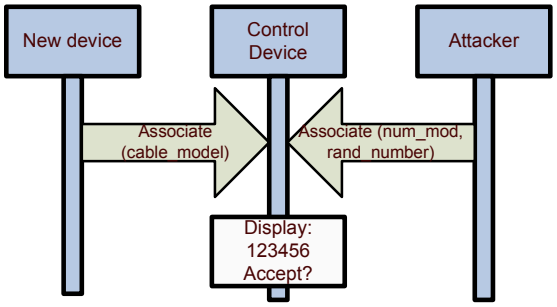

Figure 4: Requesting explicit association while the user makes implicit association

This attack can be applied to other communication technologies. For example, when implicit WUSB cable model association is made, an attacker may initiate Bluetooth comparison or 'just works' associations to get the user to accept connections. Similarly, attackers might monitor when USB flash drive is inserted to new devices and at that time initiate e.g. Bluetooth or WUSB connections.

6 Strengthening Multi-Model Association Standards

The threats, which were identified in the previous section, can be addressed either in standardization or in implementation phase:

1. **'Man-in-the-middle between numeric comparison and 'just works' models'** attack could be countered by demanding that displays of devices believing to be in 'just works' association would anyhow show the number. Alternatively, users can be educated, e.g. in device manual, that both devices must display numbers if the user is using numeric comparison models.

2. **'Jamming the Bluetooth numeric comparison model to get the user to switch into the 'just works' model'** and **'jamming the HomePlugAV secure mode to get the user to switch into the simple connect mode'** attacks can be countered by educating the user that unsuccessfull association may be an indication of an occurring attack. A device can also itself record recent association failures and, if only weaker model seems to be working, inform the user on potential attack.

3. **'Requesting explicit association while the user makes implicit association'** attack can be countered by preventing all numeric model associations when device is associating through implicit (e.g. cable) association model and shortly after that.

7 Conclusions

The new standards for personal network, enabling association of devices in multiple ways, contribute by improving usability, by correcting known security vulnerabilities and by providing additional versatility for manufacturers and users. However, they also introduce new security vulnerabilities as attackers may utilize them to fool users to associate wrong devices. The paper identified few new attack scenarios, which haven't been addressed in the current standard specifications. Attacks types include MitM attacks between different association models, jamming particular association models as well as initiating on-line associations when implicit out-of-band associations are made.

References

[1] HomePlug Powerline Alliance. `Http://www.homeplug.org/`.

[2] HomePlug AV whitepaper. HomePlug Powerline Alliance. `Http://www.homeplug.org/`, 2005.

[3] Simple Pairing Whitepaper. Bluetooth Special Interest Group. `Http://www.bluetooth.com/Bluetooth/Apply/Technology/Research/Simple_Pairing.htm`, 2006.

[4] Windows Connect Now-NET. Version 1.0. Microsoft. `Http://www.microsoft.com/whdc/Rally/WCN-Netspec.mspx`, 2006.

[5] Windows Connect Now-UFD and Windows Vista Specification. Version 1.0. Microsoft. `Http://www.microsoft.com/whdc/Rally/WCN-UFD_Vistaspec.mspx`, 2006.

[6] Wireless USB Specification. Association Models Supplement. Revision 1.0. USB Implementers Forum. `Http://www.usb.org/developers/wusb/`, 2006.

[7] Dirk Balfanz, D. K. Smetters, Paul Stewart, and H. Chi Wong. Talking to strangers: authentication in ad-hoc wireless networks. In *Proceedings of the Network and Distributed System Security Symposium*, 2002.

[8] Preston Hunt. Certified wireless USB association models supplement 1.0. Presentation at the Wireless USB Developers Conference. `Http://www.usb.org/developers/wusb/docs/presentations/Taipei06_PH__Association_Models.pdf`, 2006.

[9] Amol Kulkarni and Jesse Walker. Easy and secure setup of personal wireless networks. *Technology@Intel Magazine*, November 2004.

[10] Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2005.

[11] Richard Newman, Sherman Gavete, Larry Yonge, and Ross Anderson. Protecting domestic power-line communications. In *Proceedings of the Symposium On Usable Privacy and Security*, 2006.

[12] Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2006.

[13] Yaniv Shaked and Avishai Wool. Cracking the Bluetooth PIN. In *Proceedings of the 3rd USENIX/ACM Conference on Mobile Systems, Applications, and Services*, 2005.

[14] Serge Vaudenau. Secure communications over insecure chnanels based on short authenticated strings. In *Proceedings of The 25th Annual International Cryptology Conference*, 2005.

[15] Ford-Long Wong and Frank Stajano. Multi-channel protocols. In *Proceedings of the 13th International Workshop in Security Protocols*, 2005.