WUSB Security and Threats: a Survey and a Discussion

Gunhee Lee[1], Dong-kyoo Kim[1], JaeSung Lim[1], SungHyun Yang[2] and MyungHyun Yoon[3]
[1]Graduate School of Information and Communication, Ajou University, Suwon 443-749, South Korea
[2]Department of Electrical Engineering, Kwangwoon University, Seoul 139-701, South Korea
[3]Ubiquitous Computing Research Center, 68, Yatap-dong, Bundang-gu, Seongnam-Si 463-816, South Korea
E-mail: {icezzoco, dkkim, jaslim}@ajou.ac.kr, shyang@daisy.kw.ac.kr, yoon@keti.re.kr

Abstract: In this paper, we review the security features specified by the draft standard of the WUSB and describe some security threats on it. At the last, we briefly discuss about the idea to handle the threats. This will help us to achieve a robust and secure WUSB envrionment.

1. Introduction

Over the past decade, wireless communication has become an integral part of our everyday lives and Ultra-Wideband will only accelerate this trend. The technology is well suited for a variety of use cases in everybody's life such as home entertainment system, instantaneous synchronization and file transfer [1]. Wireless USB is an application of the UWB [2]. It is based on the WiMedia Alliance's UWB common radio plaform and will provide an useful interface. It is designed to operate in from 3.1 GHz to 10.6 GHz frequency range and is capable of sending 480 Mbits per second at distances up to 3 meters and 110 Mbits per second at distances up to 10meters.

However, as any other communication environment does, if the security of the WUSB would not be solved, the WUSB could not be a practical solution. Thus the workgroup studies the security issues of it. As a result, the security specification of the WUSB is included in the WUSB standard.

In this paper, we review the security features specified by the draft standard of the WUSB and describe some security threats on it. At the last, we briefly discuss about the idea to handle the threats. This will help us to achieve a robust and secure WUSB envrionment.

2. Security of the WUSB

In the standard, the security feature includes encryption, integrity check, key management and authentication methods.

For protecting outgoing frames, the standard employs AES (Advanced Encryption Standard) CCM mode with 128 bits key stream. This mode produces an encrypted data block and a message authentication code [3]. Thus this will guarantee both the confidentiality and the integrity of the frame.

To use security features such as pseudo random number generator, hash value generator, and encryption algorithm, WUSB utilizes three cryptographic keys; master key, pair-wise temporal key (PTK) and group temporal key (GTK). A master key shared between a host and a client is used for generate all kinds of temporally used keys including the PTK and the GTK. It is used in long-term. A PTK is a session key shared between both ends of a communication. It protects any unicast traffic between two ends sharing it for a session. That is, whenever they create a session, they should agree a new PTK. A GTK is a session key shared among members in a network or in a group. It keeps any broadcast traffic or any multicast traffic safe. Before joining a network a client shares a master key with a host. After joining the network, the client also shares both a PTK and a GTK with the host.

When a client wants to join a network, the client and the host of the network should authenticate each other. For the mutual authentication, the WUSB employs four-way handshake mechanism. During this handshake, the host and the client are able to authenticate each other and they can share a PTK. After this procedure, the host sends the host a GTK that is encrypted with the PTK.

The handshake is started with a request of a client device. As shown in Figure 1, when a host receives the request message, it initiates the handshake process by sending a temporal key identifier (TKID) and a 128-bits random nonce HNonce to the client. Then, the client receiving them generates a key confirmation key (KCK) and a PTK by using a pseudo random number generator with four parameters; a host's address, a client's address, a host's nonce and a client's nonce. After performing that, the client conveys a message to the host. The message includes the same TKID, client's nonce and a message integrity code (MIC) over the TKID and the nonce. The MIC is generated with the pseudo random number generator with the KCK. When the host receives the message from the client, it can also create a KCK and aPTK and it verifies that these keys are the same as them of client by comparing the received MIC with the MIC generated using the host's KCK. If the MICs match, then the host installs the PTK as a session key and sends the client a message that includes a TKID, a host's nonce and a MIC generated by itself. Otherwise, the client is disconnected silently. To validate the received MIC, the client performs a MIC computation with received values and compares two MICs. If the MICs match, the client also installs the PTK as a session key between the host and itself. Otherwise it disconnects silently.

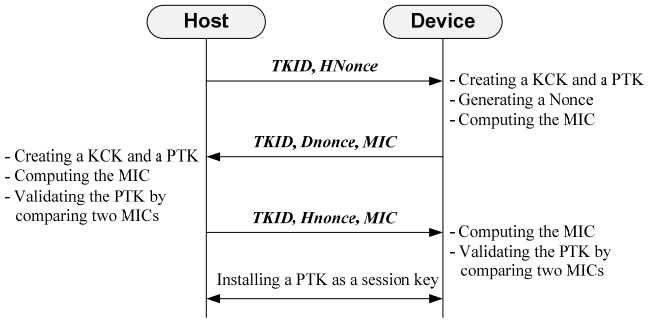

Figure 1. Four-way handshake procedure in the WUSB standard

3. Threats on the WUSB

Although there are many efforts to satisfy the security requirements in the WUSB standard, it still have some threats that can make the environment encounter dangers. In this paper we will describe 4 threats that might be considered.

3. 1 GTK Interception during Refresh Time

As we mentioned in section 2, WUSB and UWB employ a group key in order to protect any broadcast and multicast traffic. The GTK should be shared by all the members in a group or a network. Whenever a host broadcasts a packet, it encrypts the packet with a GTK. For maintaining the group or the network in secure, the GTK will be refreshed regularly or irregularly. In the case of regular GTK refreshness, the host should replace the GTK with the new one after a threshold time of GTK usage. For the irregular GTK refreshness, the host change from the GTK to a new one

whenever any member of the group or the network leaves the society.

However, there is a possibility to retrieve a new GTK during its refresh time. It is impossible to perform key refresh simultaneously. Until all the members agree to use a new GTK, the group uses the current GTK. Thus during the refresh time, the malicious left node can easily access the traffic without anyone knowing.

Moreover there is a possibility that the node acquire the new GTK. Thus we should employ more reliable GTK refresh method. If a GTK change command will be transferred to the members by broadcasting way, the command might be encrypted with the current GTK. Thus the left node intercepts the traffic and decrypt the message with the GTK, which it has. That is, even though the network employs a new GTK in secure way, the left malicious node also has the new GTK.

If the command will be sent to each client by unicast way, it would be encrypted with each one's PTK. Thus the new GTK is kept safe. However it is very expensive method. The host performs the AES function *n* times for *n* nodes and it takes longer than the broadcast way. During this long refresh time, the attacker can gather many informations from the network traffic. Additionally, the attacker can make the host be in more severe situation by repeating join and leave continously.

3. 2 Man-in-the-Middle Attack

There is a possibility to perform man-in-the-middle attack during 4-way handshake. The attacker can intercept the handshake message and send a modified or newly generated message to both side, initiator and responder.

When a host send a TKID and a its nonce to a client, the attacker is able to intercept the message in the middle between the host and the client. The attacker then replaces host's nonce with attacker's nonce and sends this new message to the client device. As the same way, when the client returns his nonce with a MIC to the host, the attacker is also able to seize the traffic. He/she then replace the nonce and the MIC with a new nonce and a new MIC that are generated by the attacker. As a result of the attack, the attacker can masquerade as an initiator (to deceive responder) or a responder (to have misled initiator), so he/she can easily take any message between the real initiator/responder.

There is another way to accomplish the man-in-the-middle attack. It is a kind of passive way, while the former is in a active manner. The attacker always sniffs the traffic to hear the request of join. Once the request is catched, the attacker just eavesdrops the traffic. As a result of this action, he/she is able to attain all the parameters of the key generation function execept for the master key. Thus the attacker might be able to computes the master key by performing dictionary attack.

3. 3 DoS Attack

There is a possibility to accomplish a DoS attack [4]. That is, any malicious node might be able to consume whole contention based command transfer area in a superframe. Because of it, any other node does not send their data to host. Thus the network does not work properly.

When a device node receives a beacon frame, the node try to find the media access slot with the distributed reservation protocol information in the beacon frame. In each MAS, micro-scheduled management command will be sent to the nodes. In the MMC, the device notification time slot is defined as a part of MAS. It is a contention-based time slot and it has 8 slots for each MMC. The device node can select a slot among them randomly and it sends a notification message to the host.

The attacker is able to find the MAS that is allocated to any node by eavesdropping the beacon frame. During DNTS time slot, the attacker can transmit any message continously in order to cause a collision. By carrying out this behavior during prolonged period of time, nodes in the network does not send any notification message. As a result of it, the network is in the state of denial of service.

3. 4 No Tamper-Resistance Mechanism

There is no tamper-resistance scheme to protect the device. The attacker, that is, easily attains the security materials, so it is able to impersonate any normal member. The attacker can access all the traffic in a network if he/she attains all the security materials of a host.

4. Discussion: How to Handle the Threats

To handle these problems properly, the best way is monitoring the network that is similar to the intrusion detection system. The host or any other specific node monitors all the behaviors of the nodes in a network. If a node perform any abnormal behavior, the host isolates the node from the network. For example, if a node emits messages continuously or it gives off more messages than a threshold in a specific time duration, the monitoring node can notice the behaviour and it makes the abnormal node leave out the network.

In addition to this, when we deploy a WUSB-base network or we set up a WUSB device in a existing network, more secure mechanism should be considered for the key agreement method. Currently, the specification encourage developers to employ display on all kinds of WUSB device. When we verify whether the generated key values between a host and a device are the same or not, the display should be used. The values are shown on the display, and the user confirm that the value is the same after he/she see the values on the display. However it is not so practical. If samll portable flash storage should have a display, the price would be much higher than the expectation of users.

We also need an robust and trustful time slot allocation scheme to avoid the DoS attack. Besides it, we should study on the tamper-resistance scheme in the WUSB environment.

5. Conclusion

The WUSB is a promising technology in a wireless domain. It may provide a useful interface at many places such as office, home, conference room and so on. However, in order to employ it practically, the security issues should be handled first. In this paper we explain the security features of the WUSB and describe 4 possible threats on the current WUSB-based network environment. This is the first step of the effort to overcome several security problems of the WUSB. We are sure that this will lead many deeper research on this kind of issues.

6. Acknowledgement

This research was supported in part by the MIC(Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-(C1090-0602-0011)).

This work was supported in part by grant No. 10024724 from the Growth Engine Technology Development Program and funded by Ministry of Commerce, Industry and Energy, Korea

References

[1] ECMA International, "High Rate Ultra Wideband PHY and MAC Standard," 2005.

[2] The Wireless USB Promoter Group, "Wireless USB Specification, Revision 1.0," 2005.

[3] "NIST FIPS Pub. 197: Advanced Encryption Standard (AES)," US Department of Commerce/NIST, 2001.

[4] P. Egli, "Susceptibility of Wireless Devices to Denial of Service Attacks," netModule Technical White Paper, 2006