Providing Secure Mobile Device Pairing Based on Visual Confirmation

Eunah Kim
Mobile Solution Group
Samsung Electronics (SAIT)
Gyeonggi-Do, Korea
eunah1004.kim@samsung.com

Wonkeun Kong
Mobile Solution Group
Samsung Electronics (SAIT)
Gyeonggi-Do, Korea
kong@samsung.com

Jeong Hyun Yi
School of Computing
Soongsil University
Seoul, Korea
jhyi@ssu.ac.kr

Abstract— **With the increase of personal mobile devices, wireless short-range communications occur frequently and security risks thereon increase since wireless communication channels are inherently easy to eavesdrop on and be under control. In this paper, we investigate a key establishment protocol focusing two properties of wireless mobile communications: 1) a short-range communication without prior trust relationship and 2) a human user who is able to verify both a sender and a receiver devices at the same time. We then propose a simple device pairing method to verify that the shared (temporal) public keys, which are later used to generate a session key, are identical by presenting short text messages on secure side channel (e.g., visual and audio channel). It is easily and intuitively recognized by a human user.**

Index Terms—short-range communication, secure device pairing

I. Introduction

Recently various types of personal mobile devices such as PDAs, smart phones, multimedia players and Ultra Mobile Personal Computers (UMPCs) are introduced and being popular. Due to the increase of these mobile devices, it is so often to enjoy short-range wireless networking technologies such as Wi-Fi, Bluetooth [5] and infrared. A typical example of short-range wireless network is a Wireless Personal Area Network (WPAN) which consists of heterogeneous devices possessed in general by the same user and operates in an ad-hoc manner. A user can connect her devices with each other and/or to foreign devices (e.g., public printers, network access pointers and other users' mobile phones) resided outside her WPAN.

As the wireless communications are widely and instantaneously used, security threats thereon increase because wireless communication channels are inherently easy to eavesdrop on and be under control. In addition, messages transferred between personal devices are mostly privacy-related information. Thus it is very important to provide security solution for protecting such networks against the malicious mobile adversary. Several previous works have introduced the means of establishing a secure wireless communication channel (e.g., authenticated key exchange). However, conventional cryptographic means of key establishment are not always applicable in mobile environment because instantaneously associated devices in a short-range personal network have neither a prior context such as a shared secret nor a common point of trust such as Trusted Third Party (TTP) such as Public Key Infrastructure (PKI). It is challenging task to develop the techniques for a secure communication channel in wireless mobile environment.

The technique which makes two devices securely paired or initialized without prior context via a short-range wireless channel is called *"pairing"* in some literatures [1], [7], [8], [9], [10]. They utilize a physically authenticable channel, so- called Out-of-Band (OOB) channel, within the visible range of human user. The OOB channel includes a visual and an audio channel as well as a physical connection. It is assumed that a human user can verify OOB channel and thus an adversary cannot manipulate messages on this channel.

In this paper, we propose a key establishment protocol focusing two properties of wireless mobile communications: 1) a short-range communication without prior trust relationship and 2) a human user who can verify a sender device and a receiver device at the same time. We propose a simple device pairing technique to verify that the shared (temporal) public keys, which are later used to generate a session key, are identical by presenting short text messages on the visual or audio OOB channel. Our proposed scheme can be used to initialize the communicating devices in almost any standard public key cryptography based key exchange protocols including Diffie-Hellman protocol [11].

This paper is organized as follow: Section II overviews the related work. Next, Section III describes a proposed key establishment protocol and its implementation details and usage scenario are given in Section IV. We then conclude in section V.

II. Related Work

A. Key Establishment Protocol

To secure wireless communication, a shared secret key (e.g., session key) which protects subsequent communications is set up between devices. Generally used Diffie-Hellman (DH) key exchange protocol [11] allows two devices that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be

978-1-4244-2976-9/09/$25.00 ©2009 IEEE

1. A generates a temporal key pair (a, pk_A),
   $pk_A = g^a \mathit{mod}\, p$
   $A \rightarrow B$: g, p, pk_A
2. B generates a temporal key pair (b, pk_B),
   $pk_B = g^b \mathit{mod}\, p$
   and calculates a shared key K *as* $(pk_A)^b$
   $B \rightarrow A$: $pk_B, cert_B, E_K(S_B(pk_B, pk_A))$
3. A calculates a shared key K *as* $(pk_B)^a$
   $A \rightarrow B$: $cert_A, E_K(S_A(pk_A, pk_B))$
4. A shared key is established as $K = (g^b)^a = (g^a)^b \mathit{mod}\, p$

Notation
g, p: public parameters of DH protocol
$cert_X$: public key certificate of device X
$E_Y()$: message encryption using key Y
$S_X()$: message signing using X's private key

Figure 1. Station-to-Station protocol

used to encrypt subsequent communication using a symmetric key cipher. However DH protocol does not provide authentication of the communicating devices and is thus vulnerable to a Man-in-the-Middle (MITM) attack [12].

To prevent this type of attack, the Station-to-Station (STS) protocol based on classic DH protocol [13] supports a mutual key and entity authentication. Figure 1. shows a brief description of STS protocol. The protocol starts by A and B exchanging their temporary public keys, K_A and K_B respectively. To avoid MITM attack, they verify the digital signature of exchanged temporal public keys using previously distributed certificates, $cert_A$ and $cert_B$ respectively. However this authentication is not always applicable in mobile environment because devices cannot always have a prior context or a common trust relationship such as Certification Authority (CA) [6] and Trusted Third Party (TTP) such as Public Key Infrastructure (PKI).

We investigate the method to authenticate the target devices and verify that the same key is shared between two devices using the OOB channel.

B. Device Pairing methods

There has been a considerable amount of earlier studies to solve the secure device pairing problem using OOB channel. OOB channel is an auxiliary physically authenticable channel which is within the visible range of human user. It enables to establish a secure communication channel without prior context between two devices connected via a short range wireless channel. On OOB channel, a human user sometimes has capability of manually identifying the target devices or verifying some security materials presented by devices and thus an adversary cannot manipulate messages.

Stajano et al. [3] initially proposed to establish a shared secret key using standardized physical interfaces and cables as OOB channel, which are burdensome to mobile devices in many cases. Balfanz et al. [2] extended this approach through the use of infrared. Based on Balfanz et al. [2], McCune et al. [4] proposed the Seeing-is-Believing (SiB) device pairing method which uses two unidirectional visual OOB channels: One is to encode a 2D barcode and display it and the other is to read the barcode using a camera. SiB requires the user operations to read the barcode using a camera and this operations give some kinds of burdens to a user [14]. In addition, without camera equipped devices in both sides, SiB cannot attain mutual authentication. Saxena et al. [1] improved SiB and show how strong mutual authentication can be achieved with a unidirectional visual channel.

Recently, Goodrich et al. [8] introduced the Loud and Clear (L&C) system which use the audio OOB channel along with vocalized MadLib sentences derived from the hash of a device's public key. This approach makes use of a speaker on one device and a speaker or a display on the other. The user is required to compare the two MadLib sentences which contain 8 words and make a decision to accept or abort the device pairing. We employ an L&C-like approach that uses the audio/visual OOB channel for secure device pairing. Another recent device pairing method is HAPADEP [9]. It uses the audio channel to exchange both data and verification information among devices equipped a microphone and a speaker.

There are several experimental investigations. Uzun at al. [15] presented a comparative evaluation of the recent device pairing methods to derive insights into the usability and security as well as strategies for implementing them. Kumar et al. [14] present the first experimental evaluation of prominent device pairing methods. Its results show that some simple methods (e.g., visual number and image comparison) are quite attractive overall, being fast and secure as well as acceptable by users. We focus the fact that the secure pairing methods need to be easily and intuitively perceived by a human user and then propose a simple pairing method using audio/visual OOB channel.

III. The Propsed Scheme

In this section, we describe our proposed key establishment protocol using human-assisted visual or audio confirmation. We start with unidirectional authentication method based on general public key cryptography such as RSA. We then apply our authentication method to DH key exchange protocol. In proposed authentication method, a human user compares a short text message to share an identical temporal public key between two devices.

A. Unidirectional authentication

When A is a target device which a user wants to connect to and B is a user's device, the target device generates a temporal public and private key pair and sends a public key with its signature. The signature ensures the integrity of transmission. Next, A calculates a hash value of its public key and encodes the hash value into a short human readable text message. The user device B also calculates a hash value of received A's public key and create a text message by the same manner. Presenting these short text messages on the display or the speaker of each side, a user can compare both sides of text messages at the same time. If each text message is identical, a user can believe that an adversary do not interfere in the communication. From now on, a user device B creates a session key, encrypt it using authenticated A's public key, and delivers to A to protect subsequent communications.

1. *A* generates a temporal key pair (sk_A, pk_A)

   $A \rightarrow B$ (wireless channel): pk_A, $S_A\ (pk_A)$
2. *A* calculates h_A as $h(pk_A)$ and t_A as $t(h_A)$ which is a text version of h_A

   $A \rightarrow User$ (auxiliary channel): $t(h_A)$
3. *B* calculates h_A' as $h(pk_A)$ and t_A' as $t(h_A')$ which is a text version of h_A'

   $B \rightarrow User$ (auxiliary channel): $t(h_A')$
4. *User* compares both sides of text, t_A and t_A' and accepts pk_A if $t_A = t_A'$ or aborts.

Notation

$S_X()$: message signing using *X'*s private key

h(): one way hash function

t(): function which encode hash value into text message

Figure 2. Unidirectional authentication method

We consider the several methods to encode a hash value to short human readable text message. To convert a hash output which is generally 128 bits or 160 bits long (e.g., MD5, SHA-1 hash function) into a short text message within several characters, a modified hash function, exclusive disjunction operation, etc. can be used. Since a human user cannot recognize normal binary strings, shortened hash value should be encoded into human readable letters such as alphabet, numbers. We discuss this text conversion in Section IV again. Figure 2 shows proposed unidirectional authentication method.

B. Seession key establishment protocol

Applying unidirectional authentication method described in advance, we suggest a session key establishment protocol based on classic DH protocol [11] and it is divided three phases as depicted in Figure 3.

In first setup phase, *A* and *B* start the key establishment protocol by generating random secret keys, *a* and *b*, and public keys, pk_A and pk_B, respectively. Public DH protocol parameter *g* is over a finite cyclic group *G* which is a subgroup of Z_p^*, the multiplicative group of non-zero integer modulo a large prime *p*.

In second authenticated public key exchange phase, *A* and *B* exchange their public key via insecure wireless communication channel. To defeat MITM attack, a user manually confirms that each public key is shared identically between two devices via a secure auxiliary channel. In proposed key establishment protocol, visual and audio channel is used as an auxiliary channel. If two devices are display equipped ones, they can show short text messages on their display. On the other hand, only one device has a display and the other has not but a speaker, a user can verify the displayed text message hearing the other device's text message at the same time.

After the authenticated key exchange procedure, two devices can calculate a session key using their own secret key and shared public keys.

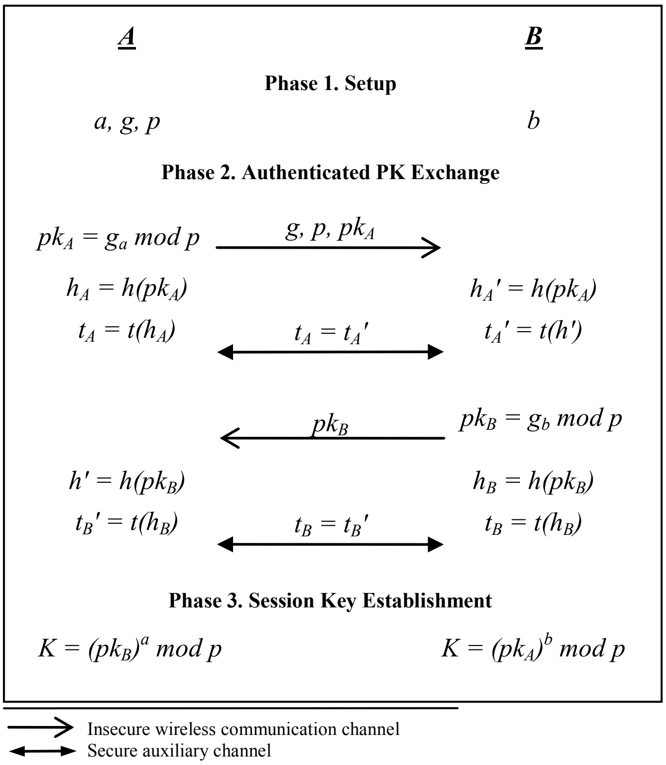


Figure 3. Propsed session key establishment protocol

IV. Implementation

We built our session key establishment protocol for concept proofing with common device pairing scenario, mobile payment. In our usage scenario, a user who has a smart phone connects to a mobile payment system which is in an outdoor store or other such place. Note that user's private information (e.g., credit card numbers) transmitted to the payment system should be protected. To ensure the user that the communication channel between two devices (user's smart phone and the mobile payment system) is secure, we applied our session key establishment protocol to each device. Using a short text message based authentication, a user can manually verify that exchanged public keys are identical between two devices and thus, two devices can share a session key securely. In addition, we employed an active attacker device which is capable of eavesdropping on a wireless communication channel. If a secure session is established, the attacker would not be able to sniff user's private information.

Figure 4. Device pairing scenario

Figure 4 shows our device pairing scenario:

- a laptop PC as a payment system running Windows OS
- a smart phone as a personal mobile device running Windows Mobile OS version 5.0
- a UMPC with Wi-Fi network sniffing software as an active attacker running Windows OS.
- Wireless communication via Wi-Fi or Bluetooth [5]

To implement our proposed protocol, we use Visual C++.net framework which runs on any series of windows OS.

In implementation of DH key exchange protocol, we use the SHA-1 cryptographic hash function for all hashing operations. To convert 160-bit SHA-1 hash value of public key into 8 ASCII characters, we use exclusive disjunction operation. First, 160-bit binary string is divided into three binary strings: 56-bit string, 56-bit string, and 48-bit string added 8-bit padding. Next, three binary strings are applied to exclusive disjunction operation to make a 56-bit binary string. Then, we match each 7-bit binary string with a random entity of human readable ASCII character set which consist of capitalized alphabet and numbers sequentially. Because 7 bits can represent 2^7 kinds of binary string though the character set has only 36 entities, redundancy is occurred. Thus, we try that all characters is matched as equally as possible. We remain the study of improved text conversion method as a future work.

Figure 5 contains photographs of proposed key establishment protocol using visual confirmation of exchanged public key. A user can authenticate each device based on short text message easily and intuitively.

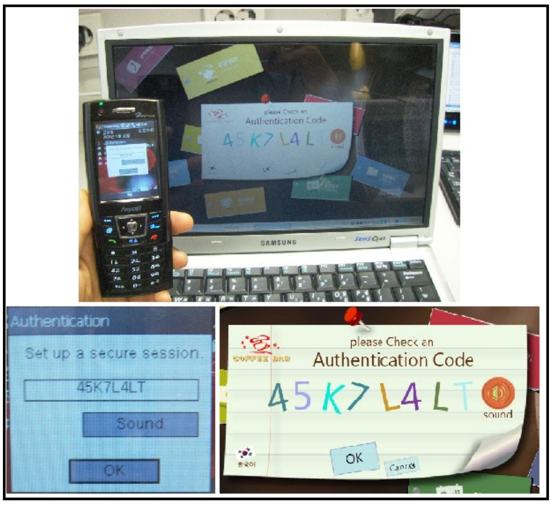
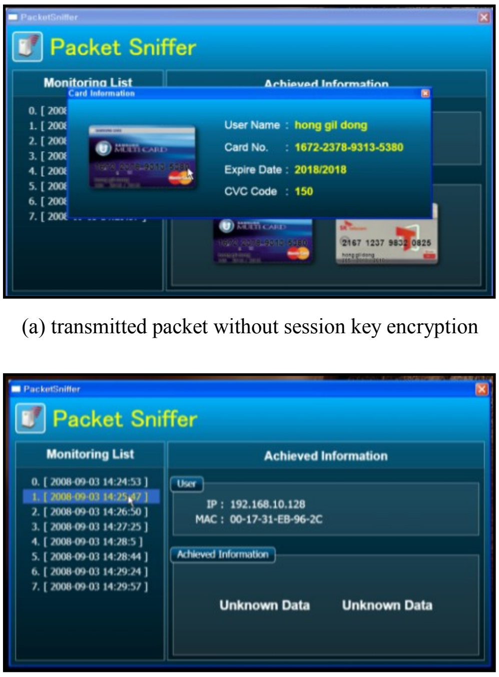


Figure 5. Visual confirmaion procedure

After visual confirmation procedure, two devices can calculate a session key using their own secret key and exchanged public keys. To show how a user can transmit her private information to other device, we performed a simple MITM attack experiment. As depicted in Figure 6, user data is protected when a session key is successfully established.



0. [2008
1. [2008
2. [2008
3. [2008
4. [2008
5. [2008
6. [2008
7. [2008

User Name : hong gil dong
Card No. : 1672-2378-9313-5380
Expire Date : 2018/2018
CVC Code : 150

(a) transmitted packet without session key encryption

0. [2008-09-03 14:24:53]
1. [2008-09-03 14:25:47]
2. [2008-09-03 14:26:50]
3. [2008-09-03 14:27:25]
4. [2008-09-03 14:28:5]
5. [2008-09-03 14:28:44]
6. [2008-09-03 14:29:24]
7. [2008-09-03 14:29:57]

IP : 192.168.10.128
MAC : 00-17-31-EB-96-2C

Unknown Data Unknown Data

(b) transmitted packet with session key encryption

Figure 6. MITM attack experiment

V. CONCLUSION

In this paper, we discussed a key establishment protocol which is applicable in wireless mobile environment focusing two properties of wireless mobile communications: short-range communication without prior trust relationship and existence of a human user who can verify the security materials on auxiliary channel between two devices.

We proposed a simple but novel device authentication method and applied it to a well-known Diffie-Hellman key exchange protocol [11]. With our proposed scheme, a user can verify that the shared public keys are identical and the shared secret is presented as a short text message on the visual or audio channel. This method is very easy to use and intuitively perceived by a human user, and can be used to initialize the communicating devices in almost all standard key exchange protocols based on public key cryptography. We also showed the implementation details of the proposed scheme using real mobile devices along with feasible usage scenarios.

REFERENCES

[1] N. Saxena, J. -E. Ekberg, K. Kostiainenm and N. Asokan, “Secure Device Pairing based on a Visual Channel (Short Paper),” In *IEEE Symposium on Security and Privacy (S&P)*, 2006.

[2] D. Balfanz, D. Smetters, P. Stweart, and H. C. Wong, “Talking To Strangers: Authentication in Ad-Hoc Wireless Networks,” In *Network and Distributed System Security Symposium (NDSS)*, Feb, 2002.

[3] F. Stajano and R. J. Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks,” In *Security Protocols Workshop*, 1999.

[4] J. M. Mccune, A. Perrig, and M. K. Reiter, “Seeing-Is-Believing: Using Camera Phones for Human-verifiable Authentication,” In *IEEE Symposium on Security and Privacy*, May, 2005.

[5] J. C. Haartsen, “The Bluetooth Radio System,” In *IEEE Personal Communications Magazine*, pp.28-36, 2000.

[6] L. M. Kohnfelder, “Towards a Practical Public-key Cryptosystem,” B.Sc thesis, MIT Department of Electronical Engineering, 1978.

[7] S. Laur, and K. Nyberg, “Efficient Mutual Data Authentication Using Manually Authenticated Strings,” In *International Conference on Cryptology and Network Security (CANS),* vol.4301, pp.90-107, Springer, 2006.

[8] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, “Loud and Clear: Human-Verifiable Authentication Based on Audio,” In *IEEE International Conference on Distributed Computing Systems (ICDCS),* 2006.

[9] C. Soriente, G. Tsudik, and E. Uzun, “HAPADEP: Human-Assisted Pure Audio Device Pairing,” In *Information Security*, pp.385-400, 2008.

[10] N. Saxena, M. B. Uddin, and J. Voris, “Universal Device Pairing using and Auxiliary Device,” In *Symposium on Usable Privacy and Security (SOUPS)*, 2008.

[11] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” In *IEEE Transactions on Information Theory*, pp.IT-22(6): 644-654, 1976.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, “*Handbook of Applied Cryptograpny,”* CRC Press Series on Discrete Mathematics and its Applications, CRC Press, 1997.

[13] W. Diffie, P. C. van Oorschot and M. J. Wiener, “Authentication and Authenticated Key Exchanges,” In *Designs, Codes and Cryptography*, vol.2, pp.107-125, Kluwer Academi Publishers, 1992.

[14] A. Kumar, N. Saxena, G. Tsudik and E. Uzun, “Caveat Emptor: A Comparative Study of Secure Device Pairing Methods,” In *7th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2009.

[15] E. Uzun, K. Karvonen, and N. Asokan, “Usability Analysis of Secure Pairing Methods,” In *International Workshop on Usable Security (USEC)*, 2007.