Self-authorized Public Key Management for Home Networks

Hyoungshick Kim and S. Jae Oh

Home S/W Platform Team, Software Laboratory, Samsung Electronics
416, Maetan-3Dong, Yeongtong-Gu, Suwon-City, Gyeonggi-Do, Korea 443-742
{hyungsik.kim, sjae.oh}@samsung.com
http://www.samsung.com

Abstract. This paper describes the key management method which allows secure communication channels between devices in home networks. Home network technologies have developed to enable various kinds of home devices to access the digital information between the devices. Without security framework, however, the digital information including a user's private data may be exposed to a malicious attacker. Although conventional public key cryptosystems generally provide security features such as confidentiality and integrity, the distribution of the keys is vulnerable to man-in-the-middle attack without a trusted third party. In general home networks are dynamically set up without relying on any pre-existing infrastructure or central administration. Therefore, we must implement key distribution schemes without the assumption of a trusted third party. In this paper, we present self-authorized public key management for home networks. Our idea is to bind the device owner's authorization information to the public key of a device. Our protocol enables the distribution of the authenticated public key using an identity-based encryption scheme. We also provide heuristic analysis of various security properties.

Keywords: security framework, public key, home network, authorization, identity-based encryption.

1 Introduction

In recent years, the introduction of home networking technologies overcomes the barrier of sharing digital information in home. Consumer appliances such as TV, set-top box, mobile phone and digital camera have become tightly connected to each other through Internet based network connectivity. Many industrial standard organizations such as Digital Living Network Alliance (DLNA) [1], Home Audio-Video Interoperability (HAVi) [2], the Open Services Gateway Initiative (OSGi) [3] and Universal Plug and Play (UPnP) Forum [4] have made significant efforts to develop home network technologies. Home networks promise a major shift in our home. For example, a user watches some movie on the TV screen in the living room where the film is stored in set-top box in the bedroom and it is

M. Denko et al. (Eds.): EUC Workshops 2007, LNCS 4809, pp. 425–434, 2007.

rendered using the software in his children's PC. Without secure communication channel between devices, however, consumers may be skeptical about using the dreamy technologies of enabling the device connection for cooperative services. In particular, when home networks are connected to the Internet, the consumers will face even greater threats from a new class of Internet criminals who are likely to target home networks using Internet access to facilitate mayhem and mischief. Therefore, the security protection of such a networked appliance system will be expected as paramount to all others [13].

There are many security threats and vulnerabilities in home networks. In particular, a home-based wireless network may be more vulnerable to attacks such as eavesdropping without tapping cables since the technology's underlying communication medium, the airwave, is freely open to anyone. While wireless technologies such as IEEE 802.11 have made participating in the online world easier and more convenient, attackers can also intercept or modify the network traffics through the open communication channels. Unauthorized users may gain access to A/V services, corrupt a device's data, consume network bandwidth or capture the user's private information such as credit card number over the networks. Therefore, our work focuses on a wireless network which requires more secure procedures to defend against them.

For securing wireless networks, many solutions have been or are currently being developed. In particular, the IEEE 802.1X and 802.11i specifications identified several services to provide a secure operating environment. The three basic security services defined by IEEE for the wireless LAN environment are as follows [14]:

- Authentication: Authentication is to provide a security service to verify the identities of communicating devices. This provides access control to the network by denying access to client stations that is not authenticated.
- Confidentiality: Confidentiality is to protect the sensitive information against eavesdropping by intruders.
- Integrity: (Message) Integrity is to ensure that messages are not modified in transit between communicating devices.

An easy and secure setup of a wireless connection between communicating devices is a challenging issue in home-based wireless networks due to its characteristics of home users. Home-based wireless devices are usually installed by non-technical consumers and are often left in an insecure configuration due to a lack of knowledge. Effectively securing wireless devices such as router without assistance requires understanding several basic concepts in encryption and networking, and many consumers simply lack any form of training in these disciplines. Also, some consumers do not want to secure their devices since they do not understand the risks associated with an open node, while others understand the risk but judge the risk to be small enough to accept. A problem here is that many consumers do not aware that how the information that they do not protect may be abused due to the complicated impact of the threats. Currently, wireless network security is scarcely applied in a home. More than 80% of wireless network in a home is not using security features since people are having difficulty in configuring AP despite a minimum user interactions such as typing a network identifier or a corresponding secret code [6]. Therefore, an innovative setup of security framework should be provided, which does not require troublesome user interactions and makes it easy to add and remove devices from the network.

In order to provide secure communication channels between devices, the devices must share secret session keys. The main problem is to distribute the session keys over initial networks which have not been securely configured. For the secure key distribution, it may seem strange that another secure channel is required for delivering keys again. Using Diffie-Hellman [19] or some other public key based key exchange [18] for this purpose, the problem of establishing shared keys over an insecure wireless channel is reduced to the problem of preventing a man-in-the-middle attack. In home-based wireless environment, it is possible that attacker can pose itself as a valid home device and participate in creating the secure session channel with other valid devices. The typical man-in-the-middle attack is described in Fig.1.

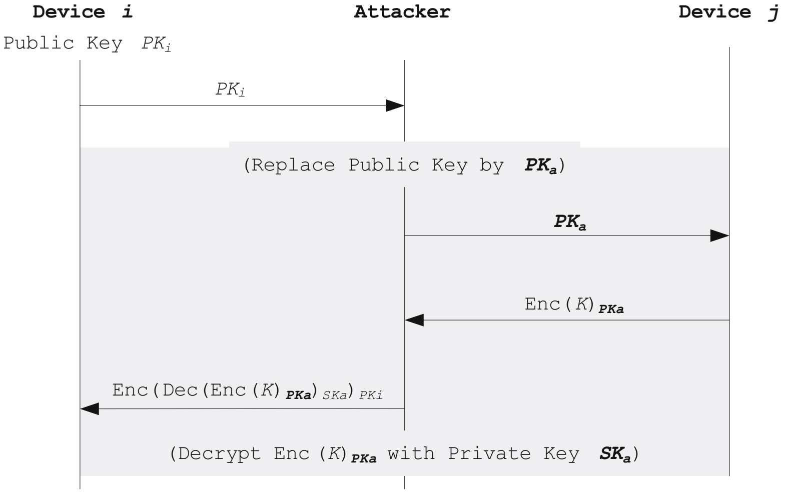
Device i
Attacker
Device j
Public Key PK_i
PK_i
(Replace Public Key by PK_a)
PK_a
Enc(K)$_{PKa}$
Enc(Dec(Enc(K)$_{PKa}$)$_{SKa}$)$_{PKi}$
(Decrypt Enc (K)$_{PKa}$ with Private Key SK_a)

Fig. 1. Public Key Replacement

As shown in Fig.1, the attacker's device intrudes into the communication between the device i and the device j. The attacker captures device i's public key and replaces the public key to the attacker's own public key as an intermediate network node by some method (e.g. DNS spoofing, ARP poisoning, etc).

To solve the above problem, the simplest approach is to use a trusted third party. The authenticated key distribution is achieved with the notion of certificate by a Certificate Authority (CA). For example, TLS [5] typically uses X.509 certificates [20]. In contrast with conventional networks, however, home networks usually do not provide on-line access to CA or to centralized servers due to temporal disconnection to Internet or the limited capability of the client devices. For these reasons, traditional security solutions that require on-line CA or certificate repositories are not well suited for securing home networks. In this paper, we propose a fully self-organized public-key management system that allows home devices to generate their public-private key pairs and then to perform authentication without any centralized services. Furthermore, our approach does not require any trusted third party, not even in the network configuration phase. For this purpose, we assume existence of some out-of-band channel which human operators managed. The detailed information on the manual authentication protocols can be referred to [15][16][17].

In this paper, we propose a key management system using Identity-based encryption (IBE) [8][9][10] without a trusted third party. IBE is a useful tool for this purpose since it reduces the overhead for managing certificates. However, conventional IBE schemes still need a trusted third party for generating private keys and distributing public functions in a secure manner. Therefore we focus on the secure distribution of public parameters in a IBE scheme and the generation of private key without a third party.

To construct the authorized device's identifier, the proposed protocol uses a device owner's authorization information. One concern for this method is that the owner's authorization information is likely to be memorable information. Therefore, we should design the system which is protected against known dictionary attacks as one of our goals [11]. Also, a human operator's interactions must be minimized as much as possible. Our proposed solution enables users to use secure applications over home networks without managing any security mechanism.

The remainder of the paper is structured as follows: In section 2, we describe how the proposal was implemented. In section 3, we present some analysis of the proposed protocol. Finally, we conclude the paper and give an overview of future activities in section 4.

2 Protocol

In this section we propose a system for key establishment over home networks. We assume that there are two types of communication channels in home. The first one is an insecure, but high bandwidth communication channel between devices. In addition to this, a home device and the device owner share the other type channel which is a low bandwidth communication channel over which they can securely exchange the messages with the size of at most l bits. In practice, the human operator manually inputs data to a home device through the devices' input interfaces such as keypad. Operator-to-device transmissions are assumed to be secure.

In secure applications over home networks, devices try to share the common secret key by using two communication channels defined above. Without loss of generality, we assume that the size of the shared key is much bigger than the maximum bandwidth l allowed by the low bandwidth communication channel since the device owner cannot manually inputs many data. Our proposed protocol is based on an IBE scheme for sharing secret key. Before getting into the protocol details, we will first introduce IBE scheme.

2.1 Identity-Based Encryption

An IBE scheme resembles an ordinary public key crypto system, involving a private and a public transformation. Instead of explicit public keys, the public key could be constructed from participant's publicly available information since an arbitrary string may serve as a valid public key. Conventional public keys are authenticated via certificates issued by a trusted certifying authority by binding participants' identities to the explicitly published public keys. The authenticity of the public keys provided by the signature of CA assures that only the entities hold their public keys. Therefore, in a certificate-based system, participants must verify other participants' certificates first before using their public keys. Consequently, a traditional public key crypto system requires a large amount of computing time and storage for managing keys and certificates. Shamir proposed the idea of IBE scheme in 1984 [7], but a practical fully-functional system was not found until recently by Boneh and Franklin [8]. Shortly after that, many identity-based cryptographic protocols were developed. In particular, the protocols based on pairings are currently an area of very active research [9][10].

In an IBE scheme, public key distribution ceases to be a concern since a participant's public key is simply a string that represents its identity. For example, a system has been developed where the email addresses are public keys. In this setting, a sender encrypts a message using a receiver's email address as the public key. Note that this can also be done offline. There is no need to look up, retrieve or verify public keys.

With IBE, the private keys are generally distributed by a trusted third party, often called the Private Key Generator (PKG). No private key can be computed without knowledge of a certain master secret, held only by the PKG. In contrast, public keys can be generated by any participants in the system. In practice, this master secret can be split among several PKGs. In this case, the system is compromised only if every PKG is successfully attacked. The detailed information on key management for IBE can be referred to [8][9].

For home networks, a natural approach based on IBE is to use the combination of the device owner's authorization information and the device identifier as a valid public key. We assume that the device owner holds the secret authorization information such as password for managing the home devices.

The advantages of using IBE to implement home networks layer security are readily apparent. No handshake, exchange of certificates, or verification of certificates is necessary as the devices can simply send a message encrypted with the public key computed using the authorization information in home. In this section, we describe how to construct our system from well-known IBE schemes.

2.2 Protocol Description

We construct the proposed protocol using the IBE scheme which Boneh and Franklin originally devised [8]. They used the bilinear maps relying on the Bilinear-Diffie-Hellman (BDH) assumption and the Random Oracle model [21][22].

For using the IBE scheme, an elliptic curve group G_1 of prime order q and a finite field G_2 of prime order q with a bilinear mapping $e : G_1 \times G_2 \longrightarrow G_2$, the bilinear mapping e and a generator P as the IBE scheme parameters, the master secret key $s_i \in_R \mathbb{Z}_q^*$ and the corresponding master public key $s_i \cdot P$ are embedded in the device i.

A device owner explicitly types a device identifier ID_i or use the default identifier which was initially installed into a device. After typing the device identifier, the owner securely stores the owner's secret authorization information *auth* with the size of l bits such as password in the device as one of authorized devices. The authorization information *auth* is not stored in clear text but $g^{auth \cdot ID_i}$ using a generator g in a cyclic group G_3 of prime order q to protect the owner's authorization information. For constructing common security framework in home, the information *auth* must be identically applied to every device at home.

For exchanging sensitive information between the device i and the device j, a secure communication channel must be firstly created. Without loss of generality, we assume that the device j triggers the protocol. After receiving the request message for creating secure session channel, the device i instantly responses it with the master public key $s_i \cdot P$ and the device identifier ID_i to the device j. In home, these values can be distributed to all home devices through a specific message delivery mechanism such as the discovery protocol in a UPnP network.

After receiving the master public key $s_i \cdot P$ and the device identifier ID_i, the device j checks whether the communicating device is revoked. The device j searches the received device identifier ID_i in the revoked devices list. If the device identifier ID_i is found in the list, the device j stops communicating with the device i since the searched result means that device i is a revoked. Otherwise, the device j randomly chooses a symmetric session key K_{ij} and then computes the unique identifier for the communication with the device i using a random oracle H_1 as follows:

$$Q_{ij} = H_1((g^{auth \cdot ID_j})^{ID_i} || s_i \cdot P) \tag{1}$$

Here $H_1 : \{0,1\}^* \longrightarrow G_1$ is the random oracle and the value $g^{auth \cdot ID_j}$ has been initially stored in the device j. In the next step, the device j computes the mapping result g_i using Q_{ij} as follows:

$$g_i = e(Q_{ij}, s_i \cdot P) \tag{2}$$

The device j encrypts the key K_{ij} using g_i as follows:

$$Enc(K_{ij})_{PK_i} = \langle r \cdot P, K_{ij} \oplus H_2({g_i}^r) \rangle, r \in_R \mathbb{Z}_q^* \tag{3}$$

Here $H_2 : G_2 \longrightarrow \{0,1\}^*$ is the random oracle. Finally the device j sends the encrypted symmetric session key $Enc(K_{ij})_{PK_i}$, the random number r, and the device identifier ID_j through the insecure high bandwidth communication channel.

On receiving the message from the device j, the device i starts to decrypt the session key using the stored $g^{auth \cdot ID_i}$, the master secret s_i and the received message. The device i firstly computes Q_{ij} as follows:

$$Q_{ij} = H_1((g^{auth \cdot ID_i})^{ID_j} || s_i \cdot P) \tag{4}$$

Q_{ij} is clearly computed from the fact that $(g^{auth \cdot ID_j})^{ID_i}$ is the same as $(g^{auth \cdot ID_i})^{ID_j}$ due to the cyclic property of the group G_3. The device i's secret key SK_i is computed as $SK_i = s_i \cdot Q_{ij}$. The server extracts the symmetric session key K_{ij} from $\langle r \cdot P, K_{ij} \oplus H_2({g_i}^r) \rangle$ using the server's secret key $s_i \cdot Q_{ij}$ as follows.

$$Dec(\langle r \cdot P, K_{ij} \oplus H_2({g_i}^r) \rangle)_{SK_i} = K_{ij} \oplus H_2({g_i}^r) \oplus H_2(e(s_i \cdot Q_{ij}, r \cdot P)) \tag{5}$$

By bilinearity property, $H_2(e(s_i \cdot Q_{ij}, r \cdot P))$ is the same as $H_2(e(Q_{ij}, s_i \cdot P)^r)$. That is, the decrypted result is computed as $K_{ij} \oplus H_2({g_i}^r) \oplus H_2({g_i}^r)$. Therefore, the device i and the device j share the symmetric session key K_{ij} and then can securely communicate with each other using the shared session key K_{ij}. In practice, some meaningful text must be appended into the session key K_{ij} to prevent against modification of the messages in the protocol. The device i can verify integrity of the previously received $Enc(K_{ij})_{PK_i}$, r, and ID_j from the device j by checking whether the appended text is regularly decrypted without trouble.

According to circumstances, the device i and the device j may confirm each other's knowledge of the symmetric session key K_{ij}. One way is to exchange the encrypted r with the agreed symmetric session key K_{ij}.

It is intuitive to prove that the proposed protocol is correct in the sense that the participating devices in the construction of a secure communication channel are guaranteed to agree on a common session key if the valid authorization information is predefined by the device owner.

2.3 Revocation

The device owner should be able to revoke a device when it is lost or stolen. In our protocol, the revocation mechanism is very simple and efficient. The owner simply adds the information of revoked device to the revoked devices list without changing the owner's authorization information. The owner explicitly types the revoked device's identifier. This value is added to the revoked device list.

3 Analysis

In this section, we show that the proposed protocol satisfies the security properties in home networks. The general information on the security properties for home networks can be referred to [12].

It may be difficult to show the proposed protocol is formally secure. In general, the formal security analysis requires many assumptions in the context of the adversary models. In general terms, an attacker, who is defined here as a malicious third party interested in subverting communication between home devices i and j, must not be able to obtain the meaningful information of the symmetric session key K_{ij} or the device owner's authorization information $auth$ by observing the messages exchanged during a successful run of the protocol or modifying them. Most requirements are directly satisfied by a cryptographically secure IBE scheme.

For confidentiality, it is apparently impossible to eavesdrop the symmetric session key K_{ij} which is encrypted with the device i's public key PK_i. The secrecy of the key K_{ij} is protected unless the device i's the secret key SK_i is computed. For computing it, an attacker needs the device i's the master secret key s_i. The computational infeasibility of s_i is based under a secure IBE scheme. Also, no useful information about the owner's authorization information $auth$ is revealed during the successful run of the protocol since the computed results with $auth$ as input are not exposed to the attacker. Therefore, the proposed protocol is also secure against the dictionary attack.

For a device authentication, it is apparently impossible to masquerade as a valid home device using an attacker's device. In the view of device i, the attacker cannot compute $Q_{ij}\prime$ in the equation (4) without $g^{auth \cdot ID_i\prime}$, when the attacker wants to forge the master public key $(s_i \cdot P)\prime$ or the device identifier $ID_i\prime$ without regard to the device owner's authorization information $auth$. Also, in the view of device j, the computation of valid $Q_{ij}\prime$ is also impossible without $g^{auth \cdot ID_j\prime}$ in the similar manner. The only attack is to guess the owner's secret authorization information $auth$. In this way, the attacker successfully guesses it with probability $\frac{1}{l}$ when $auth$ is randomly selected. Therefore the attacker cannot intrude into the communication with the construction of secure session channel with valid home devices under some assumptions.

In home environment, however, devices may be corrupted by an attacker since the devices can be lost or stolen. Therefore, we need to consider some additional requirements defined in the group key management protocols [23].

For forward secrecy, it is also impossible to compute SK_i even if an attacker holds the device i's the master secret key s_i. The attacker may try to construct a secure session with other valid home devices through the stolen device. For avoiding the test of revoked devices, the attacker must use a new device identifier ID_a. Given values $g^{auth \cdot ID_i}$, ID_i and ID_a, however, the attacker cannot efficiently compute $g^{auth \cdot ID_a}$ since $g^{auth \cdot ID_i}$ is the same as $(g^{ID_i})^{auth}$. Therefore, it is secure under the assumption of computationally infeasibility to the discrete logarithm problem.

For key Independence, the public-private key pair per session is used instead of group key mechanism. Clearly, this approach is more useful for home environment since sharing of the group key may intrude on a user's privacy.

4 Conclusion

In this paper, we have presented a new security framework based on IBE schemes for home networks.

To construct a secure channel between authorized devices, the proposed protocol provides authenticated key distribution. Our approach, which is based on an IBE scheme, satisfies security requirements for home environment. We generate a valid public key which is associated with the device owner's authorization information. By this way a secure channel can be simply constructed. No other mechanism for authenticating the exchanged public key is necessary while conventional methods need a trusted third party.

We expect that the proposed protocol provides a reasonable level of security against attacks related to applications over home networks. In practice, our proposed protocol can be used for many applications such as e-commerce, home shopping and health care over home networks.

It would be interesting to extend to the construction of secure group communication consisting of n devices. Secure group communication is designed to provide a pool of devices communicating over a public network with a session key. In the future, we plan to investigate how our system can be efficiently extended. We will also investigate a formal security proof of the system.

References

1. DLNA: DLNA Overview and Vision (2006), http://www.dlna.org/en/industry/about/dlna_white_paper_2006.pdf
2. HAVi: HAVi, the A/V digital network revolution (1999), http://www.havi.org/pdf/white.pdf
3. Marples, D., Kriens, P.: The Open Services Gateway Initiative: An Introductory Overview. IEEE Communications Magazine, 110–114 (2001)
4. Miller, B.A., Nixon, T., Tai, C., Wood, M.D.: Home Networking with Universal Plug and Play. IEEE Communications Magazine, 104–109 (2001)
5. Dierks, T., Allen, C.: The TLS Protocol ver. 1.0. RFC 2246 (January 1999), http://www.ietf.org/rfc/rfc2246.txt
6. Tsang, P.: APEC TEL wireless (802.11) security, workshop: Nextsteps. In: APEC TEL Conference (2004)
7. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
8. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Gorantla, M.C., Gangishetti, R., Saxena, A.: A survey on id-based cryptographic primitives. Cryptology ePrint Archive, Report 2005/094 (2005), http://eprint.iacr.org/
10. Dutta, R., Barua, R., Sarkar, P.: Pairing-based cryptographic protocols: A survey. Cryptology ePrint Archive, Report 2004/064 (2004), http://eprint.iacr.org/
11. Jablon, D.P.: Strong Password-Only Authenticated Key Exchange. In: ICM SIGCOMM Computer Communication Review, vol. 26, ACM Press, New York (1996)

12. Ellison, C.M.: Home Network Security. Intel Technology Journal 6 (November 2002), http://developer.intel.com/technology/itj/index.htm
13. Moyer, S., Marples, D., Tsang, S.: A Protocol for Wide-Area Secure Networked Appliance Communication. IEEE Communications Magazine 6, 52–59 (2002)
14. Karygiannis, T., Owens, L.: Draft: Wireless Network Security - 802.11, Bluetooth and Hondheld Devices. USA. National InstiNle of Standards and Tcchnalagy (2002)
15. Gehrmann, C., Mitchell, C.J., Nyberg, K.: Manual authentication for wireless devices. RSA Cryptobytes 7(1), 29–37 (2004)
16. Vaudenay, S.: Secure communications over insecure channels based on short authenticated strings. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 309–326. Springer, Heidelberg (2005)
17. Hoepman, J.-H.: Ephemeral paring on anonymous networks. In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, pp. 101–116. Springer, Heidelberg (2005)
18. Rivest, R.L., Shamir, A., Adleman, L.M.: A Method for Obtaining Digital Signatures and Public-key Cryptosystem. Communications of the ACM 21, 120–126 (1978)
19. Diffie, W., Hellman, M.E.: New Directions in Cryptography. IEEE Transactions on Information Theory IT-22, 644–654 (1976)
20. Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Internet Standard. RFC 2459, The Internet Society (1999)
21. Bellare, M., Rogaway, P.: Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In: Proceedings of ACM CCS 1993 (1993)
22. Canetti, R., Goldreich, O., Halevi, S.: The Random Oracle Methodology, Revisited. In: Proceedings of Symposium on the Theory of Computing, ACM, New York (1998)
23. Kim, Y., Perrig, A., Tsudik, G.: Simple and fault-tolerant key agreement for dynamic collaborative groups. In: Proceedings of ACM CCS 2000 (November 2000)