A Novel Approach for SMS security*

Jongseok Choi and Howon Kim†
*Information Security and System LSI Laboratory,
Computer Engineering Department,
Pusan National University, Busan, Korea*

Abstract

In this paper, we present Common Public Key Cryptography for SMS security. An SMS has two discussions. At the first, an SMS should be monitored by adapted agency or government because it can be abused to crime. Next the SMS increases a double charge in occurrence of communication. For these reasons, our scheme has been designed to fully satisfy the issues. We employed SMS gateways as a trusted third party in our scheme. The SMS gateways fulfill mediator between two users and surveillant. In order to avoid doubled-charge, the scheme uses a common public key rather than personal public key used in PKI. Accordingly, the designed scheme makes users communicate efficiently without sharing or exchanging their unique keys.

Keyword *Mobile Security, Android, SMS, Authentication*

1: Introduction

Recently, many researchers have studied mobile security because the Android and iOS platforms appeal to users around the world. Most researchers who are interested in mobile security[1, 2, 3] have focused on the Android platform [4, 5, 6, 7, 8] because it is based on open sources that anyone can download and modify.

In order to overcome malicious code, it is obvious that we must consider database encryption and a secure protocol or the detection of the malicious code. Numerous schemes for the detection of malicious code on the Android platform have been proposed since it became known that it is possible to insert malicious code into applications. Cerbo et al.[10] proposed a scheme that detected malicious code based on the permissions. However most of the recently developed applications provide users with an SMS and internet as mandatory requirements. As the result, it is becoming more difficult to detect malicious code used as spyware because malicious software is becoming more advanced. Accordingly, many researches[11, 12, 13, 14, 15] have been studied so far.

In this study, we designed a scheme that provides confidentiality and authentication. The designed scheme is based on pairing-based cryptography, which means the scheme uses public key cryptography without a PKI framework. We employed SMS gateways as a trusted third party in our scheme. The SMS gateways fulfill mediator between two users

*This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621).

†Corresponding author

and surveillant. In order to avoid doubled-charge, the scheme use a common public key rather than personal public key used in PKI. Accordingly, the designed scheme make users communicate efficiently without sharing or exchanging their unique keys.

2: Bilinear map

There are two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q. For clarity, we denote $\mathbb{G}_1$ using additive operation and $\mathbb{G}_2$ using multiplicative operation. Somtimes $\mathbb{G}_1$ is also written multiplicatively. We assume that P and Q are two generators of $\mathbb{G}_1$, and the bilinear map used to our scheme has to fully satisfy following properties:

Bilinearity It is satisfactory as following equation.

$$\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*, \qquad \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} \tag{1}$$

Non-Degeneracy If everything maps to the identity, that is obviously not interesting:

$$\forall P \in \mathbb{G}_1, P \neq 0 \Rightarrow \langle \hat{e}(P, P) \rangle = \mathbb{G}_2 \tag{2}$$

Computablility $\hat{e}$ is efficiently computable.

3: Designing Secure SMS

We describe a novel approach to provide a secure SMS.

3.1: Consideration

In order to design the SMS scheme, we considered the properties of an SMS. It possesses two properties. The first property is that it can be monitored. National institutions related to security or criminal investigations often monitor SMSs to apprehend criminals. As a second property, it is one-way communication. If the scheme was designed for two-way communication, this would double the cost. This means a device cannot accept the public keys of another device whenever it wants to send a message; although the device that would like to send a message does not have to request the public key of a target device, it cannot store all of the public keys of other devices.

3.2: A novel approach

We present our approach in this section. As mentioned, there are two issues to design an encryption for an SMS. For these reasons, we employ an SMS gateway as a third party entity to send messages among devices. In our scheme, the SMS gateway can transform messages encrypted by a common public key stored on the devices into messages encrypted by the personal public key of a node without decrypting the messages. Our scheme is composed of initialization and communication phases.

3.2.1: Initialization

This phase generates the parameters needed to authenticate, encrypt, or decrypt messages. Let G_1 be an additive group, G_2 be a multiplicative group, $\hat{e}$ be a bilinear map, $H_1 : \{0,1\}^* \rightarrow G_1$ be a transform map, Φ_i be a unique mobile identification for the device of the i-th user, σ be a secret key for SMS gateways and m be the number of devices registered. We assumed that υ-th user is registered and P is a element of G_1.

Step1 Generates and distributes a common public key.

$$\sigma P \prod_{k=0}^{m} \Phi_k \tag{3}$$

Step2 Generates a private key of υ-th user .

$$\frac{P \prod_{k=0}^{m} \Phi_k}{\Phi_\upsilon} \tag{4}$$

Step3 A mobile device stores the common public key and the private key $\mathcal{K}$.

$$\langle G_1, G_2, \hat{e}, H_1, P, CPK, \mathcal{K} \rangle \tag{5}$$

3.2.2: Communication

This phase is used to send messages. Because of the issues mentioned in the previous section, our scheme stores the common public key that is used to encrypt messages instead of the personal public keys of each of the devices. Let CPK be the common public key and α and β be the cellphone numbers of Alice and Bob, respectively. When Alice wants to send a message, M, to Bob, our scheme performs following steps.

Step1 Alice's device encrypts the message using the common public key, irrespective of who Alice wants to send the message to.

$$C_1 = \hat{e}(H_1(\beta), \frac{CPK}{\Phi_\alpha}) \cdot M \tag{6}$$

Step2 Alice sends the encrypted message and Bob's cellphone number to an SMS gateway.

Step3 The SMS gateway transshapes and forwards the message received from Alice by using the cellphone number included.

$$C_2 = \frac{C_1 \cdot \Phi_\alpha}{\sigma \Phi_\beta} \tag{7}$$

Step4 Upon receiving the message, Bob decrypts it by using his own private key, $\mathcal{K}_\beta$.

$$M = \frac{C_2}{\hat{e}(H_1(\beta), \mathcal{K}_\beta)} \tag{8}$$

4: Analysis

In this section, we analyze the proposed scheme. SMS messages can be monitored based on what we mentioned. In a current SMS, all of the messages can be eavesdropped on by malicious code. Our scheme has been analyzed on two issues.

4.1: Monitoring

In order to monitor messages, SMS gateways can decrypt messages irrespective of the intended recipient. Because of this, our scheme derived the common public key from a secret key of a server and the identifications of all the devices. Note that all of the identifications should be stored at the server or SMS gateways. If a national institution wants to monitor the messages related to a specific user, they can decrypt all of the messages going to that user or coming from him or her. In order to extract a plain text message, they use the server's secret key and all of the identification stored with the cooperating telecommunication corporations.

$$\begin{aligned} M &= \frac{C_1 \cdot \Phi_\alpha}{\hat{e}(H_1(\beta), \sigma P \prod_{k=0}^{m} \Phi_k)} \\ &= \frac{\hat{e}(H_1(\beta), \frac{CPK}{\Phi_\alpha}) \cdot M \cdot \Phi_\alpha}{\hat{e}(H_1(\beta), \sigma P \prod_{k=0}^{m} \Phi_k)} \\ &= \frac{\hat{e}(H_1(\beta), CPK) \cdot M}{\hat{e}(H_1(\beta), \sigma P \prod_{k=0}^{m} \Phi_k)} \end{aligned} \tag{9}$$

4.2: Eavesdropping

In order to eavesdrop on messages, there are two types of attack. The first scenario is to attack it using malicious code. In this scenario, malicious applications have to know the decryption key. However, malware cannot recognize it because the private key is not revealed at any step. In the next scenario, the attacker eavesdrops on sessions: user-gateway or gateway-user. In order to break C_1 in the communication phase, the eavesdropper needs the mobile identification of Alice. This is difficult because the identification is known only to the server and owner. If the adversary wants to break C_2, he/she has to know the server's secret key, σ, and Bob's mobile identification. However, there is no way for the adversary to determine these parameters.

5: Conclusion

In this paper, we designed a scheme that satisfied various considerations. In reviewing these considerations, the first issue was that national laboratories are available to monitor the messages of selected users. The next issue was that an SMS cannot use two-way communication because this would double the cost. The devices that want to send messages cannot request a personal public key whenever they send a message. To overcome these issues, we employed the novel concept of a common public key. This means that all of the devices use the same public key to encrypt messages. However, note that it does not mean that all of the messages are encrypted by the same key. Briefly, our scheme has three points to satisfy the considerations. The first point is encryption. In the encryption process, a device encrypts a message using its own public key derived from the common public key. The next point involves the roles of an SMS gateway. SMS gateways can know all of the messages because all of the keys are produced by mobile identifications that are stored in a server. They transform a sender's public key into the private key of the receiver. The final point is decryption. In the decryption steps, the device can easily decrypt the message by using its own private key stored in the device.

Acknowledge

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621).

References

[1] Chih-Lin Hu and Chien-An Cho, A Novel Mobile Content Delivery Scenario with Simple Double-Key Secure Access Control, IJSIA Vol. 3, No.1, pp1-16 (2009)

[2] Qiang Yan, Robert H. Deng, Yingjiu Li, and Tieyan Li, On the Potential of Limitation-oriented Malware Detection and Prevention Techniques on Mobile Phones, IJSIA Vol. 4, No.1, pp21-30 (2010)

[3] D. Kothandaraman, A. Amuthan, Dr. C. Chellappan and Dr. N. Sreenath, Prevention of Vulnerabilities on Location- based Geocasting and Forwarding Routing Protocol in Mobile Ad-hoc Network, IJSIA Vol. 5, No.1, pp65-76 (2011)

[4] SeungJoon Lee, Min Chul Kim, Yeo Sun Kyung, Kyung Kwon Jung, JooWoong Kim, Yong Gu Lee and Ki Hwan Eom, A Design of U-system for Group Management Using Wireless Sensor Network and Android Device, IJAST, Vol. 35, pp61-72 (2011)

[5] Nae Joung Kwak and Teuk-Seob Song, Joint Tracking and Transmission System for Simulating Motion of the Human Body on Android Smart Phone, IJCA, Vol.4 No.4, pp81-90(2011)

[6] Adrienne Porter Felt, Helen J. Wang, Alexander Moshchuk, Steven Hanna and Erika Chin, Permission re-delegation: attacks and defenses, Proceedings of the 20th USENIX conference on Security, p.22-22(2011);August 08-12, San Francisco, CA

[7] Michael Dietz, Shashi Shekhar, Yuliy Pisetsky, Anhei Shu, and Dan S. Wallach. Quire: Lightweight Provenance for Smart Phone Operating sSstems. In 20th USENIX Security Symposium(2011)

[8] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, and A.-R. Sadeghi, XMAndroid: A New Android Evolution to Mitigate Privilege Escalation Attacks. Technische Universitat Darmstadt, Technical Report TR-2011-04(2011)

[9] New Directions in Cryptography W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, vol.IT-22, pp644654(1976)

[10] Francesco Di Cerbo, Andrea Girardello, Florian Michahelles and Svetlana Voronkova, Detection of Malicious Applications on Android OS, IWCF 2012, LNCS, pp138-149 (2011)

[11] Yuanyuan Zeng, Kang G. Shin and Xin Hu, Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets, University of Michigan, Tech. Rep. CSE-TR-562-10, (2010)

[12] James Brotherston, Colin Hilchey, Kelvin Tsui and George Wang, Implementation of SMS Application with Mutual Authentication and Perfect Forward Secrecy, University of British Columbia, tech. rep. EECE-412-101, (2009)

[13] Aubrey-Derrick Schmidt, Hans-Gunther Schmidt, Jan Clausen, Ahmet Camtepe, and Sahin Albayrak, Enhancing Security of Linux-based Android Devices, In 15th International Linux Kongress (2008)

[14] Collin Mulliner and Charlie Miller, Injecting SMS Messages into Smart Phones for Security Analysis, In Proceedings of the 3rd USENIX Workshop on Offensive Technologies (WOOT) (2009)

[15] Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, and Marcel Winandy, Privilege Escalation Attacks on Android, In Proceedings of the 13th information Security Conference(ISC'10) (2010)

Jongseok Choi

He is currently a master's candidate in the Computer Engineering Department, Pusan National University. He received B.S. in Information Security, Tongmyong University, Republic of Korea, in 2011. His researches include mobile security, privacy, public key cryptography.

Howon Kim

received the BSEE degree from Kyungpook National University, Daegu, Rep. of Korea, in 1993, and the MS and PhD degrees in electronic and electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Rep. of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Rep. of Korea. He is currently working as an assistant professor with the Department of Computer Engineering of Pusan National University, Busan, Rep. of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems and their security issues. He is a member of the IEEE, IEEE Computer Society, and IACR