A Secure and Efficient Application Download Architecture in 3G Mobile Environment

Chin-Ta Lin[1], Kuo-Zhe Chiou[2], Jheng-Hong Tu[2], Hsi-Chung Lin[2], and Sung-Ming Yen[2]

[1] Networks and Multimedia Institute Technology Service Center, Institute for Information Industry, Taipei 106, Taiwan, R.O.C.
cheetah@nmi.iii.org.tw
[2] Laboratory of Cryptography and Information Security (LCIS), Dept of Computer Science and Information Engineering, National Central University, Chung-Li 320, Taiwan, R.O.C.
{kzchiou, 945202043, hclin, yensm}@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/

摘要

由於第三代行動通訊的技術提升，使得第三代行動手機受到廣泛的使用。由於其高頻寬的傳輸能力，使得電信業者相繼地提供高傳輸和高品質的行動服務。不過，如果要取得該項服務，電信用戶往往需要經過復雜的程序來安裝相關的應用軟體。因此，我們提出一個有效率且安全的應用軟體下載的架構。透過此架構，電信用戶可以隨時隨地而且方便地下載該項服務的應用軟體。

關鍵詞：第三代行動通訊，用戶通用辨識模組卡，應用軟體下載，行動商務。

Abstract

The 3rd generation (3G) UMTS mobile system has been widely used because of its advances in telecommunication technology. Due to its high-speed transmission capability, numerous high speed and high quality services are (and will be) provided based on 3G mobile system. However, the subscribers need to download and install new service programs before enjoying the numerous applications. In this paper, an efficient and secure application download architecture is proposed. By employing this architecture, the subscribers can securely download new applications and install them anytime and anywhere.

Keywords: 3G mobile environment, USIM card, Application download, M-commerce.

1. Introduction

Along with the tremendous development of mobile environment, the widespread adoption of mobile devices, especially mobile phone, has paved the way for the development of many innovative mobile services. Today most people never leave home without their mobile phone. Its storage, computation, and transmission capabilities make it an ideal device for the purposes of communication and purchase. So, m-commerce intrigues many ISPs to provide various mobile services, e.g. emome [9] and i-mode [10].

Now, it was widely thought that the next generation of mobile phone technology, 3rd generation (3G) UMTS mobile system, would be the pre-eminent mobile services platform. Because it has high-speed transmission capability and supports the 3G and wireless channel, the 3G mobile phone offers the subscriber unparalleled speed and quality services, including video watching, e-mail/news transmission, games/music downloading, mobile payment, and so on.

Although the transmission capability of the 3G mobile phone facilitates the data transmission between the server and mobile phone, the security issues on Internet also challenge the mobile environment. For example, how to prevent a subscriber from downloading the application program with viruses, worms, and Trojan Horses? How to protect privacy information from being stolen? A secure download protocol or mechanism is always required to solve the problems.

1.1 The security issues in 3G mobile environment

When the subscriber would like to enjoy the mobile service, his mobile phone has to install the related applications to communicate with the server. The application can be classified into program and applet. The program is run on the mobile phone platform. For example, the media player for watching video, the outlook application for receiving/sending e-mail, and the IE browser for looking stock information. However, there are some security issues in the platform of mobile phone. The platform provides the basic environment for running application. Unfortunately, many manufactures of mobile phone always fail to provide the basic features

for secure computing, including memory protection for processes, file access control, and authentication of resource. A malicious program is possibly installed in the mobile phone and it can influence directly operation system or control other applications to be executed incorrectly. Moreover, if the mobile phone is loss, any one who picks it up can arbitrarily read any information in the phone. Therefore, it is inappropriate to keep critical program, private information, and secret key in the platform.

The applet is also a program but executed in the USIM card in 3G mobile phone. The applet is always a critical program such as electronic wallet that requires high secure execution environment. So, the USIM card is a appropriate choice. The USIM card is a secure device that it not only supports cryptographic computation but also can protect secret information from being stolen. Moreover, only the manufactures or an authenticated entity can read/write secret data and install an applet into USIM card by sending APDU command [11]. Therefore, it is reasonable to use the USIM card to handle this kind of program and secret data.

If the subscriber would like to enjoy new service, he has to install the corresponding application. It is easy to design an application download approach to get the program and install it in the mobile phone. However, it is difficulty to give a fine solution to install an applet in the USIM card. The applet installation procedure, defined in [11], is done by sending sequent APDU commands for authenticating the outside entity. But in the mobile environment, the outside entity is the mobile phone which is an insecure platform. As a result, it seems impossible to install an applet in the USIM card because it can not delegate or give directly the installation right to the mobile phone.

One possible solution could be the following scenario that the mobile phone just transmits the package of APDU command between the server and the USIM card. In other words, just let the server send APDU commend to the card directly via the assistance of the mobile phone. However, it has to assume that the executed application is trusted that it does not modify the content of APDU command and does not reveal any useful information to the potential adversary. According to the above security discussion on mobile phone platform, the assumption is unreasonable.

The other possible solution is to use OTA mechanism [7][8] that it can dynamically update the application list menu in the USIM card and download and set up the general program in mobile phone. However, the mechanism has high computation cost because of PKI is involved.

1.2 Contribution and Organization of the Paper

In this paper, a new application download architecture is proposed, which adopts the improved EKE protocol and a new applet installation procedure. By the improvement EKE protocol, the subscriber download efficiently and securely the application. Moreover, the new applet installation procedure also allows the USIM card to securely set up an applet sent from mobile phone.

The rest of this paper is organized as follows. In Section 2, the overview and the security issues of the proposed architecture are provided. Then the Section 3 and 4 provide the detailed introduction and security analysis, respectively. Finally, the conclusion is given in Section 5.

2. Overview of the Proposed Architecture

There are five roles and two protocols in the proposed application download architecture. The roles contain Internet Service Provider (ISP), the application download server, 3G mobile phone, download agent (DA), and USIM card. The two protocols are DA download protocol and application download protocol.

Initially, the subscriber has to register to the ISP to establish an account (phone number) and a password. This register information is also sent to the server by the ISP. Next, the subscriber downloads and installs the DA in the mobile phone via DA download protocol. Then, he can launch the DA to execute application download protocol to get application. If the application is the applet, its signature should also be downloaded for installing the applet in the USIM card using the new applet installation procedure.

The security issues including requirements and assumptions are given in the following.

- ISP

  ISP is the company that provides communication and Internet/mobile service for user. When a subscriber requests any service, he has to first register to the ISP for sharing his account (phone number) and the password selected by himself. Therefore, we believe that the ISP
  - does not reveal the register information of the subscriber to others.
  - always provides correct service to the subscriber.
- Application download server

  Application download server managed by the ISP is the machine that provides the application of service. The ISP or the service provider such as shop can provide their application. After checking the application without virus, worms, and Trojan Horses, the ISP signs on them and keeps these signatures in the server. Moreover, the server also keeps the register information of the subscriber. Therefore, we reasonably assume that the server
  - does not reveal the register information of the subscriber to others.
  - always provides the valid and correct application to the subscriber.
- Mobile phone

In our design, we assume reasonably that the operating system, JVM environment, and basic applications such as WAP browser in the mobile phone can be trusted. However, the mobile phone is an open and insecure platform. The important information such as password and secret key should not be kept in the phone. Therefore, no useful information will be exposed from the phone.

- USIM card
  The USIM card is a tamper-resistant device that can protect all important information. In addition, it has Java card capability to not only execute cryptographic operations but also run the applets. In the proposed architecture, it requires the USIM card to support the proposed applet installation procedure (detailed in Section 4) and has initially the certificate of ISP for verifying the signatures on the applet.
- Download agent
  In the proposed architecture, we assume that the mobile phone does not have the DA initially. Therefore, the subscriber has to launch DA application protocol to obtain it. The DA supports the cryptographic computation and the main functionalities of the DA are to download application from the server. If the application is a general program, then it is set up in the mobile phone. But if it is the applet, it is installed in the USIM card.
- DA and application download protocol
  In the architecture, there are two important download protocols. One is DA download protocol for downloading DA. If the update of DA is needed, this protocol also can realize it. The other one is application download protocol for obtaining the application of service. In the consideration of security, DA and applications should be obtained via a secure way. Therefore, the protocols have to be able to defend against various attacks [2][3] and achieve the security requirements, entity authentication and data confidentiality. In consideration of efficiency, the application download protocol will be executed frequently. Therefore, low computation cost is the main design purpose.

3. The Proposed Application Download Architecture

In the proposed application download architecture (see Figure.1), there are four procedures, including Register, DA Download, Application Download, and Applet Install.

In our architecture, when subscribing the ISP, the subscriber is required to complete the two procedure, register and DA download. The former procedure requires the subscriber, the ISP, and the server to share an account and the password and the DA can be obtained and set up through the latter procedure. Then, the subscriber can start to download the application that he expects from the server by launching application download protocol. If an applet is required by the subscriber, it will be sent to USIM card via the designed mechanism by using secure messaging.

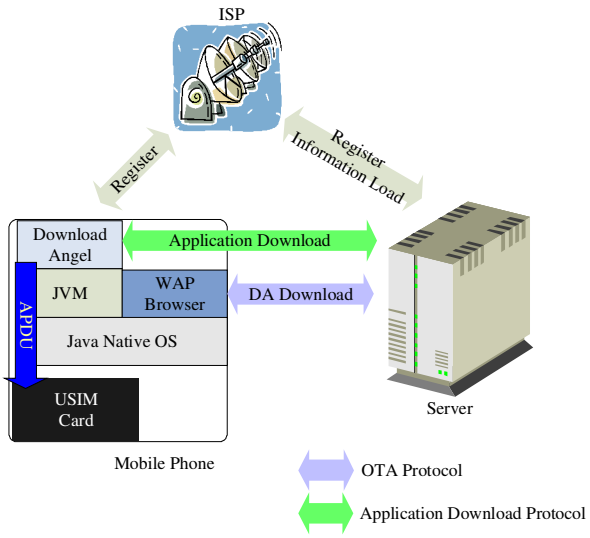

Figure 1: The application download architecture

The following content will provide the detailed introduction to our architecture.

3.1 Register

The main purpose of the register procedure is to share an account and a password among the subscriber, the ISP, and the server. This procedure is separated into two steps. The first step is to require the subscriber to register to the ISP through web on Internet. Then the subscriber and the ISP share an account (usually it is the phone number) and a password. To keep the register information secure, SSL can be adopted to protect transmission channel. The second step is that the ISP stores the register information in the server under secure channel.

3.2 DA download

Initially, the mobile phone is possessed of not only OS and basic application but also JVM environment, WAP browser application, and the certificate of ISP. By launching WAP browser, the subscriber can download the DA via OTA protocol. OTA is a mobile technique that allows the subscriber to download and install the application via 3G and wireless. There are totally five rounds in the OTA protocol (see the figure. 2).

The first two rounds are to download the application list provided by the server. The list which is formed by JAD will guide the subscriber to get the application DA (formed as MIDlet Suite JAR) in the

third and fourth rounds. Note that the corresponding signature of the ISP should be downloaded together to ensuring the application is provided by ISP. Then WAP browser will check the validity of the application by verifying the signature (the public key of the ISP can be derived from the certificate). Finally, the WAP browser responses the installation result. In our architecture, hence, DA can be obtained securely by the above approach.

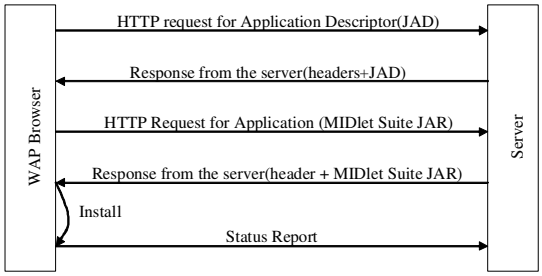

Figure 2: The OTA protocol

3.3 Application download

After setting up the DA, the subscriber can get service from the server by launching the DA to execute the application download protocol. The EKE [1] is a password-based protocol with low computation cost and high security. Unfortunately, we found that it is vulnerable to the parallel session attack (see Appendix. A). To overcome this disadvantage, we propose an improved EKE protocol by which a secure application download protocol will be developed. The detailed description of the protocol is given as follows. (The definition of notations are the same as in [1]).

(1). The DA first decides the private key SK under probabilistic encryption algorithm (e.g. ElGamal [4]), and calculates the corresponding public key PK. Then it asks the subscriber to input his password (PW for short). To encrypt PK under symmetric encryption algorithm (e.g. DES [5], AES [6]). Then the DA sends

$$E_{PW}(PK),\ ID_{sub} \qquad \text{(E.1)}$$

to the server, where ID_{sub} means the account of the subscriber.

(2). When receiving E.1, the server decrypts it by using PW of the subscriber to get PK and selects a random number K randomly as the session key. Then the server sends

$$E_{PW}(PK(K,\ ID_{server})) \qquad \text{(E.2)}$$

to the DA.

(3). The DA will try to use PW and SK to derive ID_{server} from E.2 to ensure the identity of the server. Then he encrypts N_{DA} with the obtained K, where N_{DA} is a number chosen randomly by the DA. Therefore, the message sent from the DA to the server is

$$E_K(N_{DA}) \qquad \text{(E.3)}$$

(4). After obtaining N_{DA} by decrypting E.3, the server also selects a random number N_{server} and then responds

$$E_K(N_{DA},\ N_{server}) \qquad \text{(E.4)}$$

to the DA.

(5). Finally, after ensuring the N_{DA} in E.3 and E.4 is the same one, the DA give

$$E_K(N_{server}) \qquad \text{(E.5)}$$

to the server.

If the server can derive N_{server} correctly from E.5, then the server starts to send the DA the application which is encrypted with key K.

3.4 Applet install

In [11], Secure messaging (SM) is achieved by applying one or more mechanisms and it defines many various cryptographic primitives (or called SM data object) such as cryptographic checksum, public key, digital signature, and so on. The data filed in SM format (called SM field) in APDU command or response is reserved for SM data objects. Therefore, an APDU command and response with SM field can fulfill certain security mechanism. In the proposed architecture, the OS of USIM card has to support the following applet installation functionality. An APDU command is used to require the card to install an applet. The SM field in the command must include the applet and the corresponding signature. When receiving the command, the card OS is able to parsing it and then verify the signature. By the verification, the OS can ensure the source is the ISP and the validity of applet is guaranteed. Accordingly, the OS then changes the security status of DF in the card for installing the applet. Note that, because the signature verification is required, the USIM card should have initially the certificate of ISP and the signature on applet should be downloaded together with the applet in application download procedure.

4. Security Analysis

It is implicit in our security issues that the proposed architecture does not leak any useful information to a potential adversary. That is, it should not keep important information in the mobile phone platform and the download protocol should achieve the defined security requirements and can defend against various attacks.

It is obvious that because the mobile phone does not keep any important information, including password and secret key, it is impossible to expose the information from the mobile phone.

In the DA download procedure, the mobile phone launches WAP browser to get the DA. Because this procedure is realized by the OTA protocol, the DA can be downloaded and set up securely. Here the security requirement of data confidentiality can be ignored because the DA could be a public application. So it can be transmitted in the clear.

In the application download procedure, the improved EKE protocol is used to download

application. The protocol inherits the design conception of the original EKE protocol. Mutual entity authentication and key confirmation is still achieved. Moreover, the improved KEK protocol is secure. On the one hand, the identity of the server is involved and protected in E.2, the attacker can not impersonate the server to respond $E_{PW}(PK(K, ID_{server}))$ to the DA without knowing *PK and PW*. Therefore, the improved KEK protocol can defend against parallel session attack. On the other hand, although the fixed information, the identity of the server ID_{server}, is involved, the improved protocol is still against offline dictionary attack, replay attack, man-in-the-middle attack, and reflection attack are still prevented. The detailed explanation is given as follows. First, the attacker can try to guess a password *PW'*, and then derives *PK'* from E.1 (but it is computational infeasible to obtain the corresponding SK'). We assume the attacker is also aware of session key *K* luckily and ID_{server} is public and fixed information. Then he can compare $E_{PW'}(PK'(K, ID_{server}))$ with E.2. If the result of comparison is identical, then the attacker obtains the correct password. However, because *PK'*(.) is probabilistic encryption algorithm, the attacker can not obtain the same ciphertext, even the encrypted message is the same. In other words, $PK'(K, ID_{server})$ can not be the comparison basis. Therefore, the improved protocol is still against offline dictionary attack. Besides, it is obvious that the protocol also can defend against replay attack, man-in-the-middle attack, and reflection attack.

To sum up, the proposed application download architecture is secure because no useful information is revealed from the mobile phone and the two download protocols.

5. Conclusion

Because of the capability of 3G mobile system, more and more mobile high quality services are provided constantly. For getting new services, the subscriber has to set up the corresponding application (program or applet) in the mobile phone or the USIM card. In this paper, a secure application download architecture is proposed by which the subscriber can employ the 3G mobile phone to download the desired applications. According to our analysis, the proposed architecture achieves high performance and security.

References

[1] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," Proceedings of the IEEE Symposium on Security and Privacy, pp.72-84, 1992.

[2] D. Dolev and A.C. Yao, "On the Security of Public Key Protocols," IEEE 22nd Annual Symposium on Foundations of Computer Science, pp.350-357, 1981.

[3] W. Mao, "Modern Cryptography - Theory and Practice," First Edition, Prentice-Hall PTR, 2004.

[4] T. ElGamal, "A Public-key Cryptosystem and A Signature Scheme based on Discrete Logarithms," IEEE Transactions on Information Theory, IT-31, No.4, pp. 469-472, 1985.

[5] National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, 1977.

[6] NIST, "FIPS-197: Advanced Encryption Standard," Federal Information Processing Standard, FIPS-197, 2001.

[7] Introduction to OTA Application Provisioning, available at: http://developers.sun.com/techtopics /mobility/midp/articles/ota/index.html.

[8] MIDP2.0 (JSR-118), available at : http://java.sun.com/products/midp/index.jsp

[9] The emome of Chunghwa Telecom, available at: http://www.emome.net/cgi-bin/MASP/jsp/emome Web/index.jsp

[10] The i-mode of FarEastone, available at: http://www.imode.net.tw/

[11] ISO/IEC-7816-4 2005, available at: http://www.iso.ch/iso/en/ISOOnline.frontpage.

Appendix A

In this appendix, we show that EKE protocol is vulnerable to parallel session attack by breaking the security requirement: mutual entity authentication.

The detailed attack process is given in Figure.3.

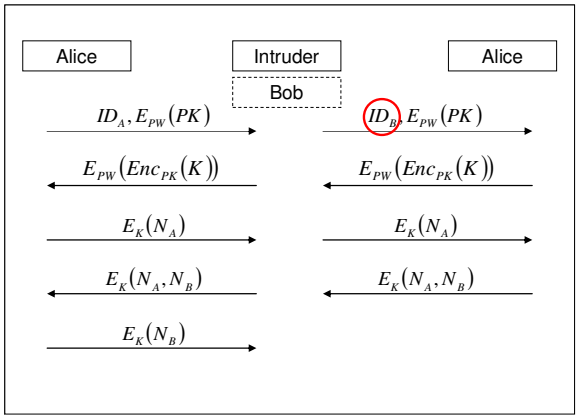

Figure: 3 The parallel session attack on EKE protocol

When Alice tries to communicate with Bob, she sends the first message to Bob. But this massage may be intercepted by the intruder, and then the intruder responds Bob with the same message but ID_A is replaced by ID_B (the identity of Bob). The intruder then can impersonate Bob to communicate with Alice. In other words, there are two communication sessions. The first one is that Alice tries to talk with Bob but the all messages sent from Alice are intercepted by the

intruder. The other one is that the intruder impersonates Bob to talk with Alice. This forms the parallel session attack that besides the first round, the intruder just resends Alice the received message from Alice. Because all the transmission messages are generated by Alice, she can decrypt them correctly. Finally, Alice will believe that she is talking to Bob, but indeed she is talking to the intruder.