Research on Secure Payment Model Based on Improved AKA Protocol

Ying Wang
School of Software & Communication Engineering,
Jiangxi University of Finance & Economics, Nanchang, China
esp_net@163.com

Keywords: ESP-AKA, Secure Payment, ATM Network
Abstract. Mobile payment is the core application of mobile terminals such as smart mobile phone, PDAs or notebook computers via SMS, WAP or RFID for shopping, paying bills, bank transfer and other business activities. Research of security issue is very important for the development of mobile payment system. In this paper, an enhanced mobile communication security system model for mobile payment is proposed by study of EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement) protocol. Safety transmission of authentication vector signals is protected by this model to build a security core network for terminal transactions. Security mechanism of end to end terminal business have discussed in the following parts of this paper.

Introduction

The current mobile communications networks such as GSM to provide certain security features, support one-way user authentication for protection of the confidentiality of communication data, but there are still some flaws. Mobile network insecurity directly results in an unsafe mobile terminal business. The business operations constructed on current mobile communication network maintain its security from two aspects. One is entirely rely on mobile network authentication and key distribution mechanism by checking the MSISDN number from SIM card in user mobile terminal to authenticate the user's identity. Another is using a complex password system on the application level to provide security for the business, such as WAP, J2ME etc. The first approach cannot provide high level security for large payment because of the natural defects of AKA (algorithm deficiencies, only one-way authentication, the key is too short, etc.) Due to restrictions on mobile devices (small memory, low processing capability and difficult to carry out complex input operations, etc.), the security mechanism of second approach is restricted by terminal hardware.

Currently, next-generation communication networks (3G/4G) are gradually developed. The 3rd Generation Partnership Project (3GPP) security standards in WCDMA have been greatly improved than GSM. 3GPP AKA mechanism has some new features such as support mutual authentication to prevent false base station attack, provide data integrity protection, more open and secure encryption algorithm and longer key. These series of measures greatly improve the security of the 3G/4G mobile communication networks. By researching of wireless communication security mechanism and terminal business, an enhanced model of core network security and a mobile terminal security mechanism are proposed in this paper.

Mobile communication security model based on AKA Protocol and ATM network

The process of AKA protocol in GSM wireless communication is shown in Figure 1. In the process, the SIM card in the mobile terminal and the AuC of network side shared secret key Ki. Challenge/Response policy implement the network-side certificate authentication on the user's identity, while simultaneously generate session encryption key Kc.

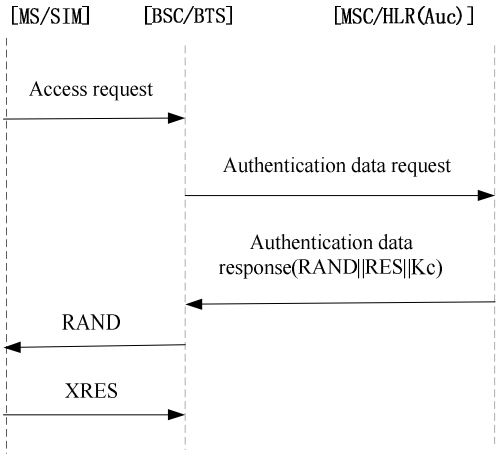

Figure 1. AKA process in GSM

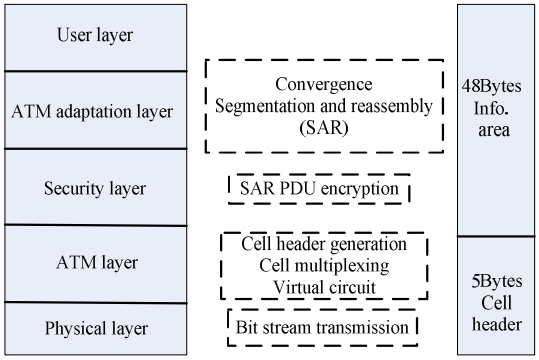

Figure 2. ATM Network Security

Fake base station attack can be launched in this security mechanism. The attack will fail if the user's business information is encrypted with key Kc. But if the communication between the core network domain BSC / BTS and the MSC / HLR is tapped, the terminal services could not guarantee the security because of the risk of fake user's attack.

Wireless access in the WCDMA network in the AKA protocol, 3GPP Although many AKA protocols enhanced security, such as two-way authentication, to prevent the false base station attacks, more secure cryptographic algorithm, encryption keys longer, but the attacker can Mobile communication system by attacking the core of the network, certified vector. Therefore, in order to build mobile business security, need to strengthen the core of mobile communication system network security, security

Current mobile communication systems have high-speed transmission and switching, voice, data, video information on a variety of different types of business features, so you can use ATM technology to build a core network of mobile communication system. When the information carrier in the ATM network, in particular the transfer of authentication vectors such as signaling the above, the need to protect the security of information, prevent information leakage and tampering, recognized the legitimacy of sources of information. Therefore, the formation of the ATM network to provide the following security functions: data encryption, integrity checking, authentication, access control and anti-denial.

ATM protocol stack can be divided into four layers: physical layer, ATM layer, ATM adaptation layer, the user layer. The program is built on this basis, a security model, as shown in Figure 2, the program in the ATM layer and ATM adaptation layer to add a security layer between the security layer primarily by the ATM adaptation layer to complete the dismantling of the user layer of business information package SAR-PDU encryption and integrity check value generated and then passed to the ATM layer a cell header to implement ATM cell encapsulation for routing, transmission; on the ATM layer cell transfer to decrypt and integrity checking, ATM adaptation layer for users to submit business information convergence.

In this model, security level of the adjacent layer of transparent, easy to implement. Security mechanism is a fixed size SAR-PDU to operate, but also for the ATM cell header information exchange at the ATM layer is added, so the SAR-PDU can be encrypted. In addition, ATM networks may be missing cell, thus achieving the safety of ATM networks, synchronization as a basic requirement also need to consider, in the same layer of security and encryption layer to provide synchronization to avoid dealing with different layers on them, and synchronization and integrity of the testing will help reduce overhead combined to achieve mobile communications network system security requirements of ATM networks.

Security mechanism of terminal business

For General business, security issue involves at least three aspects: confidentiality, integrity and personal identification. In GSM and WCDMA security standard, only confidentiality protections of user data are provided. Therefore, the terminal operational security mechanisms, the need to consider how to provide integrity protection of business data users. The question for operational security model for mobile terminal shown in Figure 3. In the figure, through the security point of business services (SSA), mobile communication system for mobile terminals to provide secure end to end business services. When the mobile service provider, or MS / SIM request of either party of a security business services, security, business service point for mobile terminals start enhanced authentication and key distribution protocol (AKA), the agreement process is as follows:

① SSA->SIM: RAND； ② SIM->SSA:XRES||SessionRAND;

According to AKA agreement, AuC and the mobile terminals to share a secret key Ki, when the security point of business services need to authenticate mobile terminal, the security business service point request to the AuC Authentication vector, so MS / SIM and security, business services, this point can be respectively second authentication session key Kc, the security business service point of the MS / SIM authentication is completed, the security business service point, and MS / SIM simultaneously generate this encryption key security and integrity of business verification key; security business services point of these two key mobile service providers through the establishment of a secure channel of cable distributed mobile service provider, after the business session, the mobile terminals and mobile service providers directly with the key CK, IK session information to achieve confidentiality, integrity, and thus the establishment of an end-to-end business model.

The model implicit validation of the network side, an effective attack against the pseudo-base impact. Security operations in each session, the mobile terminal and security operations through shared services, dynamic key points of the random numbers generated by mobile terminals to conduct certain operations SessionRAND produce the session key (encrypted secret key CK and integrity check key IK), if false base station attack, unable to get CK, IK, also not informed of the user's business information.

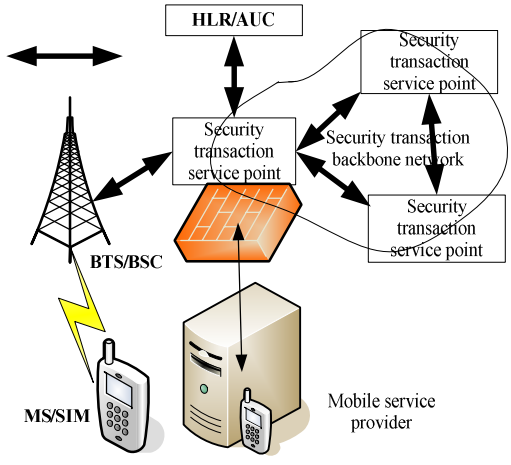

Figure 3. Mobile terminal security model

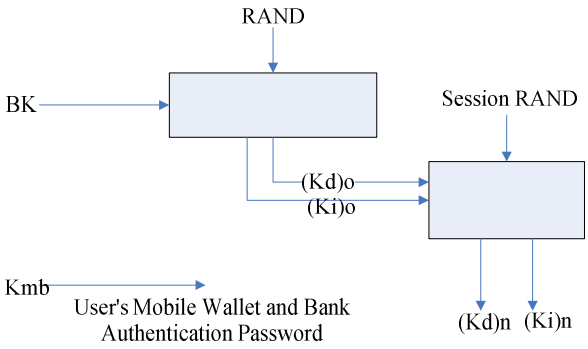

Figure 4. Relationships between terminal and bank

Security policy in mobile payment scheme

Confidentiality and integrity include the security of the information transmitted from the mobile terminal to the merchant, the mobile terminal to the issuer's two logical links. The mobile terminal to

the merchant's security logic chain is proposed to guarantee the terminal business security mechanism.

The mobile terminal and the bank share a secret static root key BK, and the session key is generated dynamically according to the random number generated by each payment service. The mobile terminal has a key in the service session with the issuing bank.

BK: root key, used to send the card and the mobile wallet to share the static root key, the root key to generate a dynamic session key, the root key in the card to write SIM card;

Kd, Ki: together is called dynamic session keys, one for the protection of the confidentiality of data, one for the protection of the integrity of the data, and the user mobile phone wallet and issuer server and in and re synchronization register; each transaction in the future, the random number through the dynamic key encryption this session, the new key as a new dynamic session key and update the user mobile phone and wallet card issuer server central session key;

Kmb: the user mobile phone wallet with the issuer server shared authentication key, the issuing bank generated by the key MAC code of user authentication, can be updated on-line by the user through the mobile phone and wallet card issuer server;

The relationship between the keys is shown in Figure 4. Kd generated by the user's mobile wallet and Ki generated by the issuing bank server Synchronously, if not consistent, use a timestamp based resynchronization strategy for resynchronization.

Conclusions

By presents an enhanced core network security in mobile communication system model, security authentication vector signaling in the core network transmission, build a secure mobile communication core network terminal service security mechanism. Using the improved AKA protocol for wireless access in mobile communication systems, an end-to-end mobile terminal security mechanism is proposed. According to the security mechanism of mobile terminal business, a secure and reliable mobile payment scheme is proposed according to the characteristics of mobile payment which can greatly improve the security of mobile payment consumer confidence.

Acknowledgements

This work was financially supported by the Jiangxi social science research project of 2010 (10TW13). The authors are grateful for the anonymous reviewers who made constructive comments.

References

[1] SETco:SET Secure Electronic Transaction Specification Book 1:Business Description，http://www.setco.org

[2] 3G TS 133.120.3G Security: Security Architecture, Version 3.6.0, October 2000.

[3] ETSI/SAGE Specification, v1.0-1999, Specification of 3GPP confidentiality and integrity algorithm, part1: f8and f9 specifications[S] , part2: KASUMI specifications[S].

[4] 3GPP TS33. 401. 3rd Generation Partnership Project. Technical Specification Group Service and System Aspects. 3GPP System Architecture Evolution/Security Architecture. (Release 12) [R], 2014: 45-78.

[5] ATM Forum(1996) phase 1,ATM Security Specification[R].

[6] Purkhiabani M, Salahi A. Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks. Proc[C]// IEEE 3rd International Conference on Communication Software and Networks (CCSN),2011:557-563.

[7] Li X, Wang Y. Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network[C]‖ Proc. Wireless Communications, Networking and Mobile Computing,2011: 1-4.