published as: Ge Zhang, Feng Cheng, Christoph Meinel: Towards Secure Mobile Payment Based on SIP.
IEEE Press, Belfast, Northern Ireland, UK, March 2008, pp. 96 - 104, ISBN: 978-0-7695-3141-0;
15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems

Towards Secure Mobile Payment Based On SIP

Ge Zhang, Feng Cheng, Christoph Meinel
Hasso Plattner Institute, University of Potsdam, Germany
{ge.zhang, feng.cheng, christoph.meinel}@hpi.uni-potsdam.de

Abstract

Mobile payment has some unique advantages over more traditional payment methods in, for example, TV shopping and mobile multimedia services. Unfortunately, most existing mobile payment solutions rely heavily on underlying communication infrastructures, which are platform-dependent and have no unified implementation criteria. This limitation is reducing, however, through the rapid spread of the Voice over IP (VoIP) telephony service and its integration with mobile phones. The Session Initiation Protocol (SIP) is currently the standard signalling protocol of VoIP. Mobile payment is expected to be implemented and deployed in an SIP environment in order to keep pace with the evolution of the mobile phone network. The goal of this paper is firstly to propose a new mobile payment scheme based on SIP. The protocol of the proposed framework is thoroughly analysed. Secondly, we evaluate security issues and propose enhanced solutions to make this new framework applicable in practise.

1. Introduction

During the last few decades, mobile phone becomes an indispensable communication tool so that almost every person owns at least one. Being popular and easy-to-use, the application of mobile phone can be further extended from a simple telecommunication terminal to other commercial function. We have witnessed the successful integration of video games, stock exchanges and internet browsing into mobile phones. Furthermore, a payment method using mobile phone also appears in the world. Mobile payment (MP) is defined in [1]: “Any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment can be considered as a mobile payment.”

MP can be seen as an alternative of traditional credit/debit card. It is especially beneficial for those people who do not have a credit card. For example, users of Nonoh (a VoIP service vendor [2]) can simply buy credits for their Nonoh account by sending special text messages using their mobile phones. Besides, MP is also more competitive in some special scenarios. In its latest report, Juniper Research predicts that MP will achieve a volume of approximately USD 22 billion by 2009 [3]. However, promising as it seems, there are still a lot of problems to prevent the popularity of MP, which have been its critical bottleneck. First of all, the implementation of high security protection on MP is not an easy task. MP security includes not only authentication, confidentiality and integrity, but also non-repudiation and privacy. Current mobile infrastructures with low bandwidth and limited processing capability are insufficient to achieve all of these security criteria. Secondly, convenience is another important issue. MP users expect their service to be available at any time, in any place. For this purpose, as an electronic device, mobile phone needs more additional support than cash or credit card (e.g., battery power and wireless signal intensity). Otherwise, it is easy to be out of service. Thirdly, additional expense has to be spent on MP service integration. For example, users may need to buy special mobile phones which support the MP function. In a word, the characteristics of high-security, low-cost and convenience, which are key factors to make MP more usable [4], cannot be easily achieved by traditional mobile phone infrastructures.

On the other hand, the evolution of mobile network creates a new platform for MP. VoIP telephony, with its benefits, such as low-cost and easy-to-extend, will be widely employed in the future. According to an advisory firm’s analyst report [5], there will be more than 250 million VoIP users over mobile networks by 2012. Since the MP is an application totally carried over mobile network, existing MP mechanism is no longer suitable for the next generation mobile network. As a result, it makes sense to implement an innovative MP scheme to support new platform. Driven by this idea, we will design a MP model based on SIP [6], which is one of the mainstream VoIP signaling protocol. Besides the tendency, SIP with its infrastructures provides an open and flexible context to

978-0-7695-3141-0/08 $25.00 © 2008 IEEE
DOI 10.1109/ECBS.2008.21

MP services. Many mature security models (e.g., S/MIME, IPSec) can easily be realized in this framework. We will firstly propose the system architecture, and then discuss protocol and security.

This paper is organized as follows. Section 2 shows an overview of related work in the field and statements our research motivation. Section 3 gives some background of SIP and MP. A SIP-based MP framework is proposed in section 4. Section 5 discusses the security issues of this new prototype. We will summarize our research and depict future work in section 6.

2. Related Work and Motivation

2.1. Related work

As early as 2001, K. Wrona, et al., described electronic payment solutions and their technical problems [7]. They proposed that the technical capabilities of current mobile infrastructures were too limited to afford re-using internet payment protocols. N. Kreyer, et al., suggested that MP providers were supposed to tackle three problems, cost, security and convenience to make it success [4]. Y. Choi, et al., showed the tendency of mobile technology was growing. However, they also proposed that some problems, such as security and privacy, must be handled clearly at first [8].

There were a lot of researches focused on how to improve the security of MP system. S. Karnouskos et al., presented a Secure Mobile Payment Service (SEMOPS) which was an innovative solution for delivering a global mobile payment service [9]. SEMOPS had enhanced security, trust and privacy issues. Based on SEMOPS, J. Liu, et al., proposed an improve model and protocol [10]. This new model was made to improve the signature validating and privacy issues. Furthermore, M. Hassinen, et al., designed a MP system based on Public Key Infrastructure (PKI) [11], providing the protection of confidentiality, privacy and non-repudiation. C. Yang and M, Qi proposed a theoretical application of MP based on 3-D protocol [12]. They applied a mature secure payment protocol in the new environment. The new scheme was better in efficiency and resource utilization.

To avoid complicated security designing, S. Fong and E. Lai proposed a simplified and practical MP scheme especially for mini-payment, or micro-payment [13]. The transaction can be realized using Short Message Service (SMS). There was no additional security mechanism applied because Global System for Mobile communications system (GSM) itself offers cryptographic algorithm within its relatively closed environment. Furthermore, J. Gao, et al., proposed a peer-to-peer wireless payment system based on Bluetooth communications [14]. They designed a 2-dimensional transaction protocol integrated several security solutions.

2.2. Motivation

Most current MP applications are designed for second-generation wireless telephone technology (2G) network, which is not flexible to deploy existing secure transaction models. The high cost and complicated configuration also limit the development of MP. In the contrast, SIP platform is extensible, low-cost and easy-to-configure. Therefore, we are motivated to implement a SIP-based MP framework.

Firstly, the amount of VoIP users is expanded. With its benefit on low-cost, VoIP has been widely accepted by people these years. However, due to some issues on usability and performance (e.g., bandwidth), current VoIP is seldom used in mobile phone. Nevertheless, it can be predicted that VoIP will be integrated with mobile phones in the near future. Many works, such as third-generation Partnership Project (3Gpp) is under construction and SIP is designed as the signalling protocol for the next generation IP Multimedia Subsystem (IMS) [15]. It is a tendency that more and more mobile services are pushed to be down in the new platform. As one of the promising mobile services, MP is exactly a suitable application which is worth to be integrated into IMS architecture. However, 2G and 3G are built on different infrastructure with different protocols. Thus, the design of a SIP-based MP framework in reference to the traditional MP in 2G is a great challenge.

Secondly, SIP is supposed to provide a more security supports for MP services. So far, the security of MP is its prime bottleneck. Such issues as authentication, trust management and privacy protection are still not perfectly tackled. That is why MP has not been considered as a mainstream payment method. The main problem could be that traditional mobile infrastructure is insufficient to allow re-using internet payment protocol with strong authentication and cryptographic algorithm. However, in the SIP environment, mobile phone is treated as an IP endpoint. So any classical internet model of transaction and security can be applied directly.

Thirdly, SIP supports a more convenient platform for merchants. Compared with traditional payment method, merchant is not treated as a service centre any more. Such responsibilities as authentication and transaction handling are passed to a trusted third party (TTP). In the SIP network, any customers or merchants are treated as au pair. This online business model can be implemented in a simpler way, similar as the most popular platform, ebay [16], without too many extra requirements for the merchants.

Last but not least, low-cost is another advantage for both customers and MP providers. SIP exploits the existing internet infrastructures and develops new services. All the services are realized on internet. Theoretically, users do not need to pay any additional money for taking advantage with MP services. Moreover, the architecture of SIP is peer-to-peer and easy to manage. Therefore, the MP providers can also save some operating expenses.

3. Background

3.1. Mobile Payment

Customers and merchants are limited to be face-to-face in the traditional cash transaction model. Although people can purchase remotely by remittance or post, it often takes too much time. The development of IT technology offers people more alternative methods of payment, such as credit cards and debit cards. In recent years, with the popularity of mobile phone, a new payment method using mobile phone is also accepted by people. In some special occasions (e.g., TV shopping), MP is the most suitable candidate. A typical MP scenario is shown in Figure 1. There are three entities in the procedure:

- Customer, who pays for goods or services using a mobile phone.
- Merchant, to provide goods or services and accept customer's payment.
- Payment Gateway (PG), a third party which transfers money from customer to merchant. The transaction can happen inside (based on mobile phone billing) or outside (based on bank account transferring). In this research, we will chiefly focus on the inside transaction.

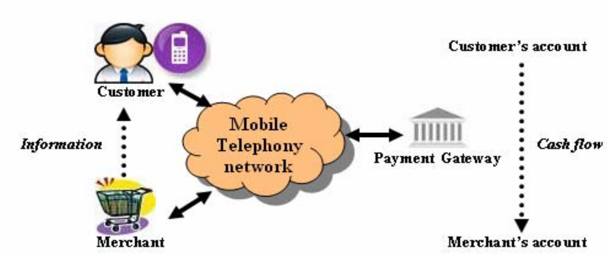


Figure 1. A typical mobile payment scenario

Mobile payment technology not only acts as an alternative of payment, but also brings more benefits to both retailers and consumers. According to a survey of N. Mallat, et al., there are at least three advantages of MP [17] for merchant. Firstly, MP has the potential to increase impulse purchases. The reason is that it is easy to operate so that MP makes it possible for consumers to buy things as soon as they have the stimulus to buy. Secondly, since it is based on the existing telecommunication infrastructure, it will also save on costs and increase profitability in the long run. Thirdly, MP provides convenience to those who have no credit cards.

However, the problems of MP are also obvious. First of all, the implementation of secure solutions with authentication, non-repudiation and privacy is a big problem. Most already existing online transaction protocols cannot be employed due to the limitation of infrastructures. For example, current mobile phones are insufficient to support powerful cryptographic algorithms. The second problem is the inflexibility of architecture. Current 2G network is located in a closed environment where it is difficult and expensive to configure. Last but not least, too much work needs to be done to improve the compatibility. The standards are blurred between different Mobile Network Operators (MNO) due to the closed mobile network environment. So, the service is hardly available to the users from other MNO.

3.2. Session Initiation Protocol

SIP is a text based protocol designed to establish or terminate a session between two partners. It is a standard for VoIP services in the internet and next generation networks. The message format is similar to HTTP protocol, with message headers and corresponding values. The destination of a SIP message is provided in the first line of the message, the request line. Additionally, several other message headers are dedicated to routing purpose in the network. A concrete example is shown in Figure 2 (b).

Generally, a basic SIP architecture consists of User Agents (UA) and SIP proxies, including registrar server, proxy server and redirect server (see Figure 2 (a)). The UA generates or terminates SIP requests. A registrar server is the server where users log in and announce their availability in the SIP networks. A proxy server regulates routing SIP messages in the network, while a redirect server allows SIP proxy servers to forward SIP messages to others.

Compared with traditional telephone network, SIP is scalable, easy-to-implement, and flexible. It is easy to extent and integrate more services. It is also a peer-to-peer protocol over existing internet, requiring no re-implementation in the network level. The logic is implemented at the communication endpoints, which may be in hardware or software level. Since SIP can be used to modify any session in progress, a normal telephone call session can be converted into a multiparty videoconference. Users can join in the session no matter what kind of terminal he is using or where he is located. They may be logged on to Internet using their laptop, or they may travel with a cell phone. However, since it is deployed in an open environment, additional security enhancement on the server and its infrastructures is necessary.

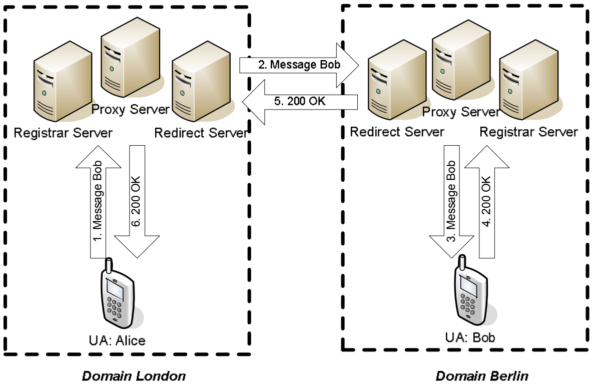
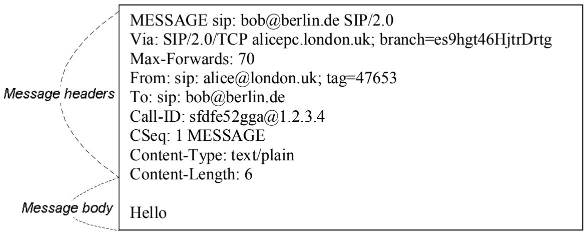


Figure 2(a). SIP architecture with IM procedure


Message headers
Message body

```
MESSAGE sip: bob@berlin.de SIP/2.0
Via: SIP/2.0/TCP alicepc.london.uk; branch=es9hgt46HjtrDrtg
Max-Forwards: 70
From: sip: alice@london.uk; tag=47653
To: sip: bob@berlin.de
Call-ID: sfdfe52gga@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: text/plain
Content-Length: 6

Hello
```

Figure 2(b). An example of SIP IM message

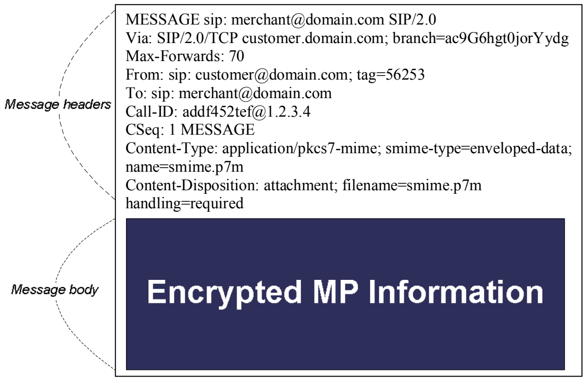
Figure 2. Instant Message Extension in SIP architecture

The most important function of SIP is to build sessions between two partners. However, we will emphasis on another method provided by SIP in this paper. Instant Messaging (IM) has been already widely used in the real world. It is defined as exchange text or media content between two entities in near real time. Now, it is one of the most frequently used services in current 2G network. Therefore, as the signalling protocol of next generation network, SIP also supports IM service. B. Campbell, et al. proposed an SIP extension for IM processing [18]. Shown as Figure 2, Alice issues a SIP request using the new MESSAGE method to its local SIP servers. The request will traverse between some proxies in order to reach its final destination. And the receiver, Bob, will reply “200 OK” message to denote that it has got the message. Generally, IM request have a higher requirement for security than other SIP requests so that end-to-end authentication, body integrity and body confidentiality mechanisms are compulsory to be implemented. In our research, we adopt SIP IM services to carry MP information.

4. SIP-based MP Framework

4.1. Requirement

Our goal is to implement a SIP-based MP framework without modifying existing SIP protocol and infrastructures. Our MP protocol is designed by using the SIP MESSAGE method. The MP information is carried by SIP IM message in the payload. Most security and transport tasks are accomplished by SIP so that we can easily implement payment logic in MP. Figure 3 shows an example of such a SIP message, sent from customer@domain.com to merchant@domain.com. The detail purchase request is encapsulated in the dashed line box.


Message headers
Message body

```
MESSAGE sip: merchant@domain.com SIP/2.0
Via: SIP/2.0/TCP customer.domain.com; branch=ac9G6hgt0jorYydg
Max-Forwards: 70
From: sip: customer@domain.com; tag=56253
To: sip: merchant@domain.com
Call-ID: addf452tef@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
handling=required

Encrypted MP Information
```

Figure 3. Example SIP message carrying MP protocol

Furthermore, we make two assumptions:

- Both customer and merchant trust PG, which acts as a TTP and handles all the payment transactions.
- Customer and merchant have already successfully exchanged their session keys.

The payment protocol is derived from Secure Electronic Transaction (SET) [19]. In this framework, we can achieve privacy protection by separation of Order Information (OI) and Payment Information (PI).

The customers can simply send the merchant a purchase message, which includes both OI and PI. The OI confirms the purchase of items and the PI contains payment details (e.g., Personal Identification Number (PIN)). Neither the merchant needs to know customers’ PIN included in the PI nor the PG needs to know which item the customer wants to buy. The PI is encrypted in such a way that it should be kept as a cipher to merchant. After receiving the request, the merchant will decrypt the request and forward PI to PG to commit the transaction. Then, PG will ask the customer to confirm his payment request. If the confirm is replied, PG will update accounts of both the customer and merchant to accomplish the transaction.

Also, OI and PI must be linked in a way by which potential conflicts can be solved. Since it is the merchant to pass the PI to PG, the merchant can claim that a forgery OI goes with the PI rather than original OI. The linkage is necessary so that the customer can prove this PI is only intended for a particular order, not for other goods or services. A dual signature (DS) scheme [19] can be employed to protect the integrity of OI and PI. The entities with their functions are shown as follows.

4.2. Architecture

Figure 4 shows the architecture of the proposed MP model. There are five separated entities involved in the framework: customer, merchant, PG, proxy and accounting database.

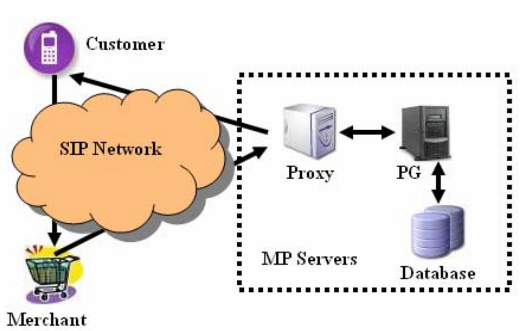


Figure 4. The architecture of the proposed MP model

Customer: It acts as one of SIP UAs including User Interface, SIP IM module, security module and payment module.

- **User Interface**: It provides an input device (e.g., keyboard) for user to type in purchase information and an output device (e.g., screen) to display response.
- **SIP IM Module**: This module supports SIP instant message interactions over internet. It is implemented according to RFC 3428. It allows customer to communicate with merchant and PG by instant messages.
- **Security Module**: It employs General internet security protocols such as (IPSec, TLS and S/MIME). Key management is also an important component for this module. Incoming messages will be decrypted and outgoing messages will be encrypted here.
- **Payment Module**: It handles purchase request by the information gathered from user interface. OI, PI and DS will be generated here. The entire procedure is transparent to users.

Merchant: It is also another of SIP UAs including SIP IM module, verification module and payment module.

- **SIP IM Module**: it is similar to the SIP IM module on the customer side, which allows merchant to communicate with each component by instant messages.
- **Security Module**: It is another terminal point for security measures which has been introduced into this framework.
- **Order Verification Module**: It verifies the availability of OI to avoid the situation that the target goods have been sold out.
- **Payment Module**: It forwards PI to the PG in order to request the transaction. Also, it will offer a copy of hashed OI in favour of PG to verify the PI.

PG: It works as a SIP UA but located on the server side. It communicates with customer and merchant to accomplish the transaction. Its main components can be listed as follows.

- **Payment Verification Module**: It verifies incoming payment request in three aspects. Firstly, it checks the integrity of OI and PI. Secondly, it authenticates the customer by user PIN. Finally, it checks whether the current customer has enough balance to complete the transaction.
- **Log Management Module**: It logs every transaction in favour of customer inquiry.
- **Transaction Module**: It can directly operate the user accounting database to complete transactions. The charging method is phone-bill-based, which means credits will be transferred from the customer's mobile phone account to the merchant's.
- **SIP IM Module**: This module supports SIP instant message interactions over internet. However, due to security consideration, PG will refuse all the traffic which does not come from the local Proxy.
- **Security Module**: It performs the same function as the security module on customer and merchant.

Proxy: It regularly routes all the SIP messages to or from PG including registration messages and payment messages.

Account Database: It is a database server which records user accounting. The credits will be transferred here.

4.3. Transaction Work-Flow

Figure 5 presents the detailed procedure for performing a MP transaction using our proposed framework. The solid lines indicate messages based on SIP protocol and the dashed lines represent messages are transferred through other communication approaches. The whole procedure can be divided into five phases: payment request, merchant verification, PG verification, customer confirmation and transaction operating, shown as follows.

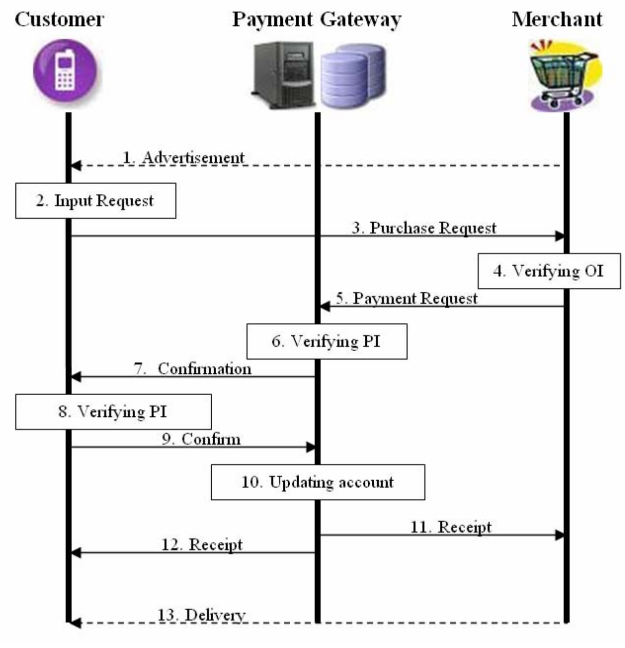


Figure 5. The working flow of the proposed MP model

Purchase request (step 1, 2, 3): Firstly, the customer gets information of products or services, e.g., identity, price, and category, from the merchant. This information can be delivered via any kinds of media (e.g., TV, post advertisement, catalogs, etc). Then, the customer may be interested in something and select the goods he wants to pay. So, the customer inputs a valid ID of the goods with price and his user PIN. Finally, an encrypted OI and PI with a DS can be automatically generated by UA. DS is a message digest of signed OI and signed PI in order to protect the message integrity. PI is encrypted by the public key of PG so that only can be read by PG. The whole message including OI, encrypted PI and DS is encrypted by the session key shared between customer and merchant. The operation can be summarized as:

(1) C->M: [[PI, DS]k_{up}, OI]k_s;
C: Customer
M: Merchant
k_{rc}: Private key of customer
k_{up}: Public key of PG
k_s: Session key of customer and merchant
H(): Hash function
DS: [H(H(OI)||H(PI))]k_{rc}

Merchant verification (step 4, 5): The merchant will decrypt the incoming message using its session key. However, only OI is readable and the merchant will verify the order information, especially, the price should be correct and the goods should be still available. If there are any unexceptional or abnormal, the transaction will be terminated immediately. Otherwise, merchant will forward the encrypted PI, DS with a hashed OI to PG. The Operation can be summarized as:

(2) M->P: [PI, DS]K_{up}, H(OI);
P: PG

PG verification (step 6, 7): After decrypting the payment request, PG has three verification tasks. Firstly, it will generate a new DS by PI and the hashed OI in order to compare with original DS. If two DS are same, it will prove whether the linkage of PI and OI is valid. Otherwise, the transaction will be terminated. Secondly, the PG will authenticate customer with user PIN. The user PIN should be correct, otherwise, the payment request will be discarded. Finally, PG will also check whether the customer has enough account balance to complete the transaction. If all of these three verifications are successfully passed, a confirmation request contained PI and a transaction identity will be sent to the customer. The message is encrypted by the public key of customer. The Operation can be summarized as:

(3) P->C: [CR]K_{uc};
CR: Confirmation request
k_{uc}: Public key of Customer

Customer confirmation (step 8, 9): The customer will verify the CR, and feed back an acknowledgement to continue the transaction. The Operation can be summarized as:

(4) C->P: [CA]k_{up};
CA: Confirmation ACK

Settlement (step 10, 11, 12, and 13): Receiving the right confirmation, the PG will credit the billing account of the customer and debit the merchant account at the same time. Receipts will be sent to both sides to notify the successful deal before goods delivery.

5. Security Consideration

Security is one of the most important factors for mobile commence. After being transplanted into a new environment, the SIP-based MP framework has to take new threats into account. We will evaluate some possible threat models with existing security protocol and infrastructures in this section.

5.1. Threat Model

Previously mentioned Weak authentication mechanism using user PIN could be a potential vulnerability in the MP transaction. In some situation, only user PIN is insufficient to prove the perchance requester is the customer himself. If the user PIN is released, attackers may impersonate customers and spend customers' money. It may result in a huge loss for customers.

Masquerade, which takes place when one entity pretends to be a different entity, is another serious threat. In the SIP network, the location of customers is identified by IP addresses. After a customer successfully registers on SIP server, the SIP registrar will record the customer contact IP address in favour of the service. Exploiting it, a potential attacker can pretend to be the customer by IP spoofing so that the server may be cheated to send messages to the attacker.

Confidentiality can be protected by cryptographic algorithms. The message content should be encapsulated during the transmission. However, most message header fields (e.g., TO, VIA) must always be kept in plaintext because such header fields are required in both requests and responses.

Denial of Service (DoS) should also be taken into account. Since the new framework is based on internet, an open environment, these essential infrastructures (e.g., SIP proxies) have to face the public internet in order to accept requests from other IP endpoints all over the world. It is possible for attackers to create millions of bogus purchase requests that contain a falsified source address. An excessive amount of traffic created by attackers will cause the MP services unavailable.

Furthermore, most SIP services are implemented as software server running on normal operating systems. It is possible for attackers to exploit some vulnerabilities of MP software or operating system to take over the total control of the infrastructure. As a result, the attackers may bypass our security mechanism and intrude PG directly.

5.2. Security Enhancement

To avoid the potential attacks, we need to improve the security of our proposed SIP-based MP framework. The basic and intuitive idea to enhance the security is to integrate methods and protocols which is also one of our motivations for realizing MP in SIP network. Fortunately, the flexibility of SIP and extensibility of our architecture make this goal possible.

HTTP Digest [20]: This stateless, challenge-based mechanism provides message authentication and anti-reply protection. It consists of User-to-User authentication and User-to-Proxy authentication. In our MP schemes, as soon as the merchant receives the purchase request, it will continue processing but reply the customer a challenge. The customer has to resubmit the request including correct response to the challenge. Since the challenge consists of random nonce which is different from time to time, replayed purchase request from attackers will not be processed.

S/MIME [21]: Both integrity and confidentiality can be ensured by carrying S/MIME bodies. A message content digest will be generated and attached in order to ensure the content is not modified during the transmission. Moreover, message content can be encrypted in case of eavesdropping attack. However, the protection is limited to the message content because most message headers (e.g., TO, VIA) should be keeping in plaintext and changeable. Furthermore, the key exchange scheme of MIME is vulnerable to man-in-the-middle attack.

IPSec [22]: The purpose of IPSec is to protect integrity and confidentiality of IP packets. Since SIP-based MP is based on TCP/IP protocol, the IP layer protection is significant. Besides the protection of integrity and confidentiality, IPSec also authenticates the communication parties, which countermeasures the IP spoofing attack.

Lock-Keeper: Lock-Keeper [23] is a high-level security solution based on the simple "Physical Separation" idea. It is a hardware-based device and works like a sluice to provide secure data exchange between the physically separated networks. It does not replace the functionality of the conventional firewall but is generally used in combination with firewall to enhance the security of the protected network. Moreover, other content filtering mechanisms can also be flexibly integrated with Lock-Keeper to prevent some application-level attacks, also referred to as "offline attacks". It will be deployed between SIP server and internet to defend possible permeation attack. Even in the worst case, attackers still cannot visit PG directly. Shown as Figure 6, the packets from internet have to go through the Lock-Keeper before enter internal SIP server network. The Lock-Keeper will check the incoming packets according to security mechanism. The packets from attackers which contain malicious content should be discarded. Furthermore, there is no direct physical connection between outside environment (SIP Network) and internal MP Servers at any time. Most connect-oriented threats and unknown attacks can be avoided.

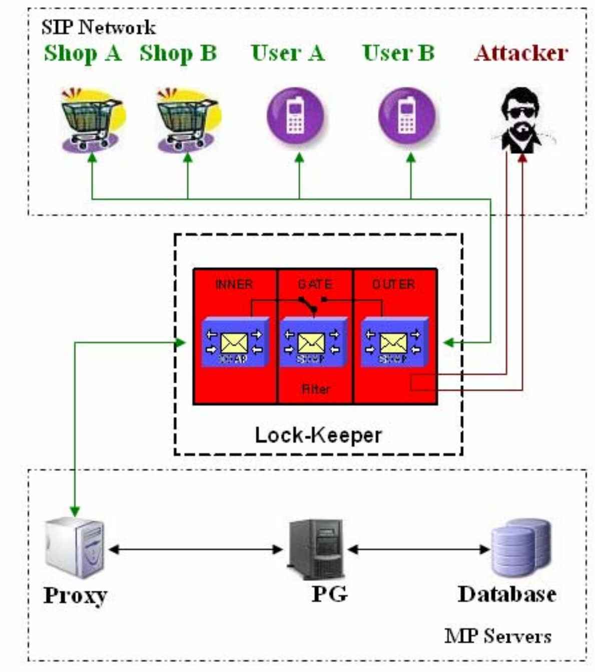


Figure 6. The Lock-Keeper will be deployed between SIP Network and internal MP Servers

6. Conclusions and Future Work

In this paper, we present a novel MP scheme based on SIP in favour of the next generation mobile network. Compared to current MP techniques, it provides more security features, supports P2P payment method and reduces the cost. The MP information is carried in the payload of SIP messages. And a basic payment protocol is presented. Furthermore, we evaluate the security of this prototype using several classical threat models. Finally, we propose several methods to countermeasure them.

Future wok should involve evaluation of performance and enhancement of security. We will launch a series of experiments in this framework and evaluate the performance of it. Furthermore, we will use formal method to verify our payment protocol.

7. References

[1] S. Karnouskos, "Mobile payment a journey through existing procedures and standardization initiatives", *IEEE Communications Surveys*, Vol.6, No.4.

[2] Nonoh, an online VoIP vendor, see www.nonoh.net, visited at 26th-Oct-2007.

[3] Juniper Market Research, news report, http://www.wirelessweek.com/Juniper_Market_Research.aspx, visited at 26th-Oct-2007.

[4] N. Kreyer, K. Pousttchi and Klaus Turowski, "Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce", in proceedings of *E-Commerce and Web Technologies*: Third International Conference, 2002.

[5] Webitpr, Over 250m VoIP Users Over 3G Mobile Networks by 2012 --- Disruptive Analysis Report, http://www.webitpr.com/release_detail.asp?ReleaseID=7122, visited at 15th-Nov-2007.

[6] J. Rosenberg, et al., "SIP: Session Initiation Protocol", *IETF RFC 3261*, 2002.

[7] K. Wrona, et al., "mobile payment - state of the art and open problems", in proceeding of *Electronic Commerce, Second International Workshop*, WELCOM, 2001.

[8] Y. Choi, "The state-of-the-art of mobile payment architecture and emerging issues", Int. J. *Electronic Finance*, Vol. 1, No. 1, 2006.

[9] S. Karnouskos, et al., "Security, Trust and Privacy in the Secure Mobile Payment Service", in proceedings of *3rd international conference on mobile business 2004*, New York City, 2004.

[10] J. Liu, et al., "A System Model and Protocol for Mobile Payment", in proceedings of *the 2005 IEEE International Conference on e-Business Engineering* (ICEBE' 05), 2005.

[11] M. Hassinen, "An Open, PKI-Based Mobile Payment System", in proceedings of *Emerging Trends in Information and Communication Security*, Freiburg, 2006.

[12] C. Yang and M, Qi, "Scheme and Applications of Mobile Payment based on 3-D Security Protocol", in proceedings of *the 3rd conference on mobile technology, applications and systems*, 2006.

[13] S. Fong and E. Lai, "Mobile Mini-Payment Scheme Using SMS-Credit", in proceedings of *conference on Computational Science and Its Applications*, 2005.

[14] J. Gao, et al., "P2P-Paid: A Peer-to-Peer Wireless Payment System", in proceedings of *the second IEEE International Workshop On Mobile Commerce and Services (WMCS'05)*, 2005.

[15] 3rd Generation Partnership Project (3GPP), http://www.3gpp.org/, visited at 26th-Oct-2007.

[16] ebay, http://www.ebay.com/, visited at 29th-Oct-2007.

[17] N. Mallat and V.K. Tuunainen, "Merchant Adoption of Mobile Payment System", in proceedings of *the international conference on Mobile Business*, 2005.

[18] B. Campbell, et al., "Session Initiation Protocol (SIP) Extension for Instant Messaging", *IETF RFC 3428*, 2002.

[19] "Secure Electronic Transaction Book 1: Business Description", Feb. 23, 1996,

[20] J. Franks, et al., "HTTP: Authentication: Basic and Digest Access Authentication", *IETF RFC 2617*, 1999.

[21] S. Dusse, et al., "S/MIME Version 3 Message Specification", *IETF RFC 2633*, 1999.

[22] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", *IETF RFC 2401*, 1998.

[23] F. Cheng and Ch. Meinel, "Research on the Lock-Keeper Technology: Architectures, Advancements and Applications", *International Journal of Computer and Information Science*, 2004.