A NOVEL PROTOCOL FOR ENHANCING THE SECURITY OF ELECTRONIC TRANSACTION USING GSM AUTHENTICATION

[1]Kamalrulnizam Abu Bakar, [2]Abdirizak Omar Mahamoud, [3]Zafril Rizal M.Azmi

[1,3]Faculty of Computer Science & Information System, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia

[2]Center for Advanced and Software Engineering (CASE), University Technology Malaysia, City Campus, 54100 Kuala Lumpur, Malaysia

[1]knizam@utm.my, [2]furso2003@yahoo.com, [3]zafrilrizal@yahoo.com

Abstract

In fully developing the so-called information society, the use of new technologies for commercial transaction by electronic means and without the traditional paper support is increasingly common. This gives rise to the advantages of higher speed and lower costs in carrying out business activities, as well as the possibility of expanding the potential offers market for business. Secure Socket Layer/Transport Layer Security (SSL/TSL) protocol remain by far the most widely used means for providing security services for e-commerce transactions, despite the fact that these protocols were designed to provide security for communications links, and not for entire e-commerce transactions. Hence, does not support client authentication, which in turn makes certain frauds during online electronic transaction to take place. Though a large number of researches have been carried out in securing electronic transaction there is a lack of research been done in securing client authentication. This paper is to propose a different way of using the GSM Authentication to enhance the security of electronic transactions, which will also in return in increase the mobility when making an Internet transaction.

Keywords: E-Commerce Security, Authentication, GSM Security

1. Introduction

The Internet is inherently insecure for transactions as it can be compromised at several points, including the user's computer, the merchant's or service provider's system or at any intermediate point between them on the network.

This is because the Internet consists of many different computer networks that are all interconnected using a common protocol. Due to this open network architecture, messages traverse many different networks between source and destination. For example, when a user transmits a credit card number over the Internet to a merchant, this number passes through several computer systems, including systems of other network users before reaching the merchant's computer. The integrity of the message could be compromised at any of the intermediate points. Furthermore, as business on the Internet grows, it will become more difficult for both the buyer and the merchant to know whether each is legitimate. Hence, this paper will propose a payment protocol, which will utilize the security services provided in the GSM air interface to support user authentication.

Two very important technological trends in recent years have been the wide acceptance of mobile phones around the world and the growth of e-commerce. For example, mobile phone usage is forecast to reach almost 80% of the population in Europe by 2005 [1]. Key characteristics of the mobile phone include the fact that it is ubiquitous, personal, and that the average user is reasonably competent in using it. This fact suggests that it can be used for authentication and authorization in electronic payment transactions, since it already contains a physically secure cryptographic device (i.e., the Subscriber Identity Module (SIM)).

However, despite all the advantages that a mobile phone has as a means of electronic payment, there are also several drawbacks, including the following.

a. Usability

Mobile phones are small, have limited processing power, use low-bandwidth communication technologies, use batteries with limited life spans, and often have a relatively limited user interface.

b. Theft

A number of current mobile communication systems store all the subscriber-specific information needed to use a mobile phone inside a smart card (e.g., a GSM SIM). To protect the phone, the user can be required to enter a PIN, although it would appear that this security

measure is not widely used. However, even if a PIN is used, the smart card typically remains unlocked until the phone is switched off or the SIM loses power. From a security point of view the most important risk that arises is loss or theft of the phone and the embedded smart card. An attacker with a stolen SIM is potentially able to make fraudulent transactions at the owner's expense, at least until the SIM is reported stolen and blocked, assuming that the SIM is not PIN protected. Furthermore, if the SIM was stolen in an unlocked state, an attacker could gain access to any personal information in the SIM and Mobile Equipment (ME). Thus a payment scheme based on use of a GSM SIM to help secure the transaction may need to be combined with another authentication method, e.g. username and password, if the fraud threat arising from use of a stolen SIM is to be addressed. In such a case an attacker would need both the user SIM and password to impersonate the user to a seller.

c. Radio interface threats

Mobile communications between a mobile phone and a serving network appear to be more susceptible to eavesdropping and interference than current Internet traffic through fixed networks. This is because of the intrinsic greater vulnerability of radio networks to interception. Moreover, the quality of the communications channel can be highly variable when a mobile device is used in a built environment. Thus transmitted data should be protected in terms of authentication, confidentiality, and integrity. The protocol requires the buyer to have a public key pair. This key pair would typically be stored in the buyer PC, and hence the buyer has to use this particular machine every time a transaction is to be made. Although a smart card could be employed to store the key and enhance mobility, not many user PCs are equipped with smart card readers.

However, the GSM-based scheme described in this paper does not require such a key pair to be generated, since its security relies on the secret keys stored in a GSM SIM. Moreover, basing security on a mobile phone also inherently supports a level of user mobility.

In this paper the protocol we will propose will reduce the threat posed by the storage of un-encrypted card numbers in a merchant server by reducing the value of stolen card numbers to a fraudster. This is achieved by requiring the user to possess both a debit/credit card and a GSM Mobile Station (MS), i.e. a GSM Mobile Equipment (ME) and a GSM Subscriber Identity Module (SIM), which must be registered under the same name as appears on the card.

2. Mobile Infrastructure And Services

The existence of a suitable transport infrastructure is important for enabling the use of mobile phones in electronic payments. In this section we describe the security services provided by the GSM and UMTS mobile communications systems. A brief description of the SMS and SIM Application Toolkit services is also given.

a. GSM Security

A GSM network can be divided into three functional entities [2]. These are the mobile station carried by the subscriber, consisting of a Mobile Equipment (ME) with its Subscriber Identity Module (SIM), the network subsystem which performs the switching of calls between the users and between mobile and fixed network users, and the Base Station subsystem, which controls the air interface between the mobile station and the network subsystem. The main security services provided by the GSM air interface are [3]:

i. *Subscriber identity confidentiality*
ii. *Data confidentiality*
iii. *Subscriber identity authentication.*

Hence we will go into detail of Subscribers identity authentication, as this is the issue we will solve it in this paper.

i. Subscriber identity authentication.

Within every SIM there exists a long-term secret key, *Ki*, which is unique and known only to the SIM and Authentication Centre (AuC) of the home network operator of the subscriber. The home network operator is the organization with whom the subscriber has a contractual arrangement for the provision of service, and which the subscriber pays for this service.

To authenticate a SIM, the visited network needs a *triplet* which consists of a random number (*RAND*), the expected response (*XRES*), and a secret cipher key (*Kc*). The (*RAND*, *XRES*) pair enables the network to verify the authenticity of the SIM without having the key *Ki*, while *Kc* is used for encryption. To compute a triplet, the AuC generates a *RAND* and passes it with *Ki* as parameters to algorithms *A*3 and *A*8, which are specific to a network operator. The outputs of *A*3 and *A*8 are *XRES* and *Kc* respectively.

The AuC generates triplets as required, and passes them to whichever network needs them. When a SIM is requested to authenticate itself to a network, a *RAND* from a triplet provided by the SIM's home network is sent from the network to the SIM. Since the SIM is equipped with the function *A*3 and the secret key *Ki*, it can generate the Signed Response (*SRES*) using *RAND* and *Ki* as inputs. The SIM then sends the *SRES* to the network where the *SRES* is compared with the *XRES*. If they match, SIM verification is successful.

Each mobile network operator maintains two databases: the Home Location Register (HLR), and the Visitor Location Register (VLR). The HLR is used to store information regarding the subscribers of this operator. The VLR holds information on subscribers, which have roamed into its network. GSM air interface security is based on a secret key shared by the subscriber's home network and the SIM. The secret keys of the subscribers of a network are stored in an Authentication Center (AC) maintained by that network, which generates security parameters on request by the HLR. The AC is usually implemented as part of the HLR [4].

Each SIM has a unique international mobile subscriber identity (IMSI) and a secret key *Ki* shared only with the subscriber's network operator AC. During authentication, two keyed functions (*A*3*; A8*), and a stream cipher encryption/decryption algorithm *A*5 are used. To authenticate a subscriber (holder of a SIM) to the network, the subscriber sends its IMSI to the VLR, which, in turn, sends a request to the subscriber's HLR. The HLR requests the AC to generate a triplet (*R*, SRES, *Kc*), where *R* is a random challenge, SRES (the expected response to the challenge) = *A*3*Ki*(*R*), and *Kc* (the session encryption key) = *A*8*Ki*(*R*). This triplet is then provided to the VLR, which sends *R* to the mobile device, and hence to the SIM, which recomputes SRES and *Kc* using its stored copy of K*i*, and returns SRES. If the returned value agrees with the value in the triple, the mobile is deemed authentic, and data exchanged between the mobile and the network is subsequently encrypted using *Kc*. This encrypted channel is also used to transfer a temporary identity (TMSI) for the mobile to provide a measure of mobile anonymity (avoiding the need for the IMSI to be routinely sent across the wireless channel).

b. UMTS/3GPP Security

UMTS (Universal Mobile Telecommunication System) is a third generation (3G) mobile telecommunication system whose security system is somewhat similar to, although more sophisticated than, that used in GSM. UMTS offers the following security services in addition to those provided by GSM [5]:

i. Mutual authentication between the user and network.
ii. Assurance that authentication information and keys are not being re-used.
iii. Integrity protection of signaling messages against replay or modification.
iv. Encryption is mandatory, and the encryption algorithm used is stronger.
v. Termination of the encryption further into the core network to encompass microwave links.

3. Using GSM Authentication For Electronic Transaction

Within every SIM there exists a long-term secret key, K_i, which is unique and only known to the SIM and Authentication Center (AuC) of the home network operator and subscribe.

To authenticate a SIM, the visited network needs a triplet, which consists of a random number (RAND), the expected response (XRES), and a secret cipher key (K_c). The (RAND, XPRES) pair enables the network to verify the authenticity of the SIM without having the key K_i while K_c is used for encryption. In order to compute a triplet, the *AuC* generates a RAND and passes it with K_i as parameters to algorithm A3 and A8, which are specific to a network operator. The outputs of A3 and A8 are XRES and K_c respectively.

The *AuC* generates triplets as required, and passes them to whichever network needs them. When a SIM is requested to authenticate itself to a network a *RAND* from a triplet provided by the SIM's home network is sent from the network to the SIM. Since the SIM is equipped with the function A3 and the secret key K_i, it can generate the Signed Response (*SRES*) using *RAND* and K_i as inputs. The SIM then sends the SRES to the network where the SRES is compared with the *XRES*. If they match, SIM verification is successful.

4. Entities Involved

In a typical debit/credit card payment system there are four parties involved, namely a *client*, a *merchant*, an *acquiring bank* and a *card issuing bank*. The precise interactions between these roles will vary depending on the transaction type. During a transaction, on-line

connectivity may be limited to certain subsets of roles. The underlying payment model is shown in Figure 1.1.

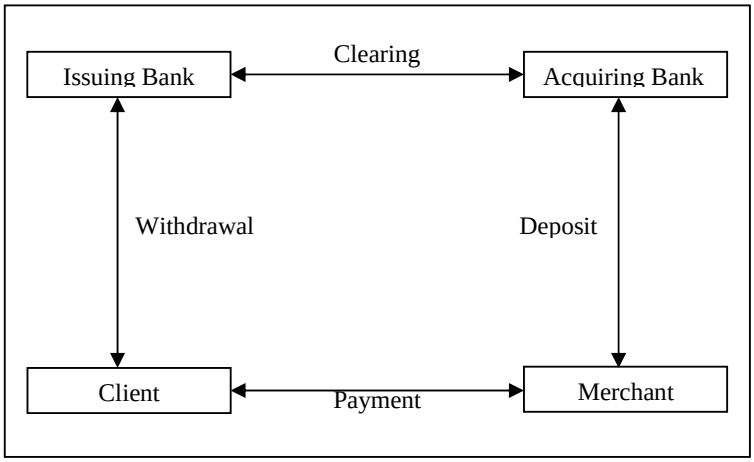

Figure 1.1: Debit/Credit Card Payment System

a. Issuer

A financial institution that issues a payment card to the cardholder.

b. Cardholder

An authorized holder of a card supplied by the issuer. The card stores the cardholder's payment data and is capable of generating authentication data and verifying a cardholder's PIN. The cardholder is associated with a Primary Account Number (PAN), stored on the card that identifies the cardholder account and the issuer. During a transaction, the card has a connection only to the merchant, which passes authorization messages to the issuer via the acquirer.

c. Merchant

This is the business that accepts the card payment for purchased goods. It uses a terminal to interact with the card. The terminal also interacts with the issuer (via the acquirer) to receive authorization for transactions.

d. Acquirer

This is a financial institution that processes card payment authorizations and payments for the merchant. The acquirer and the issuer communicate via a secure financial network.

5. Security Requirements

As shown in Figure 1.1, a typical card payment system involves four parties, namely a card issuer, an acquirer, a merchant and a client. The security requirements for each party vary and hence they will be examined individually.

However, the security requirements for acquirers and issuers are discussed together since they are both financial institutions; they are both contractually obliged to abide by the rules of the relevant payment system.

a. Issuer and Acquirer

i. Non-Repudiation

Issuers and acquirers need to ensure that neither clients nor merchants can deny their participation in a transaction (where the transaction may involve a refund from merchant to client). In order to achieve non-repudiation, identity authentication may also be needed. The main goal of non-repudiation service is to collect, maintain, make available and validate indisputable evidence.

ii. Integrity

It is also important to ensure that once details of a transaction have been confirmed, no one can maliciously modify them. Merchants must not be able to alter the amount that a client has agreed to pay. To be more specific, it should not be possible for a merchant to change the amount after it has been authorized by the card issuer. Similarly, a client must not be able to change the amount that has been authorized.

iii. Authentication

Client authentication is required for the issuers and acquirers so that they can prove that it is the client who authorized the payment and that he/she is a legitimate cardholder. Otherwise, a client can deny making a transaction and the issuer may end up being liable for refunding the amount to the client. On the other hand, if an electronic transaction is found to be fraudulent, merchants are liable for ‘card not present’ chargeback’s. Therefore, it is important for the acquirer to ensure merchant non-repudiation to prevent them challenging their liability.

iv. Replay protection

A malicious merchant should not be able to use a once authorized transaction to obtain a repeat payment. Additionally, merchants should not be able to use an old transaction to request a new payment authorization no matter how many similar transactions the client has made with them. Issuers and acquirers need a mechanism to detect if a transaction has been replayed so that they do not authorize an illegitimate transaction.

b. Merchants

i. Non-Repudiation

A merchant needs evidence that a customer has agreed to pay the amount associated with a transaction. A merchant also needs to verify that the client is the legitimate cardholder; otherwise, the merchant can be liable for chargeback's. This occurs when a client tells his/her issuer that a particular transaction was not made. The card issuer then immediately submits a chargeback to the acquirer to recover the amount from the account of the merchant in question. Within a predefined period of time, the merchant can dispute the chargeback by providing evidence of, for example, purchase or delivery. Therefore, it is important for merchants to have non-repudiation evidence of the transaction, i.e. to have client non-repudiation. Furthermore, an issuer should not be able to deny having authorized a payment.

ii. Integrity

No one should be able to change the details of a transaction once they have been agreed upon otherwise the integrity of the transaction is damaged. A merchant will not wish to be credited with payment for less than the amount agreed. In addition, an acquirer or issuer should not be able to modify a transaction that has been authorized.

iii. Authentication

As stated before, merchants need client authentication to make sure that the client is the legitimate cardholder. Moreover, they need to be sure that they are communicating with the genuine acquirer. Otherwise, an adversary may masquerade as an acquirer and authorize an illegitimate transaction.

iv. Replay protection

A malicious client should not be able to present an old proof of purchase to claim for repeat delivery of goods. Likewise, it should not be possible for an acquirer to claim that a merchant has obtained a payment using an old transaction.

c. Client

i. Non-repudiation

Clients also require non-repudiation, for example a proof of payment so that no one involved in the transaction can repudiate that a payment has occurred.

ii. Integrity

As for the other parties, transaction integrity is important to the client. No one should be able to maliciously modify the transaction details once they have been confirmed. Clients will not want an adversary to change a delivery address, the price, or the description of the merchandise after they have agreed a payment.

iii. Confidentiality and privacy

Transaction confidentiality, especially card information, may be the security service of most concern to users. It is important that cardholder account details are kept secret from any party except the issuer and its bearer, since they are the main basis on which Internet payments are made. Moreover, some users may require confidentiality protection for the nature of their transactions.

iv. Authentication

A client needs to be sure that he/she is dealing with a trustworthy merchant. When shopping on the Internet, it is relatively easy to be attracted into visiting a site that appears to sell something but is actually simply collecting card details. Even though a client may have made a purchase from a site before, it is not always obvious whether the page that is being fetched is authentic.

v. Replay protection

Clients need a mechanism to ensure that a malicious merchant or an adversary will not be able to reuse previously authorized payments to make a repeat charge.

6. System Architecture

Three main system components are involved in our payment protocol. These are a User System, a merchant server, and an *AuC*. The system architecture is:

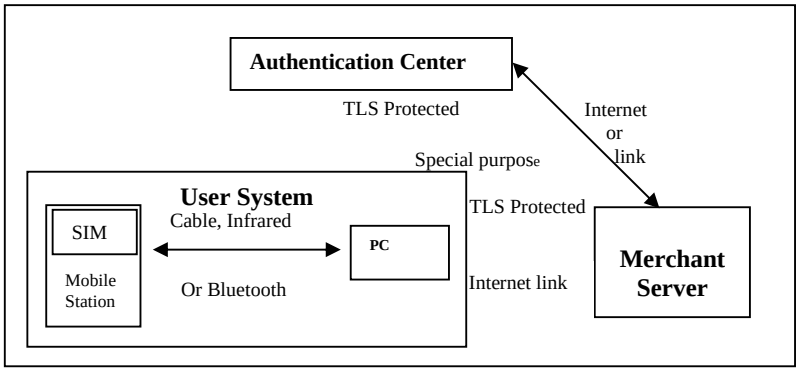

Figure 1.2: System architecture - GSM-based cardholder authentication.

a. User System

The user system consist of a GSM Mobile Station (MS), i.e. a GSM Mobile Equipment (ME) and a GSM Subscriber Identity Module (SIM), and a PC. The MS is responsible for outputting the SRES. Therefore, although an ME is needed to interact with the SIM, the protocol can work without an ME if there is an alternative means for the SIM to communicate with the user's PC. The means of communication used between the MS and the user PC is not mentioned here. However, infrared, cable, or Bluetooth[1] could be employed for the purpose. In a recent version of the SIM Toolkit (U-SIM Application Toolkit), there is a command called 'AT Command' which enables a U-SIM to tell an ME to open an infrared or Bluetooth channel. The U-SIM Application Toolkit (USAT), therefore could be used to implement the proposed protocol.

b. Merchant Server And Authentication Center

The merchant server is the component that interacts with the User System to support electronic transactions. The communication link between the Merchant Server and Cardholder system is the Internet. The merchant server also interacts with the AuC in order to retrieve values required in the user authentication process. The AuC is required to supply the merchant server with values necessary for the GSM identity authentication process. It takes inputs from the merchant server and produces the values used for identity authentication. The choice of the communication link between the two is again not an issue here. However, it can be SSL/TLS protected Internet session or a special purpose link provided by the mobile network operator.

[1] http://www.bluetooth.com

We suppose that the integrity and confidentiality of the merchant server /AuC link is protected in some way, e.g. via encryption and MACs or signature; however, the means by which this is achieved is outside of the scope of this paper.

7. How The Transaction Is Processed

The protocol assumes that the consumer and the merchant wish to perform a specified transaction. Hence, the protocol starts with a consumer has decided to make a payment.

The consumer first fills in a typical Internet purchase form using the PC. In this protocol however, the form is required to contain a field for a mobile phone number. Upon receipt of the form, the merchant server extracts the mobile number form the form and the identity authentication process begin. The procedure is illustrated below:

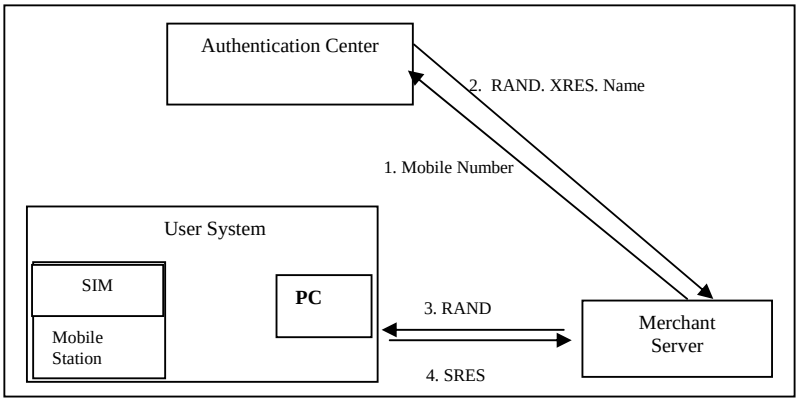

Figure 1.3: GSM Identity Authentication Process

The merchant server first sends the consumer's mobile number to the AuC in order to receive three values: A random number (RAND), an expected response (XRES), and the subscriber name (SRES). This corresponds to the message 1 in figure 1.3.

Upon receipt of the merchant server request, the AuC generates the (RAND, XRES) pair using the key K_i of the requested mobile number with algorithm A3. It then sends the (RAND, XRES) pair, along with the name of the subscriber, to the merchant server, as shown in the message 2 in figure 1.3. Upon receipt of the message 2, the merchant server first compares the name of the cardholder with the subscriber names received from the AuC. If they match, the RAND will be sent to the PC as in message 3 of figure 1.3. Otherwise, the identity authentication process fails and the protocol ends.

After receiving the RAND, the user PC forwards it to the Merchant (ME). The ME then sends the RAND values to the SIM just as it would if the RAND was sent via the radio interface by a GSM base station. The SIM now generates SRES using the received RAND and its stored K_i as inputs to algorithm A3. The SIM then passes the generated SRES back to the ME, again just as it would normally (i.e. no special functionality is required to have the SIM). The ME then sends the SRES to the PC, which forwards the value to the merchant server (Message 4). At the merchant server, the *SRES* is compared with the *XRES*. If they match, the consumer is deemed to have been authenticated. The Internet transaction processing may now continue.

8. Threat Analysis

In this section, we consider threats to the proposed protocol. The threats can be divided into three categories: threats to the User System, threats to the two communications links (user system/merchant server and merchant server/AuC), and threats in the merchant server and the AuC.

a. Threats in the User System

As stated previously, the User System consists of a user PC and a MS. Since this protocol does not require the user PC to contain sensitive information, the threats arising from the PC are minimal. Although information that passes via the PC can be cached, this information is not confidential. A debit/credit card number can be cached and compromised but the protocol still requires a corresponding SIM to make an electronic transaction. In any event, such a threat would exist in any PC-based e-commerce protocol.

Threats to the MS are divided into two scenarios, depending on the amount of information an attacker has. Clearly, if he/she has neither the SIM nor the card details, a transaction cannot be made and hence there is no threat. It should also be clear that if the attacker has both a complete set of card details and a stolen SIM for the cardholder, then the system cannot prevent an attack unless, of course, the SIM has been reported stolen and blacklisted by the network, or the SIM has been PIN protected by its owner. We therefore consider the two main `intermediate' scenarios.

i. **Scenario 1 :** Attacker has a stolen SIM without the corresponding card details.

In this scenario, if an attacker has stolen a SIM and the subscriber name of the stolen SIM is unknown, although a valid *SRES* can be generated, he/she will not be able to create a matched cardholder name necessary to pass the authentication process.

By contrast, if the attacker knows the subscriber name, it is possible to complete the protocol successfully using a fabricated set of cardholder details as long as the fabricated details include a cardholder name corresponding to the subscriber name. However, the fraud will become clear soon after the merchant tries to charge the card. In the most typical case for an e-commerce transaction, the merchant will try to charge the specified payment card before the goods are dispatched. In such a case, the threat is therefore small. Nevertheless, the threat can be more serious if the goods are, for example, information or music, which will be delivered instantly via the Internet. However, even in this case, the threat can be avoided if, as is often the case, the merchant server seeks payment authorization before authorizing delivery of the goods. If the card details are fabricated then the card issuer will, of course, reject the payment.

A possible way to prevent such attacks is for the SIM to be PIN-protected. It is also important that the PIN is never entered on an untrusted device.

ii. **Scenario 2 :** Attacker has stolen card details without the corresponding SIM.

If an attacker has only card details, without the SIM, it will not be possible to generate a valid *SRES*. This threat is therefore addressed by the scheme described above. Thus, to be successful, an attack on the user system needs both the victim's SIM and the corresponding debit/credit card details to complete a fraudulent transaction.

b. Threats to the communications links

If any of the information transferred across either of the links is modified, then the protocol will fail. Hence, a theoretical denial of service attack exists, although there are many simpler ways to prevent the completion of a transaction. We now consider other threats arising to the two links.

c. Threats on the PC/merchant server link

The confidentiality and integrity issues apply to the payment information transferred across this link. However, we assume that the Internet link between the PC and merchant server is protected using SSL/TLS throughout the transaction procedure.

Note that a possible alternative to the protocol described here would be to use GSM authentication to enhance the security of the SSL/TLS initialization process. However, if such an approach is followed, it is not clear how to achieve the desired link between the GSM subscriber name and the cardholder name.

d. Threats on the merchant server/AuC link

Threats on this link can be further divided into two types, namely integrity threats and confidentiality threats.

i. Integrity threats

There are a number of ways in which an attacker could manipulate this link in order to persuade the merchant server to accept an impostor. Perhaps the simplest method would involve the attacker using an arbitrary (valid) SIM and ME in combination with stolen card details (which, of course, will not match the GSM subscription name). In message 2 the AuC will provide a valid *RAND* and *XRES* for the attacker's SIM, and will return the name associated with the attacker's GSM subscription. An active attacker could change this name to the name associated with the stolen card details, and the merchant server will accept message 2. The remainder of the protocol will complete correctly, and the account for which the details were stolen will be charged for the transaction.

An alternative attack, again using stolen card details, does not require the attacker to have a valid SIM at all. The attacker supplies an arbitrary (but valid) GSM number with the stolen card details. In message 2, the AuC will send a (*RAND*, *XRES*) pair for the arbitrarily chosen GSM subscription, along with the subscriber name. The active attacker can then replace the contents of message 2 with the name for the stolen card details, along with an arbitrary (*RAND*, *XRES*) pair. The merchant server will accept message 2 because the names match, and will send the manipulated *RAND* to the attacker in message 3. The attacker simply returns the manipulated *XRES* value in message 4, and again the attack will succeed. The existence of these attacks means that it is vital that the integrity of the link between AuC and merchant server is protected.

ii. Confidentiality threats

There are also a number of serious confidentiality threats. First note that a passive eavesdropper can perform an attack similar to the second integrity attack described above. Suppose an attacker has a set of stolen card details and also knows the GSM number for the owner of the stolen card details. The attacker initiates the protocol using the stolen card details and the known GSM number. Message 2 will be accepted by the Merchant server because the GSM number belongs to the valid cardholder. However, if the attacker can intercept message 2, then the *XRES* value can be obtained. The attacker then simply inserts this value into message 4 and the protocol will complete successfully.

Also note that, in the absence of integrity and confidentiality, the merchant server/AuC protocol could also be used to find the subscriber name corresponding to any GSM number. This would be a significant breach of GSM subscriber confidentiality.

These attacks mean that it is important to provide both confidentiality and integrity for this link, and this is why we assume throughout this section that this link is both confidentiality and integrity protected.

e. Threats in the merchant server and the AuC

Since the merchant server is responsible for the identity authentication process, in particular the comparison of names and *XRES* with *SRES*, it is important to protect the server against any attack, which might cause the protocol to be bypassed.

Over and above the integrity of the user authentication process, the merchant server will have access to large volumes of potentially sensitive subscriber information. As part of the user authentication process, the merchant server retrieves from the AuC the account holder name for any GSM telephone number. Not only this a sensitive privacy issue, but also requiring the AuC to supply such information may potentially be in breach of its licence and/or data privacy legislation. It is therefore vital that the merchant server be protected and trusted so that this information cannot be abused.

The AuC is then required to compare the name supplied in message 1 with the name it has associated with the GSM number. If they do not match, the protocol should not proceed. If they do match, in message 2 the AuC simply provides a (*RAND*, *XRES*) pair.

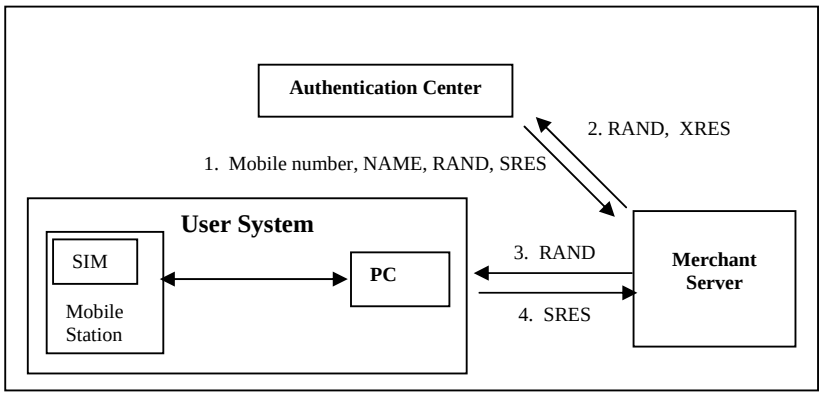

Figure 1.4: Revised Protocol

Another way to reduce this threat is for the merchant server to create and send a *RAND* to the User System and thence the SIM. Upon the receipt of the *RAND*, the SIM generates the *SRES* and sends it to the merchant server via the user PC. The merchant server subsequently sends the cardholder's name, his/her mobile number, the *RAND*, and the *SRES* to the AuC to verify. The protocol is shown in Figure 1.5.

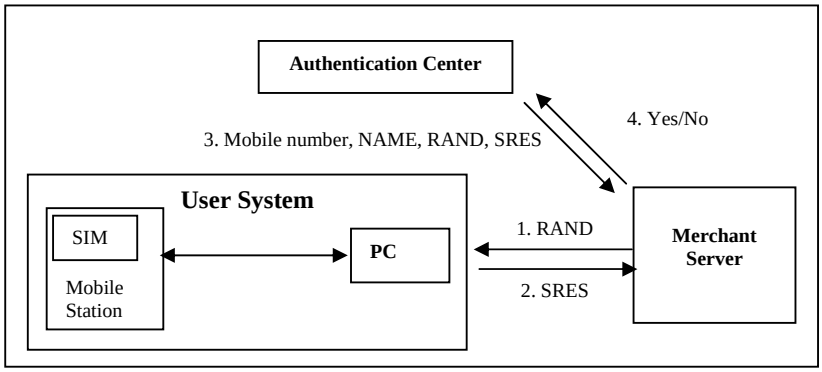

Figure 1.5: Another revised protocol.

These modified protocols have the advantage that the AuC retains control of sensitive subscriber information. However, it has the disadvantage of requiring additional processing by the AuC. If the integrity of the AuC could be compromised, then there are possible attacks to the security of the user authentication process. However, in such an event there are also many other serious attacks to the security of the GSM network itself, and so we assume that the AuC is well protected.

9. Conclusion

We have proposed a way in which GSM subscriber identity authentication can be used to enhance e-commerce security. The protocol provides user authentication and hence significantly reduces threats arising from misuse of misappropriated card details. It therefore also indirectly reduces the risk of storing card details in unencrypted from a merchant server. The protocol works with 'standard' GSM SIM and requires only appropriate equipped Mobile Equipment and a user PC. It therefore, imposes minimal overheads on the user, thus increasing the like hood of successful use. The gains for the merchant in terms of reduced chargeback also appear significant, and the possibility of an increased revenue stream may also make the system attractive to the GSM operators.

Reference

[1] N. Barnett, S. Hodges, and M. J. Wilshire . M-commerce: An operators manual. McKinsey Quarterly, 3:162-173, 2000.

[2] M. Walker and T. Wright. Security. In F. Hillebrand, editor, GSM and UMTS: The creation of global mobile communication, chapter 14, pages 385-406. John Wiley & Sons, 2002.

[3] European Telecommunications Standards Institution (ETSI). Digital cellular telecommunications system (Phase 2+); GSM Security Aspects (GSM 02.09 version 8.0.1), June 2001.

[4] S. M. Redl, M. K. Weber, and M. W. Oliphant. An Introduction to GSM. Artech House, Norwood, MA, USA, 1995.

[5] C. W. Blanchard. Security for the third generation 3G mobile system. Information Security Technical Report, 5(3):55-65, 2000.

[6] 3rd Generation Partnership Project (3GPP). *3GPP TS 33.102: Security architecture*, December 2002.

[7] V. Anupam and A. Mayer. Security of web browser scripting languages: Vulnerabilities, attacks and remedies. In *Proceedings of the seventh USENIX Security Symposium*, pages 187-200. USENIX, January 1998.

[8] H. Berghel. Caustic cookies. *Communications of the ACM*, 44(5):19{22, May 2001.

[9] C. W. Blanchard. Wireless security. In R. Temple and J. Regnault, editors, *Internet and Wireless Security*, pages 147-162. The Institution of Electrical Engineers, London, 2002.

[10] K. Boman, G. Horn, P. Howard, and V. Niemi. UMTS security. *Electronics Communication Engineering Journal*, 14(5):191-204, October 2002.

[11] Bureau of Export Administration, Department of Commerce. Revisions to encryption items. *Federal Register*, 65(203), October 2000.

[12] The CERT Coordination Center. malicious HTML tags embedded in client web requests, February 2000. Available at http://www.cert.org/advisories/CA-2000-02.html

[13] B. Hancock. Security views: Some cookies are not tasty. Computers & Security, 17(5):374-376, 1998.

[14] B. Haselton and J. McCarthy. Internet Explorer open cookie jar. Available at http://www.peacefire.org/security/iecookies/, May 2000

[15] V. Hassler. Security Fundamentals for E-commerce. Artech House Publishers, 2001.

[16] V. Hassler and O. Then. Controlling applets' behaviour in a browser. In Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC'98, Dec 7-11, 1998, Scottsdale, Arizona, USA), pages 120{128. IEEE Computer Society Press, 1998.

[17] Institute of Electrical and Electronics Engineers (IEEE). IEEE P1363: Standard specifications for public key cryptography, 2000.

[18] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Geneva. ISO/IEC 11770-1: Information technology - Security techniques - Key management - Part 1: Framework, 1996.

[19] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Geneva. ISO/IEC 10118-3: Information technology - Security techniques - Hash Functions - Part 3: Dedicated hash functions, 1998.

[20] ITU-T. Recommendation X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. Geneva, March 2000.