Comput Syst Sci & Eng (2009) 4: 13–20

International Journal of
Computer Systems
Science & Engineering

A SIM-based electronic transaction authentication system

Manzur Ashraf[1] and Syed Mahfuzul Aziz[2], M. Lutful Kabir[3] and Biswajit K. Dey[3]

[1] *Institute for Telecommunications Research. E-mail: Manzur.Ashraf@postgrads.unisa.edu.au*
[2] *School of Electrical and Information Engineering, University of South Australia, Mawson Lakes, SA 5095, Australia E-mail: Mahfuz.Aziz@unisa.edu.au*
[3] *Institute of IT, University of Dhaka, Dhaka 1000, Bangladesh*
E-mail: {lutful_bd, biswa.bd}@gmail.com

This paper presents a SIM-based tool for user authentication in various service areas such as financial transactions in e-commerce. Other remote services can use SIM as an authentication tool over existing GSM technology through GPRS, which is an additional packet data feature for the GSM network. GPRS enables packet-switched traffic to exist in predominantly circuit-switched GSM infrastructure. As GPRS is designed to support packet based protocols, such as the Internet Protocol (IP) based burst and uneven traffic flow, it enables new services such as reasonably fast access to the Internet, electronic mail and other data oriented services. These services have been too inefficient in traditional circuit-switched digital mobile networks. Using GPRS features the e-commerce applications can use SIM for user authentication in transactions. SIM can also be a tool for user identity and authentication around the corporate intranets. This can reduce security infrastructure setup and investment overhead for the security concerned organizations. This paper presents an electronic payment protocol that uses SIM based authentication along with illustration of its formal modelling and verification results. The proposed authentication system offers more robust security features than other electronic transaction systems proposed to date.

1. INTRODUCTION

The business community is always eager to add value to the existing infrastructure and always search for new ways to enhance productivity. The GSM (Global System for Mobile communications) network is being used widely around the world. Now-a-days GSM technology is used by more than 800 million end users in 190 countries representing over 70% of the worldwide digital wireless market. GSM already provides strong security features including authentication and data encryption over the air interface. GSM, by tradition, supports circuit switched fixed channel architecture which can only provide 9.6 kbps data rate and 160 character short message services. GPRS (General Packet Radio Service) is a bearer service over the existing GSM infrastructure that enhances the GSM network functionalities by providing an additional packet data feature. This allows both packet switched and circuit switched traffic to exist in the same GSM infrastructure. GPRS achieves the high speed by transmitting packets of data in parallel. Eventually GPRS enables GSM to support the Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS), and internet communication services such as email and World Wide Web access. As GPRS works over GSM infrastructure it inherits almost all the security features of GSM including authentication and over the air data encryption. GSM security features include key management which is independent of equipment, subscriber identity protection, detection mechanism for compromised equipment, subscriber authentication, signalling and user data protection etc [1].

In this paper, we propose a simple SIM-based authentication protocol for electronic transactions using the mobile phones. In general the IMSI (International Mobile Subscriber Identity) stored in the SIM of a mobile phone is not used for any authentication purpose for the high security risk factors described in [2]. In the protocol proposed in this paper the mobile number (which is registered at the relevant Financial Organization beforehand) is used in conjunction with the encryption methods used in e-transactions. The protocol uses an asymmetric authentication

from the mobile terminals to the authentication server, which indirectly reduces the threat posed by the storage of un-encrypted card numbers in a Merchant server. It therefore makes sense to use any GSM based authentication in conjunction with GPRS to provide network services. In short, the protocol makes use of the mobile station portability and the GSM authentication mechanism to provide user authentication in a way that also supports user mobility.

The paper starts with an overview of the problems associated with "password only" authentication and related works on SIM based authentication in Section 2. Section 3 presents definitions and descriptions of the entities required to support the proposed authentication protocol. Section 4 highlights the proposed electronic payment protocol based on SIM authentication provided by the GSM network. Section 5 presents the pros and cons of SIM based authentication. The formal modelling and verification of the protocol are presented in Section 6. Finally Section 7 concludes the paper.

2. OVERVIEW AND RELATED WORKS

Traditionally user ID and password are commonly used for user authentication. This method has a serious drawback. Anyone, even a totally unknown person, can somehow get those confidential entities easily by means of social engineering [3]–[5]. When one enters a password in an open environment it can be guessed by others. As password is the key factor in authentication, anyone who achieves this key can unlock any confidential account. This defeats the purpose of authentication. Passwords are also vulnerable to brute force attack, dictionary attack etc. [6].

In early days of e-commerce this type of authentication was deemed to be sufficient for most traditional systems and services. But now-a-days massive use of technology and information systems in almost every sphere of organizational, social and personal life means that key management for authentication is problematic. Almost everywhere we go for a service we need authentication. Mobility makes it more challenging to authenticate the right entity properly.

Suppose we have a bank account and we want to use a credit card. The credit card number and password are vulnerable to social engineering. Consider another scenario, where we have three accounts in different banks and hence three credit/debit cards. We need to remember three passwords and keep these secret. If we unfortunately loose these cards we need to inform three organizations to lock the accounts temporarily and reissue new passport for these accounts. Even the newest authentication technology, such as 3-D Secure [7] developed by Visa, uses a PIN/Password based authentication for its card holders and it inherits similar authentication drawbacks as the traditional systems [8].

Among other features, existing GSM based payment protocols make use of messaging or customer interactions, asking them to register with an e-wallet or receive phone calls. For example, the proposal of Claessens et al. [8] provides user authentication using SIM by means of extensive use of SMS messages. Other GSM based payment systems such as those proposed by Mint and Paybox [9] need customers to first open an e-wallet. Transactions in these two protocols involve either making or receiving calls using the delegated mobile phone. In the GiSMo scheme [9] consumers open an electronic wallet over the internet and provide mobile number there. Every internet transaction is thus validated with a password over the mobile phone using a SMS message, which results in lack of user-flexibility and excessive computations.

Nonetheless the work in this paper is close to [9], where a cardholder's identity as well as the GSM subscriber identity in conjunction with his/her debit/credit card is used in transaction authentication. However, it lacks user flexibility and is inappropriate for situations when either device is absent. Furthermore, the GSM identity itself should not be used for authentication purpose unless some complex cryptographic measure is incorporated as was suggested in [2]. The serious drawback is that the Merchant server is aware of the credit card and the SIM information of the user as well as the corresponding purchases in every instance. Hence user privacy is not preserved at all. This paper addresses these issues.

We propose a simple SIM-based protocol (where the mobile phone number is used in conjunction with asymmetric ciphering) as a single alternative to all the above schemes to manage authentication in a simple, efficient and secure way. It replaces the need for a card against an account. Therefore people can do transactions using either cards or mobile phone. Due to the asymmetric ciphering [2] the security risk however is almost same in the proposed protocol as in [9].

3. ENTITIES IN SIM BASED AUTHENTICATION

Entities that are required in the proposed architecture are based on some assumptions. These entities are presented next.

3.1 Consumer (or user)

The customer needs a Mobile Station (MS), which contains a Mobile Equipment (ME) such as a handset, a SIM (Subscriber Identification Module) and a Token Generation Server (TGS) on the handset. The Token Generation Server is preinstalled into the phone/handset. The request for a token to initiate a transaction is passed from the Merchant's Service Terminal (ST) to the TGS on the phone. The MS is also capable of performing asymmetric key cryptography [2].

1) *Subscriber Identification Module (SIM):* The Subscriber Identification Module (SIM) is a subset of Smart Card – a single chip computer containing a simple International Mobile Subscriber Identity (IMSI, which is unique for each user), operating system, file system and applications protected by PIN (Personal Identification Number). It is generally owned by operators who are supposed to be trusted. Applications related to SIM can be written using SIM Toolkit [10].

A customer who has an account in a financial organization (such as a bank) is supposed to have an MS and the account is registered against the Mobile Number (MN).

3.2 Merchant

The Merchant needs to have a Service Terminal (ST), which contains a Token Request Client (TRC) to request the TGS residing

in the consumer's MS for a token to submit a transaction request to the financial organization. The ST is residing between the Merchant and the User (Consumer) and is capable of communicating with the MS.

3.3 Financial organization (FO)

The Financial Organization (FO) (such as a bank) is registered with an Authentication Centre (see below) for authentication purposes. The consumer's account should be registered against a SIM (i.e., Mobile Number) and it replaces credit/debit cards.

3.4 GSM mobile network (GMN)

The GSM Mobile Network (GMN) is responsible for authentication. Its Authentication Centre (AuC) keeps a database of subscriber authentication information (such as IMSI- International Mobile Subscriber Identity or TMSI - Temporary Mobile Subscriber Identity, Ki-Shared Secret Key between SIM and AuC). IMSI/TMSI is used to identify a SIM in its network and Ki is used for authentication and key generation for GSM mobile communication. For our protocol the financial organizations need to be registered with the AuC to get authentication services.

3.5 Communication processes

The dialogue between the consumer and the Merchant is shown in Figure 1. The overall communication process is shown in Figure 2. We describe the communication process next.

1) *Between Consumer and Merchant:* The key and token data exchanges between Consumer and Merchant are encrypted using Bluetooth baseband encryption [11]. The phone establishes a remote connection via Bluetooth. Bluetooth is a low power short range radio technology, originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets and portable computers. Bluetooth has revolutionized the way people interact with the information technology landscape around them. People no longer need to connect, plug into, install, enable or configure device-to-device communications. The Bluetooth specification is an open, global specification defining the complete system from the radio up to the application level [12].

2) *Between Merchant & FO, FO & GMN:* This link can use Virtual Private Network (VPN) for communication.

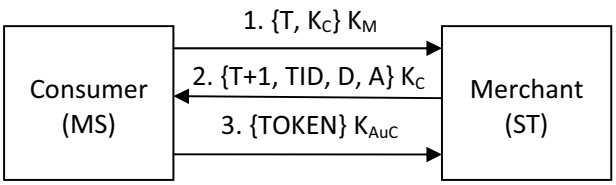

Figure 1 Dialogue between Consumer (MS) and Merchant (ST).

3) *Between GSM Mobile Network (GMN) and Consumer:* The consumer's MS communicate with the AuC within its GSM Mobile Network perimeter via radio link and GSM security protocol infrastructure.

4. PROPOSED ARCHITECTURE AND PROTOCOL

4.1 Assumptions

We proceed with some assumptions to make the proposed protocol simpler and easy-to-use.

- Each customer is assumed to have one account associated with the SIM.
- In the series of communication paradigm described below we do not assume any message loss, denial of service, retransmission or time out. However these issues can easily be resolved using protocol engineering approaches described in [13].

4.2 Steps

Our proposed authentication protocol is described in the following steps.

Step 1: The Consumer will initiate the process by sending the Time Stamp (T) and Consumer's Public Key (K_C) by encrypting it with the Merchant's Public Key (K_M) to the Service Terminal (ST) at the Merchant side.

Step 2: The Merchant sends a TOKEN request with timestamp T+1, Transaction ID (TID) and Amount (A) by encrypting them with K_C to the TGS of MS. T+1 ensures that the TOKEN request is from the actual Merchant from whom the consumer is intending to purchase items.

Step 3: If the Consumer agrees with the received information then the TGS sends a TOKEN encrypting it with GMN's Public Key (K_{AuC}) to the ST of the Merchant. The TOKEN contains International Mobile Subscriber Identity (IMSI), Validity Period (V), Transaction ID (TID), Source Account Information (S), Destination Account Information (D), Mobile Number (MN) and Amount to Transfer (A). IMSI is used to identify the Consumer's SIM and V for protection against replay attack. If the actual request arrives within V then the request is valid to the Consumer for the first entry only.

Step 4: The Merchant sends the TOKEN along with the Consumer's Mobile Number (MN), Transaction ID (TID), Destination Account Information (D) and Amount to Transfer (A) to the Consumer's Financial Organization (such as a bank) for transaction.

Step 5: The financial organization will send the TOKEN received from the Merchant to GMN's AuC to authenticate the request. AuC decrypts the TOKEN with its Private Key (K_{AuC}^{-1}).

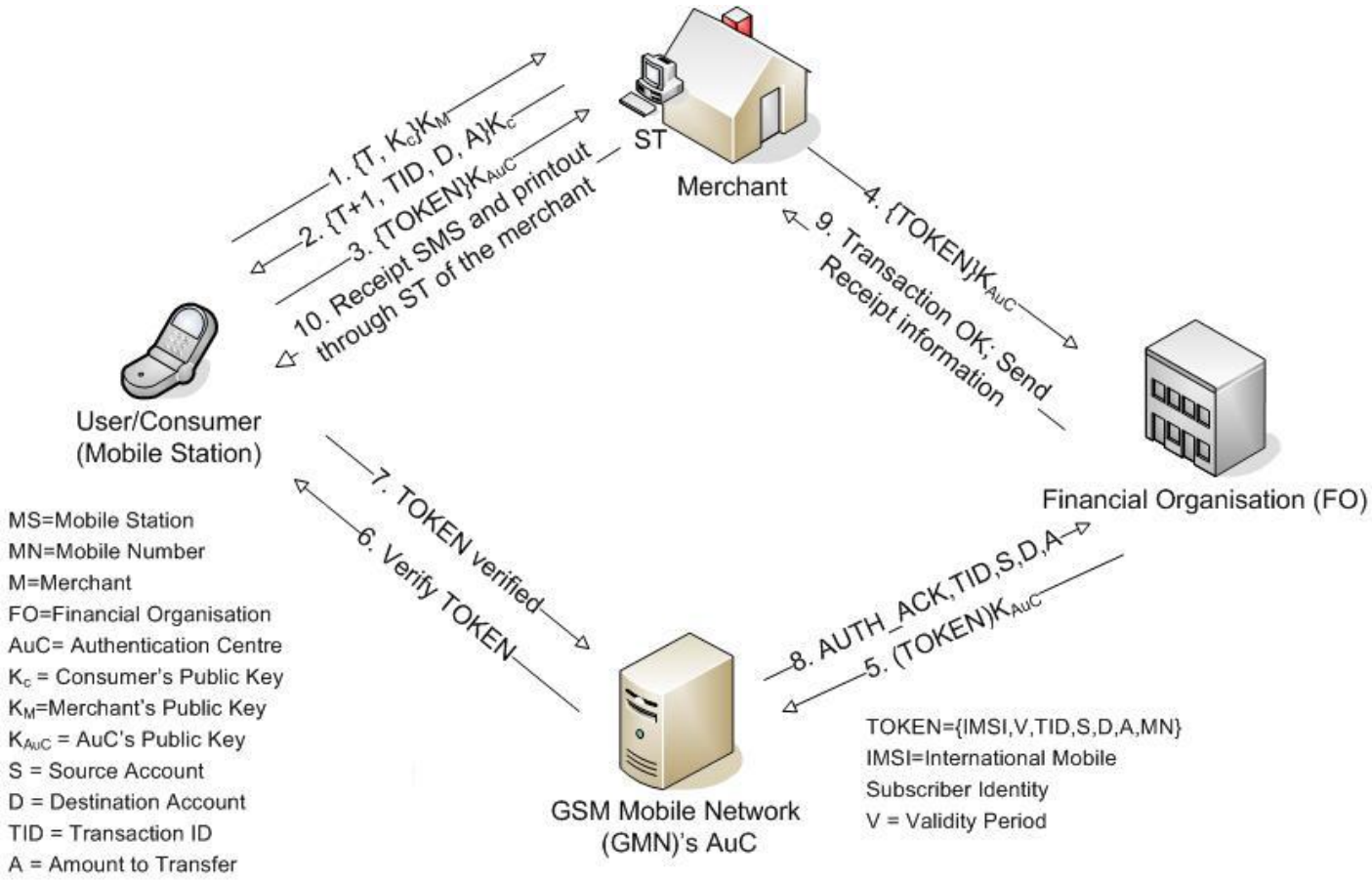

Figure 2 SIM-based authentication and electronic payment protocol.

Step 6: GMN's AuC sends a verification request to the Consumer's MS.

Step 7: Consumer's MS sends verification acknowledgement to the AuC.

Step 8: GMN's AuC sends Authentication Acknowledgement (AUTH_ACK), TID, S, D and A to the Financial Organization (FO).

Step 9: If successful (i.e., TID, D and A matches with those sent by the Merchant) then the FO will complete the transaction with the Merchant against the TID. The FO sends the purchase information, e.g. partial information of the sender card (for security), purchase date, amount etc. to the Merchant.

Step 10: The Merchant sends a SMS receipt to the MS. Optionally a printout of the receipt is generated through the Service Terminal (ST) of the Merchant.

4.3 Dialogue summary

1. Consumer → Merchant: {T, K_C} K_M
2. Merchant→ Consumer: {T+1, TID, D, A} K_C
3. Consumer → Merchant: {TOKEN} K_{AuC}
4. Merchant → FO: MN, TOKEN, TID, D, A
5. FO → GMN's AuC: Authenticate TOKEN Req.
6. GMN AuC → Consumer: Verify TOKEN Req.
7. Consumer → GMN AuC: TOKEN Verified Ack.
8. GMN AuC → FO: AUTH_ACK, TID, S, D, A
9. FO → Merchant: Send purchase information, e.g. partial information of the sender card (for security), purchase date and amount.
10. Merchant → MS: SMS receipt and printout receipt through Merchant's terminal (ST).

5. SECURITY ANALYSIS

5.1 Basic assumptions and security breaches

We assume that AuC and FO are trustworthy servers. However, if the integrity of AuC is somehow compromised then there will be possible attacks on the authentication process. In such a case the GSM network itself will be vulnerable to security breaches. Hence we assume that the AuC is secured. Furthermore, as soon as the AuC receives the TOKEN for authentication (in step 5 above) it performs a certificate based authentication [14] to

identify an FO. This step is required if we relax the assumption of a secured FO in the network.

As shown above a purchase receipt is provided to the MS in step 10. In case of an erroneous system operation or if the correct purchase amount is changed due to a compromised AuC or FO or Merchant, the consumer can claim it back using the receipt.

5.2 Security enforcement using the TOKEN

The TOKEN contains Destination Account Information (D) to use for further verification of the actual transaction request from the Merchant against a TID. If a third party gains the TOKEN and uses it to initiate a fraudulent transaction the AuC will break the TOKEN and ask MS for its validity with its D. The transaction can only proceed after this validation. As the TOKEN is encrypted with the public key of the AuC only AuC can break it for verification, determine the Source Account Information (S) and send to the FO for transaction after successful authentication. The time stamp (T) information is used to properly maintain all subsequent flow of control or data messages among the entities (User, Merchant, FO, AuC). In case of packet losses the time stamp information is used to refrain from any duplication error in possible retransmission mechanisms.

5.3 Threats in the merchant server

In [9], the Merchant server interacts with the user (mobile terminal) and AuC server. AuC is required to supply the Merchant server with the parameters necessary for the GSM identity authentication process. A serious drawback therefore is: what will happen in case a Merchant server is compromised by an adversary? Alternatively can a user trust a Merchant or seller to give his/her own information (e.g. GSM identity or phone number for a transaction)? Our protocol overcomes this problem by not requiring the disclosure of user information to the Merchant. In other words, the Merchant is not concerned about the Consumer's account. It keeps the Consumer's account anonymous. The user information is sent using an asymmetric authentication procedure via the Merchant server to the FO. Furthermore, FO to Merchant connectivity is done using a VPN, where the authenticity and security risks are handled predominantly from the FO side. Hence the proposed protocol can be regarded as secured and feasible.

5.4 Threats in the mobile station

There appears to be a weakness in the proposed system in case of stolen mobile handsets. An optional device specific PIN number (now-a-days such firm-wired provision is built into most of the mobile phones) can be used to tackle this problem. Furthermore, for rigid security requirements, user password as well as PIN number can be incorporated into the overall system. Due to the presence of GPRS further encryption of user passwords may be feasible in this context.

There is a probability that the SIM may be cloned [15], for example by a legitimate user. This may be harmful for the security of the authentication process. To prevent cloning the SIM design should be clone resistant. It will incur a cost though. Eventually the GSM network does not support two SIM to be alive at the same time with the same Identity.

5.5 Threats in the communication links

We assume that the communication links between the MS and Merchant server is secured using the latest Bluetooth security [16]. Bluetooth provides a frequency-hopping scheme (1,600 hops/second) combined with radio link power control (to limit the transmit range), which provides some protection from eavesdropping and malicious access. The frequency hopping scheme, mainly a technique to avoid interference, makes it slightly more difficult for an adversary to locate the Bluetooth transmission. Moreover, a Bluetooth device initiates a security procedure applying its Mode 3 operation (the link-level security mode) before the channel is established. This mode supports authentication (unidirectional or mutual) and encryption for a secured communication.

We also assume that no corrupt base station is connecting to an MS, since such security features are actively handled by the GSM network itself.

Each communication step (step 1 to 10) is repeated for a number of times in case of operational errors such as low signal from an MS to a base station. If the number of repeated unsuccessful operations exceeds a predefined limit the total operation is stopped and started again according to user intervention.

5.6 Providing anonymity

One of the open problems in the current e-commerce authentication is the scenario where either the buyer or the seller or both want to maintain anonymity [17]. This raises the issue of providing an authentication without identity disclosure. For instance, a seller may want to sell items to buyers without disclosing his/her identity, so that this information remains hidden to the competitors. Therefore a quality (properly secured) authentication is needed even without identity authentication directly between the buyer and the seller. Nevertheless the identities of both the parties are authenticated by the FO and GMN's AuC. Our proposed mechanism attains this combined authenticity, where the user information is hidden to the Merchant server while transaction is performed securely. In other words, neither the source account nor the mobile number is given to the Merchant, as they are encrypted as a part of the TOKEN using the public key of AuC. Therefore, the Merchant or the FO cannot collect purchase history of the consumers through their mobile numbers.

6. ADVANTAGES

As we have stated earlier the existing GSM authentication mechanism does not have a means of mutual authentication [18]. It means that the operator can authenticate the SIM and hence the subscriber but the subscriber cannot authenticate the operator. A

third party can act as operator and can make the authentication process insecure. However, mutual authentication is performed smoothly in our proposed method.

As GPRS provides higher bandwidth [15] we can use more complex authentication mechanisms to make the process more secure for high value transactions.

Can the proposed SIM-based electronic transaction authentication system be extended for use globally or in any place where GSM networking service is available? The International Subscriber Mobile Identity (IMSI) is a unique 15-digit number associated with every SIM used in the GSM and UMTS mobile phones. The first 3 digits are used for country code and the remaining digits represent a unique subscriber under a particular network operator. Hence our proposed protocol can be extended using both IMSI and mobile phone number (f (IMSI, mobile number)) instead of only mobile number (f (mobile number)) to do the aforementioned authentication.

7. MODELLING AND VERIFICATION OF THE PROTOCOL

Modelling can be seen as a process of abstracting the functional specifications of a system into a minimal working example that enables us to understand and analyse a particular aspect of the system more closely. Verification means the process of examining this specification for the presence of various errors that could lead to improper system operation. First we explain the need for a formal modelling and verification of the proposed authentication protocol as follows:

- In case of message interchange in a real-time system (Figure 2), deadlock or race condition may appear. Any message flow A, depending on another flow B, may not proceed since flow B also waits for flow A or for the completion of another non-terminating event. We can identify all possible deadlocks/race conditions using a Finite State Machine (FSM) based tool.
- In designing a complete protocol, *retransmission* and *timeout* events need to be properly handled in case of channel uncertainties or congestion in the medium resulting in packet losses. We can identify the possible retransmission policies required among the entities in the protocol and tune the protocol functionalities completely so that it continues to work full time.

There are five elements of specifications for a protocol, namely service part, assumption, vocabulary, encoding (format) and procedure rules [13]. SPIN [19] is a verification system that supports the design and verification of finite state asynchronous, distributed and concurrent systems. In the remainder of this section we discuss the five characteristics of the proposed protocol and verify the protocol using SPIN.

7.1 Services and procedure rules

The proposed SIM-based authentication protocol performs authentication between many-to-many authenticating peer and the authenticator (four entities: Consumer, Merchant, Financial organization and Authenticating server). Therefore this protocol is used for the client server architectural model. This allows it to be used in a large variety of M-commerce applications for authentication procedure as well. The protocol itself doesn't maintain any state but performs correlation and coordination between messages. For example, during the authentication process, the authenticator sends multiple requests to the peer and receives multiple responses. Each subsequent request depends on the response to the previous request. It is the responsibility of the authenticator and authenticating peer to define such combined processing.

7.2 Assumptions about the environment

The major assumptions about the messaging framework of the proposed authentication processing model are:

a) Request/Response is sent to an Authenticating Peer/Authenticator via zero intermediaries.

b) Underlying protocol handles message corruption and disruption.

c) Message fragmentation mechanism is not considered.

d) Each message contains a sequence number r = (r + 1) *%message_range*.

e) A new session will always be established after successful authentication.

7.3 Protocol vocabulary and message format

For simplicity and the abstraction levels required, we intend to use the minimum number of channels. They are: *toConsumer, toMerchant, toFinancialOrganization* and *toAuthenticatingServer*. Upon receiving data through a particular channel, entity in the next step (shown in the dialogue summary in Section 4.3) will continue sending data through the appropriate channel.

7.4 Simulation and verification results

After constructing the code in the XSPIN environment [19] we ran the simulation. The snapshot of the message sequence chart obtained from simulation is shown in Figure 3.

1) Correctness: We would like to prove that correct implementations of the model acting in all combinations of roles are well behaved. By this we mean that the rules of the protocol prevent the system from entering undesirable states such as deadlock (all agents blocked or waiting for others to act) or live lock (agents interacting in a way that produces no "progress"). Alternatively correctness properties can be expressed as (a) properties of reachable states (Safety) and (b) properties of sequences of states (Liveness). Checking 'Safety' comprises two things: (1) checking local process assertions and invariants (if any), and (2) checking proper termination points of progress (end state levels

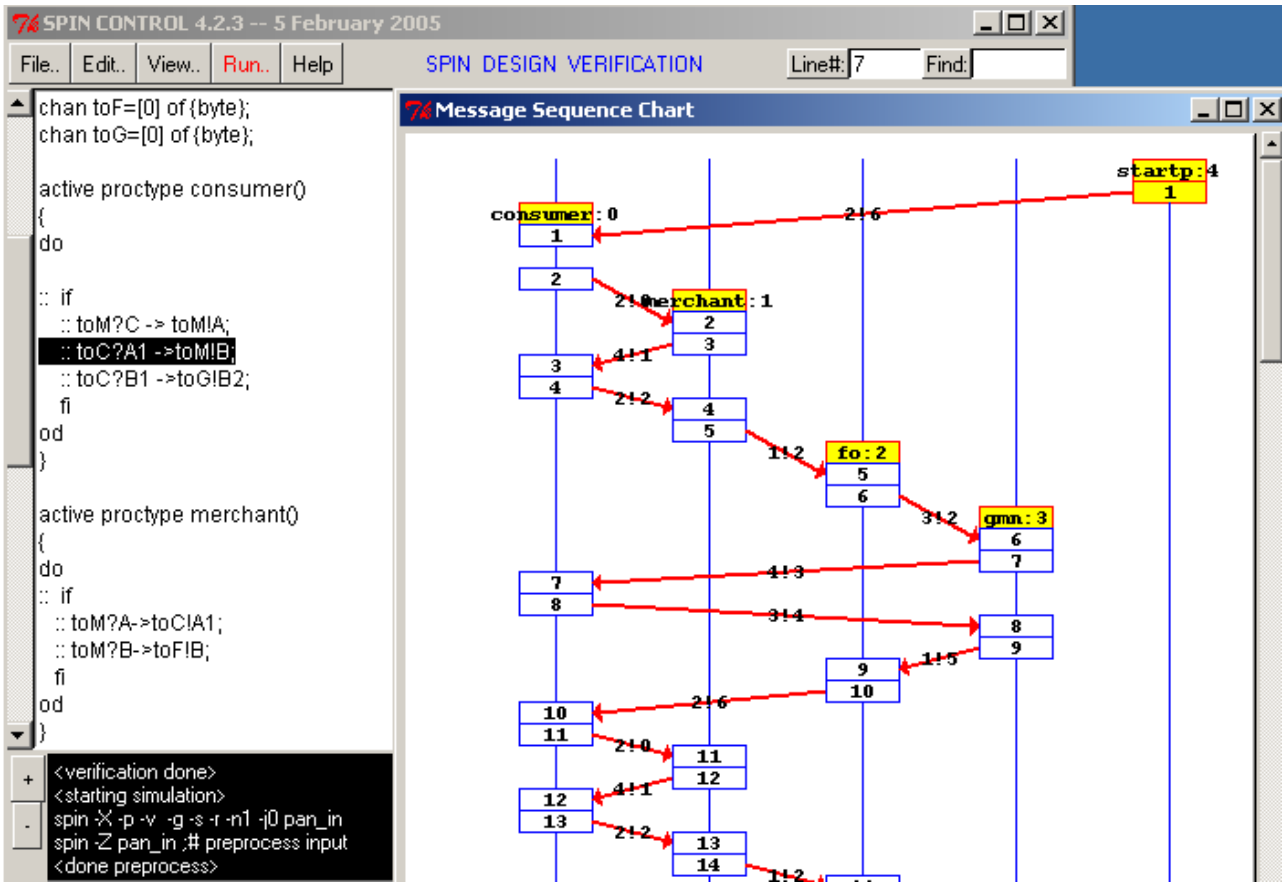

Figure 3 XSPIN output of the simulation run.

if any). Validating 'Liveness' comprises (1) looking for acceptance cycles, (2) looking for non-progress cycles, (3) using never claims - which defines an observer process that executes synchronously with the system, and (4) trace assertions - to reason about valid or invalid sequences of send or receive statements.

The result of 'Bit State Search' is as follows: State-vector is 48 byte, depth reached 20, errors = 0. Hash factor is 6.10081e+006 (best if hash factor is greater than 100).

Statistics on the memory usage (in Megabytes) is 0.001; equivalent memory usage for states (stored*(State-vector + overhead)) is 16.777; memory used for hash array ($-$w26) = 0.360; memory used for DFS stack ($-$m10000) = 0.467; other (proc and chan stacks) usage = 0.097; memory lost to fragmentation = 17.342.

From the verification results, hash factor is very large ($>$100). This means that we are confident about sufficient coverage [13]. All the validation runs confirm that correctness requirements of our proposed authentication protocol are properly met.

Incorporating the (re)transmission request among all the entities we can include and explore the following managerial requirements into the protocol:

- How long a User or a Merchant will wait in case of channel uncertainties or server congestions?
- If AuC or FO fails, how will the procedure proceed? We extend the protocol using a credit based customer benefit approach. In case of a mutual trust between a Merchant and a User, the Merchant can place the User on a list and can give credits based on his/her past records. It is similar to a credit card mechanism where the customer pays the bank later. In case of unavailable FO or AuC, the Merchant can do the same and do batch processing for trusted customers at a later time. There is no need for the instantaneous TOKEN verification (Steps 5 to 8) in this *credit based customer benefit approach*.
- We can further extend the protocol including *a negotiation-based price fixation* [20]. In this case an online server between the Merchant and User fix the price based on some negotiation rule so that the protocol can be extended for use in the Internet (online) as well.

7.5 Scalability

In the simulations we can incorporate a large number of user requests with an unbounded buffer size in all entities. Sequence numbers are required to put into the packet numbers (as another extension of the protocol) to facilitate the flows from the User to AuC. There might be a number of FOs and AuCs present in the network for better network services. In that case the Merchant should connect the FO with the shortest or less congested route. The connectivity of FO and AuC is also through the optimal link. All the AuCs must synchronously update the central database. While connecting the User to its nearest AuC the token verification process will use the mutual authenticities of all the AuCs with the corresponding central database. While performing this scalable scenario in simulation we did not get any inconsistencies or race conditions.

8. CONCLUSIONS

In this paper we have proposed a simple and efficient SIM-based authentication mechanism for electronic transaction systems. In this authentication mechanism the user identity is not disclosed to the Merchant, as opposed to existing SIM-based authentication systems [9]. The TOKEN generated by the user's mobile station (MS) is verified by the Authentication Centre (AuC) using direct encrypted communication with the user's MS. This provides far greater security than the Merchant-based authentication mechanisms [9]. With the widespread use of GSM technology worldwide the proposed model can be used effectively to provide the framework for implementation of a global electronic passport. Although it has some inherent weakness and limitations, microprocessors and memory chips are increasingly gaining more power with the efficiency of cost. It is expected that the SIM will provide more computing power and memory space in the near future. So it will be able to run more sophisticated and complex procedure for authentication and key generation. SIM will soon be capable of running applications related to biometrics for secure authentication.

REFERENCES

1. J. Quirke, *Security in the GSM system*, http://www.ausmobile.com/, May 2004.
2. Y. Xiao, *Security in distributed, grid, mobile and pervasive computing*, Auerbach publications, 2007.
3. R. Farrow, *Social Engineering*, Watchguard publications, http://www.watchguard.com/infocenter/, 2005.
4. S. Granger, *Social Engineering Fundamentals part II: Combat strategies*, Crime-Research, http://www.crime-research.org/library/razum2.htm, 2005.
5. *The problem with password*, A report by Articsoft Inc., http://www.articsoft.com/, 2004.
6. *3D secure System overview version 1.0.2*, http://international.visa.com/, 2003.
7. *3D Secure Protocol Specification core functions version 1.0.1*, http://www.visa.com/, 2001.
8. J. Claessens, B. Preneel, and J. Vandewalle, "Combining world wide web and wireless security", Advances *in Network and Distributed Systems Security*, vol. 99, no. 11, pp. 153–171, January 2001.
9. V. Khu-smith and C. Mitchell, *Enhancing E-commerce Security Using GSM Authentication*, Springer Berlin/Heidelberg, 2003.
10. V. Ramasami, *Security, Authentication and access control for mobile communications*, http://citeseer.ist.psu.edu/456876.html, 2000.
11. J. Bray and C. Sturman, *Bluetooth1.1: Connect Without Cables,* Prentice Hall, 2nd edition, ISBN 0-13-066106-6, 2002.
12. C. C. Lee, M. S. Hwang, and W.P. Yang, "Extension of authentication protocol for GSM", *IEE Communications*, vol. 150, no. 2, pp. 91–95, April 2003.
13. G. Holzmann, *Design and verification of protocols*, Prentice Hall, 1990.
14. A. Kukec, S. Gros, and V. Glavinic, "Implementation of certificate based authentication in ikev2 protocol", *Proc. 29th International Conference on Information Technology Interfaces*, pp. 697–702, 2007.
15. J. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, "Partitioning attacks: Or how to rapidly clone some GSM cards", *IEEE Symposium on Security and Privacy*, vol. 1, no. 1, pp. 31–40, January 2002.
16. T. Karygiannis and L. Owens, "Wireless network security 802.11, bluetooth and handheld devices", Tech. Rep., NIST, 2002.
17. A. Basu and S. Muylle, "Authentication in e-commerce", *Communications of the ACM*, vol. 46, no. 12, pp. 159–166, December 2003.
18. L. Yi-Bing, R. Herman, and C. Imrich, "General packet radio service (GPRS): architecture, interfaces, and deployment", *Wireless Communications and Mobile Computing*, vol. 1, no. 1, pp. 72–92, January 2001.
19. G. Holzmann, *SPIN and XSPIN tools*, http://spinroot.com/spin/whatisspin.html, 1990.
20. M. M. Ashraf and M. Ashraf, "Negotiation life cycle and AI-based negotiation modeling for interactive marketing system", *Proc. EEE Intelligent Automation Conference*, December 2003, pp. 799–803.