An Overall Cost-effective Authentication Technique for the Global Mobility Network

Chang-Kuo Yeh[1] and Wei-Bin Lee[2]
(Corresponding author: Chang-Kuo Yeh)

Department of Information Management, National Taichung Institute of Technology[1]
129, the 3rd Section, San Ming Rd., Taichung, Taiwan, 404, R.O.C.
Department of Information Engineering,
Feng Chia University, Taichung, Taiwan, 407, R.O.C.[2]
(E-mail:yehliny@ms18.hinet.net, lwb@fcu.edu.tw)

(Received Oct. 11, 2008; revised and accepted Nov. 24, 2008)

Abstract

Designing an efficient and secure authentication technique to detect fraudulent behavior is a very important subject in mobile network systems. However, treating each transaction as a suspect seems to contradict the fact that most communication behaviors are honest. Based on this fact, it is reasonable to design a more efficient authentication protocol despite its loss of efficiency in dishonest communication situations. In such a way, an overall cost-effective solution can be obtained. In this paper, the BGSW protocol is redesigned under the concept and a cost-effective solution is shown. However, we have to emphasize that main purpose of this paper is not to improve the BGSW protocol, but to show the new idea that it is reasonable to design a more efficient authentication protocol despite its loss efficiency in dishonest communication situation.

Keywords: Authentication, cryptosystem, challenge-response, global mobility network

1 Introduction

There is a steadily increasing amount of services offered through mobile networks since mobile networks provide a very convenient way of communications. The exponential growth of wireless and mobile networks and their use for business applications over the Internet have brought vast changes for the mobile devices, middleware development, standards and network implementation [17, 18]. However, because no physical circuit is required in mobile networks, security problems must be considered. Owing to restricted resources of portable devices, efficiency should also be taken into account. Authentication should be possible for the receiver of a message to ascertain its origin and ensure that the network service will not be obtained fraudulently. Providing secure and efficient authentication solutions for mobile networks has become very important when Internet and wireless communication applications have been increasing recently [4]. As a result, many authentication techniques of Global Mobility Network have been proposed. These authentication techniques benefited from the utilizing of cryptosystems [13] including Secret-Key based systems [3, 7, 9, 11, 16] and Public-Key based systems [5, 6, 8, 12, 14], and are designed to be able to detect fraudulent behaviors. However, if communication frauds occur too frequently, the entire communication system will be paralyzed; consequently, most communication behaviors should be honest to keep the entire communication system work smoothly. Treating each transaction as suspicious seems to contradict the fact that most communication behaviors are honest. Based on the fact, it is reasonable to design a more efficient authentication protocol despite its loss efficiency in dishonest communication situation. In this paper, the BGSW protocol [7] is redesigned to benefit from this observation and is shown to be a cost-effective solution. BGSW authentication protocol proposed by Buttyan et al. presents cryptanalysis and improvement on the protocol proposed by Suzuki and Nakada [16]. BGSW protocol not only has the same architecture as GSM [15] and UMTS [1] but also has a transparent process for mutual authentication between mobile user, visited network and home network. Thus, we adopt the scheme as an example to show the feasibility of our idea. The main purpose of this paper is not to improve the BGSW protocol, but to show the new idea that it is reasonable to design a more efficient authentication protocol despite its loss efficiency in dishonest communication situation. In the next section, the BGSW protocol is briefly reviewed. Our scheme will be illustrated in Section 3 and the security and performance analysis will be discussed in Section 4 and Section 5. Finally, the conclusion is given in Section 6.

2 Review of BGSW Scheme

Before describing BGSW scheme, some notation should first be defined. $X \rightarrow Y : Z$ denotes that a sender X sends a message Z to a receiver Y. U, V and H denote a roaming user, visiting network and home network, respectively. UID, VID, and HID denote the identity of U, V and H, respectively. $R0$, $R1$, $R2$ and $R3$ are random numbers. K_{VH} denotes the secret key shared by V and H, K_{UH} denotes the secret key shared by U and H, and K$_{UV}$ denotes the session key shared by U and V. $[M]N$ denotes a message M encrypted by key N.

The scheme is illustrated as follows.

Step 1. $U \rightarrow V : Request, R0$

Step 2. $V \rightarrow H : R1$

Step 3. $H \rightarrow V : R2, [R1]K_{VH}$

Step 4.

1) Decrypt $[R1]K_{VH}$
2) Verify $R1$
3) Generate K_{UV}
4) $V \rightarrow H : [UID, R2, K_{UV}, R0]K_{VH}$

Step 5.

1) Decrypt $[UID, R2, K_{UV}, R0]K_{VH}$
2) Verify $R2$
3) H $\rightarrow V : [VID, K_{UV}, R0]K_{UH}$

Step 6. V $\rightarrow U : R3, [VID, K_{UV}, R0]K_{UH}$

Step 7.

1) Decrypt $[VID, K_{UV}, R0]K_{UH}$
2) Verify $R0$
3) $U \rightarrow V : [R3]K_{UV}$

Step 8.

1) Decrypt $[R3]K_{UV}$
2) Verify $R3$
3) $V \rightarrow U : [[R3]K_{UV}]K_{UV}$

Step 9.

1) Decrypt $[[R3]K_{UV}]K_{UV}$
2) Verify $[R3]K_{UV}$

Challenge-response technique [10] is employed to provide security and service authentication here. V authenticates H and U by verifying $R1$ and $R3$ in Step 4 and Step 8, respectively. H authenticates V by verifying $R2$ in Step 5. U authenticates V by verifying $[R3]K_{UV}$ in Step 9. To prevent replay attack, U verifies $R0$ in Step 7.

In honest communications, BGSW scheme needs to complete the entire authentication process so that five encryptions $(2K_{VH}, 1K_{UH}$, and $2K_{UV})$ and five decryptions $(2K_{VH}, 1K_{UH}$, and $2K_{UV})$ are needed. However, if an attack is made, such as a masquerading H' trying to pass through the authentication process, it will be detected by V through verifying $R1$ in Step 4 and the authentication process is hence terminated at Step 4. The number of computations is significantly reduced to only one encryption (K_{VH}) and one decryption (K_{VH}). Obviously, BGSW does its best to detect the fraud as early as possible. The question is that is it worth the time to screen for fraudulent behaviors when they seldom occur? Based on the fact most communication behaviors are honest, there still has room to do optimization by reducing the number of cryptographic operations in most of the cases.

3 Our Scheme

The idea behind our scheme is that we do our best to promote the overall performance of the authentication process as efficiently as possible. The overall efficiency of our scheme is expected to be better than BGSW protocol in case honest communications constitute the majority of total communications. The details are described as follows and Figure 1 illustrates the new authentication protocol.

Step 1. U generates a random number $R0$, and then sends a service request and $R0$ to V.

Step 2. V forwards the service request to H.

Step 3. H generates a random number $R1$ and sends it to V.

Step 4. V generates a random number $R2$ and session key K_{UV} used by U and V, and then sends $M1 = [UID, K_{UV}, R1, R2]K_{VH}$ to H.

Step 5. H decrypts the message $M1$ to get UID, K_{UV}, $R1$ and $R2$, and verifies whether $R1$ is the same as what was sent to V in Step 3. If $R1$ passes the verification, V is authenticated by H. Then, H sends $M2 = [VID, K_{UV}, R2]K_{UH}$ and $R2$ to V.

Step 6. V verifies whether $R2$ is the same as what was sent to H in Step 4. If $R2$ passes the verification, H is authenticated by V. Then sends $M2$ and $M3 = [R0]K_{UV}$ to U.

Step 7. U decrypts the message $M2$ to get VID, K_{UV}, and $R2$, and then decrypts $M3$ to get $R0$. Then U verifies whether $R0$ is the same as what was sent to V in Step 1. If $R0$ passes the verification, V is authenticated by U. And then U responds to $V's$ challenge with the $M4 = [R2]K_{UV}$.

Step 8. V decrypts the message $M4$ to get $R2$ and verifies whether $R2$ is the same as what was sent to H in Step 4. If $R2$ passes the verification, U is authenticated by V.

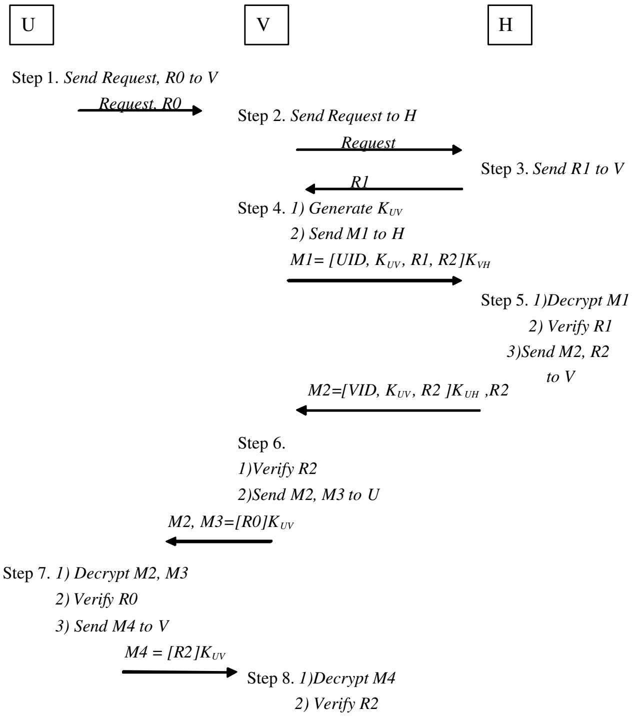

Figure 1: Our authentication protocol

4 Security Analysis

Anyone trying to masquerade as the U, V, or H cannot pass the authentication process, because all possible fraudulent behaviors will be found through fraud detection. In our protocol, H authenticates V by verifying $R1$ in Step 5, V authenticates H by verifying $R2$ in Step 6, U authenticates V by verifying $R0$ in Step 7, and V authenticates U by verifying $R2$ in Step 8. Figure 2 shows the authenticators $R0$, $R1$ and $R2$ utilized in authentication between the three entities U, V and H.

4.1 H Authenticates V by Verifying $R1$ in Step 5

In Step 5, H decrypts the response message $[UID, K_{UV}, R1, R2]K_{VH}$ return from V to obtain $R1$. Because H is the only other entity that knows the key K_{VH} and therefore V is authenticated if the decrypted authenticator $R1$ is the same as what was sent to V in Step 3. It is impossible to forge the message $[UID, K_{UV}, R1, R2]K_{VH}$ to pass the authentication process because there is no way to alter bits in ciphertext to produce the desired changes in the plaintext without knowing key K_{VH}. A forged V will be detected by H in Step 5.

4.2 V Authenticates H by Verifying $R2$ in Step 6

By verifying the correctness of the authenticator $R2$, V can assure the responder has the ability to decrypt the message $M1 = [UID, K_{UV}, R1, R2]K_{VH}$ sent to the alleged H in Step 4. Only H known the secret key K_{VH} can decrypt the message $M1$ to get $R2$ in Step 5, so without knowing the key K_{VH}, any fraudulent behaviors from H will be detected by V in Step 6.

4.3 U Authenticates V by Verifying $R0$ in Step 7

By decrypting the message $M2$ to get K_{UV} firstly and then decrypting $M3$ to obtain the authenticator $R0$, V can be authenticated if the value $R0$ is the same as what U was sent to V in Step 1. Because the key K_{UV} is hidden in $M2$, any attacker has no way to forge the message $M3 = [R0]K_{UV}$ to pass the authentication process unless obtaining the legal $M2$. It is obvious that $M2$ can only be created by H while passing the authentication of V in Step 5. Only the legal V can get the help from H to pass the verification in Step 7.

4.4 V Authenticates U by Verifying $R2$ in Step 8

To response $M4 = [R2]K_{UV}$ for the seed $R2$ with the key K_{UV}, U must have the ability to decrypt $M2 = [VID, K_{UV}, R2]K_{UH}$ encrypted by H and further forwarded by V. Only the legal U having the knowledge of secret key K_{UH} can obtain the correct key factors K_{UV} and $R2$, so the fraud will be detected by V in Step 8. In summary, the security of our protocol is based on the secret shared keys, KV_H, K_{UH}, and K_{UV}. Thus, in order to successfully pretend to be a legal mobile user (U) or service provider (including H and V), an attacker must forge some sensitive data to pass the authentication process. Fortunately, these attacks cannot work since all sensitive data is protected by these secret shared keys which are unknown to attackers. The authenticator $R0$, $R1$ and $R2$ are used to identify the legal entity and can prevent replay attack because they are changed from time to time. The usage of these random numbers guarantees the receipt of a fresh message.

5 Performance Analysis

Communication situations consist of honest and dishonest communication behaviors. In honest communications, the entire authentication process must be completed. However, in dishonest communications, the authentication process will be terminated upon detecting fraudulent behavior. The evaluation of efficiency of the protocol is based on the number of computations including encryption and decryption. It is reasonable to assume that each

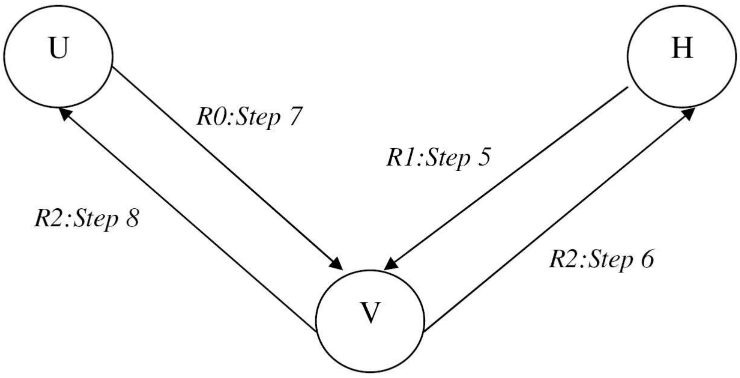

Figure 2: The authenticators utilized in authentication between U, V and H

Table 1: Number of computations for BGSW and our protocol

	BGSW Protocol	Our Protocol
Honest communication (complete the process)	10	8
Dishonest communication		
1. Fraud V detected by H	4	2
2*. Fraud H detected by V	2	3
3. Fraud V detected by U	10	6
4. Fraud U detected by V	8	8

* : Fewer Computations in BGSW protocol

encryption or decryption takes the same CPU time in conventional cryptosystem [13]. Different situations may take a different number of computations for both BGSW and our scheme. The less computations of the protocol, the more efficient it will be. In this section, the efficiency of the two schemes is compared according to the two different situations.

5.1 Honest Communication Situation

In an honest communication situation, both our scheme and BGSW protocol need to complete the entire authentication process so that all computations must be performed. The total number of computations for BGSW protocol is ten including five encryptions ($2K_{VH}, 1K_{UH}$, and $2K_{UV}$) and five decryptions ($2K_{VH}, 1K_{UH}$, and $2K_{UV}$). Compared to BGSW protocol, eight computations including four encryptions ($1K_{VH}, 1K_{UH}$, and $2K_{UV}$) and four decryptions ($1K_{VH}, 1K_{UH}$, and $2K_{UV}$), two less than BGSW scheme, are needed in our scheme.

5.2 Dishonest Communication Situation

Frauds can be found by verifying the authenticators $R0$, $R1$ and $R2$ in different steps. However, each kind of fraud detection takes a different number of computations in the two protocols. According to the different case of fraudulent behaviors mentioned in Sections 4.1 ∼ 4.4, the following sections calculate the numbers of computations of BGSW and our scheme and the results are shown in Table1. The detailed computations for each U, V and H are shown in Table 2. According to Table 2, in our protocol, the computations are needed in U are the same as BGSW scheme. There is no extra computational cost increased in U. But, apparently, computational costs are reduced in V and H when compared with BGSW scheme in most situations. It implies V and H can afford more services for other users. The overall system performance is hence promoted.

5.2.1 H Authenticates V

The fraud occurred from V will be detected by H in Step 5 by verifying $R2$ and $R1$ for BGSW and our protocol, respectively. Four ($4\ K_{VH}$) and two ($2\ K_{VH}$) computations are needed for BGSW and our protocol, respectively.

5.2.2 V Authenticates H

In BGSW protocol, the fraud occurred from H will be detected by V through verifying $R1$ in Step 4 and two computations ($2\ K_{VH}$) are needed. In our protocol, the fraud will be detected by V through verifying $R2$ in Step 6 and three computations ($2\ K_{VH}$ and $1\ K_{UH}$) are needed.

5.2.3 U Authenticates V

The fraud occurred from V will be detected by U in Step 9 through verifying $[R3]K_{UV}$ for BGSW protocol. Ten

(4 K_{VH}, 2 K_{UH} and 4 K_{UV}) computations are needed. In our protocol, the fraud will be detected by U through verifying $R0$ in Step 7. Six (2 K_{VH}, 2 K_{UH} and $2K_{UV}$) computations are needed.

5.2.4 V Authenticates U

The fraud occurred from U will be detected by V in Step 8 through verifying $R3$ in BGSW protocol. Eight (4 K_{VH}, 2 K_{UH} and $2K_{UV}$) computations are needed. In our protocol, the fraud will be detected by V through verifying $R2$ in Step 8. Eight (2 K_{VH}, 2 K_{UH} and 4 K_{UV}) computations are needed.

5.3 Comparisons of the Two Protocols

According to Table 1, only in case of the dishonest communication situation where the H is fraud but detected by V, BGSW protocol will be more efficient than our protocol since fewer computations are needed in BGSW protocol. Therefore, adopt this worst case to our scheme.In this case, if we can prove the overall efficiency of our protocol is better than BGSW protocol based on the fact that most communications are honest, it implies the efficiency of our protocol is better no matter what fraud situations occur. Considering a different ratio of dishonest communications, the compared results for the average number of computations of the two schemes are shown in Table 3.

The more computations of the protocol, the less efficient it will be. Therefore, according to Table 3, the overall efficiency of our protocol is better than BGSW. However, if the ratio of dishonest communications is increasing, our protocol will gradually lose efficiency. Obviously, if more than 70% of communications are dishonest then our protocol will be less efficient than BGSW. It implies that if fraudulent behaviors frequently occur, our protocol is not recommended to be adopted. However, if more than 70% of communications are dishonest, it contradicts the fact most communication behaviors should be honest to keep the entire communication system work smoothly. The entire system must be hence paralyzed.

6 Conclusions

In Global Mobility Network, not only security but also efficiency should be taken into account. The main purpose of this paper is not to improve the BGSW protocol but to show the new idea – Based on the fact that most communication behaviors are honest, it is reasonable to design a more efficient authentication protocol despite its loss efficiency in dishonest communication situation. Although fraudulent communication behavior may take more time to be detected in our scheme, the overall efficiency is promoted in majority cases.

References

[1] 3GPP TS23.002 (v3.6.0), *Network Architecture*, Release 99. 2002.

[2] M. Abadi, and R. Needham, "Prudent engineering practice for cryptographic protocols," *Proceeding of the IEEE on CS Symposium on Security and Privacy*, pp. 122-136, 1994.

[3] K. Al-Tawill, A. Akrami, and H. Youssef, "A new authentication protocol for GSM networks", *23rd Annual IEEE Conference on Local Computer Networks*, LCN'98, pp. 21 -30, 1998.

[4] T. Arakawa, and T. Kamada, *The Internet Home Electronics and the Information Network Revolution*, IEICE Technical Report, OFS96-1, 1996.

[5] M. Aydos, B. Sunar, and C. K. Koc, "An elliptic curve cryptography based authentication and key agreement protocol for Wireless Communication," *2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, Dallas, Texas, Oct. 1998.

[6] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Area in Communications*, vol. 11, no. 6. pp. 821-829, Aug. 1993.

[7] L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, "Extensions to an authentication technique proposed for the global mobility network," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 373-376, March 2000.

[8] N. El-Fishway, M. Nofal, and A. Tadros, "An effective approach for authentication of mobile users," *Vehicular Technology Conference*, 2002, IEEE 55th, vol. 2, pp. 598-601, 2002.

[9] M. S. Hwang, Y. L. Tang, and C. C. Lee, "An efficient authentication protocol for GSM networks," *EUROCOMM 2000*, *Information Systems for Enhanced Public Safety and Security.* IEEE/AFCEA, pp. 326-329, 2000.

[10] C. Laferriere, and R. Charland, "Authentication and authorization techniques in distributed systems," *International Carnahan Conference on Security Technology*, pp. 164-170, 1993.

[11] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the GSM," *Wireless Networks*, vol. 5, pp. 231- 243, 1999.

[12] C. C. Lo, and Y. J. Chen, "Secure communication mechanisms for GSM networks," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 4, pp. 1074-1080, Nov. 1999.

[13] J. L. Massey, "An introduction to contemporary cryptology," Proceeding of the IEEE, vol. 76, no. 5, pp. 533-549, 1988.

[14] J. H. Park, and S. B. Lim, "Key distribution for secure VSAT satellite communications," *IEEE Transactions on Broadcasting*, vol. 44, no. 3, pp. 274-277, Sep. 1998.

Table 2: Number of computations for each entity of BGSW and our protocol

	BGSW Protocol			Our Protocol		
	U	V	H	U	V	H
Honest communication (complete the process)	3	4	3	3	3	2
Dishonest communication						
1. Fraud V detected by H	0	2	2	0	1	1
2. Fraud H detected by V	0	1	1	0	1	2
3. Fraud V detected by U	3	4	3	2	2	2
4. Fraud U detected by V	2	3	3	3	3	2

Table 3: Average number of computations[1] for BGSW and our protocol

	BGSW Protocol	Our Protocol
10% dishonest communication	9.2=10*0.9+2*0.1	7.5=8*0.9+3*0.1
30% dishonest communication	7.6=10*0.7+2*0.3	6.5=8*0.7+3*0.3
50% dishonest communication	6.0=10*0.5+2*0.5	5.5=8*0.5+3*0.5
70% dishonest communication	4.4=10*0.3+2*0.7	4.5=8*0.3+3*0.7
75% dishonest communication	4.0=10*0.25+2*0.75	4.25=8*0.25+3*0.75

1 : Considering the worst case to our scheme, assume all dishonest communication situation is Fraud H detected by V

[15] M. Rahnema, "Overview of the GSM system and protocol architecture," *IEEE Communication Magazine*, pp. 92-100, Apr. 1993.

[16] S. Suzuki, and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," IEEE Journals on Select Areas Communications, vol. 15, pp. 1608-1617, 1997.

[17] C. K. Yeh, and W. B. Lee, "A dual-purpose signature for authentication on UMTS," *Journal of the Chinese Institute of Engineers*, vol. 30, no. 2, pp. 343-347, March 2007.

[18] C. K. Yeh, and W. B. Lee, "A self-concealing mechanism for authentication on portable communication systems," *International Journal of Network Security*, vol. 6, no. 3, pp. 285-290, 2008.

Chang-Kuo Yeh received his B.S. degree from the Department of Forestry, National Taiwan University, Taipei, Taiwan, in 1985, his M.S. in Computer Information Science from New Jersey Institute of Technology, New Jersey and his Ph.D. degree in Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan in 2007. Meanwhile he is an associate professor in the Department of Information Managements at National Taichung Institute of Technology. His research interests include cryptography, Information Security, Mobile Communications.

Wei-Bin Lee received his B.S. degree from the Department of Information and Computer Engineering, Chung-Yuan Christian University, Chungli, Taiwan, in 1991 and his M.S. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 1993. He completed his Ph.D. degree in May, 1997, at National Chung Cheng University. Now, he is now a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His research interests currently include information security, cryptography, computer communication and digital watermarking.