A Self-Concealing Mechanism for Authentication of Portable Communication Systems

Wei-Bin Lee and Chang-Kuo Yeh
(Corresponding author: Chang-Kuo Yeh)

Department of Information Engineering, Feng Chia University
100 Wenhwa Road, Seatwen Taichung, Taiwan 407, ROC (Email: wblee@fcu.edu.tw)

(Received Sep. 15, 2006; revised and accepted Nov. 22, 2006)

Abstract

The challenge-response technique is widely adapted for authentication of portable communication systems. For authentication the user can prove his/her identity via a secret shared key. However, this implies that the server requires secure storage and organization of a bulky database for the shared keys of all users. Evidently, such a sensitive and large database increases both maintenance loading and security concerns due to malicious intruders. In this study, a self-concealing mechanism was invented which allows to discard the bulky database and create valuable improvements for portable communication systems.

Keywords: Authentication, challenge-response, PCS, self-concealing

1 Introduction

In currently deployed Portable Communication Systems (PCS) such as GSM [5], DECT [4] and USDC [3], the challenge-response technique [17] is applied for authentication. As a secret key is shared between the authentication server and the mobile user, the authentication can be done by asking the mobile user to respond to the challenge sent by the server. Because only the user knowing the secret key can give the expected response, the mobile user can prove his/her identity to the authentication server.

For its critical position in the communication systems, authentication protocol designs draw a lot of attention from researchers for security enhancement [9, 10, 13] or efficiency improvement [2, 8, 14] of the current PCS networks. However, the challenge-response technique still plays a core function in these protocols. Thus, a database is absolutely required by the authentication server to maintain the secret shared keys of all mobile stations. Certainly, such a large database causes a high demand for maintenance and becomes itself a target for hackers. If the server is compromised, the security of the whole system will be broken down due to the leakage of sensitive information.

The concept of a self-concealing mechanism can be used to eliminate the above mentioned problem. The basic idea is that the secret shared key is concealed in a warrant and distributed to the mobile user instead of being stored in the authentication server. For security reason, only the authentication server has the ability to open the warrant and derive the secret shared key on-line. Although some temporal storage is needed for the on-line derivation, no large database is necessary in the authentication server to store the sensitive secret shared keys. Since the temporal storage will be eliminated immediately after the on-line derivation process is terminated, no security problems are involved for the temporal storage. Therefore, the risk of hacker attacks and the cost of server maintenance can both be reduced significantly.

In this approach, the shared secret is concealed by the authentication server and only the authentication server has the private key to open the shared secret. Therefore, we named the new mechanism the self-concealing approach.

The new concept initiates several positive changes. First, the sensitive and large database can be discarded. Consequently, this prevents hacker attacks to the database and reduces maintenance demand for the server. Second, the warrant can be used to guarantee the user's access rights, an issue is not addressed in the conventional challenge-response scheme. Further, on the client's side, no additional computation cost is required.

In the next section, some widely deployed challenge-response protocols are reviewed. The new challenge-response scheme will be illustrated in Section 3. Comparisons between our scheme and the conventional challenge-response protocols are made and discussed in Section 4. Finally, conclusions are given in Section 5.

2 Review of Some Important Challenge-Response Based Protocols

Here, some widely deployed PCS such as GSM, DECT, and USDC are surveyed and a generic model is constructed. To cope with generality, this paper applies a three parties structure, the mobile station (MS), the base station (BS), and the authentication server (AS) in the core assumption.

2.1 GSM

In GSM, AS and MS share a secret key k_i in advance. The major concern is how BS authenticates MS via a challenge-response technique.

First, AS randomly picks a *challenge* $RAND$ and computes the corresponding authenticator $XRES = A3(k_i||RAND)$ for BS, where $A3$ is a one-way hash function and "||" denotes a concatenation operation. Then, BS requests MS to respond to the challenge RAND. If the response $SRES$ from MS is the same as $XRES$ received from AS, MS can convince BS of its authenticity. Figure 1 shows the authentication process of GSM.

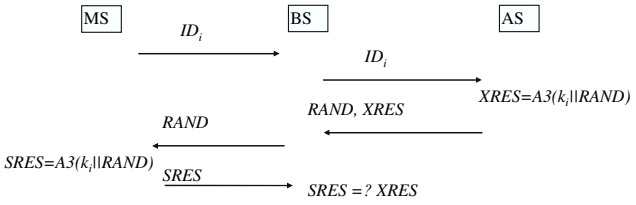

Figure 1: GSM authentication protocol

2.2 DECT

The authentication protocol of DECT is similar to the GSM protocol. The major difference is that the role of the secret key K is shared between AS and MS. Here, the shared secret key K is not directly assigned to derive a response, but to derive the key KS instead. KS is the genuine key used to generate the corresponding response. Regardless of the differences between the two underlying one-way hash functions $A11$ and $A12$ and the source of KS, the challenge-response scenario of the authentication is the same as in GSM, as can be seen in Figure 2, where RS and $RAND\_F$ are random numbers generated by AS.

2.3 USDC

In USDC, AS and MS still share a secret key $A - key$. From $A - key$, a shared secret data SSD is established through the SSD update protocol between AS and MS. The protocol is illustrated in Figure 3a, where $R1$ and $R2$ are random numbers and $CAVE(\cdot)$ is a one-way hash

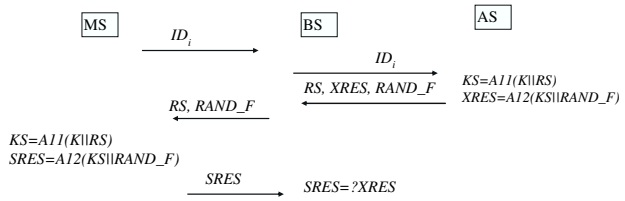

Figure 2: DECT authentication protocol

function. After the SSD is generated, the same scenario as in GSM and DECT is played (Figure 3b).

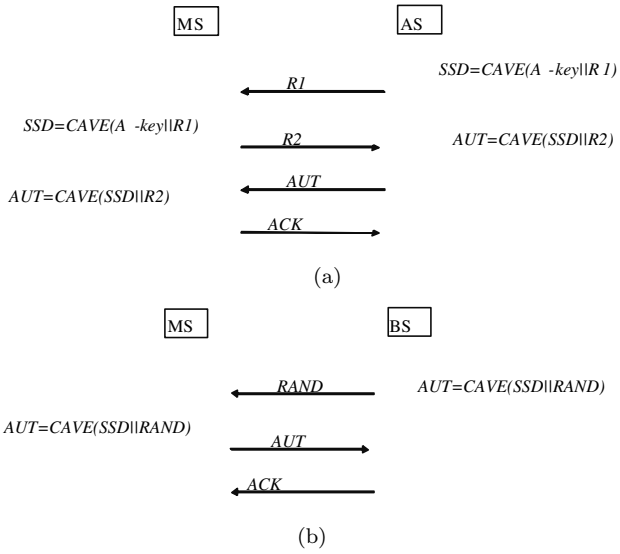

Figure 3: (a) SSD update protocol of USDC (b) USDC authentication protocol

2.4 Generic Challenge-Response Based Protocol

As we can see from the above described protocols, the critical component in the challenge-response technique is that AS generates a challenge for MS and then waits for MS to send the corresponding response by hashing the challenge and the secret key shared with AS. Table 1 shows the summary of the parameters used in the three challenge-response PCS.

From Table 1, it is easy to find out that the secret shared keys between AS and MS play the critical role in the challenge-response protocol. Regardless to the protocol GSM, DECT, or USDC, the response key is derived from the secret shared key. Therefore, all of these conventional challenge-response based protocols must maintain a database to store the sensitive keys. In the following, Figure 4, a generic model is presented describing the new idea, where $k_M A$ is the secret shared key between AS and MS and $h(.)$ is a one way hash function.

Table 1: The summary of parameters used in the current challenge-response PCS

	secret shared key	response key	challenge	response
GSM	k_i	k_i	$RAND$	$SRES = A3(k_i \| \| RAND)$
DECT	K	$KS = A11(K \| \| RS)$	$RAND\_F$	$SRES = A12(KS \| \| RAND\_F)$
USDC	$A-key$	$SSD = CAVE(A-key \| \| R1)$	$RAND$	$AUT = CAVE(SSD \| \| RAND)$

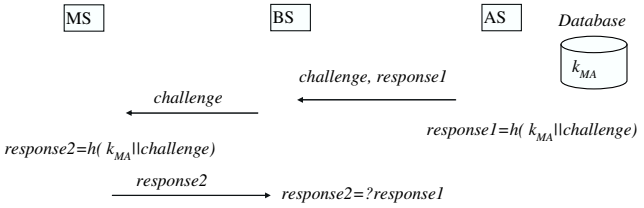

Figure 4: Generic process of the challenge-response protocol

3 Self-Concealing Mechanism Applying In The New Protocol

Based on the generic challenge-response model, the purpose of the new protocol is to discard the database but allow the server to perform its original function. In the following, initialization phase, registration phase and authentiation phase are described.

3.1 Initialization Phase

Unavoidably, AS generates the parameters p (a 1024-bit prime number) and q (a 160-bit prime factor of p-1), as well as the generator $g = h^{(p-1)}/q \bmod p$, where $h \in [1, p-1]$. Then AS selects an integer x less than q as the private key and the corresponding public key $y = g^x \bmod p$.

3.2 Registration Phase

Assume a mobile user MS wants to register in AS and requests specific access rights which are clearly stated in a warrant W. For instance, AS gives MS the access right which limits the user to use the network resources only in some restricted BSs. AS will execute the following steps to complete the authorization.

Step 1. Generate a random number k.

Step 2. Compute $r = g^k \bmod p$.

Step 3. Sign W as

$$s = h(W)x + kr \bmod q. \quad (1)$$

Step 4. Compute the secret shared key

$$k_{MA} = h(k||r||s). \quad (2)$$

Step 5. Store k_{MA}, W, r and s into a SIM card and send it to the MS.

MS can assure itself that AS grants him the rights by checking whether or not

$$g^s = r^r \cdot y^{h(W)} \bmod p. \quad (3)$$

3.3 Authentication Phase

When MS roams into a new BS, the parametersW, r and s must be forwarded to BS for authentication.

Step 1. BS passes the W, r and s to AS.

Step 2. AS derives the parameter k as

$$k = (s - h(W)x)r^{-1} \bmod q.$$

Step 3. AS computes the k_{MA} as Equation (2), where $k_{MA} = h(k||r||s)$.

Step 4. AS generates a random challenge and computes $reponse1 = h(k_{MA}||challenge)$.

Step 5. AS sends the *challenge* and $response1$ to BS.

Step 6. BS passes the *challenge* to MS.

Step 7. MS computes $reponse2 = (k_{MA}||challenge)$ with the key k_{MA} stored in the SIM card.

Step 8. MS sends the $response2$ to BS.

Step 9. If the $response2$ from MS is the same as $response1$ received from AS, MS has convinced BS its authenticity and specific access rights.

Figure 5 illustrates our new protocol.

4 Discussions and Comparisons

The signature (r, s), a type of generalized ElGamal digital signature [7], is used to guarantee the right W for the client. Due to the property of the digital signature, no one can alter the content of W without knowing the private x of AS. On the other hand, for the server the signature provides the self-concealing mechanism, which conceals the secret parameter k in the server's signature (r, s) and only the constructor AS can open it. According to its private key x, AS can derive the secret parameter k

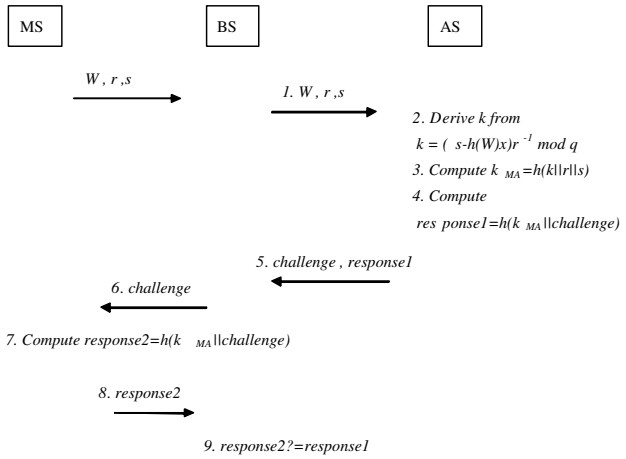

Figure 5: New authentication protocol

concealed in the signature. The derivation is elaborated as follows:

$$\begin{aligned} s &= h(W)x + kr \bmod q \\ \Rightarrow \quad kr &= s - h(W)x \bmod q \\ \Rightarrow \quad k &= (s - h(W)x)r^{-1} \bmod q. \end{aligned}$$

The parameter k can only be derived by AS because there is one unknown parameter in one equation. Therefore, it is hard to derive the parameter k by any outsider since there are two unknown parameters, k and x, in one equation.

According to the property of the derivation, all types of generalized ElGamal digital signatures listed in [7] can be applied to our scheme. Furthermore, the signature functions such as those described in [15] and [12] can also be applied in our scheme since they have the same properties. Thus, the new proposed scheme is much more flexible.

After the parameter k is derived, the authentication server computes the secret shared key k_{MA} via the combination of the secret parameter k and the signature (r, s). Since the secret shared key k_{MA} can be derived on-line via the authentication server, the database used to store the secret shared keys can be discarded.

In the following, the conventional challenge-response protocols are compared to our proposed scheme to illustrate its superiosity.

4.1 Key Management

In conventional challenge-response authentication protocols, AS has to maintain a large database for the secret keys of all mobile stations. However, in our new scheme, the secret shared key k_{MA} can be calculated on-line by AS and it is unnecessary to maintain a secure database to store the shared secret k_{MA} for AS. The cost of database maintenance and the threat of malicious attacks can be successfully reduced. The new scheme hereby provides a more efficient key management service than the conventional authentication protocols.

Our scheme employs a public key technique to guarantee the specific rights of MS through the signature (r, s) generated by AS. However, no public keys of BS and MS are involved, only the key of AS is necessary. As the number of AS is much less than that of MS and BS, the complexity of the Public Key Infrastructure (PKI) [11] is dramatically reduced.

Theoretically, the key of AS must be more strictly defined and protected than the key of MS and BS, and the key application should be long-term instead of being frequently updated. Stability is essential to the kind of key management. We designed the signature verification computation to be performed only during the registration phase to assure the rights grant and during the dispute phase to avoid rights repudiation. Consequently, the complexity of PKI construction and Certificate Revocation List (CRL) maintenance [11] will be reduced to a minimum with our new method.

4.2 Security Consideration

Based on the generic model, the major contribution is the way the secret shared key k_{MA} is protected. Without knowing k_{MA}, malicious intruders cannot compute the correct response to pass the authentication process.

At the client end, the k_{MA} is securely stored in the SIM card of the user. The SIM card is assumed to be a tamper resistant device. Nobody is able to retrieve any secret information from the SIM card - even the card owner.

Although anyone knowing the parameter k can compute $k_{MA} = h(k||r||s)$, it is infeasible for any attackers to compute k because the parameter $k$is concealed in the signature (r, s). To solve k from $r = g^k \bmod p$ is difficult due to the intractability of the discrete logarithm for a large prime p with the generator g. In addition, without knowing AS's private key x, it is also infeasible for an attacker to derive k from the equation $s = h(W)x + kr \bmod q$.

According to the above analysis, the secret shared key k_{MA} can be directly computed by AS based on the received warrant so that malicious intruders lose their target to steal the user's common secret key k_{MA} from AS. The security property of the underlying signature also provides a well-defined secure vault to conceal the seed k. Security is hence improved in the new scheme.

4.3 Computation Load

4.3.1 Mobile Station

In a wireless environment, due to hardware limitations of portable devices, the mobile station cannot support computations that require high complicity. However, the self-concealing mechanism is able to address this issue.

In our scheme, the mobile station guarantees the access rights authorized by the authentication server by checking Equation (3) which is a time-consuming computation. However, this action is required only during the registration phase and the cost can be neglected. The major concern shifts to the authentication phase where only one

hash computation is needed to generate the expected response in MS. Thus, the computation load of MS will not affect current systems.

4.3.2 Authentication Server

In order to reduce the computation cost of AS, Equation (1) can be modified as $s = h(W)x + kr^{-1} \bmod q$. With this arrangement, the derivation process of the key k is changed into $k = r(s - h(W)x) \bmod q$. Obviously, the original time-consuming computation r^{-1} can be eliminated. Readers may refer to [7] for another example of the efficiency improvement and cost-down approach.

Besides, the computation $h(W)x$ can be pre-computed before authentication if the warrant W issued from AS can be classified into several fixed forms in advance.

Actually, only one multiplication and one subtraction are needed to derive the key k. Besides, two hash computations are needed to compute $k_{MA} = h(k||r||s)$ and $response1 = h(k_{MA}||challenge)$ in AS. Both of the new computations are time saving without increasing calculation load.

In addition, when the user passes the authentication process, not only his/her legality is certified but also his/her access rights are approved by AS since the user's access rights are clearly specified in the warrant W. The process of searching for the user's access rights is therefore spared. The retrench of this searching process can further decrease the computation load for AS.

4.4 Access Rights Management

In the new scheme, the user's access rights are stated in the warrant W which has been initially issued to the user. As stated above (Section 4.3), when passing the entire authentication process, the user's access rights are also approved by AS. It is unnecessary to create a database to store all users' access rights and the process of searching for the user's access rights is, therefore, spared. In other words, the new scheme can not only ascertain the user's legality but can also simultaneously validate the access rights of the user. Apparently, our scheme provides a more efficient access rights management than the conventional challenge-response protocols.

On the other hand, AS has no way to repudiate the right it granted. The correctness of the equation $g^s = r^r \cdot y^{h(W)} \bmod p$ is a non-repudiation token for MS received from AS. Thus, AS cannot deny the signed warrant W and the rights of MS are guaranteed.

4.5 Storage Consideration

The new design generates new extra parameters, therefore, the storage capacity should be considered in a way that does not affect currently used systems.

MS must store the parameters $p, q, W, r = g^k \bmod p$, $s = h(W)x + kr \bmod q$ and the secret shared key $k_{MA} = h(k||r||s)$, where p is a 1024 bits prime number, q is a 160 bits prime factor of $p-1$, r is a number less than p, s is a number less than q, and the length of k_{MA} is 128 bits if the MD5 [16] hash function is used. The length of W can be assumed to be 1024 bits which is large enough to accommodate MS's specific access rights. Therefore, the total length of (q, s, p, r, W, k_{MA}) is 160*2+1024*3+128=3520 bits=440 bytes.

Current SIM cards contain an Electrically Erasable Programmable Read Only Memory (EEPROM) [6], which contains subscription specific data for the non-volatile memory. The capacity of EEPROM is 8 k bytes which is large enough to accommodate the above parameters of our scheme.

As a result of the previous comparisons, the new scheme has proven its superiority in key management, security enhancement and access rights management over conventional challenge-response protocols. Table 2 gives a summary of these results.

5 Conclusions

The introduction of the self-concealing mechanism can spare the requirement of a bulky database for the shared keys. With the new method, the PCS will benefit from more efficient key management and access rights management as well as less security threats. On the other hand, this new method does not result in increased computational loads or impacts on deployed PCS. Therefore, it has proven to be more efficient and economical in every aspect.

References

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

[2] 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, Mar. 2000.

[3] EIA/TIA-IS-54-B.

[4] ETSI Raft prETS, 300 175-7, 1991.

[5] *ETSI/TC Recommendation GSM 03.20*, Security Related Network Function, version 3.3.2, Jan. 1991.

[6] *European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface*, GSM 11.11 (ETS 300 608).

[7] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm," *Electronics Letters*, vol. 30, no. 24, pp. 2025-2026, Nov. 1994.

[8] M. S. Hwang, Y. L. Tang, and C. C. Lee, "An efficient authentication protocol for GSM networks," in *IEEE/AFCEA Information Systems for Enhanced*

Table 2: Comparisons of the proposed protocols

	Conventional challenge-response scheme	Our scheme
More efficient key management	no	yes
Less security threats	no	yes
Low computation loads	no	yes
More efficient access rights management	no	yes

Public Safety and Security (EuroComm'00), pp. 326-329, 2000.

[9] 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.

[10] 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.

[11] RSA Laboratories' Frequently Asked Questions about Today's Cryptography, V4.0. http://www.rsasecurity.com/rsalabs/faq/.

[12] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," in *Advances in Cryptology (Crypto'89)*, LNCS 435, pp. 729-730, Berlin, Springer-Verlag, May 1995.

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

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

[15] "The digital signature standard proposed by NIST," *Communications of ACM*, vol. 35, no. 7, pp. 36-40, July 1992.

[16] *The MD5 Message-Digest Algorithm*, RFC 1321.

[17] J. E. Wilkes, "Privacy and authentication needs of PCS," *IEEE Personal Communications*, vol. 2, no. 4, pp. 11-15, Aug. 1995.

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 an associate 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.

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