Mobile EC Service Applications by Privacy Management

Whe Dar Lin

The Overseas Chinese Institute of Technology
Dept of Information Management,
No. 100, Chiao Kwang Road Taichung 40721, Taiwan

Abstract. In this article, we shall propose an efficient privacy management for mobile EC service applications. The EC service applications embrace the problem of both privacy and authentication. We consider the mobile station on the broad contest of networking, from the wireless devices through which network communication occur to the EC service application being communicated. The privacy problem is concerned with the task of preventing an opponent from extracting message information from the communication channel on EC service applications. On the other hand, mobile station requests EC service applications on visit network authentication deals with preventing the injection of false data into channel. We can avoid employing public key cryptography in the using privacy EC service applications phase since to keep the computation cost down.

1 Introduction

A mobile EC service applications system comprises the wireless network that closely link very aspect of EC service applications and security issues. Basic operation such as authentication, access control, plus privacy management use for mobile station. The privacy managements using in confidentiality of the identity, privacy of the certificate user the state necessity of management when the situation is using the dining cryptographer problem for unconditional sender and recipient untraceability, electronic voting scheme, anonymous group discussions, untraceable electronic mail, untraceable mobile agent. [1, 2, 6, 8, 9, 11]

When mobile user roams between different visit network uses the different random name, so mobile user can keep location privacy. The structure of our paper is organized as follows: In section 2, based on the wireless communication system architecture, we shall propose our privacy management and authentication scheme. In section 3, the security issue shall be considered are proposed. Section 4, we addresses the conclusion on performance.

2 The Proposed an Efficient Privacy Management

Let M denote a mobile station MS, V denote the visit network VN of MS, H denote the home network HN of MS, and X->Y : Z denote the event that a sender X sends a message Z to a receiver Y. Let $k_{h,v}$ be the secret key shared by H and V, HD represents home identification number. Let $k_{h,i}$ be the secret key shared by H and M(ID_i), $\{m\}_{eh}$

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 259–262, 2003.

denotes the ciphertext for m encrypted by some public key cryptosystem using a public key e_h, and $(m)_k$ denotes the ciphertext for m encrypted using the secret key k of some secure symmetrical cryptosystem. Let f_1 be a secret one-way function known only to H and M. Let f_2 be a secret one-way function for use in a privacy EC service applications area known only to V and M.

The request message for privacy EC service applications protocol is as follows:

Step 1: M->V: HD, N_1, $\{ID_i, T, T_{expire}, Cert_i\}_{e_h}$

Step 2: V->H: N_1, $\{ID_i, T, T_{expire}, Cert_i\}_{e_h}$

Step 3: H->V: $(d_M, T_{expire}, D_M)_{k_{h,v}}$, N_1, $(C, T_{expire}, E_M)_{k_{h,i}}$

Step 4: V->M: N_1, $(C, T_{expire}, E_M)_{k_{h,i}}$

In step 1, M sets the time stamp T, An expiration time T_{expire}, and the certificate $Cert_i = (ID_i, T, T_{expire})_{K_{h,i}}$

In step 2, V transfers a nonce word N_1 and the received encrypted message sent to H.

In step 3, H computes

$$d_M = f_1(k_{h,i} * V),\ E_M = x_h * f_1(k_{h,i} * T_{expire}) + cC \bmod Q \tag{1}$$

$$D_M = g^{x_h * f_1(k_{h,i} * T_{expire}) + f_1(k_{h,i} * V)} C^C \bmod P \tag{2}$$

In step 4, M can check the EC service request message and see if the following equation holds or not.

$$g^{E_M} = y_h^{f_1(k_{h,i} * T_{expire})} C^C \bmod P \tag{3}$$

$$where\ g^{E_M} = g^{x_h * f_1(K_{h,i} * T_{expire}) + cC}$$

$$= (g^{x_h})^{f_1(K_{h,i} * T_{expire})} (g^c)^C = y_h^{f_1(K_{h,i} * T_{expire})} C^C$$

The using privacy EC service applications protocol is following:

Step 1:M->V: NEW-ID, T

Step 2:V->M: R

Step 3:M->V: B, J

In step 1, M computes NEW-ID as follows:

$$\text{NEW-ID} = f_2(f_1(k_{h,i} * V)) \tag{4}$$

In step 2, V sends R ($R = g^r \bmod P$) to M where the challenge R is used for freshness.

In step 3, M computes $B = g^b \bmod P$, $k_s = R^b \bmod P$, and

$$J = E_M + f_1(k_{h,i} * V) + b * f_2(f_1(k_{h,i} * V) * T_{expire}) * T * R \bmod Q, \tag{5}$$

Upon receiving the message, V uses d_M to compute $f_2(d_M)$ and gets D_M to verify B and L according to the equation

$$g^J = D_M * B^{f_2(d_M * T_{expire}) * T * R} \bmod P \tag{6}$$

If the above equation holds, then the mobile station (M) can use the privacy EC service applications on the visit domain V.

3 Security Considerations

Proposition: The visit network can authenticate the mobile station and support the privacy management on mobile EC service applications.
Proof:

The visit network can check the privacy EC service request holder to see if the following equation holds or not.

$$g^{J} = D_M * B^{f_2(d_M * T_{\exp ire}) * T * R} \bmod P, where \tag{7}$$

$$g^{J} = g^{E_M + f_1(k_{h,i} * V) + b * f_2(f_1(k_{h,i} * V) * T_{\exp ire}) * T * R}$$

$$= D_M * g^{b * f_2(d_M * T_{\exp ire}) * T * R} = D_M * (B)^{f_2(d_M * T_{\exp ire}) * T * R}$$

Even if some forger can generate (B', J') by getting the random number r as a challenge but the forger still needs to solve the equation $g^{J'} = D_M * B'^{f_2(d_M * T_{\exp ire}) * T * R} \bmod P$. However, the difficulty of solving this problem is as hard as the discrete logarithm problem even the attacker has D_M. Therefore, (B, J) cannot be forged, the authentication of the NEW-ID is well established. The intruder could give (D'_M, E'_M, d'_M, C') to forge a valid anonymous channel verification data (D_M, E_M, d_M, C). If the anonymous channel verification data is forged (D'_M, E'_M, d'_M, C') and satisfies $D'_M = g^{x_h * f_1(k_{h,i} * T_{\exp ire}) + d'_M} C'^{C'} \bmod P$ then the forged anonymous channel verification data is valid. This is exactly the discrete logarithm problem so the intruder will fail. The computations will run in exponential time.

In using privacy EC service applications protocol, when MS visits VN nodes (V_1,V_2,…,V_n), HN deducts a fixed amount of money from MS's account, then the HN broadcasts ($d_{M,1}$, T_{expire}, $D_{M,1})_{Kh,v1}$, ($d_{M,2}$, T_{expire}, $D_{M,2})_{Kh,v2}$, …, ($d_{M,n}$, T_{expire}, $D_{M,n})_{Kh,vn}$ to the VN nodes (V_1, V_2, …, V_n), where $d_{M,j}=f_1(K_{h,i} * V_j)$, $D_{M,j} = g^{x_h * f_1(A'' * k_{h,i} * T_{\exp ire}) + d_{M,j}} C^C \bmod P$, $K_{h,i}$ is the secret key shared with ID_i and the home domain, V_j is the visit domain ID number and f_1 is the secret one way function.

When the VN nodes (V_1,V_2,…,V_n) receive the message ($d_{M,j}$, T_{expire}, $D_{M,j})_{Kh,vj}$,V_j computes the NEW-ID_j = $f_2(d_{M,j})$ and stores (NEW-ID_j, T_{expire}, $D_{M,j}$) in the V_j user database.

The V_j user database stores (NEW-ID_j, T_{expire}, $D_{M,j}$). There is no information about the user ID_i.

1: NEW-ID_j=$f_2(d_{M,j})$

2: $d_{M,j} = f_1(k_{h,i} * V_j)$

There is no information about the user ID_i, the secret key $k_{h,i}$ is only known to HN and user ID_i. No attacker can get $k_{h,i}$ from $d_{M,j}$ because the hash function f(x) is assumed secure since it is infeasible to determine x such that f(x)=y for a given y. Moreover, f_1 is a one-way hash function known only to HN and the mobile station (MS). The attackers do not know the hash function $f_1(x)$. In fact, in our proposed scheme, the user ID_i is kept unknown to any attacker and V_j.

Therefore, the MS (ID_i) can use NEW-ID_j to roam VN(V_j). The different IDs used in different VNs maintain the anonymity of location service.

This is exactly the discrete logarithm problem so the intruder fails. It will run in exponential time. As mentioned above |P| >= 512, that this attack is not successful in terms of execution time.

4 Conclusion

In this article, we propose an efficient privacy management for mobile EC service applications to consider several security characteristics of wireless network. The most important feature of our proposed protocol is its untraceability issue. In our proposed method, the possible wireless network vulnerabilities that have been protected privacy management and EC service application of authorized mobile user.

Mobile station only computes addition, multiplication and hashing implement in hardware, which can satisfy the requirement of low computational, and communication cost due to the limited power of handset application. We can avoid employing public key cryptography since we regard the computation requirements as low. Our method satisfies the requirement for EC service applications contain privacy, secure, reliable, transparent and scalable for mobile stations.

References

[1] B. Pfitzmann. Breaking an efficient privacy management, Advances in Cryptology: Proc. EuroCrypt'94, Lecture Notes in Computer Science, 950, springer, Berlin, 1995,pp. 332–340.

[2] C. Park, K. Itoh, and K. Kurosawa, Efficient privacy management and all /nothing election scheme, Advances in Cryptology : Proc. EuroCrypt'93 , Lecture Notes in Computer Science, 765, Springer, Berlin, 1993, pp.248–259.

[3] D. Chaum, Untraceable electronic mail, return address, and digital pseudonyms, Commun. ACM 24 (2) (1981) 84–88.

[4] D. Chaum, The dining cryptographers problem: unconditional sender and recipient untraceability, J. Cryptology 1 (1988) 65–75.

[5] D. Naccache, and D. M. Raihi, Cryptographic Smart Cards, IEEE Micro, June 1996, pp. 14–25.

[6] D . Samfat, R Molva, N, Asokan, Untraceability in mobile net works, in: Proc. First ACM Int. Conf. On Mobile Computing and Network , November 1995, pp. 26–36

[7] ETSI: GSM recommendations: GSM 01.02-12.21, February, 1993, Release 92.

[8] L. Jianwei, W. Yumin, A user authentication protocol for digital mobile communication network, in : IEEE International Symposium on Personal , Indoor and Mobile Radio Communications, 1995, pp. 608–612.

[9] M. Beller, Y.Yacobi, Fully-fledged two-way public key authentication and key agreement for low-cost terminals, Electronic Letters 29(11)(1993) 999–1101.

[10] Whe Dar Lin, "EC Transactions Use Different Web-based Platforms," Lecture Notes in Computer Science, 2003'

[11] W. S. Juang, C. L. Lei, C.Y. Chang, Privacy management and authentication in mobile EC service applications, Computer communications, 22(1999), pp. 1502–1511.