Authentication Protocols with Nonrepudiation Services in Personal Communication Systems

Hung-Yu Lin and Lein Harn

***Abstract*— Through the combination of the public-key digital signature and the hash-chaining techniques, a new set of authentication protocols is proposed with the capability of arbitrating disputed bills. These protocols provide security services required by regular authentication protocols and are efficient in consideration of the specific Personal Communication Systems (PCS) environment. They protect subscribers from incorrect service charges and provide service providers legal evidences to collect bills that are denied. They also help identify whether an accounting error, an internal fraud, or a security breach of the service provider causes the incorrect service charge.**

***Index Terms*— Authentication, cryptography, nonrepudiation, PCS.**

NOTATIONS

$E(x, y)$	Encryption of y under key x.
$g(x, y)$	One-way output of y under the secret key x.
$h(x_1, x_2, \cdots, x_r)$	One-way hash output of the concatenation of $x_1, x_2, \cdots$, and x_r.
$Sign(x, y)$	Signature of y with key x.
$Public\_Subscriber$	Subscriber's public key.
$Private\_Subscriber$	Subscriber's secret key.
$Authentication\_Key$	Secret authentication key shared between a subscriber and his HLR.
$Service\_Key$	Temporary service key shared key between a subscriber and the VLR.
ID_V, ID_H	Identities of HLR and VLR.
IMSI	Subscriber's unique identity.
TMSI	Temporary mobile subscriber identity.

I. INTRODUCTION

THERE are many service domains in the Personal Communication Systems (PCS's), each operated under a different administration with a different level of protection. Some service domains are more vulnerable than the others to attacks from intruders or insiders. So far, most systems which include Global System for Mobile Communications (GSM) [9], U.S. Digital Cellular (USDC) [7], Digital European Cordless Telecommunications (DECT) [10], Cellular Digital Packet Data (CDPD) [5], and some others [1], [4], [16], [17] proposed by independent researchers, assume that all participants, subscribers, and service providers/network operators, are assumed to be trustworthy and the fraud can only come from outsiders. But this is not true in the real world situation. For example, a dishonest subscriber may repudiate the calls he has made. An intruder to a compromised service domain or an insider may make free calls under a subscriber's identity. The billing system may go wrong and cause the accounting error. Currently, a subscriber may simply call his service provider to complain of the incorrect bills and get the charge dropped. However, when the complaints are often and the amount of charge involved takes a significant portion of the revenue, such practice will not be acceptable. An arbitration protocol would be needed to decide whether a subscriber has maliciously repudiated services and help identify the problem if the subscriber is wrongly charged.

Manuscript received October 26, 1998. The associate editor coordinating the review of this letter and approving it for publication was Dr. L. L. Chen.

H.-Y. Lin is with the Computer Science Department, California State University, San Marcos, CA 92096-0001 USA (e-mail: hylin@mailhost1.csusm.edu).

L. Harn is with Computer Science Telecommunications, University of Missouri–Kansas City, Kansas, MO 64111 USA.

Publisher Item Identifier S 1089-7798(99)06556-4.

II. PREVIOUS WORKS

The major two techniques used in this paper are digital signature and hash chaining. These two techniques are commonly used in many applications, particularly in [2] where they are used to construct electronic cash and [12] where they are used to sign stream data. Because of the unique requirements in the PCS environment, some factors need to be considered in using these two techniques to design authentication protocols with nonrepudiation feature.

Digital signature techniques have also been used to construct authentication protocols [1], [4] for PCS-like systems. In general, these protocols cause significant delay in the computation of a digital signature. In 1995, with hash-chaining techniques, one paper [16] was proposed to add nonrepudiation feature in the authentication process to solve possible bill disputes on service charge occurred on a visited foreign domain. It requires a subscriber to fully trust his home domain (and no conspiracy between ones home system and a foreign system) and, therefore, it cannot handle fraud or billing errors caused by ones home domain. In this paper, both digital signature and hash chaining techniques are integrated in an innovative way and stronger protocols will be proposed to remove a subscribers trust on his home domain. One goal of the new protocols is to protect subscribers from being wrongly charged by any service provider. Another goal is to provide the service providers with legal evidences to collect bills in case subscribers repudiate calls that they requested. Achieving these two goals also means that insider fraud/attack from any domain can be detected. It helps to identify accounting errors

on the operators. More importantly, the new protocols must be efficient so it can be implemented on the mobile device with limited computing/battery power, and the setup delay incurred from the process must be minimal.

A trusted certification center is not required and the public-key certificate revocation problem is confined in a single service domain. No separate certificate revocation list (CRL) needs to be sent to other service domain. To reduce the computation delay on signature generation, only one signature is needed for multiple sessions and the ElGamal-type digital signature schemes [6], [8], [13], [22] can be used to minimize the computation on the mobile devices.

III. Innovation

This paper uses Lamport's one-time password/hash-chaining technique [15] to construct authentication protocols that support nonrepudiation services in the PCS communication. This technique was first proposed in 1981 and has been used in many other applications [2], [12], [14]. Let $f(x)$ be a one-way function and $f^m(x) = f(f(\cdots(f(x)\cdots)))$ be the composition of m f's. One generates the digital signature of $f^m(b)$, and then reveals $f^{m-1}(b)$, $f^{m-2}(b)$, $\cdots f(b)$, and $b = f^0(b)$ in sequence to prove himself for m times. If a service request is granted after each successful authentication of the subscriber, then a released value, $f^t(b)$, $m > t \geq 0$, serves as a nonrepudiation evidence that the subscriber has made at least m–t requests. Note that f can be easily implemented with one-way hash functions like MD5 [18] or SHA [20]. General discussion on one-way functions and one-way hash functions can be found in [21] and the implementation of one-way functions with one-way hash functions can be found in [2].

To use this hash-chaining technique the prover and the verifier must have precise synchronization. If such synchronization is lost because of the subscriber's roaming into a new domain or communication noise in authentication process, a new set of chained hash values and its digital signature would have to be recomputed and the protocol would has to be restarted. To solve this problem, we let the subscriber select n seeds, $b_1, b_2, \cdots, b_n$, compute $f^m(b_1), f^m(b_2), \cdots, f^m(b_n)$, and sign on the one-way hash value, $h(f^m(b_1), f^m(b_2), \cdots, f^m(b_n))$. Since each $f^m(b_k)$, $n \geq k \geq 1$, can be used for up to m nonrepudiation connections, the signature can be used for nm nonrepudiation connections.

IV. Proposed Security Protocols

There are four protocols in our proposal: the registration protocol, the service reservation protocol, the service key establishment protocol, and the session key establishment protocol. In general, we use HLR to denote a subscriber's home system and VLR to denote the visited (serving) system. On interdomain roaming, the VLR is a foreign system. However, if the subscriber is within the coverage of his home system, the VLR and HLR are of the same entity. Before introducing these protocols, more notations used are explained here.

B. Registration Protocol

When one subscribes to the PCS services, he picks a key pair, ($Public\_Subscriber$, $Private\_Subscriber$) and presents the public-key, $Public\_Subscriber$, to his chosen service provider along with other identification information. The area operated under this service provider is the home system of the subscriber. The home system then assigns $IMSI$ and $Authentication\_Key$ to the subscriber and stores $IMSI$, $Authentication\_Key$, and $Public\_Subscriber$ in the database. Note that a trusted public-key certification center is not required. This eliminates the revocation problem of public-key certificates that are present in many public-key based protocols.

C. Service Reservation Protocol

mobile subscriber $\rightarrow$VLR$\rightarrow$HLR

$$\{IMSI,\ f^m(b_1),\ f^m(b_2),\ \cdots,\ f^m(b_n),\ timestamp,\ Sign(Private\_Subscriber,\ h(IMSI,\ f^m(b_1),\ f^m(b_2),\ \cdots,\ f^m(b_n)),\ timestamp)\}.$$

This message provides the legal evidence of the subscriber's intention to use the service. The timestamp used here guarantees the freshness of the message and a signature on this message allows the subscriber to prove his authenticity to his HLR. As long as the value of *timestamp* is greater than the one in the previous reservation message, it suffices to detect any replayed message. The synchronization on a global clock is not needed.

D. Service Key Establishment Protocol

Message #1: **subscriber $\rightarrow$VLR$\rightarrow$ HLR**

$$\{IMSI,\ ID_V,\ ID_H,\ i,\ f^{m-1}(b_i),\ r_i\}.$$

This message is used to establish a service key between a subscriber and the VLR when a subscriber moves into a new service domain. r_i is a random number selected by the subscriber that will be used to generate the service key.

Since each signature contains n secret values of b's, it allows a subscriber to prove himself to his HLR n times. If all b's have been used or the synchronization on b's between a subscriber and his HLR is lost, the subscriber will have to invoke the service reservation protocol again. When the submitted $f^{m-1}(b_i)$ is valid, i.e., $f(f^{m-1}(b_i)) = f^{m-1}(b_i)$, the HLR will compute $Service\_Key_i = g(Authentication\_Key,\ r_i)$ and send it to the VLR in the next message. The service key will be used to generate session keys between the subscriber and the VLR in the next protocol.

Message #2: **HLR$\rightarrow$VLR**

$$\{IMSI,\ r_i,\ f^{m-1}(b_i),\ Service\_Key_i\}.$$

When the VLR receives this message, it means that the subscriber has successfully proved himself to his HLR.

$f^{m-1}(b_i)$ will be used to authenticate the subscriber. Note that a secure channel must exist between the VLR and HLR so $Service\_Key_i$ will not be available to attackers.

Message #3: **VLR→ mobile subscriber**

$$E(g(Service\_Key_i, 0), (TMSI, r_i)).$$

$TMSI$ is a temporary mobile subscriber identity used to hide a subscriber's real identity in the subsequent connections. A new $TMSI$ is needed for each session. Since only the valid VLR can obtain $Service\_Key_i$ from the subscriber's HLR and computes the right ciphertext, the presence of r_i in this decrypted message proves to the subscriber that this is the VLR that has been authorized by his HLR.

E. Session Key Establishment Protocol

With hash-chaining technique, the subscriber will orderly reveal $f^{m-2}(b_i)$, $f^{m-3}(b_i), \cdots, f^{m-m}(b_i) = f^0(b_i) = b_i$, one for each new session. Note that $f^{m-1}(b_i)$ has been used in the service key establishment protocol. Assuming that the subscriber has made $j-1$ connections, $0 < j < m$. The VLR has recorded the value of f^{m-j}, as the nonrepudiation evidence, along with the subscriber's temporary identity, $TMSI_j$. The subscriber now tries to establish the jth session. The protocol proceeds as follows:

Message #1: subscriber → VLR

$$\{TMSI_j, f^{m-(j+1)}(b_i)\}.$$

If $TMSI_j$ is valid and the computed value of $f(f^{m-(j+1)}(b_i))$ is identical to the stored value of $f^{m-j}(b_i)$, the subscriber is a legitimate one and the VLR computes the session key, $g(Service\_Key_i, j)$ for this session. The VLR also chooses a new temporary identity, $TMSI_{j+1}$, for the next round of session key establishment protocol. The new $TMSI_{j+1}$ will be encrypted under this session key and sent to the subscriber in the next message. If the subscriber fails to prove his authenticity, either because the $TMSI_j$ is not a valid one or the computed value is not correct (because of loss of synchronization), the subscriber would have to invoke the service key establishment protocol with b_{i+1} to reestablish a new service key.

Message #2: VLR → mobile subscriber

$$E(g(Service\_Key_i, j), (TMSI_j, TMSI_{j+1}).$$

The subscriber computes the session key, $g(Service\_Key_i, j)$, and decrypts this received message. This message enables the subscriber to authenticate the VLR. Because only the legitimate VLR (of course, other than the subscriber and his HLR) can compute the session key and the right ciphertext, the presence of $TMSI_j$ in the decrypted message proves the legitimacy of the VLR to the subscriber. The session key is used to encrypt all data in the jth session as well as the temporary identity for the $(j+1)$th session. When this key is compromised under some attacks such as the known-plaintext attack, the security of subsequent connections is not affected.

V. Conclusion

Authentication protocols with nonrepudiation services are proposed for the personal communication systems. These protocols provide mutual authentication, weak subscriber ID confidentiality, and session-independence. They are also efficient in terms of computation and communication delay. With the nonrepudiation feature, a subscriber cannot deny the services that he has used and a service provider cannot overcharge a subscriber for the services that he did not request. This feature helps identify fraud, unexpected security breach, and errors on the billing system.

References

[1] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area network," *IEEE Personal Commun.*, First Quarter, pp. 25–31, 1994.
[2] R. Anderson, C. Manifavas, and C. Southerland, "NetCard—A practical electronic-cash system," in *Proc. Int. Workshop on Security Protocols*, Cambridge, U.K., Apr. 10–12, 1996, pp. 49–57.
[3] N. Asokan, G. Tsudik, and M. Waidner, "Server-supported signature," in *Proc. 4th Eur. Symp. on Research in Computer Security, Lecture Notes in Computer Science.* 1996, vol. 1146, pp. 131–143.
[4] M. J. Beller, L. Cheng, and Y. Yacobi, "Privacy and authentication on a portable communication system," *IEEE J. Select. Areas Commun.*, vol. 11, pp. 821–829, Aug. 1993.
[5] Cellular Digital Packet data (CDPD) System Specification, Release 1.0, July 19, 1993.
[6] NIST FIPS PUB 186-1, Digital Signature Standard (DSS), Dec. 15, 1998.
[7] EIA/TIA-IS-54-B.
[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 469–472, July 1985.
[9] ETSI/TC Recommendation GSM 03.20, Security Related Network Function, version 3.3.2, Jan. 1991.
[10] ETSI, ETS 300 175-7, Oct. 1992.
[11] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. Kunzinger, and M. Yung, "Security issues in a CDPD wireless network," *IEEE Personal Commun.*, pp. 16–27, Aug. 1995.
[12] R. Gennaro and P. Rohatgi, "How to sign digital streams," *Adv. in Cryptology-Crypto'97*, pp. 180–197.
[13] L. Harn, "A new digital signature based on the discrete logarithm," *Electron. Lett.*, vol. 30, no. 5, 1994.
[14] L. Harn and H. Lin, "Modifications to enhance the security of GSM," in *5th Nat. Conf. on Informal Security*, Taiwan, R.O.C., May 1995.
[15] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.
[16] H. Lin and L. Harn, "Authentication protocols for personal communication system," in *ACM SIGCOMM '95*, Aug. 28–Sept. 1, 1995, pp. 256–261.
[17] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network*, pp. 26–34, Mar./Apr. 1994.
[18] R. Rivest, "The MD5 message digest algorithm," RFC 1321, 1992.
[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," *Commun. ACM*, vol. 21, no. 12, pp. 120–126, 1978.
[20] NIST FIPS PUB 180-1, "Secure hash standard," *Nat. Inst. Stand. Technol.*, U.S. Dep. Commerce, Apr. 1995.
[21] B. Schneier, *Applied Cryptography*. New York: Wiley, 1996.
[22] C. P. Schnorr, "Efficient identification and signatures for smart cards," in *Adv. in Cryptology, CRYPTO '89*, Aug. 20–24, 1989, pp. 239–252.