A Non-Repudiation Metering Scheme

L. Harn and H. Y. Lin

***Abstract*—A metering scheme enables a web server to measure the number of visits from clients. In addition, a *proof* needs to be presented by the server as evidence corresponding to this measured number. In this letter, we propose an efficient metering scheme that incorporates the hash-chaining technique and the digital signature algorithm to provide a nonrepudiation *proof* of this measured number.**

***Index Terms*—Public key cryptography, metering scheme.**

I. Introduction

A METERING scheme can be used by a web server to measure the number of visits from clients within a time frame and the server can produce a proof to collect advertisement fees. Naor and Pinkas have published a metering scheme at Eurocrypt'98 [1] and later, Ogata and Kurosawa attacked their scheme and proposed a modified one at Asiacrypt'00 [2]. Both schemes assume an audit agency to follow Shamir's secret sharing scheme [3] to generate shares/information to clients/servers. These pre-generated server information enables the server to verify a client's access privilege by examining the client's submitted share on each visit. Later, based on the reconstructed secret, the server is able to produce a proof to show that at least a certain number of clients have visited the server within a certain time frame.

Digital signature technique can be used in the metering scheme to provide nonrepudiation proof. However, in case each client presents a digital signature for each visit to the server, the computational overload on both client's and server's sides would be too significant. In this letter, we propose an efficient metering scheme that incorporates the hash-chaining technique and the digital signature algorithm to provide a nonrepudiation proof of this measured number.

II. A Non-Repudiation Metering Scheme

The two major techniques used in this letter are digital signature and hash chaining. Similar techniques can be found in authentication protocols [4] used for the Personal Communication Systems (PCS).

Our proposed scheme uses Lamport's one-time password/hash-chaining technique [5] to produce nonrepudiation proof. Let $f(x)$ be a one-way function and $f^m(x) = f(f(\ldots(f(x)\ldots))$ be the composition of mf's. Each client randomly selects an integer b and register $f^m(b)$ to the server. In the first visit, the client submits $f^{m-1}(b)$ to prove himself to the server. Then, the server will update $f^m(b)$ and store $f^{m-1}(b)$ for next visit. The client reveals $f^{m-1}(b), f^{m-2}(b), \ldots, f(b)$, and $b = f^0(b)$ in sequence to prove himself for m times.

By incorporating digital signature with this hash-chaining technique to provide the nonrepudiation *proof*, the client signs on $(f^m(b), M)$, and submits the signature to the server. Here M is the information about $f^m(b)$, such as, when it expires, who the associated web server is, etc. Similarly, the client reveals $f^{m-1}(b), f^{m-2}(b), \ldots, f(b)$ and $b = f^0(b)$ in sequence to prove himself for m times. The combination of $f^{m-i}(b)$ and the digital signature of $f^m(b)$ can be used as a nonrepudiation *proof* by the server as evidence of i visits made by the client. General discussion on one-way functions and one-way hash functions can be found in [6] and the implementation of one-way functions with one-way-hash functions can be found in [7].

To accommodate multiple time frames, the scheme described above can be generalized as follows. We let the client randomly select n seeds, $b_1, b_2, \ldots, b_n$, where n is the number of time frames, and compute $f^m(b_1), f^m(b_2), \ldots, f^m(b_n)$, and digitally sign on the one-way hash value, $h(f^m(b_1), f^m(b_2), \ldots, f^m(b_n))$, where h is a one-way hash function. Again M can be included in the signature to tell the servers how this proof can be used. Since each $f^m(b_k), n \geq k \geq 1$, can be used for up to m nonrepudiation visits, one signature can be used as a *proof* for at most nm nonrepudiation visits.

III. Security

The security of this proposed scheme is based on the security of one-way chaining and the digital signature scheme used to sign the one-way hash value, $f^m(b)$. The one-way chaining algorithm prevents all users, except the legitimate client, to compute backward values from a published one-way value. Therefore, the combination of $f^{m-i}(b)$ and the digital signature of $f^m(b)$ serves as a nonrepudiation *proof* that the client has made i visits.

IV. Conclusion

We have proposed an efficient metering scheme that enables a server to measure the *exact* number of visits made by each client. In addition, the server is able to present a nonrepudiation *proof* and no participation of the audit agency is required in this scheme.

References

[1] M. Naor and B. Pinkasm, "Secure and efficient metering," *lecture Notes in Computer Science*, vol. 1403, pp. 576–589, 1998.

Manuscript received May 24, 2001. The associate editor coordinating the review of this letter and approving it for publication was Dr. L. Chen.

The authors are with the Computer Science Department, California State University at San Marcos, San Marcos, CA 92096 USA (e-mail: hylin@csusm.edu).

Publisher Item Identifier S 1089-7798(01)11064-1.

[2] W. Ogata and K. Kurosawa, "Provably secure metering system," in *Proc. Advances in Cryptology—ASIACRYPT 2000*, pp. 388–398.
[3] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.
[4] H. Y. Lin and L. Harn, "Authentication protocols with non-repudiation services in personal communication systems," *IEEE Commun. Lett.*, vol. 3, pp. 236–238, Aug. 1999.
[5] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981, submitted for publication.
[6] B. Schneier, *Applied Cryptography*. New York: Wiley, 1996.
[7] N. Asokan, G. Tsudik, and M. Waidner, "Server-supported signature," in *Proc. 4th European Symp. on Research in Computer Security (Lecture Notes in Computer Science)*, vol. 1146, 1996, pp. 131–143.