International Journal of Soft Computing 1(3): 184-186, 2006
© Medwell Online, 2006

A New Payment Protocol for Distance Learning

Wei-Kuei Chen
Department of Computer Science and Information Engineering,
Ching-Yun University, 229, Chien-Hsin Road, Chung-Li, 320 Taiwan

Abstract: The proposed protocol makes it possible for a learner to pay money to a course provider efficiently. Besides, the proposed method is based on a generic digital signature scheme, so it can be implemented on the payment protocols which are based on digital signature techniques without affecting their infrastructures.

Key words: Digital signatures, payment protocol, distance education

INTRODUCTION

Since the technical progress of computer science, the speed of data processing and the efficiency of information generation have been largely improved. Due to the techniques of networks largely shorten the communicating time among distributed entities, many modern network services have been proposed in the literatures to take the advantages of the techniques such as distance education. Distance education makes it possible for a learner in a remote site to learn a course anytime and anywhere.

In carrying out distance education over the Internet, it is necessary to consider how a learner to pay money to course providers. In this study an applicative scheme is presented to make it possible for a learner to pay money for a designated course to its provider. Electronic course exchange voucher (e-voucher) makes it possible for a learner to transmit her/his e-voucher through communication networks during transactions efficiently. Because the security and privacy of e-voucher can be guaranteed, only two parties are involved in the proposed scheme and the extra cost of the presented scheme is very cheap, the proposed scheme is applicative.

In the proposed distance education payment protocol, a learner first purchases an e-voucher from the course provider and then pays it to the course provider for some designated course. Based on digital signature cryptosystem, an efficient electronic course exchange voucher protocol is presented for payment. Furthermore, since the proposed scheme is based on a generic digital signature scheme, the method can be easily applied to protocols based on digital signature scheme without affecting their infrastructures.

Preliminaries: In this study several preliminaries used in this study will be briefly introduced. One-way hash function is first been introduced. And then digital signatures are described. Finally, a generic digital signature scheme is presented.

One-way hash function: One-way hash function is a transformation that takes an input x and returns a fixed-size string y. Examples of well-known hash functions are MD families and SHA[1]. The basic requirements for a cryptographic one-way hash function are shown in the followings. First, the input can be of any length. Secondly, the output has a fixed length. Thirdly, given x, it is relatively easy to compute H(x). Fourthly, given y, it is infeasible to compute x such that H(x) = y. Finally, it is hard to find x_1 and x_2 such that $H(x_1) = H(x_2)$.

Digital signatures: Digital signature is a cryptographic primitive. It is fundamental in authentication, authorization and non-repudiation[2]. Rivest, Shamir and Adleman presented the first digital signature scheme[3]. Two parties, a signer and a group of users, participate in a digital signature protocol. A digital signature is a sequence of bits appended to a digital document and the purpose of digital signature is to provide a method for a signer to bind its identity to a piece of information. When public-key cryptography[4] is used to calculate a digital signature, the signer encrypts the document with its own private key. Anyone with access to the public key of the signer may verify the signature. This technique can prevent authorized messages from being forged. Besides, the signer can link a signature shown for verification to the instance of the protocol produces that signature.

In practical application, to create a digital signature, one usually signs the hashed value of the message instead of the original message itself. This saves a considerable amount of time and avoids the multiplication attacks[2,5,6]. Examples of well-known digital schemes are RSA, DSA, Elgamal, Rabin and Schnorr[7,1,8-10].

A generic digital signature scheme: In this study a generic digital signature scheme will be presented. Let M be the underlying set of messages. The proposed generic digital signature scheme consists of three elements (H, S, V) where

- The public one-way hash function H, where $H: M \to M$.
- The private signing function S, where $S: M \to M^K$. Signer has to keep S secret. K is a positive integer, where $M^K = M$ when $K = 1$ and $M^K = M^{K-1} \times M$ when $K \geq 2$. Without S, it is infeasible to compute $S(H(m))$, which is called the signer's signature on m in the scheme.
- The public verification function V, where $V: MK \times M \to \{true, false\}$. $V(l, m) = true$ where $l \in M^K$ if and only if l is the signer's signature on m, i.e., $l = S(H(m))$.

The corresponding protocol is described below.

Signing: The signer applies S to message m and then sends $S(H(m))$ to the user.

Verifying: After receiving the signing result $S(H(m))$ and m, the signature and message pair $(S(H(m)), m)$ can be verified by examining whether $V(S(H(m)), m) = true$ or not. The user shows the signature-message pair $(S(H(m)), m)$ for verification and the tuple can be verified by examining whether $V(S(H(m)), m) = true$ or not.

The proposed scheme: The proposed scheme is introduced as follows. The identity of a learner is embedded into her/his e-voucher to make this protocol more practical. The proposed protocol consists of two parties (learners and a group of course providers) and four stages (initializing, enrolling, learning and depositing). The course provider and the learners of the proposed protocol are regarded as the signer and the users of the digital signature scheme, respectively. The protocol is described below.

Initializing: Initially, every learner performs an account establishment protocol with the course provider to open an account. Let M be the underlying set of messages.

Enrolling: When a learner wants to learn a course elaborated by a course provider, she/he has to purchase an e-voucher which costs w dollars from the course provider. First, she/he with identity a forms a message $(H(a\|r)\|b) \in M$ where b is the expiration date information, $r \in R$ is chosen at random by the learner and $\|$ is the string concatenation operator. She/He computes and submits $H(H(a\|r)\|b)$ to the course provider. After verifying the identity of the learner through a secure identification protocol[2,11], the course provider computes $S(H(H(a\|r)\|b))$ and sends it back to the learner. The signature-message pair $\alpha = (S(H(H(a\|r)\|b)), H(a\|r), b)$ is an e-voucher in the protocol.

Learning: When the learner decides to learn a course, she/he sends α to the course provider. After verifying $V(\alpha) = true$, the course provider has to check whether the e-voucher is double-used or not. If α is not found in the course provider's database which records all used e-voucher, then the course provider will accept this e-voucher. Finally, the course provider stores the e-voucher in its database for future double-used checking.

Depositing: When the course provider's database is full or some event specified by the course provider occurs such as time expires, the provider has to calculate the number of e-vouchers stored in its database. Suppose the number of a learner *a*'s e-vouchers stored in course provider's database is n. After verifying all e-vouchers, the course provider has to deduct $n \times w$ dollars in learner's account. Since every e-voucher was issued by course provider itself, all course providers can check whether the e-voucher is double-used or not by itself. Therefore, the traffic load is very low.

DISCUSSION

In the tuple $\alpha = (S(H(H(a\|r)\|b)), H(a\|r), b)$ produced by the proposed protocol, $S(H(H(a\|r)\|b))$ is the signer's signature on $H(a\|r)\|b$. According to S and V we have that $V(\alpha) = true$ and it is computationally infeasible for any one to compute the signature $S(H(H(a\|r)\|b))$ on $H(a\|r)\|b$ without the signing function S. In other words, the strength of the proposed scheme depends on the security of the chosen digital signature scheme. Besides, since the computation load of one-way hash function H is very cheap, the presented scheme is efficient.

In some special situations such as to claim the ownership of a lost or stolen e-voucher, the e-voucher owner has to convince the course provider or others of the ownership of her/his e-voucher. When a learner decides to prove that she/he is the owner of her/his e-voucher $(S(H(H(a\|r)\|b)), H(a\|r), b)$, then she/he just needs to show $(a\|r)$. Due to the uninvertability property of the one-way hash function H, given $H(a\|r)$, no one except the learner knows the value of $(a\|r)$. In fact, a can be replaced by any other meaningful messages for other specific purposes.

CONCLUSION

A scheme is presented to provide an easily implemented solution for distance education payment protocol. Since the proposed method is based on a generic digital signature scheme, it can be implemented on payment protocols which are based on digital signature techniques without affecting their infrastructures. Moreover, since the course providers in the proposed scheme can issue e-vouchers by themselves without the help of other parties such as bank, the proposed protocol is simple and applicative.

REFERENCES

1. Ferguson, N., 1994. Single term off-line coins. Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-Verlag, pp: 318-328.
2. Menezes, A., P. Van Oorschot and S. Vanstone, 1997. Handbook of Applied Cryptography. CRC Press LLC.
3. Rivest, R.L., A. Shamir and L.M. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21: 120-126.
4. Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Transactions on Information Theory, 22: 644-654.
5. Schneier, B., 1996. Applied Cryptography. John Wiley and Sons.
6. Simmons, G.J., 1992. Contemporary Cryptology: The Science of Information Integrity. IEEE Press.
7. Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31: 469-472.
8. Pointcheval, D. and J. Stren, 1996. Provably secure blind signature schemes. Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp: 252-265.
9. Rabin, M.O., 1979. Digital signatures and public-key functions as intractable as factorization. MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR212.
10. Schnorr, C.P., 1990. Efficient identification and signatures for smart cards. Advances in Cryptology-CRYPTO'89, Springer-Verlag, LNCS, 435: 235-251.
11. Okamoto, T., 1992. Provably secure and practical identification schemes and corresponding signature schemes. Advances in Cryptology-CRYPTO'92, LNCS 740, Springer-Verlag, pp: 31-53.