A Digital Signature Scheme in Web-based Negotiation Support System

Yuxuan Meng [1] and Bo Meng [2]
1 Department of Computer Science, University of Saskatchewan, Saskatoon, Saskatchewan, S7N 5C9, Canada yxmeng68@yahoo.ca
2 School of Computer, Wuhan University, Wuhan, P. R. China, 430072
bmengwhu@sina.com

Abstract. With the rapid development of electronic commerce, digital signature is very important in preventing from forging, tampering, and disavowing electronic contract in web-based negotiation support system (WNSS). Based on the requirements of electronic contract in WNSS and several techniques widely used in digital signatures, a digital signature scheme for electronic contracts is presented in the paper. Public key algorithm, hash function and interceders are used in the scheme. The feasibility and implementation of the scheme in WNSS are discussed.

1 Introduction

The web-based negotiation support system (WNSS) has been developed and applied in electronic commerce, which could be used to support the negotiators to negotiate through Internet [1, 2]. WNSS can provide real-time remote supports and services in every phases of negotiation. Negotiators can use WNSS to deal with business negotiations and bargaining at any place of the world conveniently.

In the traditional business negotiations, two parties of the negotiation usually sign or stamp on the paper contract, if the negotiation is successful, namely 'black and white'. In this way we can identify trade associates, confirm the reliability of contract and prevent from disavowing. However, when the negotiators agree with a protocol or electronic contract in WNSS, we also need credible identification and implement digital signature to prevent from disavowing. Furthermore, the electronic contract without signatures is easily modified. And the integrity and authenticity of the contract can't be assured.

Based on the requirements of electronic contract in WNSS and several techniques widely used in digital signatures [3-8], this paper presented a digital

signature scheme for electronic contracts in WNSS, which use public key algorithm, hash function and interceders. The digital signature scheme can assure the reliability of electronic contracts and prevent from disavowing effectively. The feasibility and implementation of the digital signature scheme in WNSS are discussed.

2 Digital Signature and Digital Certificates

2.1 Digital Signature

The real purpose of a signature is for an individual/entity to provide a stamp of approval of the data or document under review. In today's world, almost every legal financial transaction is formalized on paper. A signature or multiple signatures on the paper guarantee its authenticity. The signature is typically used for the purposes of user authentication and document authentication. Signatures on the paper have two functions. One is preventing from disavowing, so that we can confirm that the file has been subscribed. Another is preventing from copying, so that we can confirm the reality of the file.

Digital signatures have the same functions of paper-based signatures. However, the digital signatures are more different from paper-based signatures. Because the digital signatures are so dependent on the actual data content, they are very suitable for digital data, which can be tampered with quite easily. The digital signatures have especial problems to be solved. Firstly, the digital file is easily to be copy, even the digital signature is difficult to forge, but cutting and plastering valid signature is so easy. Secondly, the digital file is easily to modify after the digital signature, and the modified file won't leave any trace. Thus simple graphic tag that simulates manual signature can't be used for digital signature.

Digital signature should have some characteristics as follows.

(1) Digital signature should use the information that can only identify signatory.

(2) The content of the message that would be signed can be authentication before signature.

(3) Digital signature could be validated by the third party in order to resolve dispute.

Obviously digital signature not only has the function of identification, but also authentication. Digital signature can be used to preventing from forging signature, tampering information, sending message in the name of other people and denying the information that has been sent/received.

2.2 Digital Signature Algorithms

2.2.1 Symmetric algorithms with interceder

The precondition of this algorithm is that sender and receiver fully trust interceder. Let S, T, R denote sender, interceder and receiver respectively. Then the algorithm is described as follows [3, 4].

(1) S and T share key K_A, R and T share key K_B.

(2) S encrypt file M with K_A to generates K_A (M). Then S sends K_A (M) to T.

(3) Because only S and T share K_A, if T can decrypt K_A (M) with K_A, T can confirm the message coming from S. Then T write a declaration D to prove that he have received the M from S. At last T use K_B to encrypt M and D: K_B (M, D).

(4) T sends K_B (M, D) to S.

(5) S use K_B to decrypt K_B (M, D), then gets M and D. From D, S could assure the M comes from S.

2.2.2 Public key algorithms

Public key algorithms are asymmetric algorithms, which are very suitable for digital signature, because they have public key and private key. It is very important to choose the private key for using Public key algorithms to encrypt file. The keys must meet three conditions: ① SK(PK(M))=M，PK(SK(M))=M. ② To calculate SK from PK is very difficult. ③ It is impossible to determine the M from part of plaintext. The algorithm is described as follows [3, 4].

(1) S encrypts plaintext M with his own private key SK to generate SK (M).

(2) S sends SK (M) to R.

(3) R decrypts with S's public key PK to get M.

If R could carry out step (3), the digital signature of S is valid.

2.2.3 Public key algorithm with hash function

The efficiency of using public key algorithm to encrypt long file is very low. Therefore hash function is always used with public key algorithm at the same time, in order to improve efficiency. In this way, sender needn't encrypt the whole file, he only to encrypt the hash value of the file. The sender and receiver should negotiate and determine the hash function and digital signature algorithm in advance. The algorithm is described as follows [3, 4].

(1) S uses a hash function to generate hash result H (M) of the file M.

(2) S encrypts H(M) with his own private key SK to get SK(H(M)), namely digital signature.

(3) S sends M and SK (H (M)) to R.

(4) R also uses the same hash function with S to generate H′(M) of the M, and decrypts SK(H(M)) with S's public key PK to get H(M). If H′(M)=H(M), then the digital signature is valid.

2.3 Digital Certificates

If digital signature is based on public key algorithms, there are two problems obviously. At first, how to ensure the owners of the public keys are authentic. Secondly, how to deal with the production, distribution and management of the public keys. Certification Authority (CA) can resolve above problems. The authenticity of public keys may be established by a trusted third party. A guarantee of the identity of the owner of a public key is called *certification* of the public key. A person or organization that certifies public keys is known as a Certification Authority (CA). The digital certificate is the evidence as identity of the person or organization on Internet. It includes the owner's name, public key, CA's digital signature, the

period of validity of the digital certificate, etc. Digital certificate can provide identity and authenticity, so it is widely used in electronic commerce.

3 A Digital Signature Scheme in WNSS

3.1 Requirements of Digital Signature in WNSS

It is very important for both negotiators to sign the contract by the end of the negotiation, because the signed contract is the voucher of the business trade. To insure the validity, fairness of the signature and prevent from disavowing, the digital signature in WNSS should satisfy the following requirements.

(1) The digital signature of both negotiators of the negotiation is authentic. Any negotiator can confirm the signature he received comes from the other party of the negotiation, but not from someone else.

(2) The digital signatures of the negotiators can't be forged. Only negotiators can sign the contract, anyone else can't forge their signatures.

(3) The digital signatures of the negotiators can't be used repeatedly by other people. The signature is a part of the contract. Anyone else can't transfer the signature to other files.

(4) The context of the contract that both negotiators should sign must be same. In the process of transfer, the context of the contract can't be tampered.

(5) The digital signature of both negotiators is of non-repudiation. After both negotiators have signed the contract, they can't deny their signatures.

(6) The digital signature of both negotiators is fair. At the end of the process of signature, the result is both negotiators having received the other party's signature or both negotiators having not received the other party's signature.

(7) If the context of the contract was very confidential, it could be seen by both negotiators only.

3.2 The Digital Signature Scheme in WNSS

Taking into account of the requirements of digital signature in WNSS and several algorithms widely used in digital signatures, we designs a new digital signature scheme for electronic contracts in WNSS, which uses public key algorithm, hash function and interceders.

Let A and B be two negotiators of the negotiation respectively. Let PK_A, PK_B, PK_C be the public keys of the negotiator A, B and interceder respectively. Let SK_A, SK_B be private keys of the negotiator A, B respectively. Let H be hash function. Let M be the plaintext of the electronic contracts. The digital signature scheme is described as follows.

① A encrypts M with B's public key PK_B to generate $PK_B(M)$. A use hash function to generate hash result H(M). Then, A encrypts H(M) with his private key SK_A to sign the M. And $SK_A(H(M))$ is called the digital signature. Furthermore, A

encrypts H(M) and SK_A (H(M)) with C's public key PK_C to generate a information packet ATC: PK_C (H(M)，SK_A (H(M))), which would be transferred to C by B.

② A sends PK_B (M), H(M) and ATC to B.

③ B will decrypt PK_B (M) with his own private key SK_B to get M. Then B uses the same hash function as A to generate his own hash result H′(M). If H(M)= H′(M), then B can be sure M has not been changed during transference. Then B encrypts H′(M) with his own private key SK_B to sign the M. And SK_B (H′ (M)) is B's digital signature.

④ B sends H′(M), SK_B (H′(M)) and ATC to C.

⑤ C decrypts ATC with SK_C to get H(M) and SK_A (H(M)). Then C will compare H(M) with H′(M). If it is different, then M is changed during transference. Hence the digital signatures of both negotiators are invalid. If it is same, then the M that B signed is the same as that A signed. Then C will decrypt SK_A (H (M)) and SK_B (H′(M)) with PK_A and PK_B respectively. If $H(M) \neq H'(M)$, the digital signatures by both negotiators are incorrect, then the signatures are invalid. If H(M)=H′ (M), then C can ensure the signatures by both negotiators are valid.

⑥ If the digital signatures by A and B is valid, then SK_B (H′(M)) is time-stamped and sent to A by C, and SK_A (H(M)) is also time-stamped and sent to B by C.

3.3 The Feasibility Analysis of the Scheme

The feasibility of the scheme is analyzed as follows.

(1) The digital signatures are authentic. Because C is a trusted interceder by both negotiators, the digital signatures that received by each negotiator are verified and confirmed by C.

(2) The digital signatures are not forged. Because only negotiators have their own private keys, if interceder can decrypt signatures with negotiators' public keys respectively, he will know the signatures are not forged.

(3) The digital signatures can't be used repeatedly. Because that the negotiators signed is the hash result of contract, the signatures can't be copied to another contracts.

(4) The digital signature scheme can satisfy the integrity requirement of the contract. In the step ⑤ of the scheme, if the context of H′(M) and H(M) is different, we can discover the context of contract that each negotiator signed is different and the contract is changed by someone else in the transfer process.

(5) The digital signature scheme can satisfy the requirement of non-repudiation. Because both negotiators receive signed contract that is time-stamped and sent by interceder, they can't deny their signatures. The interceder can verify and prove the signatures of the both negotiators.

(6) The digital signature scheme can satisfy the fairness requirement. After the interceder has verified that the signatures are valid, both negotiators can receive the other negotiator's signature of the contract. Otherwise, both negotiators can't receive the other negotiator's signature of the contract. Both negotiators are in the strong fairness situation. And the interceder couldn't see the context of the contract.

(7) The execution efficiency of the scheme is very high, because negotiators only encrypt the hash result and the interceder needn't to transfer the contract. The interceder only do a few public key operations and signature verifications, then sent verified signatures to negotiators.

(8) In the digital signature scheme, the transferred contract can also be encrypted with keys that are different from signature keys in order to improve the security of the scheme further.

3.4 Implementation of the Digital Signature Scheme in WNSS

Generally a trusted third party is needed to provide service and intercede negotiation through WNSS. The third party can aid the negotiators in the process of the negotiation. Therefore, the trusted third party in WNSS can act as the interceder of the digital signature scheme. Because we use public key algorithm to encrypt contract, we need a CA to provide certificate service. In a similar way, the trusted third party can act as CA.

As we all know, MS NT 4.0 is widely used in Intranet and Internet. And in the Option Pack the software named Certificate Server1.0 can be used to construct our own CA conveniently and to realize the authorization and certification to the web server and client. The both negotiators can adopt X.509 certificate. The digital certificate can not only implement the bi-directional authentication in SSL connection, but also implement digital signatures with the keys in the certificate.

RSA is one of public key algorithm that is well known with its high security. It is especially suitable for using in digital signature. The algorithm of RSA is as follows.

Public key: $n = p\,q$. (p and q are two large prime numbers and are secret.)

Private key: $d = e^{-1} \bmod ((p-1)(q-1))$. (e is relatively prime to (p-1)(q-1). e and n are public.)

Signature procedure: $S = M^{d} \bmod n$

Validation procedure: $V(M, S) = TRUE \Leftrightarrow M = S^{e} \bmod n$

Up to now many hashing algorithms have been designed, such as Rabin hash algorithm, N-hash algorithm, MD2, MD4, MD5, SHA and so on. MD5 produces a 128-bit (16-byte) hash result. The security of MD5 algorithm is higher and its operation speed is very fast, so that it is widely used. In WNSS we use RSA and MD5 to implement digital signatures for electronic contract.

As a network programming language, JAVA is rapidly developed and widely used in Internet. JAVA integrates a number of security tools. It can be used to develop multifunctional application programs that include identity certification, digital signature, encryption, decryption, etc. JAVA is also used to implement web-based negotiation support system. Therefore we use JAVA to develop and implement our digital signature application programs in WNSS.

4 Conclusions

Based on the requirements of electronic contract in WNSS and several techniques widely used in digital signatures, a new digital signature scheme for electronic contracts is presented in the paper. Public key algorithm, hash function and interceders are used in the scheme. The feasibility of the scheme is analyzed. It has been implemented in our web-based negotiation support system.

Digital signatures could be used to prevent from forging, tampering and disavowing, so it is one of the important techniques in electronic commerce. With the development of electronic commerce, the techniques in network security that include digital signature will be more and more important in our lives.

Acknowledgment

This research was supported by China Scholarship Council and the Natural Science Foundation of Hubei province of China (Project No. 2001ABB058).

References

1. B. Meng and W. Fu, An Overview of Theories and Models in Group Decision Making and Negotiation Support Systems, *Proceedings of '99 International Conference on Management Science and Engineering*, 1999.

2. W. Gao and B. Meng, Research and Development of Web-based Negotiation Support System, *Computer Engineering,* **29**（19）, 63-65(2003) (in Chinese).

84. 3. Mohan Atreya, et al., *Digital Signatures* (McGraw-Hill, Berkeley, Calif., 2002).

85. 4. J. C. A. van der Lubbe, *Basic Methods of Cryptography* (Cambridge University Press, New York, 1998).

86. 5. Timothy P. Layton, *Information Security: Design, Implementation, Measurement, and Compliance* (Auerbach Publications, Boca Raton, 2007).

6. Elena Ferrari and Bhavani Thuraisingham, *Web and Information Security* (IRM Press, Hershey, Pa., 2006).

7. Aashish Srivastava, Electronic Signatures: A Brief Review of the Literature, Proceedings of the 8th International Conference on Electronic Commerce: The new e-commerce: Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet ICEC '06, August 2006.

8. Mark Stamp, *Information Security: Principles and Practice* (Wiley-Inter Science, Hoboken, N.J., 2006).