December 2004
Volume 2, Number 12

Bank Fraud & IT Security REPORT

Prepared by
Southeast Consulting, Inc.
SCI

Securing eBusiness with Cryptographic Technology

By Dr. Yongge Wang
Assistant Professor of Software and
Information Systems
UNC Charlotte

Cryptographic techniques are playing an increasingly important role in Internet security. However, it is crucial to apply the right cryptographic techniques in the right places.

What is Cryptography? Cryptography is generally understood to be the study of principles and techniques about encryption and decryption. In fact, it is a specialized branch of information theory with many complex components that could be used to protect the eBusiness infrastructure. In particular, cryptography is often used to achieve the following functionalities:

❑ *Encryption and decryption.* Encryption techniques are used to protect the communication between customers and financial servers so that no one else could learn any useful information from these communications.

❑ *Authentication.* Authentication techniques are used to allow the customer to verify his or her identity to remote financial servers. In most cases, the credentials that the customers use to achieve this goal are proprietary account numbers and passwords. When secure authentication techniques are used, an intruder should not be able to masquerade as another customer.

❑ *Integrity.* Integrity techniques are used by both the customer and the server to verify that the messages communicated over the Internet have not been modified in transit. Thus a fraudster should not be able to substitute a false message for a legitimate one.

Table of Contents

Editorial Board

A.S. Pratt & Sons

❑ *Non-repudiation.* When secure non-repudiation techniques are used, a customer should not be able to falsely deny later that he or she submitted a transaction, and a server should not be able to falsely deny later that it has processed a transaction.

These cryptographic functionalities are achieved by using one or more cryptographic primitives such as private key ciphers, public key ciphers, signature schemes, and one-way hash functions. The popular cryptographic primitives that have been used in financial services include DES, AES, and RSA cipher; RSA and DSA signature schemes; MD5; SHA-1; and SHA-2.

Applying the Right Cryptographic Techniques. It is well known that the security level of an entire system depends on the weakest point of that system. Thus it is crucial to apply the right cryptographic techniques in the right place. For example, if one chooses to use AES-128 and SHA-1 in one system at the same time, then one can only achieve 80 bit security.

There are no bullet-proof cryptographic techniques. It is also advised that security managers of financial services should regularly pay attention to news from the cryptographic community and replace any broken cryptographic systems. For example, MD5 has been broken recently and it has been extensively used by the financial services industry. Accordingly, it is critically important for bank IT security managers who are using MD5 cryptography to replace these systems.

Newly Discovered MD5 Vulnerabilities. At the CRYPTO conference in Santa Barbara, California, during August 2004, several weaknesses in common one-way hash functions including MD5 and SHA-1 were reported. Though these results have no immediate threat to Internet security, this development does mean that significant progress has been achieved on mathematical techniques that could be used to attack hash functions. These techniques may eventually be used to design practical attacks on current financial services. Accordingly, it is now time for the cryptography community to create new hash function standards and for the financial services industry to give up security tools that still rely on MD5 and SHA-1 technologies.

One-way hash functions are used in almost all security applications. Generally, hash functions are utilized in conjunction with public-key algorithms for digital signatures to achieve integrity, authentication, and non-repudiation. Professor Rivest from MIT designed a hash function Message Digest 4 (MD4) in 1990. To address several MD4 weaknesses, in 1992 Dr. Rivest designed an improved one-way hash function, Message Digest 5, which was an improvement on MD4. In 1993, the National Security Agency (NSA) published a one-way hash function SHA (Secure Hash Algorithm), which is very similar to MD5. Then, in 1995, the NSA made some changes to SHA and announced a new hash function designated SHA-1 which is the most popular one-way hash function in use today. Over the years, the NSA has reported that some weaknesses in SHA have been found but, to date, the agency has refused to elaborate on these limitations.

One-way hash functions should have three properties:

- They must be easy to evaluate.
- They are hard to reverse. This means that it is easy to take a message and compute the hash value, but it is impossible to take a hash value and recreate the original message.
- They are collision resistant. This means that it is impossible to find two messages that hash to the same hash value.

In particular, the cryptographic reason for the third property is as follows: When Alice signs a contract M, she should not be able to claim that she has signed a different contract M' in the future, thereby achieving non-repudiation. It also implies that the following scenario is impossible, thus achieving authentication and integrity. Bob creates a contract M="I, Alice, will pay 10$ to Bob" and a fake contract M'= "I, Alice, will pay 1000$ to Bob," and ask Alice to sign the contract M. Some time later, Bob claims that Alice signed the contract M'. Breaking a hash function means showing that some or all of those three properties are not true.

At the August 2004 CRYPTO conference, Doctors Xiaoyun Wang, Xuejia Lai, Dengguo Feng, and Hongbo Yu from various Chinese national universities announced many message pairs that could be hashed to the same hash values when MD5 is used. Thus, the collision-resistant property of MD5 has been broken. In other words, the authentication, integrity, and non-repudiation properties are no longer guaranteed for security systems that use MD5 as one of the building cryptographic blocks.

New Attacks Likely. This development is a huge step in cryptanalysis techniques and the attack is a substantial advance forward in cryptographic research. The techniques used to attack MD5 are likely to be used to attack other one-way hash functions. However, security systems that use MD5 are not suddenly insecure. Significant progress is still needed to use these attacks to break the signature schemes that are used by the banking and financial services industry. However, bank fraud prevention and IT security managers should readily consider the use of hash functions employed by SHA-256, SHA-384, and SHA-512, which have been designed by NSA to replace their existing MD-5 encrypted systems.