SECURE OFFICIAL DOCUMENT MAIL SYSTEMS FOR OFFICE AUTOMATION

Chung-Huang Yang[*1], So-Lin Yen[2], Hwang David Liu[2], Kuei Liu[2], Bor-Shenn Jeng[* 3,4], Kung-Yao Chang[4], Min-Shin Chang[4], Yu-Ling Cheng[4], Jo-Ling Liang[4], Don-Min Shien[4]

[1] Dept. MIS, National Institute of Technology at Kaohsiung, Yenchao, Taiwan, ROC

[2]Scientific and Technical Research Center, MJIB, P.O. Box 3562, Taipei, Taiwan, ROC

[3]Institute of Optical Sciences, National Central University, Chung-Li, Taiwan, ROC

[4]Telecommunication Laboratories, CHT, P.O. Box 71, Chung-Li, Taiwan, ROC

Abstract – Electronic mail or email system is by far one of the most widely used applications in the office automation systems. However, due to the lack of communication security services and the impose of export controls, sensitive official document of government organizations could not be transited securely over open networks using off-the-shell email systems. In this paper, we present the result of a joint effort between the Chunghwa Telecom and the Ministry of Justice Investigation Bureau of Taiwan to integrate security services into existing official document mail systems.

Introduction

Office automation (OA) has become the most urgent work to improve the working productivity for the governmental branches in Taiwan. The most common means of information security measure used in the OA system [1] is by applying the *logon* procedure. Each legitimate user is provided with an unique ID and a regularly expired password, and then access to the system is allowed only when the user input the correct ID/password. However, this basic security measure provides no protection against eavesdropping for any information transmitted over communication channels, such as the case in the electronic mail (email) system. There is not question that more security measures are needed for email.

* This research was supported in part by the National Science Council, Republic of China.

Cryptography [2,3,4] is the only practical means for sending information over an insecure channel. The increasing use of electronic means of data communications, coupled with the growth of computer usage, has extended the need to protect information. Considerable progress has been made in the techniques for encryption, decryption, and fending off attacks from intruders over the last decade. Nevertheless, the impose of export controls [5] on those computer software or hardware devices involving encryption have precluded the use of secure products or made such imported products very expensive. This is the primary motivation for the Chunghwa Telecom Co., Ltd. (CHT) and the Ministry of Justice Investigation Bureau (MJIB) of Taiwan to have a joint effort in integrating security services into existing official document email systems.

Secure official document email systems

The objectives of our efforts on the development of secure official document email systems are to provide security services to the original email systems which did not think about information security at the first place. The security services [6, 7, 8] include data confidentiality, authentication, access control, data integrity, and non-repudiation. For the email system in consideration, we are mainly concerned about the security risks occurred during message transmission and the access control service will not be considered. In other words, our goals are (a) to provides confidentiality (only the authorized recipient can meaningfully read the message), (b)

0-7803-3913-4-9/97/$4.00 ©1997 IEEE

to provides authentication of both message originator and recipient (they are who they claim to be), (c) to provide data integrity (message should not be altered without being detected during the transmission), and (d) to provide non-repudiation of transmission (originator can't say it didn't come form him/her).

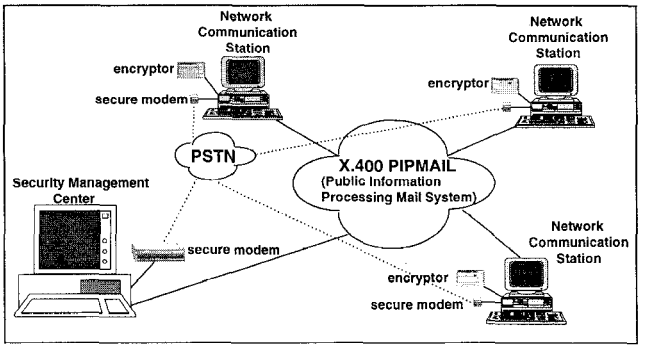

Fig. 1. System diagram of the secure email system

In our design, shown in Fig. 1, each of the Network Communication Station (NCS) in originally official document mail systems is equipped with two security devices, an *encryptor* and a secure modem. The encryptor will provide email encryption and key management functions for the transited document while the secure modem will communicate with the Security Management Center (SMC) which is responsible for auditing and network management. Both encryptor and secure modem are communicated with NCS through RS-232C interface.

Fig. 2 shows the block diagram of the low-cost encryptor developed by the Telecommunication Laboratories of Chunghwa Telecom (CHT). It is mainly consisted of two processors working together, a DSP chip (Motorola DSP56002) and a 8-bit single-chip microcomputer (Motorola MC68HC705B16). The high-speed DSP processor provides the necessary computational power for cryptographic functions while the single-chip microcomputer acts like a smart card and stores personalized information of NCS. Each encryptor must perform personalization process, stores default PIN and the so-called *private key* data, before it could be operated with NCS.

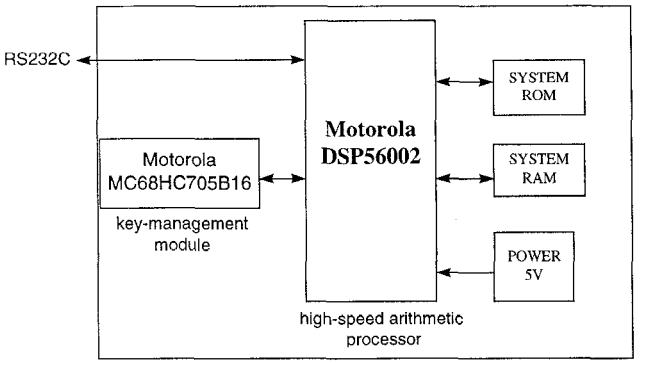

Fig. 2. Block diagram of the developed security device, *encryptor*

The security services is primary based on the public-key cryptography. Each entity, such as the NCS, has a pair of public key and private key. Private key is generated locally and will be kept secretly at every entity and individually stored at the built-in EEPROM area of the single-chip microcomputer while the public key is openly available to each other entity from the Security Management Center.

Data Confidentiality: Data secrecy is provided by applying encryption. Two encryption methods are selectable by user, one is based on the block cipher where the Data Encryption Standard (DES) [9] is implemented, the other is based on the stream cipher where an enhanced EBU's pseudo-random bit generators (PRBGs) [10] are proposed. The DES is configured only in the triple encryption manner where a 112-bit encryption/decryption key is used in order to combat brute-force exhaustive search attack on the 56-bit DES. The EBU's PRBG is known to have a cryptographic weakness [11] and we propose to enhance its cryptographic strength by the concept of bilateral step control [11]. The resultant PRBG circuitry is illustrated in Fig. 3.

Our system also makes use the idea of *digital envelope* [4] of the RSA [12] public-key cryptography. The advantage of public-key cipher is in its key management capability but its execution performance is quite slow in comparison with the secrete-key cipher. In the digital envelope scheme, public-key cipher is combined with a secret-key cipher to achieve both high-speed encryption and easy key management. The

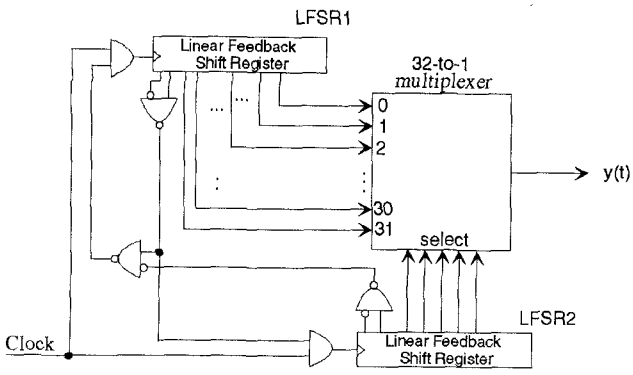

Fig. 3. Circuit diagram for the proposed pseudo-random bit generators (PRBGs)

email message originator first encrypts the message with secret-key cipher, using a randomly chosen key, the *session key*. Then originator looks up recipient 's public key from the Security Management Center and uses it to encrypt the session key. The secret-key-encrypted message and the public-key-encrypted session key together form the digital envelope and are sent to recipient. Upon receiving the digital envelope, recipient decrypts the session key with his/her private key, then uses the session key to decrypt message itself.

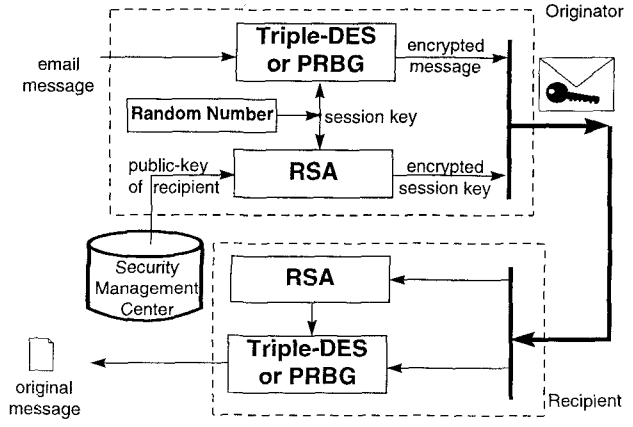

Fig. 4. Digital envelope for email message confidentiality

In the RSA public-key methodology, its security strength is related to the discrete logarithm problem and the factorization problem. The size of private key must be properly chosen; too small will enable attackers to crack the system easily, and too large will degrade the encryption and decryption performance. The size of RSA key in our implementation ranges from 512 bits to 2048 bits, configurable by the system administrator.

Authentication, data integrity, and non-repudiation: The authentication framework is based upon the ITU-R X.509 [13] certificate framework and employs digital signature to verify the authenticity of email message. A digital signature algorithm allows an entity to electronically sign a message and generate a signature which is dependent on both message itself and the entity's private-key information. The computed signature is then attached to the message and sent with the message. The signature verification process could be performed by any receiving party and cannot be repudiated. Recipient could verify the signature by doing some computation involving the received message, the attached signature, and sender's public key. If the results properly hold in a predefined mathematical relation, the signature is accepted as genuine; otherwise, the signature may be fraudulent or the message altered. Mutual authentication between the Network Communication Station and the Security Management Center is also enforced for protection against attackers designed to capture NCS communication.

At present, we implement the RSA algorithm for use on both digital envelope and digital signature. A message digest algorithm, NIST's SHA-1 [14], is used with the RSA algorithm for signature generation and signature verification shown in Fig. 5. The message digest algorithm [2,3] is an irreversible function, so-called one-way hash function, that takes an arbitrary sized message and output a fixed length hash value. Therefore, instead of directly applying RSA digital signature scheme on a long message, we efficiently sign on the message's hash value which is only 160 bits for SHA-1.

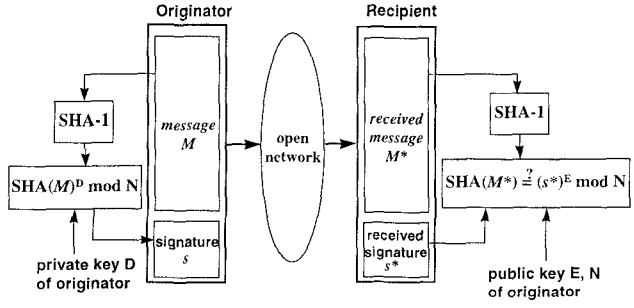

Fig. 5. Digital signature for message authentication and non-repudiation

Finally, the field trial of our security-enhanced email system has been performed at three CHT sites: headquarters, International Business Group, and Telecommunications Laboratories. The implementation has been successfully tested and it is expected to have a much larger scale of trials in the near future.

Summary

We have presented a design of secure email system where communication security was made an integrated part within the system. To protected both classified and sensitive official documents, we propose to use a key-dependent pseudo-random bit generators based on bilateral step control. We also developed a low-cost security devices to server out needs. Our system makes use of the idea of *digital envelop* and *digital signature* of the public-key cryptography and we successfully implemented a secure official document mail which meets the required security services.

REFERENCES

[1] V. Murphy and D.A. Roberts, "Office Automation Security," Br. Telecom. Technol. J. Vol. 9, No. 1, January, 1991, pp. 105-114.

[2] Gus Simmons , *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, 1992.

[3] Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, Prentice-Hall, Inc., 1995.

[4] RSA Labs Frequently Asked Questions on Cryptography, http://www.rsa.com/rsalabs/newfaq/.

[5] "Administration Of Export Controls On Encryption Products," Executive Order, White House, November 15, 1996, http://www.bxa.doc.gov/eo13026.htm.

[6] ISO 7498-2, "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture," 1989.

[7] Stephen T. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM*, Vol. 36, No. 8, August 1993, pp. 48-60.

[8] Bruce Schneier, *E-Mail Security*, John Wiley & Sons, Inc., 1995.

[9] National Institute of Standards and Technology, "Data Encryption Standard," Federal Information Processing Standard, FIPS PUB 46-2, December 1993.

[10] European Broadcast Unit (EBU), *Specification of the Systems of the MAC/Packet Family*, EBU Tech. 3258, 1986.

[11] Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei and T.R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography," *IEEE Computer*, Vol. 24, No. 2, February 1991, pp. 8-17.

[12] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Feb. 1978, Vol. 21, No. 2, pp. 120-126.

[13] ITU-T Recommendation X.509 "Information Technology - Open Systems Interconnection - The Directory : Authentication Framework," 1993.

[14] National Institute of Standards and Technology, "Secure Hash Standard," Federal Information Processing Standard, FIPS PUB 180-1, April 1995.