IMPLEMENTATION STUDY OF PUBLIC KEY CRYPTOGRAPHIC PROTECTION IN AN EXISTING ELECTRONIC MAIL AND DOCUMENT HANDLING SYSTEM*

J. Vandewalle, R. Govaerts, W. De Becker, M. Decroos+
ESAT Laboratory, K.U. Leuven
Kardinaal Mercierlaan 94, 3030 Leuven, Belgium
and G. Speybrouck
Telindus, Geldenaakse Baan 335, 3030 Leuven, Belgium.

1. Introduction.

The problem which is addressed in this paper is to study the public key data protection (privacy, integrity and signatures) of an existing electronic mail and document handling system. This is not a trivial and straightforward problem since the protocols have to be tailored to the user's needs and since many trade-offs are involved between speed, security and ease of use. Moreover the final security of the overall system not only depends on the choice of the cryptographic algorithm, but also on the communication protocol, the key management and their implementation (physical security and computer security). In other words the security is a property of the whole system [3]. Although many of the arguments described in the paper are rather system dependent, it is expected that the approaches taken here are valuable for other applications too. The readers are however cautioned not to transfer the conclusions blindly.

In the paper we first describe in Section 2 the protection needs in and threats to the existing system. Section 3 presents a protection scheme which is tailored to these needs and to the system. A choice of the cryptographic system is made (RSA public key). In Section 4 the key management is described, while in Section 5 the communication protocol is presented. Section 6 presents the conclusions.

2. Protection needs in the existing system.

The Belgian Information System by Telephone (BISTEL) is the information network of the Belgian Goverment. It comprises more than 120 videoterminals, word processors, laserprinters and telexterminals spread over the remote ministerial departments. In the department of the Prime Minister an interconnection through a Local Area Network (LAN) is provided. All these remote sites are connected with a central computerroom

*Supported by the Services of the Prime Minister of Belgium under the BISTEL projekt.
+Part of this text has been elaborated within the framework of the Belgian Programme for the reinforcement of the scientific potential in the new technologies - PREST (Prime Minister's Office for Science Policy). The scientific responsibility for the text is assumed by its authors.

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 43-49, 1986.

through the Public Switching Telephone Network (PSTN), the telexnetwork, or the X.25 packet switching network (DCS) of the Belgian R.T.T. The central computerroom is equipped with computers, databases and disk storage and a communication processor controlling the local network. This computerroom is physically protected against unauthorized access. The system is highly automated and can be operated day and night in a very user-friendly way (menu driven) by politicians as well as administrators. The system first of all performs the function of electronic mail between the terminals (editing and mailing of texts, chats). The electronic mail system operates in much the same way as ordinary mail. A sender A makes the central computer store a letter in the mailbox of the receiver B. B can read this message at his leisure. With the document handling facility one can store electronic mail, documents and telexes temporarily (3000 Mbyte disc) or archive (4000 Mbyte disc) them in a central database (document handling). The system also distributes telexes of international press agencies (UPI,AFP, Reuter, Belga) (media). The system also allows to consult databases. The general experience with the system is positive.

It is well known that passwords do not provide data protection and can only provide some barrier against unauthorized access. Even this barrier is not very resistant against computer hackers. The goal of this project is to study and evaluate protection alternatives for the system with a net speed which is not too much lower than the actual speed of 1200 bps, while maintaining the user-friendliness. One should achieve high standards of privacy protection, message as well as sender authentication and signature protection during the transmission through the network as well as during temporary or permanent storage. Here one should bear in mind that the protection of the system should not be based on a simultaneous presence of both the sender and the receiver (handshaking or mutual protocols) since it is more intended for electronic mail than for chats. In order to be able to compare the effectiveness of alternative protection schemes it is important to understand the major security threats of the system. By wiretapping the telephone, telex or packet switching network or by unauthorized access to the computer, one can obtain sensitive data (threat to privacy). The authenticity of messages is threatened by the injection of false or old messages or modification of blocks (replacing, inserting, deleting, modifying, ...) of existing messages either through the network or inside the computer. Moreover the classical subjective recognition of a sender by his handwriting in a letter or by his voice in the phone is no longer possible in the electronic mail. Hence it is important that the transmission as well as the storage of data in the system is protected against masquerade i.e. an intruder pretending to be an authorized user of the system (sender authentication). Finally it should not be possible for a sender to deny his sending a message nor for the receiver to deny the receipt (certified mail and electronically signed documents [1;4,p.14]). This implies that an independent third party can confirm the identity of the sender and the receiver of a message.

3. Selection of the protection scheme.

In the next three sections we compare and motivate the engineering choices related to the kind of encryption (symmetric versus asymmetric), the encryption algorithm and scheme, the key management and the communication protocol. Then we explain how the proposed protection scheme counters the major threats described in the previous Section. The choice between three kinds of encryption [4] classical or symmetric system, public key distribution system, and public key system is made in favor of the last one because of several reasons. First of all classical cryptography requires much processing

of keys. Either it needs a different key for any pair of users which implies already 7140 keys for 120 users or in case session keys are used a vast key management is necessary. For practical algorithms (like DES) the key may have to change often in time. Hence this requires much bookkeeping of the encrypted documents and the corresponding keys. Of course these keys have to be stored in a protected way. Moreover the symmetric nature does not provide a signature protection. The second alternative (the combination of a public key distribution scheme for key transmission and a classical algorithm for data transmission) is not so appealing because it requires the implementation of two algorithms (more hardware or software). Moreover the inconvenience of updating and securely storing the keys of the classical scheme remains. A public key encryption is preferred because it requires less keys which last longer and because only one algorithm can provide many different protections (privacy, authentication, signature and even special needs [5]).

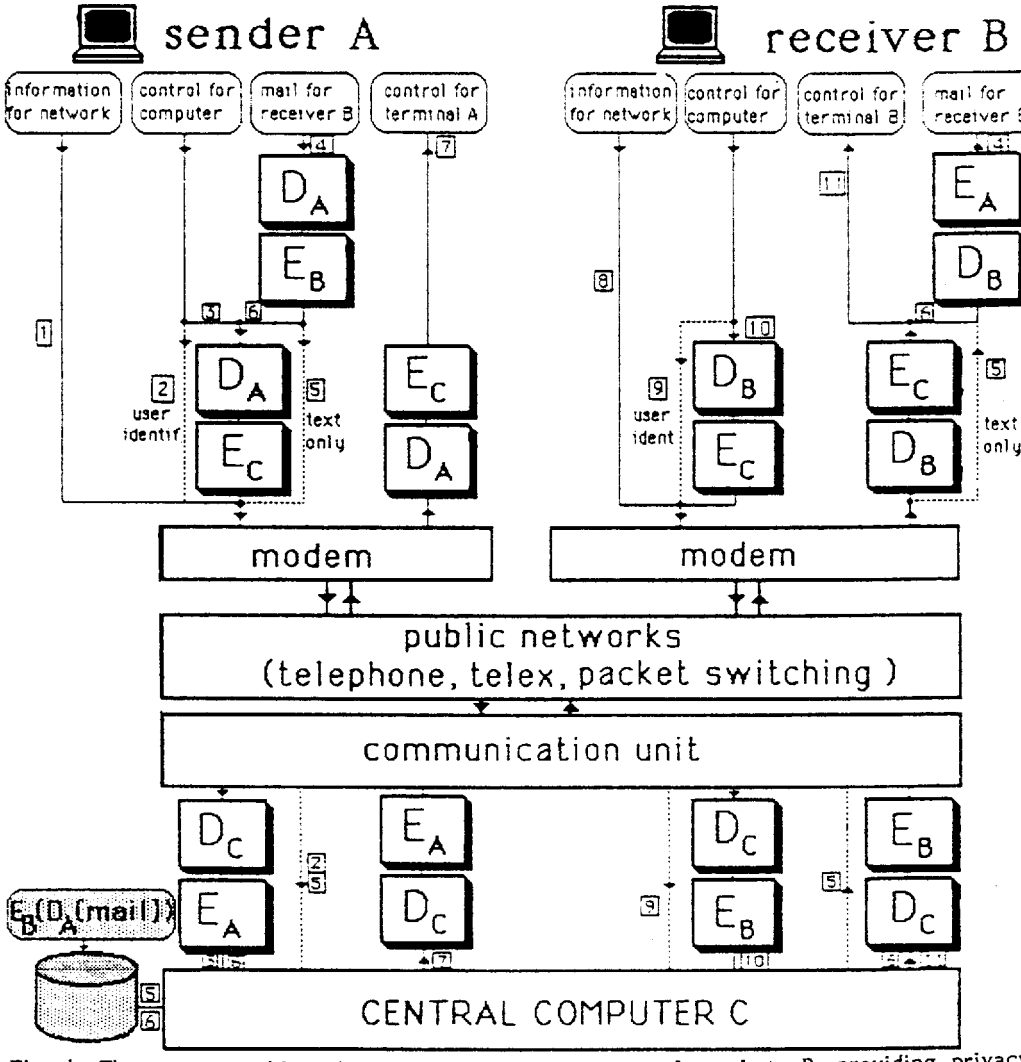

Fig. 1. The cryptographic scheme for mailing a message from A to B, providing privacy protection and authentication.

Although classical schemes and public key distribution schemes generally provide higher speed of data transmission, the required speed of 1200 bps does not exclude public key schemes.

The selection of RSA [6] as the public key cryptographic algorithm is motivated by the following arguments. The alternative algorithms are either broken (Merkle Hellman knapsack [7]) or not yet fully investigated (the most general knapsack [8]). The RSA algorithm with 200 decimal digits however is generally considered to be secure for several years to come [9]. Indeed intensive and diverse efforts over more than 5 years have shown only weaknesses which can be easily overcome. The scheme allows all types of protection and is most likely to become an ISO standard in a couple of years [1]. Moreover encryption and decryption speed of 1200 bps required for this system is certainly feasible.

In the sequel we denote by (e_X,n_X) the public key of user X (exponent e_X, modulus n_X). A transformation with key (e_X,n_X) is denoted by E_X (.). Any user of the system can perform this operation in order to make his message only understandable by X or in order to verify the authenticity of a message sent by X. User X can utilize the corresponding secret key (d_X,n_X) of X in the transformation D_X (.) in order to decrypt the encrypted message he receives or in order to authenticate his message.

In order to achieve a high security the cryptographic scheme (Fig.1) provides an end-to-end protection of privacy and authenticity of the mail as well as a link protection of the privacy and authenticity of the communication with the central computer. Thereby the data which are transmitted or stored are protected as much as possible. The data (i) which are available at certain points in the diagram of fig. 1 are numbered from (1) to (11) and put in a box in Fig. 1.

4. Key management.

The keys are generated at the place and on a workstation which is physically disjoint from the central computer thereby separating the responsibilities. Referring to Table 1 we describe for all the keys their function, storage and back-up. The first three types of key-pairs are used to protect data, respectively personal messages (mail), control data for the computer and messages to all members of a group. The master key-pair is used to protect the authenticity of the transmitted keys.

The personal key-pairs are of course different for each user and remain the same at least for a long period. The computer key-pair is the same for each user and changes much more often, because of its intensive and widespread use. It is transmitted to the user at each session, protected by the masterkey. The group key-pair is the same for all members of a group. It remains the same for a period comparable to that of a personal key-pair. The master key-pair is different for each user. Unlike the other keys, both "public" and "secret" key are kept secret. It can therefore remain the same for a very long period. In practice it can be changed at the same time as the personal key. The public personal key, the public computer key and the public group key are all stored in the central computer. The public personal key of all users and the public group key of all groups are also stored in non-volatile memory in each user's terminal. This allows an independent verification of the public keys sent by the computer. The public master key is stored in a memory chip or chipcard together with the secret personal key because they are very long to remember and difficult to type in correctly. The user is however responsible for the physical security of the "hardware" key. As an extra protection a part (say 6 characters) has to be entered in order to be able to use the keys in the memory. This is an extra barrier for the finder or thief to overcome

KEYS	FUNCTION(S)	STORAGE	BACK-UP
1.a)public personal key of A (e_A,n_A)	encrypt and verify authenticity of mail	locally on diskette verified with a copy authenticated by computer	no problem
b)secret personal key of A (d_A,n_A)	decrypt and authenticate mail	memory chip or chipcard a part is entered on the keyboard	in safe (sharing)
2.a)public computer key (e_C,n_C)	encrypt and verify authenticity of communication with computer	sent by computer with secret masterkey authentication and public personal key protection then stored on cryptocard in terminal	no problem
b)secret computer key (d_C,n_C)	decrypt and authenticate communication with computer (same for all users but varies often)	control computer	no problem
3.a)public group key of group A (e_G,n_G)	encrypt messages to group G	same as 1	no problem
b)secret group key of group G (d_G,n_G)	decrypt messages to the group	same as 1b) or 2a)	same as 1
4.a)public master key of A (e_{MA},n_{MA})	verify authenticity of computer key	memorychip or chipcard	no problem
b)secret master key of A (d_{MA},n_{MA})	transmit computer key (different for each user A)	central computer in protected memory	no problem

Table 1. Key management.

before (s)he can use the key. The secret computer key remains in protected area in the computer. The secret group keys are stored in the same protected area. The keys are authenticated with the secret personal key of the groupleader and for each groupmember they are protected by his (her) public personal key. The secret master keys are stored in protected area in the computer as it is used for authentication of the keys transmitted by the computer.
The back-up of keys requires special attention only for the secret personal key and the secret group key since no messages are stored with encryption under either master key or computer key. In order to have a secure back-up when the secret personal key and the secret group key are lost or destroyed, the keys are partitioned over different safes so that only a sufficiently large subset of parts can reconstruct a key (sharing). Of course if a lost key is compromised a new key should be generated and the stored data which were protected with the compromised key should be recuperated quickly. If certificates are used in the protocol, a backup of the public masterkey of each user is necessary.

5. Basic steps of communication protocol for securely sending mail from A to B.
Part I Transmission of a protected message from A to the central computer.
1. The network information like the phone number (1) is sent to the network in clear

2. After connection to the host computer the electronic mail function is activated.
3. Then the identification (name) of the sender (2) is transferred in clear to the computer. After receiving the necessary keys (see Section 6) the encrypted password is sent to the computer. Though the security of the system does not depend critically on the password protection, its barrier along with a possible call-back system can detract many computer hackers.
4. The control for the computer mail program (3) is then sent authenticated by A with D_A and encrypted with E_C. Of course in order to be able to verify the authenticity each block has to contain a sufficient number of redundant bits.
5. The control to the terminal in response (7) is authenticated by the computer with D_C and encrypted with E_A.
6. The mail (4) from A to B is authenticated by A with D_A and encrypted with E_B. When it is combined in a block with control (6) an additional authentication with D_A and encryption with E_C of the complete block happens as in step 4. The authenticated and privacy protected mail is stored on disk.
7. At the end of the session A sends a disconnection message to the computer authenticated by D_A and encrypted with E_C.
8. The terminal switches to off-line condition.

Part II Reading of the protected message by B from the central computer.
As shown in Fig. 1 B proceeds analogously as A in part A. Of course in 6 the computer sends the protected message to B.

6. Basic steps of the key transfer protocol.

Communication beween user A and computer (Part I,3)

1. The computer sends (e_C,n_C) authenticated with (d_{MA},n_{MA}) to A. Remember from Table 1 that (d_{MA},n_{MA}) is stored in protected memory in the central computer.
2 A sends the initialization of the message (author, destinee, subject) to the computer authenticated with (d_A,n_A) and privacy protected with (e_C,n_C).
3. a. The computer sends (e_B,n_B) authenticated with (d_{MA},n_{MA}).
   b. If a signature is desired the computer sends a certificate of (e_A,n_A) and (e_B, n_B) containing among others (A, B, (e_A,n_A) (e_B,n_B), time T, subject) authenticated with (d_{MA},n_{MA}). Each user has the obligation to report to the central computer a loss of his secret key immediately. Hence this certificate states that (d_A,n_A) and (d_B,n_B) were not compromised at time T.
4. A obtains (e_B,n_B) from D_{MA} $((e_B,n_B))$ or from the certificate.

At this moment user A disposes of all the keys (e_C,n_C), (e_B,n_B) (s)he needs for sending securely his mail to B and communicating securely with the computer C.

Communication between user B and computer. (Part II, 3.)

1. The computer sends (e_C,n_C) authenticated with (d_{MB},n_{MB}) to B.
2. B sends the number of the message (s)he wants to read to the computer authenticated with (d_B,n_B) and privacy protected with (e_C,n_C).
3. a. Computer sends (e_A,n_A) authenticated with (d_{MB},n_{MB}).
   b. If a signature is desired the computer sends a certificate of (e_A,n_A) and (e_B, n_B) containing among others (A,B,(e_B,n_B), time T', subject). (e_A,n_A) and (e_B,n_B) are the keys that were used to generate $E_B(D_A(\text{Mail}))$ at instant T.

4. B obtains (e_A,n_A) from $D_{MB}((e_A,n_A))$ or from the certificate.
At this moment user B disposes of all the keys (e_C,n_C), (e_A,n_A) (s)he needs for reading the protected mail from A and for the secure communication with the computer C.

Let us now verify that this protocol meets the requirements of privacy, authenticity and if desired signature of Section 2. First of all the storage as well as the transmission of the mail can only be deciphered by B (end-to-end encryption). The transmission of the control data between computer and terminal is privacy protected (link encryption). The same reasoning can be given for the authenticity of the sender and the message. Observe that a message is always first authenticated and then encrypted (privacy protection). If the order was reversed, anybody could easily take off the authentication and abuse the resulting encrypted data. The signature with the mail is guaranteed by a certificate by the computer with (d_{MA}, n_{MA}) of the authenticity of the sender, the receiver and the keys used at time instant T. Users A and B are unable to alter the certificate, nor can they claim that their keys were lost, because they have the responsibility to report any loss of their keys. A can prove to a third party that B and only B has read the message, while B can prove to the same third party that A and only A has sent the message.

7. Conclusions.

The cryptographic protection of the BISTEL system is both necessary and feasible. The use of RSA and a hardware implementation is advocated. A proposal for the cryptographic scheme and the communication protocol is presented. It provides privacy protection, authentication and signature protection. Additional physical and computer security measures have to be taken. It appears that an acceptable trade-off between security, speed and ease of the use can be realised for this system.

REFERENCES

[1] ISO, "Public key cryptosystem and mode of use, Annual report 1984", Report ISO/TC 97/SC 20/WG 2 N, Dec. 1984.

[2] S. Weinstein, "Smart credit cards; the answer to cashless shopping", IEEE Spectrum, Vol. 21, n°2, pp.43-49, Febr. 1984.

[3] D. Davies and W. Price, "Engineering secure information systems," Proc. Eurocr.1985.

[4] D.E. Denning, "Cryptography and data security," Addison-Wesley, Reading, 1982

[5] D. Chaum, "Untracable electronic mail, return addresses, and digital pseudonyms", Comm. ACM, Vol. 24, pp. 84-88, Febr. 1981.

[6] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Comm. ACM, Vol. 21, pp. 294-299, April 1978.

[7] R. Merkle and M. Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inform. Theory, Vol. 24, pp. 525-530, Sept. 1978.

[8] Y. Desmedt, J. Vandewalle, and R. Govaerts, "A general public key cryptographic knapsack algorithm based on linear algebra", IEEE Proc ISIT, pp. 129-130, 1980.

[9] Davis J.A., Holdridge D.B., Simmons G.J., "Status Report on factoring", Sandia National Laboratories 1-33, 1984.

[10] S. Serpell, C. Brookson, B. Clark, "A prototype encryption system using public key", Proc. Crypto 84.