A PROTOTYPE ENCRYPTION SYSTEM USING PUBLIC KEY

Authors: S C Serpell, C B Brookson and B L Clark.

British Telecom Research Laboratories, Martlesham Heath, Ipswich,
Suffolk, IP5 7RE. United Kingdom.

BACKGROUND

The use of cryptography to produce a secure method of user authentication and to encipher traffic on data or digital links has been the aim of many of those defining theoretical schemes and techniques. This paper describes an experimental realisation of these aims in hardware, in order to provide a secure and authenticated communications channel.

The communications channel in this case could be part of almost any service, such as videotex, teletex, Local Area Networks, packet data systems, telex or conventional telephone data links.

SYSTEM REQUIREMENTS

The basic objective is that authorised users, and only authorised users, should be able to exchange meaningful data over a link. This statement actually conceals not one but two tasks; firstly, verifying the identities of the would-be link users to one another (authentication), and secondly, processing their data so as to make it unintelligible to eavesdroppers (encipherment). Both criteria have to be met by electronic means without any excessive operational constraints or overheads.

The traditional approach to the problem is for users' encryption equipments to deploy a conventional algorithm such as British Telecom's B-Crypt (1) or the American Data Encryption Standard DES (2). Users exchanging information have to be party to the same key. Successful interworking then gives implicit proof of the user identities, but the need for the secure distribution of pre-agreed secret keys represents a massive overhead which becomes impractical in large systems. It is impossible to set up a secure communications link without an exchange of keys prior to link set-up, and this represents a severe if not prohibitive drawback in services such as LANs or teletex.

Another approach is to use a public key algorithm such as PSA (3). This can reduce the key management overhead to an acceptable level and at the same time authenticate user identity, allowing the secure links to be established between strangers. But most implementations of public key so far have been relatively inefficient, generally limited to a speed of operation of a few tens of bits per second. Thus they do not support the encipherment rates needed in many applications (4).

However, by combining the conventional and public key methods in a system, it is possible to obtain the best of both worlds. Public key procedures are used at link set up time to prove user identities and establish a secret key which is used in the conventional encipherment of the data. This combination, in order to be applicable to most communications links and easy to use, needs to be defined carefully to overcome any inherent risks and to obtain an operationally secure system.

The experimental system described here was designed to meet the

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 3-9, 1985.

following requirements:

SECURITY To use public keys of up to 512 bits and any conventional algorithm desired. No long-term sensitive information to be within the equipment.

SPEED The equipment should allow automatic set up of a secure link within 3 seconds.

COMMUNICATONS LINK The units to be able to work on most types of links, at transmission speeds of up to 19 bytes, and be tolerant of link errors.

USER FRIENDLINESS The interface and requirements placed on the system user to be secure as possible.

USER IDENTITY The individual user to be identified by tokens, defining him and his access rights and privileges. The token needs to be unforgeable.

USERS It should be possible to use the equipment for inter-terminal communications as well as for services involving hosts and databases.

ENCIPHERING METHOD

Bilateral Communications

A participant A in an RSA-type public key system is provided with three entities; an exponent EA and a modulus MA which are public knowledge and comprise the 'public key', and a further exponent DA which is known to A alone and comprises the 'secret key'. A message P may be enciphered by raising P to the power EA (or DA) modulo MA to form ciphertext C. The original plaintext P is recovered by raising C to the power DA (or EA) modulo MA. Since DA is known only to A, this permits the following authentications:

- Only A can recover the message enciphered under EA, so a user who enciphers data under A's public key can be confident that only A may understand the message,
- Only A could originate a message enciphered under DA, so a user who deciphers a message using A's public key can be confident that only A could have sent the message.

A number of possible public key protocols are possible which take advantage of these properties (5,6). The set-up protocol adopted in the experimental system create a random number R between A and B, keeping R secure against eavesdropping, as follows:

1 An unenciphered link is established.
2 A invents a random number RA, and enciphers it under B's public key to form SA=EA exp (EB) [mod MB]. Similarly, B forms SB=RB exp (EA) [mod MA].
3 The users exchange SA, SB.
4 User A recovers RB-SB exp (DA) [mod MA], user B recovers RA=SA exp (DB) [mod MB].
5 Both users form R=RA xor RB.

The conventional key subsystem then derives a key K so that the users may communicate:

6 Both users truncate R in the same way to obtain a key K and a initilisation vector IV.

7 Both users load K to encrypt all following data using the conventional algorithm.

Unless both parties use the same K and commence secure communication with the same initialisation vector IV, the information exchange will fail, so authentication is complete in the first subsequent exchange of data.

Multiple Users

The simple protocol above can be modified to include multiple users, so that:

1 User A creates RA and forms SAB=RA exp (EB) [mod MB], SAC=RA exp (EC) [mod MC]..., while user B forms SBA, SBC...., C forms SCA, SCB.... etc.
2 Users then exchange SAB, SAC...., SBA, SBC...., SCA, SCB.... etc.
3 A then recovers RB=SBA exp (DA) [mod MA], RC=SCA exp (DA) [mod MA]...., B recovers RA, RC...., and C recovers RA, RB.... etc.

The conventional algorithm is then used for communication as before.

Certification of Keys and Provileges

In a secure system a user could obtain the public key and privileges of access of his desired partner by interrogating a reliable public key directory. This limits the flexibility and response time of the system as a secure call to the directory must be made before key exchange can take place.

A method of certifying keys is therefore introduced using a system public key known to an issuing authority. Extra steps are needed to establish the certificates which are then issued to the users:

a System public key values ES, MS and DS are established.
b ES, MS are widely distributed so that each user is assured of their values; DS is kept secret by the issuing authority.
c each user is issued with a certificate of his identity, public key, and any other useful information (eg. access rights, privileges, name etc) protected using the system secret key DS. Thus user A's certificate could be CA=ZA exp (DS) [mod MS] where ZA is the string formed by the concatenation of A:EA:MA:...., or alternatively a certificate could be formed by appending a banking- message type authenticator at the end of the string A:EA:MA.... based on DS (7).

The public key protocol now commences:
1 Users A, B establish unenciphered links.
1a Users A, B exchange certificates.
1b User A obtains B's public key EB, MB from ZB=CB exp (ES) [mod MS], while B similarly obtains A's public key.

This certificate system is also available for multiple users.

SYSTEM REALISATION

The experimental hardware is built to realise the protocols and enciphering processes already described. The ease of use of the hardware, together with the security it could afford, were the two maxims that were employed when designing the system. Figure 1 shows the system block diagram.

Equipment Interface

The system is housed in a stand-alone case, and uses V24 (RS232) serial interfaces to interconnect the user (terminal or system) to the communicatons link (modems, local area networks etc). Another replica unit is employed by the communicant at the other end of the communications link.

Token

The certified part of the key, ZA for user A (containing his privileges and public key), his secret key (DA) and A's copy of the system public key ES and MS are stored in this realisation on a DataKey (8), which is essentially a block of memory in the form of some Electrically Alterable Read Only Memory (EAROM) encased in plastic in the shape of a key. This key is certified, and the secret key is protected by being combined with an seven digit randomly selected number which is the Personal Identity Number (PIN) of the key holder. Other forms of token, such as magnetic cards, are equally suitable.

Use

The link is first established between the users in unencrypted mode, and the user requiring encipherment inserts his key into a receptacle. The key is then read, and the user is requested to enter his PIN by a message displayed on a liquid crystal panel. After his PIN has been entered, a message is sent to the distant user inviting him to insert his key and enter his PIN. The exchange protocol then takes place, and each user should then finish up with the same random number, which is used to derive the conventional enciphering key and initialisation vector.

Finally, a verification message is then passed between enciphering systems to establish that the exchange has been successful. Each user is able to inspect the certified names of his partners as they are displayed on his own enciphering equipment. The user equipment is now able to conduct an enciphered communications session.

The link is terminted by the withdrawal of a key, and the enciphering units are returned to plaintext mode.

HARDWARE DEVELOPED

User View

The hardware developed in the initial phase consists of the user interface presented to the operator and three other sub-systems described below which implement the protocols adopted. The subsystems are integrated into a small rack unit in this prototype realisation.

The user connects the enciphering unit between his terminal and the communications link using the serial ports. He is presented with four interfaces:

- A display to provide plain language instructions, status and fault conditions,
- An audio sounder to draw attention to operating conditions requiring attention,

- A numeric keyboard to input the PIN,
- A key receptacle for the DataKey.

Exponentiator

A hardware public key exponentiator capable of exponentiation of numbers up to 512 bits in length. This uses conventional TTL integrated circuits. The exponentiation of a 512 bit number takes about one second. The exponentiator connects to a controlling microprocessor by serial interfaces.

Stream Cipher

The conventional encryption is performed by equipment using B-Crypt in additive stream cypher mode or DES in cipher feedback mode. The control microprocessor loads the key and IV through a specially dedicated serial port, and the plaintext and ciphertext through a pair of serial ports.

Control Microprocessor

An Intel 8085 is used as the control microprocessor. Serial ports connect the control circuitry to the user and communications link, and the exponentiator and stream encryptor. Parallel ports control liquid crystal display and PIN input pad. The protocol is implemented in software.

RESULTS

Two experimental units have been produced, and these have been tested on various links such as on a local area network and a modem line connection. The hardware has operated reliably, and is capable of going into encrypted mode within 3 seconds of initiation. This interval of time has proved acceptable to users.

The experimental equipment produced has proved to be a valuable step towards the proof of the system viability. This concept forms the basis of a 'universal' encryption system, and further continuing evaulation and development is being carried out. The particular conventional and public key algorithms used in the initial stage are also subject to further scrutiny and evaluation. The overall system size is being reduced by adopting integration techniques on the various circuit elements.

ACKNOWLEDGEMENTS

Acknowledgement is made to the Director of Research of British Telecom for permission to publish this paper.

REFERENCES

1. B-Crypt Specification, BT Cryptographic Products, June 1984.
2. 'Data Encryption Standard', National Bureau of Standards, FIPS PUB 46, 1977.
3. Rivest, R L, Shamir, A, and Adleman, L, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm. ACM, 1978, 21, Pp 120-126.
4. Davies, D W, Price, W L, and Parkin, G I, "Evaluation of Public Key Cryptosystems", Information Privacy, 1980, 2, Pp 138-154.
5. Schanning, B P, "Applying Public Key Distribution to Local Area Networks", Computers and Security, 1982, 1, Pp 268-274.

6. Ingemarsson, I, "A Conference Key Distribution System", IEEE Trans, Inf. Theory, 1982, IT-28, Pp 714-720.
7. American National Standard X9.9, "Financial Institution Message Authentication".
8. 'DataKey' Handbook, DataCard International, drayton House, Chichester, Sussex, March 1983.

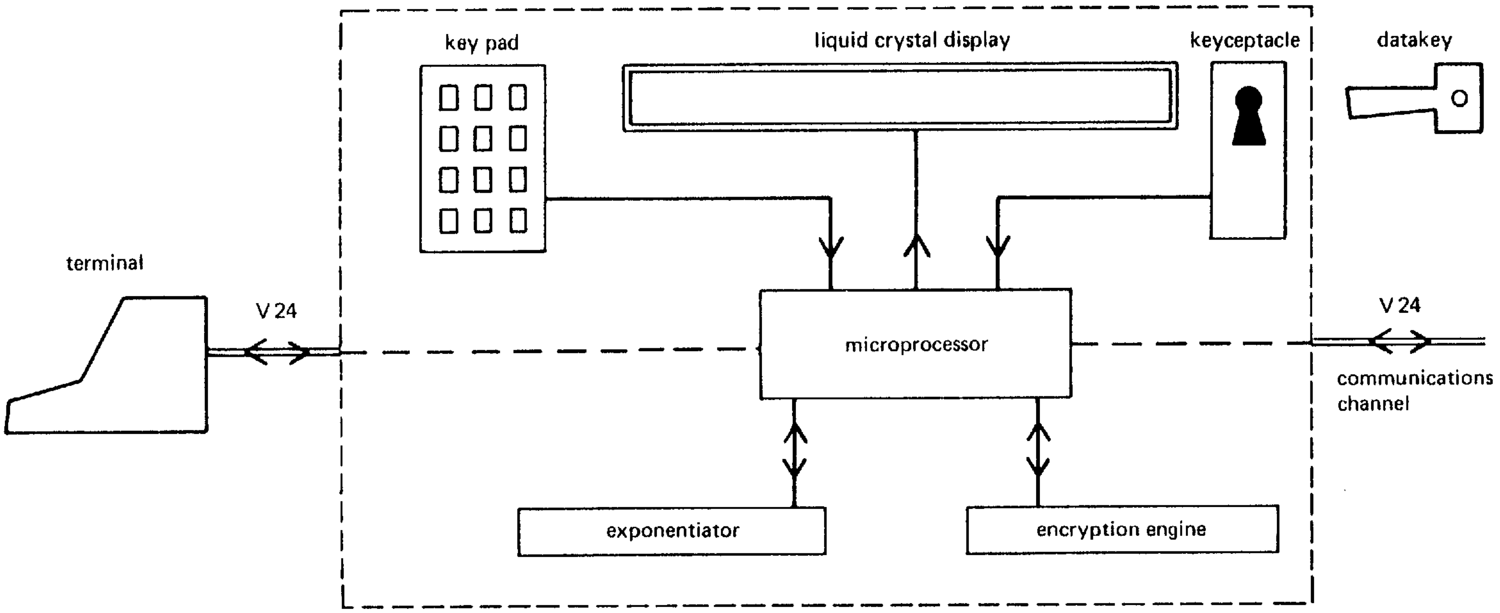

Figure 1 Public key cryptosystem realisation