HYBRID PROTOCOL USE FOR THE SECRET COMUNICATION IN NETWORK

Lecturer drd. Dascalescu Cristina

Abstract

A cryptographic system is effective when it keeps the balance between what is needed and what is possible. To create such a system is needed to build a well- made infrastructure that would contain the following components: symmetric cryptographic algorithms, asymmetric, dispersive functions, by a digital signature and an infrastructure of the required keys. In this sense, the article proposes a hybridize structure that can successfully ensure information security in a computers network, including the Internet network by using in a combined mode some cryptographic primitives, so the requirements referring to the vulnerability of a cryptographic system (confidentiality, authentication, integrity, non-repudiation) are fulfilled.

1. Protocols for symmetric cryptographic communications

Each transformation of coding, E_k, is defined by an coding algorithm, common to all the family transformations, and a key, K, which is distinct from a conversion to another. Similarly, each transformation of deciphering, D_k is defined by a deciphering algorithm D, and by the key K. For a given K, D_k is the inverse of E_k.

A confidential communication protocol between A and B be, is as follows:

(1) A and B are in agreement on a symmetric cryptosystem;

(2) A and B choose a key k (secret), the best being the key for single use (one time pad) for a communication;

(3) A sends to B message M encrypted with key k:

$$C = E_k (M)$$

(4) B decrypts the encrypted message received from A, using the same key k:

$$D_k(C)= D_k(E_k(M))=M$$

The data must be protected so that the unauthorized users can not reconstruct the clear text from an intercepted coded text. In this respect, it is necessary to ensure:

- *the unauthorized user cannot determine the systematic transformation decipher, Dk, from the intercepted coded text of C, although the text clearly known, M, is correspondent;*
- *the unauthorized user can not reconstruct the text clearly, M, from the coded text, C, without knowing the transformation of Dk*

From the above observations, it can conclude the following:

- the key must remain permanently secret in (at least) two distinct;
- the key k must be distributed in secret, which is a particular problem for large systems;
- require a secure channel of communication, at least for the transmission the key. This becomes difficult especially for systems that require frequent changes of the encryption / decryption keys.

• whether to use different keys for each pair of users, the number of keys grows rapidly with the number of users (n): $C_n^2 = \frac{n(n-1)}{2}$

2. Protocols for asymmetric cryptographic communication (public key)

In case of the cryptosystems with public keys, each user has a pair of transformations (keys):

E_x – the public transformation (key), publicly accessible;

D_x – the private transformation(key), kept secret.

The decipher key (secret) is derived from the coded key(public) by a hard reverse transformation (one-way). In public key systems, the protection and authentication are achieved through different transformations.

Consequently, to ensure the confidentiality, two partners A and B of a protocol that uses a public key cryptosystem will have (E_A, D_A) and (E_B, D_B), where E_A and E_B are public keys that can be taken from a public file similar to a phone book.

The protocol for communication between A and B has the following steps:

1) A and B are in agreement on a public key cryptosystem and select from a database the public keys of communication partners E_B, E_A respectively;

2) A encrypts the message or EA with the public key B : $E_B (M_A)= C_A$ and sends it to B.

3) B decrypts CA using its private key D_B and finds the MA: $D_B (C_A)= D_B(E_B(M_A))$

B encrypts the message or M_B with the public key of A: $E_A(M_B)=C_B$ —>A and sends it to A.

4) A decrypts CB using its private key and finds the M_B: $D_A(C_B)=D_A(E_A(M_B))$

Remarks:

• The key management is much easier in case of the public key cryptosystems, the number of key pairs being equal to the users, and to communicate it is not necessary to transmit secret keys between users, but only the public key of the correspondent which can be easily read from a database accessible to the public.

• The public key cryptosystems is vulnerable to attack with clear text at option (because the encryption key is public), but the attacks are difficult because E and D are irreversible functions with hatch (so the ignorance of the hatch makes almost impossible the deduction of M from E (M)).

• The speed of the public key algorithms (even the most performing) is several times lower than those with secret keys.

• The key size used is higher (1024-bit RSA compared to 64 or 128 bits for symmetric algorithms).

3. Protocols for digital signatures

The handwritten signature is evidence of the quality of the author of a document; it also attests that the signatory is agreeing with the content of the document.

Practical problems related to rapid transmission of documents to be certified as authentic by signature have led to the necessity of using electronic signatures.

The digital signature S [Menezes(1997)] is a sequence of bits obtained from processing the message (M) and a secret information, known only by the issuer. Any digital signature must be verified, the result of this function can only be "true" or "false".

Thus any signature protocol consists of a signature algorithm which is secret and a public verification algorithm.

The digital signature protocols may use the technique of symmetric encryption and also the public encryption, the last being more used.

The digital signatures based on public key are part of the so-called the Public Key Infrastructures (PKI). This infrastructure implies the existence of certification services providers (CSP) which provides large-scale implementation of SE.

PKI is a combination of hardware and software, policies and procedures that ensure the necessary basic security so that two users, who do not know or are in various points around the globe, can communicate safely. At the base of PKI are the digital certificates, a kind of electronic passports that maps the digital signature of the user to its public key. These informational objects are the bricks that form the basis of a PKI implementation and represent the way of digital identification of each subject participating in a relationship carried out by electronic means.

The hybrid cryptographic protocol

From the analysis of the cryptographic protocols described above, it can see that each has a number of complementary advantages. This underlines the need to use them in combination. That's way in practice, an efficient security protocol should occur in a hybrid form, the cryptographic primitives working together to effective achievement of the information security problems.

Thus to ensure the requirements needed to ensure the information security in computer networks and also on the Internet, the following aspects can be specified:

• ***The confidentiality and data integrity*** is achieved most effectively by the symmetric cryptographic algorithms;

• ***The data authentication and non-repudiation*** can be effectively achieved by using digital signatures using public cryptographic systems.

In order to define *the infrastructure of the hybrid cryptographic systems* we focus on the problem that occurs in exchange of the confidential information through a vulnerable network, as the Internet: avoiding the possibility that the information to be read by someone else than the recipient, the possibility to identify the information source, the possibility to detect any alteration of the information. The components needed to satisfy the above requirements are:

- the symmetric cryptographic algorithm for encryption of information flow;
- the infrastructure of the used keys (generation, organization, storage, distribution, maintenance keys);
- the session keys, the keys used by symmetric cryptographic algorithms;
- the terminal keys used to encrypt the session keys (using public key infrastructure - PKI);

- the asymmetric cryptographic algorithm (for the exchange of session keys);
- the digital signature to authenticate the data source;

In a hybrid communication protocol with public key systems may be used for the transmission of the secret session key used for the communication in systems with symmetric keys (figure.)

The communication protocol in a hybrid cryptosystem comprises the following steps:

• A and B agree on an cryptosystem public key and obtain the public keys of the partner E_B respectively E_A;

• A generates a random session key k that encrypts with E_B:

$$C_A = E_B(k) \text{ and sends it to B}$$

• B decrypts the C_A with its private key D_B and gets the session key

$$D_B(C_A)=D_B(E_B(k))=k$$

In the following communications, for privacy, A and B will use the same session key k and a symmetric cryptosystem.

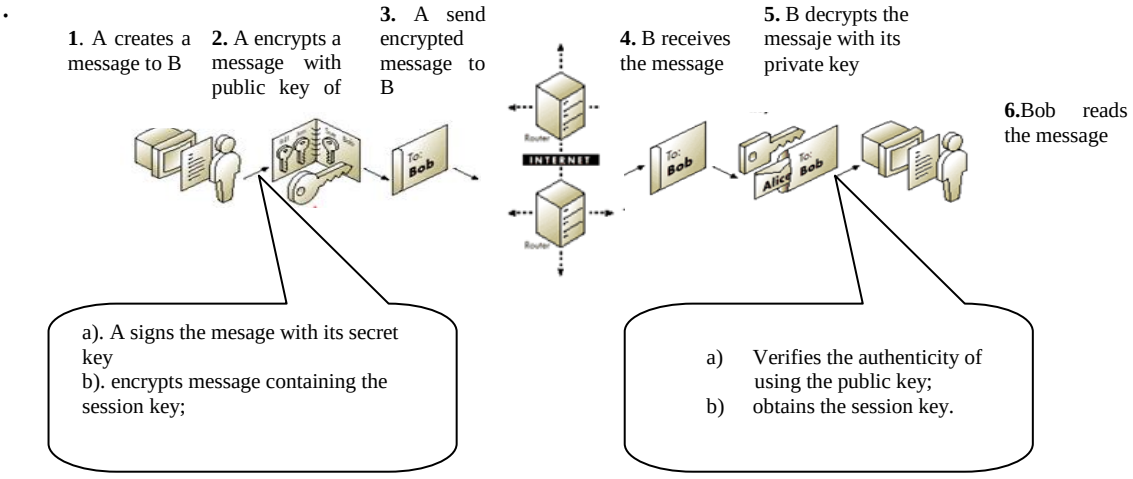

Fig.1 – Hybrid Protocol

This cryptographic system is proposed as a solution to information security issues, and can be done both for computer systems that have Internet connection with constant IP and for the ones which the IP is generated with the connection and also in distributed information systems.

The general architecture of the hybrid cryptographic system is composed of the following applications:

• server application with features for generating, signing and managing the licenses for each user;

• user applications that will communicate between themselves and with the server.

The server application provides the following services:

• generates the digital certificates for each user;

• keeps track of the users who have issued certificates;

• signs the certificates to be able to check the validity;

• will pursue what certificates were cancelled or expired.

The certificate that contains the secret key cryptographies on the basis of a phrase entered by the user and the public key certificate will be kept in a public database so that each user can have access to it.

The user application has the following options:

1. Connect to another user:
   - initilly will be verified the user's identity by key phrase;
   - the creation of a connection request to the desired application. The application contains the following data:
     - ♣ the subject of the application;
     - ♣ the public key certificate;
     - ♣ the encrypted session with the public key of the recipient;
     - ♣ the digital signature of the source .

2. Accepting a connection from another user:
   - ♣ verify the authenticity of the source;
   - ♣ extraction, decryption of the key session.

3. Encryption / decryption of data flow with a session key;
4. Loading from the application server of the digital certificate public key .

Conclusions

As awareness of the benefits brought by the use of encryption, of the disadvantages of lack of information protection and that the encryption technology has become more accessible, the encryption becomes an attractive method to protect data, whether the secret data transmitted over the network or usual data stored in the calculation system.

A cryptographic system is effective when it keeps the balance between what is needed and what is possible. To create such a system is needed to build a better infrastructure and that would contain the following components: symmetric cryptographic algorithms, asymmetric dispersive functions, digital signatures and an infrastructure of the required keys.

In this sense, the article proposes a hybridized structure that can successfully ensure information security in a network of computers, including Internet network by using in combination way of some cryptographic primitives so that the requirements reffering to the vulnerability of a cryptographic system (confidentiality, authentication, integrity, non-repudiation) are fulfilled.

Bibliography

[1] A. Menezes, P. Oorschot, S. Vanstome, *Handbook of Applied Cryptography* , Editorial CRC Press, 1996;

[2] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* , Second Edition, John Wiley & Sons Inc., 1996 ;

[3] A. Atanasiu , *Teoria codurilor corectoare de erori*, Bucharest University Editorial, 2001;

[4] D. Stinton, *Cryptography, Theory and Practice*, Editorial Chapman & Hall/CRC, 2002;

[5] Mohamed El – Gebaly, *Finit Field Multiplier Arhitecture for Cryptographic Applicatons*,

Editura Waterlo Canada 2006
[6] L. Song and K.K Parhi, *Optim primitive polynomials for low – area low – power Finit Field Semi-Systolic Multipliers*, Editorial NY 2003
[7] A. Salomaa, *Criptografie cu chei publice*, Military Editorial, Bucureşti ,1996;