SECURITY POLICY IMPLEMENTATION WITHIN DISTRIBUTED ORGANIZATIONS CONFIDENTIAL DATA TRANSFER

Željko Hutinski[1] and Dobrica Pavlinušić[2]

[1] Fakultet organizacije i informatike, HR-42000 Varaždin, Pavlinska 2, Hrvatska, e-mail: *zhutinsk@foi.hr*
[2] Fakultet organizacije i informatike, HR-42000 Varaždin, Pavlinska 2, Hrvatska, e-mail: *dpavlin@foi.hr*

ABSTRACT

Globalization of business systems has great influence on changes in organization and communication. Such events can also reflect on changes within structures of an information system. The most frequent form of organization of an information-communication system is distributed structure of a sub-system and its elements. Importance of the data contents defines the need of their protection which is particularly important in distributed systems, i.e. in systems that anticipate the network communication.

This paper describes the implementation of different security policies when the goal of distributed organization is to communicate securely. We are considering the threats that appear when an organization wants to communicate with its geographically distributed branches using the Internet as a medium.

Main goal is to demonstrate which methods should be employed in security policy to protect the data flow against potential threats.

Security conscious users have two methods of defense against these problems: controls and encryption. While controls provide the way to control the access to sensitive information, they do not help us much in an organization requiering to communicate securely over the Internet (or over any other public packet-based network) as a medium. The only logical choice is the encryption.

1. INTRODUCTION

We are the participants in great and continual changes that are happening in all fields of human activities. On business level, there were three big world transformations that induced modifications of business surrounding. The first one concerns the globalization of world economy. The second one concerns the transformation of industrial economy and society into economies that are based on extension of services, information and knowledge. The third transformation concerns the modification of business corporations. These modifications within business relations and surrounding are the cause of multiple changes inside business corporations and their management.

Globalization

Management and global market control
Competition on international market
Global working groups (team work) of fluctuating system and structure
Global supply services

Transformation of industrial economies

Economies based on know-how and information
Increase of productivity
New products and services
Know-how: central productive and strategic property
Timely planned competition
Shorter expiration period of products
Environment of frequent and deep transformation
Limited education of employed personnel

Transformation of business firm

Simplification of business systems and optimalization of business processes
Decentralization within organization expanding to planetary levels
Flexibility of organization and business processes
Independence of location
Low costs of transaction and coordination
Team work and work in cooperation

Successful operation of contemporary and future corporations greatly depend on their readiness for global functioning which implements functional and organizational changes. The globalization of world industrial economy extends and improves the value of information for the company thus creating new business opportunities. Modern information systems provide communication and analytic assistance required by corporations for managing business on the global level. In controlling global corporations, it is necessary to establish the communication with production, management, suppliers and distributors 24 hours a day in different national surroundings, servicing both local and international needs. It is a great professional challenge which requires powerful information systems.

Revolution of knowledge and information started at the beginning of the 20th century and gradually accelerated. By 1976, the number of employees in offices slowly exceeded the number of labourers in agricultural and manufacturing industry. Works in offices and servicing industry is primarily the work on distribution and creation of new information and know-how. In fact, the know-how and the work with information presently amount to 60% of the American GI and almost 55% of the labour power.

Since information and know-how are becoming the basic resource of the future, an information system has a task to provide the security for both the integrity of information contents and against its non-authorized utilization. Security measures for information systems are becoming one of the categories to be taken into consideration when creating an information system. Security measures are prone to frequent modifications dependent on the frequency of transformation or on the importance of data contents.

2. DISTRIBUTED ORGANIZATION AND SECURITY OF INFORMATION SYSTEMS

Ground for the development of information systems security is based on an estimated importance of the data contents and on potential threats to certain contents. The estimate importance of the data contents should be established in regard to legal regulations about preservation and protection of certain contents or in regard to requests of competent state authorities concerned by preservation of certain contents within the business system. An equal influence on the estimate of contents, i.e. of data contents importance, has also the business system to which the contents apply.

An estimate of the value concerning the threat to the data contents is based on an individual estimate of the source and the form of threats to certain data contents. Sources of threats can be devided in:

- nature as a source of threat through acts of elementary catastrophes
- a man with an attribution of intent
- a man with an attribution of unintentional act
- technical error as a source of threat

The form of threat within distributed organization and accompaning information system is shown in Figure 1.

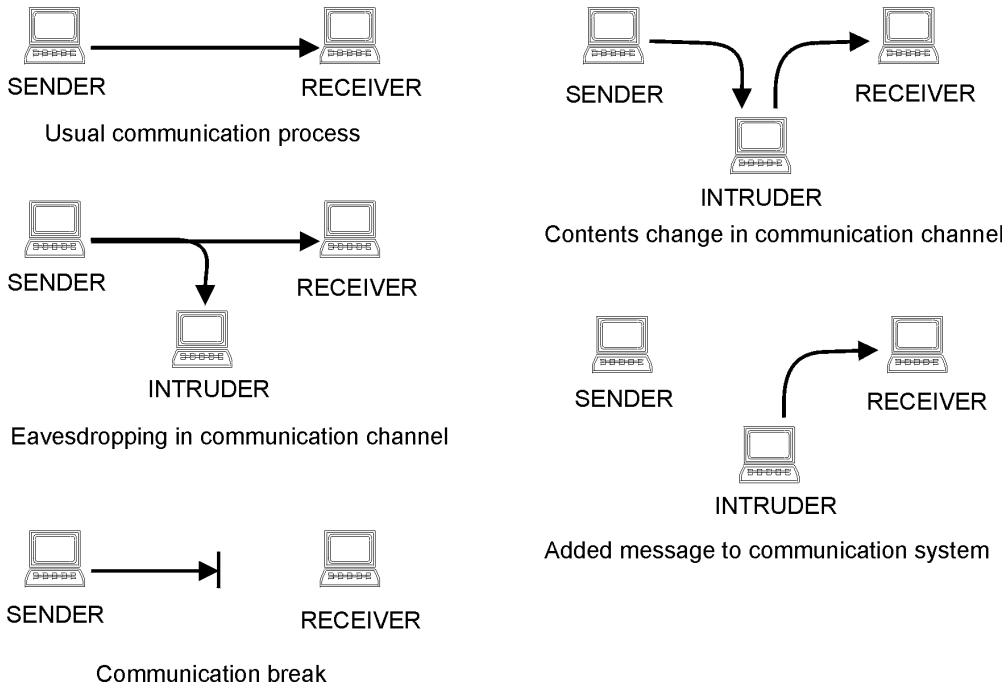

Figure 1: threats to flow of data within organization

Due to the fact that an information system should follow organizational procedures and provide for their support and management, all transformations within organizational structures are followed by technological and organizational changes within the information system. The biggest changes in information systems are caused by processes of globalization within national economies and multinational organizations. Such changes require

implementation of an information system the parts of which could be regionally dislocated from a few up to several thousand kilometers. Such a support of a business process includes a communicational channel. It can be separately constructed channel for one organizational structure or a rental of already existing communicational link. In both cases, there is a necessity to cover estimated levels of contents security within the communicational system. Regionally distributed organization in a business system can adopt various organizational solutions for information systems, but in all solutions it is necessary to maintain the network exchange of contents for which a problem of security should be resolved. The first step in resolving this problem is to determine the security policy for organizational and information system.

3. SECURITY POLICY

Security policy is created in regard to the established organizational structure of a business system, which structure bears influence on the information system, on estimated evaluation of importance of certain data contents, on estimated risk of threats to certain contents. According to these estimates, it is primarily important to define an approach to the security of the data contents. The management of a certain system can select a high risk of operation without any security measures. Another possibility of selection is a high level of security system provided that there is a justification for estimated importance of data contents and for the decision of an official authority to protect the contents for the security of which the said body is also interested. Consequently, the decision can be reached on any level between these two extremes.

By selecting the security policy we decide on the group of measures to be implemented, on the mode of application for such measures and on organizational instructions describing each separate measure within the frame of each separate working position. In selecting the security policy measures, it is important to focus on the basic principle of security implementation, meaning that expenses for security measures should not exceed the estimated damage that might occur within the system. Practical experience shows that the management, when deciding on an amount of investment into the business system security, most often goes up to 20% of the value of potential damage within the system.

Security measures can be implemented on following levels:

- program level by:
  - operational system level
  - in applicative program support
  - cryptoprotection
  - safe duplicating in other media
  - anti-virus protection

- technical equipment level by:
  - construction intervention
  - selection of material carriers for data contents
  - access prevention to the units of computer system
  - control and supervision of access within protected area
  - fire protection measures

- physical measures
  - against users of information system, both of data and information
  - against personnel working on system maintenance and development
  - through the guarding and watching service and supervision

- organizational measures by:
  - evaluation of data contents importance
  - estimation of threats to the contents
  - organizational instructions for each working position
  - checking list of security measures

Due to the fact that the communication is fundamental for observation and development of distributed organization and at the same time provides a possibility for transformation into a virtual organization, a particular attention should be paid to the security of data within the communicational system.

4. TRANSFER OF CONFIDENTIAL DATA

Networks have various problems with a transfer of confidential data. *Sharing* is the common goal of a network that is hard to connect with confidentiality of data which have to pass through it. *Complexity of system* is also a big problem. Large systems have tendency to be much more error-prone than simple ones. Fundamental theorem of firewalls described in Garfinkel and Spafford (1996) says that most host cannot meet our requirements. They run too many programs that are too large. Therefore, the only solution is to isolate them behind a firewall if you wish to run any programs at all. That is the reason why firewalls are introduced in front of local networks and services that are run inside them. *Unknown perimeter* of networks neither help in the data transfer now in *unknown path* of data packets inside network. All that leads to *many points of attack* that can be exploited to gain access to confidential data.

In other words, we try to protect *privacy* and *integrity* of data, to provide *authenticity* and *non-repudiation* so that we know which user is actually on the other side of connection. For that reason, we use encryption protocols to ensure our connections. That includes digital signatures to verify authenticity of peer side and conventional or public key cryptography to protect data that is transferred between peers.

Our goal is to connect organization using the TCP/IP protocol that is used on the Internet. For that purpose, we can use different protocols: the ssl for protection of general connection, the https to protect a well known http protocol used on the World Wide Web, the ssh (secure shell) or telnet with ssl support to provide encrypted interactive sessions or encryption on the link level using the IPsec with the IPv4 or the IPv6 alone, so that all applications using it will have an encrypted data flow. Unfortunately, the IPsec as described in Ferguson and Schneider (1999), is too complex to provide real security and the IPv6 is not yet deployed over the Internet.

4.1. Overview of encryption

There are three basic algorithms that are interesting for our purpose: symmetric (secret key) cryptography, asymmetric (public key) cryptography and hash functions.

Symmetric (secret key) cryptography shown in Figure 1 uses the same key for both the sender and the recipient, requiering to be kept secret. Main problem with this approach is that the key distribution is very complicated. Benefits include very fast operation because this method is mostly based on the bit shuffling which is dependent on the key.

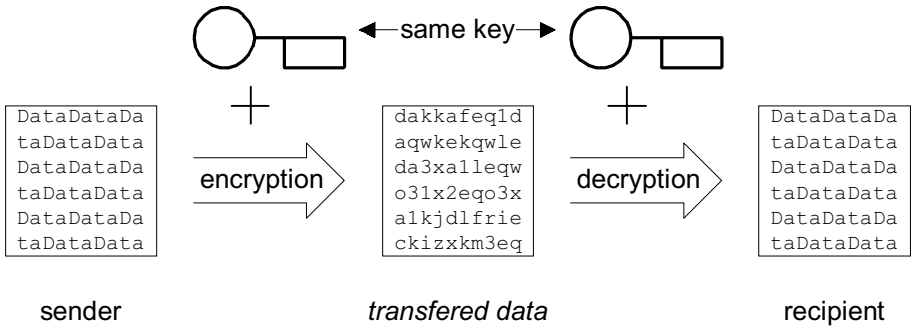

Figure 2: symmetric (secret key) cryptography

Asymmetric (public key) cryptography uses a pair of keys consisting of public and private key. The recipient of a message publishes his public key that is sufficient for the process of encryption, but it is not sufficient for decryption. It is enough for a public key to be authentic. It does not have to be secret. The sender uses that key to encrypt a message and the recipient uses his private key to decrypt a message. The process is shown in Figure 3.

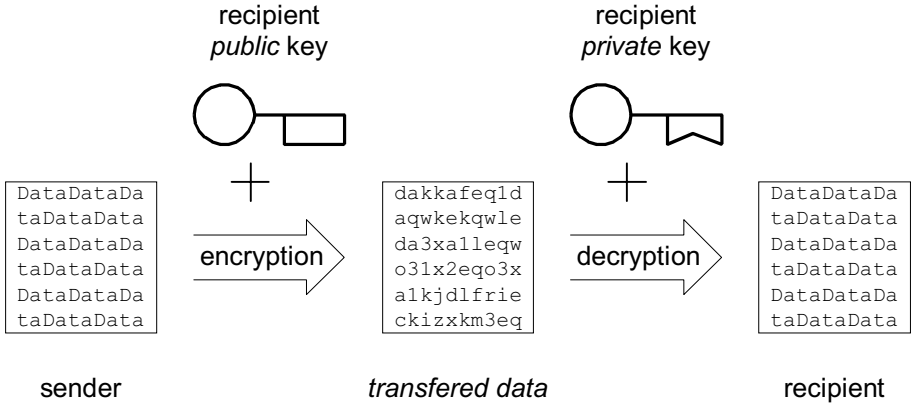

Figure 3: asymmetric (public key) cryptography

Hash functions are used for session keys and enveloping, for creation of digital signatures as well as for various kinds of certificates. They do not use any keys and they are generally one-way functions that cannot regenerate original input from the hash. They also compress down to 128 or 160 bits of data and are usually used to generate various fingerprints of the text data.

It is important to mention that the strength of ciphers is measured in the key length. However, the key length is not our concern. The key should also have sufficient entropy to protect data, but that is not our main topic here.

4.2. End-to-end encryption using the SSL

Most of the time we want to implement some kind of encryption that is standard. Presently, it is the SSL, *Secure Socket Layer*. SSL can be used to secure any connection-oriented communication. It provides an ability to authenticate the server, to protect confidentiality and integrity.

Organizations typically use the SSL for an e-commerce (to protect the input and sensitive data sent to the server), for the payment information such as credit card numbers and secure transactions over the web-based Internet and intranet services.

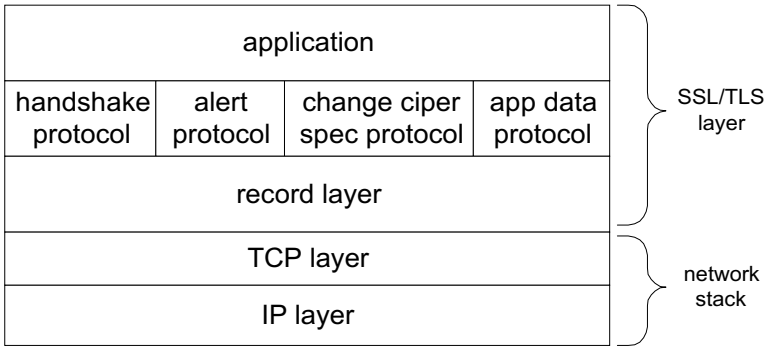

Figure 4: SSL protocol components

Figure 4 shows an overview of protocol architecture. Readers interested in more details are referred to Freier, Karlton and Kocher (1996).

4.3. Encryption at the link level: IPv6 or IPsec

The current Internet protocol in use (IPv4) has a number of security problems and lacks effective privacy and authentication mechanisms below the application layer. However, designers of the IPv6 (also known under the old name of IPng) have two integrated options that may be used singly or together to provide differing levels of security to different users.

The first mechanism, called the "IPv6 Authentication Header", is an extension header which provides authentication and integrity (without confidentiality) to IPv4 datagrams. Its placement at the internet layer can help in providing a host origin authentification to those upper layer protocols and services that currently lack meaningful protections.

The second security extension header provided with the IPv6 is the "IPv6 Encapsulating Security Header". This mechanism provides integrity and confidentiality to IPv6 datagrams.

Due to slow development of the IPv6, the IETF developed the IPsec which provides security at the link level for the IPv4 protocol.

4.4. Choosing the right method of connecting organization

Depending on the application type, organizations that have to communicate over an insecure media like the Internet, can choose one of the methods described above. However, until the Ipv6 is widely implemented, the only suitable solution will the SSL. With a minimal modification of the software or using proxy programs (as shown in Figure 5), organizations can easily transfer the data in a secure way.

However, there are some questions to be answered: does an organization have a security policy that accepts the transfer of confidential data unencrypted within the

organization (denoted on figure with a question mark) and does all data have to be encrypted during the transfer over the Internet. The latter question is particularly important: an e-mail that is received over the Internet does not have to be encrypted if sent over the Internet again - it was sent unencrypted once before. However, if all mail (confidential and non-confidential) is collected on the central mail hub and then transferred, all communication should be encrypted).

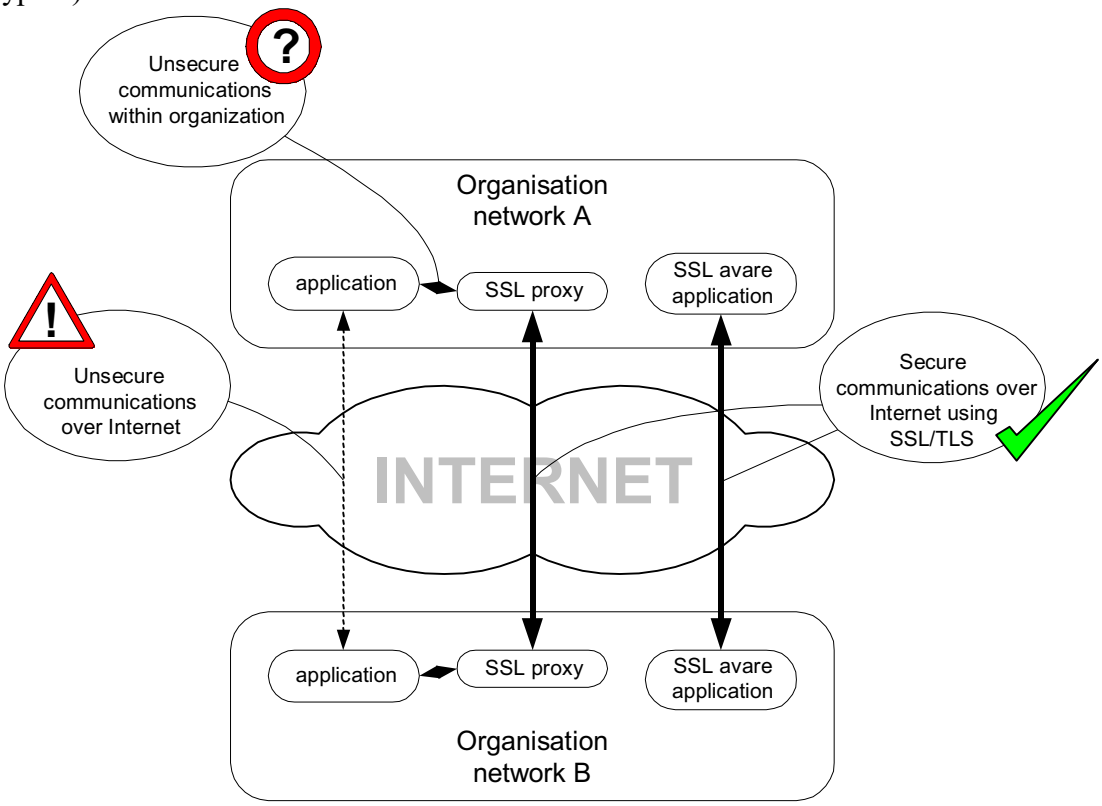

Figure 5: overview of different solutions with warnings

The SSL version 3.1 is in the process of standardization by the IETF under the name of *Transport Layer Security* (TLS). That should guarantee that it will be supported in future as well as vendor interoperability. Applications using the SSL/TLS can be deployed and used for many years without problems that often appear when the protocol is not open and freely available.

4.5. Problems which encryption can't solve

The encryption as described above solves most of the problems that distributed organizations have. However, it does not solve the problems such as hacking of the server, protecting data from being stolen, making your organization more security conscious or improving general security of an organization server. However, those problems are well known and they will not be discussed here any further. Interested readers are referred to Garfinkel and Spafford (1996).

5. CONCLUSION

In planning of information system in distributed organization, the basic principle is to define the security system for data contents. The first step in implementing the security system is to evaluate the importance of data contents and then to estimate the risk of threats to the contents. After that, it is particularly important to select the approaching policy in creating the security for information system. According to the selected policy and potential availability of financial means, the next step is to select measures through which the required level of data security in an information-communication system can be achieved.

Organizations in the present complexed environment can choose how to communicate over the Internet: insecurely, using property virtual private network (VPN) solutions or using the standard SSL protocol. The SSL protocol (known under the name of IETF and TSL) provides for the secure end-to-end connections, which include most of applications in use today. It is very important to select the encryption of the data during proper transfers because its overhead is not insignificant. If we believe in the internal network of organization, there is no need to encrypt the data within organization. So, solutions of the application level include applications that can recognize the utilization of the SSL/TSL or the special proxy software which both can transfer normal connections to the SSL/TSL. In future, the organization will be able to use the link-level encryption with the IPsec or IPv6, but for the time being, the SSL/TSL are the best solution to problems in hand.

6. REFERENCES

Cheswick W.S., Bellovin S.M. (1995), "Firewalls and Internet Security", Addison-Wesley, Massachusetts.

Ferguson N., Schneier B. (1999), “A Cryptographic Evaluation of IPsec”, *http://www.counterpane.com/*

Freier A.O., Karlton P., Kocher P.C. (1996), “The SSL Protocol Version 3.0”, Netscape Communications Corporation.

Garfinkel S., Spafford G. (1996), "Practical Unix and Internet Security", O'Reilly and Associates, Sebastopol.

Hinden R.M. (1995), “IP Next Generation Overview”, *http://playground.sun.com/pub/ipng/html/ipng-main.html*

Jankins G.H., (1979), “Information systems policies and procedures manual”, Prentice Hall, Inc., New Jersey.

Krause M., Tipon H.F., (1997), Information security management, Auerbach, Boston, London, New York, Washington.

Laudon K.C., Laudon J.P.: (1998), “Management information systems”, Prentice Hall, Inc., New Jersey.

Plfeeger, C.P. (1989), "Security in Computing", Prentice-Hall, New Jersey.