Network security – precondition of implementation of the e-commerce

Tedo Vrbanec, B. S.
Teacher training college Čakovec
Dr. Ante Starčevića 55, 40000 Čakovec, Croatia
e-mail: tedo.vrbanec@vus-ck.hr

Professor Željko Hutinski, Ph. D.
Faculty of organization and informatics
Pavlinska 2. 42000 Varaždin, Croatia
e-mail: zhutinsk@foi.hr

Abstract - E-commerce is becoming a precondition and a form of commerce in the modern settings of organized business systems. Therefore it is necessary to realize the level of security that can be achieved through implementation of various methods. One of the basic areas of security is safe communication between spatially remote subjects that work for the common goal. Along with the security, defined as a need to realize consistency of the communication and to keep the integrity of the message, there also exists the demand for protection from non-authorized use of the content in exchange. The authors provide a review of required methods and procedures, whose application for realization of the required level of network security represents necessary foundation for applicative superstructure, i.e. for realization of e-commerce. Although seemingly at the lowest level of system functioning, network security depends upon several factors. For some time already, a group of factors is being taken into consideration, for example: applied protocols, message encryption, firewalls, physical separation of services on physically removed servers, doubled hardware, manifold and alternative connections with Internet, etc. Authors provide approach to definition and application of measures of network security levels, which in turn have to envelop applicative layer; some of them envelop the choice and basic principles of operational system, or require definition, implementation, control, regular verification and modification of security policy.

I. INTRODUCTION

The problematic of network security of the computer systems required for e-commerce is a compound of many interconnected, often mutually conditioned factors. Their implementation in context of e-commerce is not an option, but an absolute necessity. Nevertheless, we will get only very occasionally an answer to the questions: *What should be done? What should be taken into special consideration if we want to achieve an optimal degree of computer network protection in systems where security is critical issue, for example e-commerce?* In the systems that support e-commerce, security and reliability are based upon electronic signature, authentication of subjects of commerce on Internet, data protection during its transfer through Internet and provision of network security of e-commerce subjects.

The protocols of authentication, designed as a result of the need for safe authentication, enable the introduction of the potential user to the system. The safety is reflecting in two aspects: the impossibility for non-authorized monitoring of authentication (because of modern systems of encryption), and the certainty of the system that the introduced user really is who he/she said, which needs to be proven in some way. The messages exchanged between the user and the system need to have properties of authenticity, integrity and uniqueness. These introductory remarks present nothing new for the informed reader. But, the question is, how to implement this? The answer to this question envelops more dimensions: physical, operative, protocolar and applicative security dimension.

Physical dimension is related to the computer and network equipment, its location, interconnection, technological level, capacity and reliability. Operative dimension or the dimension of operative system is related to analysis and/or assessment regarding the question which operational system would yield better results for given situation, considering security, reliability, simplicity, intuition, configurability and the price of implementation, use and maintenance. Protocolary dimension decides about meaning and need for use of standard or specifically made authentication and communication protocols, as well as the security standards of information systems. The applicative level is related to the technology of program system construction, with clearly defined user demands, i.e. demands of the customer.

We need to emphasize two things here. First, the sequence of consideration of the listed dimensions is reverse in practical situation. It starts with the goal and objectives of the system, its capacity and development plan, and then it decides about applicative level, which in turn creates conditions and limitations in the protocolary level, etc. As we descend toward the physical level, there are more and more conditions and limitations that have to be addressed and fulfilled. The other emphasis is related to a specific view to all four dimensions – network view to the security of such system (fig.1), which permeates it at all levels and which is the focus of this paper.

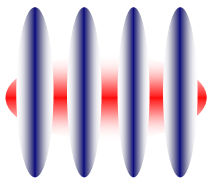


Fig. 1 Interconnection of the network view to the security and four "classical" dimensions of security

Apart from the choices and implementation of the listed "classical" security dimensions, we present the model of efficient implementation of network security. With the

increase of needed level of security, this model has to be implemented more strictly. So, how does this model look, how to introduce the most efficient level of network security that exists today?

II. NETWORK SECURITY MODEL

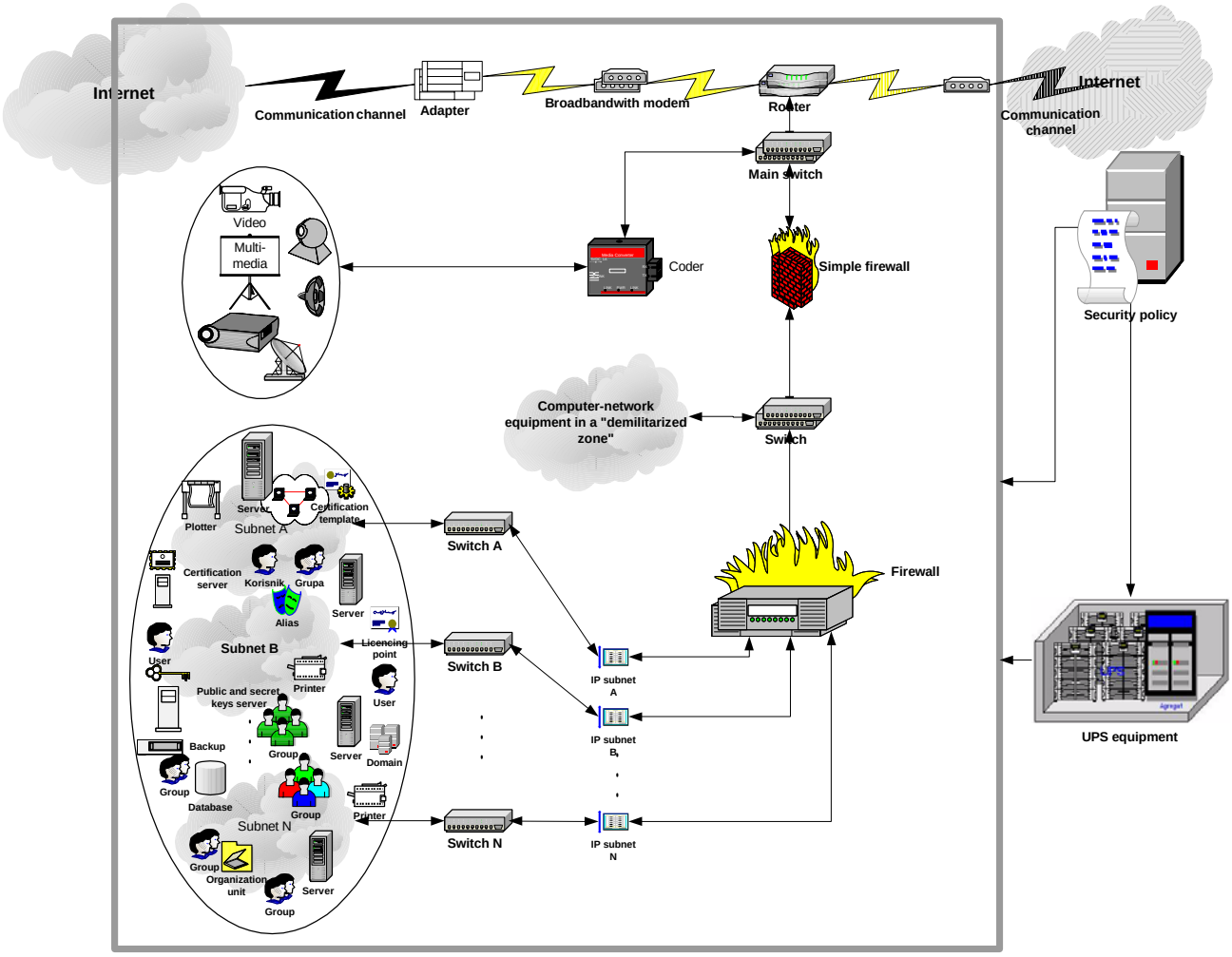


Fig. 2 Physical implementation of network-computer system – model of network security

Let us think of a computer network, which is, together with the system and applicative program support, backbone of an organization which realizes a part of its work/commerce through Internet, and which does not have wireless components, which is a subject broader than this paper. The physical entrance to the system is the permanent connection to Internet, with projected channel capacity. Besides this connection, at least one connection toward ISP (Internet Service Provider) is being introduced into the system at request; this connection is automatically established if the main connection is broken from some reason. The second connection usually has lower channel capacity; it costs more per unit of transferred data, and is realized through other ISP, and usually through other physical connections.

The systems that support e-commerce need to have rather large amount of equipment. Figure 2 shows locations that need to have at least double equipment. Namely, in the context of e-commerce, Internet is not a place where there exist words like “pause” or “rest” or “please, wait a moment”, which we can hear in telephone-based commerce and/or support systems.

Router works at the level of transmissional layer of reference model ISO/OSI. It

- Accepts data from the layer of conversation, deconstructs the data to smaller parts if needed, and forwards it to the network level,
- Realizes connection of the users/applications that communicate between them (connection from one end to another),
- Ensures transparent data transmission,
- Directs the traffic and optimizes communication services of lower layers (multiplexes or concentrates the traffic).

The example of the protocols used for the transmission layer is TPC (Transmission Control Protocol).

U The router receives all packages that reach LAN, and redirects them to the segments of network on their way to the destination. Because of its settings, it represents one of ideal locations for network and network security management, which mainly includes filtration of the packets and communication ports. Still, the routers usually do not have too many regulations, checks and limitations placed on them, because this reduces its transferability, especially in

larger or heavily used networks. The routers are usually part of the equipment of ISPs, and are consequently under their domain, so the organizations usually do not have authorization to meddle with their basic settings. In smaller, C-class networks (and their still smaller sub networks) with the maximum number of 254 IP addresses (0 is used for the identification of the network itself, while 255 is the broadcasting address), this transferability reduction is neglectable, so the functions like the firewall and the bridge can be implemented on the router.

Correctly projected and implemented network-computer system at the router does not set any regulations, conditions and filters. It is recommendable to have a "simple" or ad hoc, easy-to-maintain and replaceable firewall on the double hardware behind the router. Its only role is to prevent the communication for all the ports that the computer worms and viruses use for their advance, and it could also be used for the prohibition of the ports that use so-called peer-to-peer applications (*Kazaa*, *WinMX*, *e-donkey2000* etc), through which the users exchange often illegally acquired contents. In such way, it reduces the pressure from Internet "noise" on the "real" firewall, which stands behind. The existing simple solutions enable almost complete protection of such systems. Usually, it is not possible to access them from remote computer; it is even possible to define by the security policy, and to implement in practice, the prohibition of access from the local network. Finally, it is possible not to install services for remote access. Operational systems of such simple firewalls can be implemented even with the modest hardware, which do not need to have above average reliability, because there can be more of them in the reserve, instead of writing them off like old, useless but functional computers. The modest hardware is driven by powerful operational system of unixoid type, loaded from CD or floppy disk, to disable the possibility to write on them. As a rule, they do not have graphical interface, because they do not need it to fulfill their function. Maybe the best product of this kind that exists today is *Suse Firewall Live on CD*, and there are also many free, tested and efficient solutions, like *Coyote* or *Fli4l*. The adjustment is being done in extremely short period by the change in textual configurative database and by restarting the service or the system.

The area between two firewalls, often called demilitarized zone, could be used for the placement of such computer-communication equipment that will not make additional burden for the firewall by the large number of its packages, and that does not need to be specially protected, because it generates, for example, audio-visual data. The example for this is hardware encryptor used for transmission of the image and sound for the needs of teleconferences. Behind the simple firewall, "real" firewall is placed, which is implemented on the server hardware designed for permanent, continual work, along with RAID (Redundant Arrays of Inexpensive/Independent Disks), field of hard discs, with the possibility to change non-functional disc without turning off the computer (hot-swap). Because of its pivotal position in the system, firewall, like most of other equipment in such type of system where it is the critical factor of commerce, certainly requires the existence of doubled hardware and the devices that provide automatic and autonomous constant supply of electric energy to the pivotal computer and network equipment.

Firewall directs the packages to the sub networks, which can be created from any of the following reasons:

- Protection of local network (NAT).
- Easier system administration.
- Physical and logical placement of the computer equipment.
- Equal distribution of burden for separate network segments.

Wise implementation of the firewall requires one or two entrance and more exit channels through network adapters; in this way, the rules can be implemented easier into separate network segments. Sub networks are connected to switches, through which the physical connection is being realized. The switches, whose number depends upon physical allocation of the computer and network equipment and upon (average and maximum) burdening of the communication channel, are connected with the separate network segments that could be additionally protected by the similar principle. The technique that is being used in this is called NAT (Network Address Translation). NAT is, in fact, an Internet standard. It enables the use of one group of IP addresses in a part of local network or in its whole; it also enables use of other group of IP addresses for the traffic with the Internet. More precisely, most often it is one IP address for the protected part of LAN, on the protected gateway, in which the required translation of the addresses is being conducted. There are three main tasks of NAT:

- By introducing NAT to a machine, it becomes a kind of firewall, hiding the internal IP addresses,
- It enables the organization to use large number of internal IP addresses, according to need,
- Since IP addresses are used only locally, there is no possibility of conflict with the addresses used by other organizations,
- It enables the organization to use more connections with the providers of the access to the Internet (ISPs).

III. PROTOCOLS OF AUTHENTICATION

RADIUS

The safest existing method of authentication of the remote user to the computer system is the RADIUS (Remote Access Dialup User Service) protocol. This protocol is the connection that transmits authentication, authorization and configuration data between the access control servers and RADIUS servers.

The server for control of network access, Network Access Server (NAS), known also as Remote Access Server (RAS), (fig. 3), is the access point to the network for users accessing it through remote access protocol (telnet, ftp, PPP…).

In the case presented on the fig. 3, safety mechanisms for prevention of unauthorized access to LAN are provided by the access protocols that are used today. However, it is known that there often are security omissions in the program code of the programs that use them.

On the other hand, by using RADIUS protocol, we use unique source of information for authentication, for example, the same that are being used for Active Directory,

regardless to the access protocol. For consistent application of the rule one service – one server, we also need RADIUS server. Additional possibility of use of the RADIUS server and protocol is monitoring the frequency and time of connection of the remote users, together with summary and statistical data (accounting).

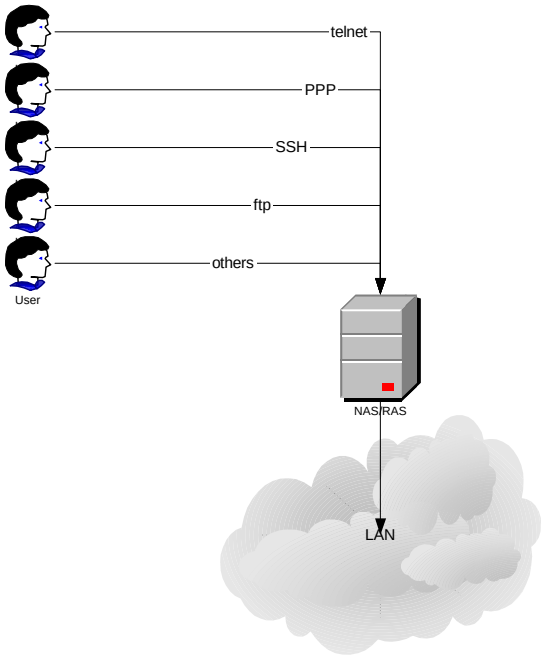


Fig. 3 Scheme of user's access to the network through NAS/RAS server

RADIUS architecture (fig. 4) regards every entity that requires access to the network resources as a user. LDAP (*Lightweight Directory Access Protocol*) directory/database identifies every user by unique identification number.

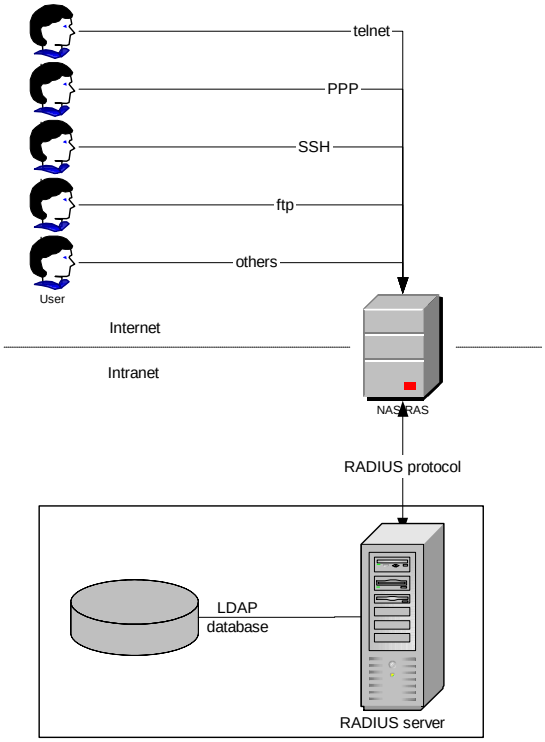


Fig. 4 Scheme of RADIUS architecture of the user's access to the network

NAS (RAS) is also leaning onto the RADIUS server, i.e. it has the role of RADIUS user. As such, it sends questions to the RADIUS server, demanding authentication status, user profile and authorization. RADIUS server authenticates NAS, and after that, it checks the identity of the remote user and authorization in the database. Therefore, it returns the user status (connection accepted or declined) and configuration data to NAS. If RADIUS server cannot authenticate NAS, the demand will be ignored. In this case, RADIUS server does not response, not even with refusal of the connection demand.

PAM (Pluggable Authentication Modules) are being used for plugging authentication mechanisms like Kerberos, RSA or smart cards over RADIUS. These modules are usually parts of operational systems, or easily accessible packages/parts.

LDAP

Connecting to Internet or Intranet, we all unconsciously use LDAP directories or similar structures (Active Directory). LDAP is expandable standard of network protocol, independent from the platform on which it is being used. It supports heterogeneity of hardware, applications and networks.

LDAP directory is like database: it can be used to store data; this data can be accessed again later. Nevertheless, it is specialized item and has the following features:

- It is designed primarily for reading, and not for writing,
- It gives static view on the data,
- It is easy to expand the data, without need for some form of transaction.

LDAP standard determines:

- Network protocol for access to the data in directory,
- Model of data that determines the form and characteristics of information,
- Way in which the data is accessed and organized,
- Model of distributed operations, i.e. it determines how the data can be distributed and used for reference.

Both the protocol and the data model are expandable: In the directory we can place all that we need (texts, photos, URL addresses, pointers (for anything), binary data, certificates for public keys etc.) LDAP directories support all types of data. Still, some implementations set limitations to the amount of data (of specific type) that could be stored. LDAP protocol directly supports strong mechanisms of authentication, privacy and integrity.

Division of the services

When we talk about the network security model, it is necessary to emphasize the principle of division of the individual services to physically separated computers. There are at least two reasons for this:

1. If one server stops with functioning, this also stops all services depending upon it.
2. The successful attack on the server from outside and the cessation of its functioning results in knowledge about the attack, while the damage is limited. Namely, the attacker needs some time to break through to the next server. Before this happens, actions can be taken to disable him/her and to gather evidence to find him/her and press charges against him/her. Frequent making of the data and system backup can help to further reduce the damage.

Authenticity of the e-commerce subjects

When the user accesses the system, he/she must be sure that he/she really is communicating with the real server. To enable the user to be sure, server must have certificate that can be issued, under certain conditions and with certain compensation, by some of the internationally accepted authorities on Internet:

- *VeriSign*
- *Thawte*
- *CAcert*

SET *(Secure Electronic Transactions)*

SET is an open protocol that enables Internet transactions with the use of credit cards. It was created as a joint venture of MasterCard and Visa, with the help of Netscape, Microsoft, GTE, IBM, RSA, SAIC, Terisa and Verisign. It was designed in such way to minimize the possibility for mistakes, and the possibility for interception and decryption of confidential information. SET requires adequate program at both sides, i.e. both the user and server [1].

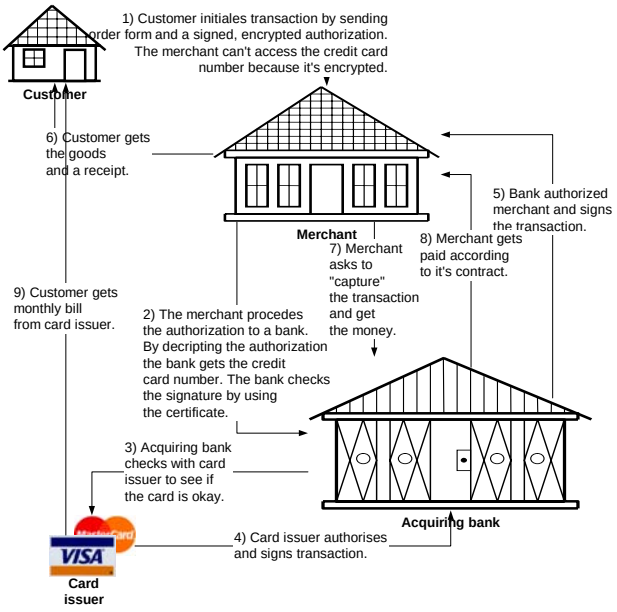
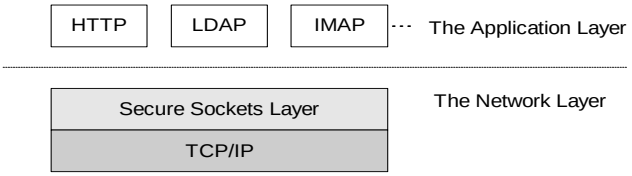


Fig. 5 Description of SET [10]

SSL (*Secure Sockets Layer*)

TCP/IP protocol manages data transmission and direction through Internet. Other protocols, like HTTP (Hyper Text Transport Protocol), LDAP or IMAP (Internet Messaging Access Protocol) function above TCP/IP in such way that all of them use TCP/IP as a support for typical tasks like showing web sites or email transmission. SSL protocol functions above TCP/IP, but under higher-level protocols, like HTTP or IMAP; it uses TCP/IP in their name (fig.6). SSL ensures that server (with support for SSL) is authenticated to the client and vice versa, and enables for both sides to establish encrypted communication.



Sl. Fig. 6 Location and role of SSL

Features of SSL, with the use of TCP/IP protocol, solve the most important problems of communication via Internet, and these are the following:

- Authentication of SSL server enables the user to be assured in the true identity of the server. Client with the program support for SSL can use standard techniques of public key cryptography to check the identity of the server, its certificate (issued by trusted third party – CA – Certificate Authority) on which the server calls upon, and the public key. This is especially important for sending credit card number via Internet, when the client wants to be sure whether the server to which he/she pays, or through which he/she pays, really is who it said it was.
- Authentication of SSL client enables the server to confirm the user identity. The same technique is used here as for server authentication. Program support at the server side that supports SSL checks client's certificate and the public key. This can be especially important if the server belongs to a bank and if it is required of the server to pass confidential financial data to the user. In that case, it must check the user's identity.

Encrypted SSL connection requires encryption of all communication between the client and the server: the application that sends the message encrypts it, while the application that receives the message decrypts it. In such way, high level of trust is achieved, and trust has the utmost importance for both sides during any transaction. Additionally, all encrypted SSL connections have the possibility to determine automatically whether the data has been changed during the transmission.

SSL protocol consists of two (sub) protocols: SSL record protocol and SSL handshake protocol.

SSL record protocol determines the way in which the data is transmitted. SSL handshake protocol uses the SSL record protocol for exchange of message sequence between the server and the client, who support the SSL while establishing SSL connection for the first time. This message sequence has the following purpose:

- Authentication of the server to the client.
- It enables the client and the server to choose cryptographic algorithm and to use keys, which depends upon support of both sides.
- Optionally, client can be authenticated to the server.
- Use of encryption technique by public key as to generate mutual secret key (by quicker, symmetrical encryption system, fig. 7).
- Establishment of encrypted SSL connection.

In the systems where any attention is being paid to the questions of security, SSL has pushed away telnet, a protocol of equal functionality, but without built-in safety mechanisms.

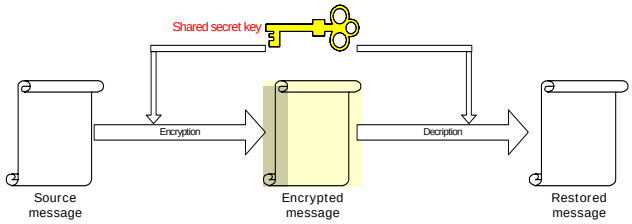


Fig. 7 Symmetrical system of encryption [1]

IV. NETWORK SECURITY SOFTWARE

There is no doubt that the authors advocate tested and maximally safe solutions vs. quick and not so safe ones. Unfortunately, it is not possible to argue that the commercial solutions are at the same time the best ones, under excuse that, in such way, the organizations have ensured support. To be more precise, we deem that there is no justification in spending tens or hundreds of thousands of Euros for operational systems and applicative support, and then again at least the same amount for their implementation and internal and external maintenance. We are witnesses of constant threats from computer viruses, worms and exploits trying to take advantage from the security omissions that exist and are frequently revealed in the existing, worldwide popular operational systems. This does not mean that such systems cannot be protected in satisfying level. Nevertheless, such protection is usually more expensive, and it cannot reach the maximal level of security and protection of open-source solutions, where the best specialists are doing the maintenance for specific areas free of charge, in the moment when the security omission in program code or any other mistake/need is discovered. In contrast to this practice, sometimes it takes several months for "big" vendors of program support, including the operational systems, to design patches that will repair certain security omissions in their program code, which were long ago discovered and published.

Proxy system

It would be a great omission if a proxy system is not started along with the implementation of firewall, regarding the huge benefits it provides to the users of local network. In this, it is recommendable to design transparent proxy system, in which the user does not need to make special adjustments of his computer to access Internet through proxy system, but it also should not cache local addresses. True, in the context of network security it is not necessary to organize proxy, but it is almost by-the-way task during implementation of the firewall. We should add to this that the firewall presents ideal settings for the proxy system. The most powerful proxy program systems for two most widely used platforms are *Squid* of unixoid operational systems and *ISA* for MS Windows servers.

Antivirus protection

A centralized and automatized antivirus protection must be an integral part of computer and information system protection. Here we recommend a choice of some of commercial solutions. The competition among them today is very strong, and the differences between several best solutions are minimal. Still, we should mention the following facts and make a warning:

1. Computers (work stations) and servers of unixoid type are usually capable of hosting unlimited number of antivirus tools, while in the case of computers with MS Windows, exclusive right is usually given just to one tool per computer.
2. All antivirus tools will soon be of doubtful usefulness if regular restoration is not conducted (maximal interval between restorations should not be longer than 6 hours, and if possible, it should be 1 hour).

We know about cases when unprotected browsing on Internet that lasted just 30 minutes, and had a purpose of downloading newest definitions of viruses for antivirus tools, was enough for computers to be infected with malign additions like viruses, trojans and worms. Additionally, we should mention that the worm Nachi infected systems of two American banks in August 2003 [13].

Newly installed machines have to be protected by regularly restored antivirus protection, with starting installation on non-infected computer in a protected area of computer laboratories.

PGP (*Pretty Good Privacy*)

PGP is a program package developed by Phil Zimmerman in 1991. It provides cryptographic routines for e-mail and data storage. With time it became a de-facto standard for encryption of e-mail. Zimmerman took the existing cryptographic systems and protocols and developed the program that could be used by various platforms. PGP enables message encryption, digital signature, data compression and e-mail compatibility. In its work, PGP uses the following algorithms:

- *ElGamal* and *RSA* for key exchange.
- *Triple DES*, *IDEA* and *CAST5* for message encryption.
- For digital signatures, it uses DSA or RSA for signature and SHA-1 or MD5 for calculation of the compression.
- For compression and data storage it uses shareware program *ZIP*.
- E-mail compatibility is achieved through use of conversion *Radix-64*.

The indicator of PGPs power is the fact that its author was three years under investigation by American authorities after it was released. The reason for this lies in the fact that even the American intelligence agencies were not able to break through PGP. Paranoia was so widespread that even the people who have written about PGP have been exposed to official informative interviews.

User application to the remote computer

Various publicly accessible programs and tools enable hostile users to crash into insufficiently protected networks and computer systems even without great expertise. Therefore it is important to motivate users to use safe access methods. It is necessary to discourage the use of unsafe methods, i.e. those that can be traced by the reverse engineering methods and reveal, if nothing else, user names and passwords. A high quality program for safe access to the remote computer, SSH (*Secure Shell*) that uses SSH1 and SSH2 protocols, gained big popularity. It includes authentication, enables safe work and communication with remote computer. There are many other solutions of no lesser quality for various platforms, some examples being *PuTTy*, *TTSSH*, *OpenSSH*…

V. OTHER MEASURES OF PROTECTION

Restoration of operational and program systems

"Non-patched" computers present a serious threat to the network security, especially in the light of new appearances of "intelligent" viruses and worms, where the antivirus protection, although it works flawlessly, is not totally efficient if the operational system is not completely patched. There is another worrying new trend emerging – use of social engineering in construction and spreading of

the newest computer viruses and worms. The choice of more robust operational systems, which may be free of charge, but also harder to use and maintain, is a promising course of action, along with the increased user education. This does not eliminate the possibility for situations of accident. The alternative is constant anxiety, convulsive and dynamical monitoring of revelation of the security omissions, urgent blockade of entrance to the potential outer threats, or opening just the checked communication ports on the firewall. In any case, the use of official patches that could contain the problem is a necessity that the system administrators should not overlook or neglect. The last drastic example of such neglect happened in summer of 2003, when the vulnerability of non-patched SQL servers was exploited. The whole Internet traffic was considerably impeded. In that occasion, CARNet warned that it would exclude some of its elements from the system, until the infected computers are not cleaned. Since then, some communication ports have been banned from traffic, and this was implemented on CARNets routers.

Server protection

Beside the presented methods of regular implementation of the security patches, regular antivirus protection and division of the services to separate servers, it is very important that the unknown user – a potential buyer of goods and services accessing the system, but also a potential attacker – has only the limited specter of necessary rights which he/she can use. These are the rights that enable him/her to realize the operations in the system – most often through web interface – that provide him/her with the limitless overview of goods and/or services, of storage or date of delivery, of price and methods of on-line shopping. Some of possibilities of such protection are redirection of addresses and ports, and/or opening limited rights account on database server and application server.

Physical, organizational and technical measures of protection of key hardware infrastructure

Not wishing to delve deeper into the complex problematic of data content protection, shown in the figure 8, we should emphasize that, on the level of network security, the consideration needs to be made about physical protection of the space and equipment upon which the functioning of the e-commerce system depends. This protection includes:

- Locking the protected equipment.
- Installing protection from burglary and alarm system in the case of burglary.
- Designing and implementation of fire protection, depending upon the circumstances.
- At the delicate places, a filter that reduces visibility within 15º should be installed in front of the monitor.
- Installation of special hardware elements that will reduce the possibility of non-authorized access to the system.
- Installation of the hardware key.
- Use of the passwords (inevitable).
- According to need and possibilities, use of biometric analysis as a precondition for entrance into the protected area or system, for example
  - Identification card
  - Fingerprints
  - Geometry of hand, head
  - Iris in the eye
  - Voice identification
- Prohibition of access into the protected area

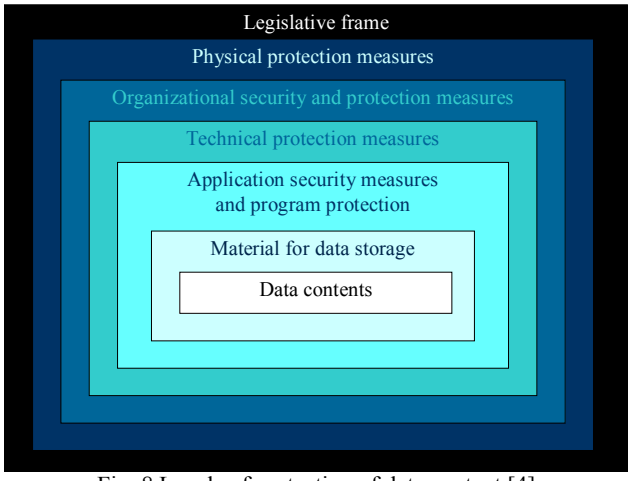


Fig. 8 Levels of protection of data content [4]

Other ways of network protection

- MAC filtering (establishing the access rights related directly to MAC (*Media Access Control*) addresses of network adapters).
- *.htaccess* files (used for establishment of the access rights to the web server for certain users).
- Use of statical IP addresses in LAN.
- Prohibition of use of DHCP.
- Removal of all shared maps, except the necessary ones, which should be hidden with obligatory authentication.
- Use of program packages – Network intrusion detectors.

Required measures that are not within the area of network security

- Database replication of SQL servers.
- Regular backup of important data and systems (imaging).
- Storage of copies in physically removed locations.
- Management of the server load during clustering (low-balancing).
- Defined, implemented, controlled and regularly updated security policy with precisely elaborated response procedures for all possible incidents, which also includes regular security assessment from independent institutions, and reporting the incidents to CERT.

VI. PROTECTION OF THE SHARED CONTENT FROM NON-AUTHORIZED USE

Electronic signature

Notions of electronic and digital signature are often mistaken one for another. Digital signature relates to the specific technology of documents and persons authentication process with the use of public key cryptography. Electronic signature relates to any electronic mark, process or inscription that fulfills legal regulations of the electronic signature problematics. Therefore, digital signature is just one type

of electronic signature. Here are examples of other types of electronic signatures:

- Digitalized image of hand-written signature.
- Address inscriptions, for example e-mail chapter.
- Biometric analysis of fingerprint or eye iris.

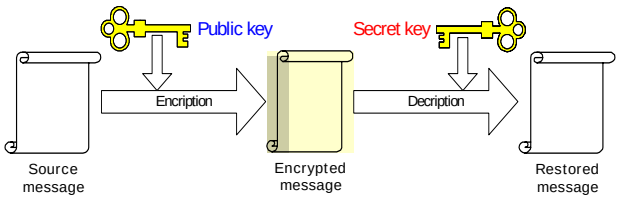


Fig. 9 Asymmetric encryption system [1]

So, the technology of electronic signature is based upon public key cryptography (fig. 9), and it protects the inalterability of the data exchanged through Internet. Electronic signature has the purpose of user identification and electronic signing of the documents that the clients/users exchange with the subject that organizes e-commerce.

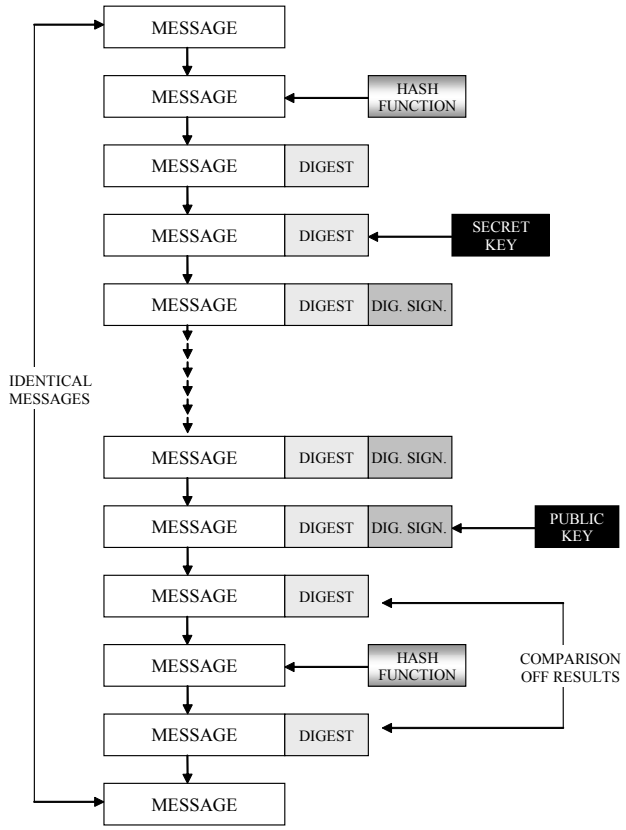


Fig. 10 Principle of functioning of the electronic signature

Electronic signature has legal value if the following preconditions are fulfilled:

1) *If it is unique for the person using it*
2) *If it could be confirmed as belonging to its user*
3) *If the person using it has total control over it*
4) *If it is permanently connected with the data in a way that it confirms both the data integrity and itself*
5) *If it is signed with the purpose of use instead of pencil and paper*.[2]

Irrefutability, i.e. impossibility for the transaction participant to dispute the fact about realization of transaction or sending of the message, is realized in such way that every transaction/message is signed by one or more users.

Positive features of electronic signature are the following:

- It protects data secrecy and integrity, and confirms the data source.
- It proves authenticity of partner in communication (through messages or transactions) – it prevents false identification.
- It is calculated on the base of message text with the help of special hash function, therefore the possibility for existence of two identical signatures is very small.

The user has both secret and public keys, which are unique. Secret key is used exclusively by the owner, while the public key is available to everyone. They are connected by complex mathematic algorithm (for example, RSA), in such way that the knowledge of the public key cannot lead to revelation of the secret key. The message encrypted with one key can be decrypted only with the other key. In this way, the identity of the user is confirmed, the fact about the sending of the message cannot be disputed, and the secrecy of the transmitted data is guaranteed. The problem lies in uncertainty of the fact whether the public key really belongs to the user, and not to someone who is falsely identifying himself/herself. To eliminate this uncertainty, a third party is included; this party issues certificates, assured that the user really is who he/she says that he/she is. The certificate is the confirmation that a public key really belongs to its user, and it is electronically signed by the one that issued it.

VII. CONCLUSION

Until recently, not enough attention has been paid to the network security. However, frequent incidents, which sometimes become cover news, and which have damaged many organizations, have changed that attitude in very short time.

Because of the commodity for the user and low costs, e-commerce via Internet is today considered to be the most profitable form of commerce. There are no time and space limits. Only in USA the annual value of Internet merchandize reaches amounts of over 70 billion dollars. It is estimated that there are some billion computers with access to Internet in the world today. It is by far the largest and the most rapidly increasing market in the world. Some 1.4 million of Croatian citizens have access to the Internet (according to the GfK Online Monitor research from June 2003), and the results of the research made on February 23rd 2004 indicate that 940000 Croatian citizens use Internet at least once per month [14].

It is certain that this type of commerce will have high increase rate for quite a long time. Serious approach to the network security problematics can significantly reduce the number and the intensity of negative occurrences. Model of network security as a precondition for e-commerce should provide at least small contribution to the fulfillment of this goal.

VIII. REFERENCES

[1] Vrbanec, T., Ž. Hutinski, *Mjere zaštite podatkovnog sadržaja, identifikacija i autentifikacija kroz aplikacije i protokole*, Znanstvena konferenca o razvoju organizacijskih ved, Portorož, 03/2002.

[2] -, *Pet obaveznih osobina e-potpisa*, Mreža, No. 12, year V, page. 11.

[3] Hutinski, Ž., T. Vrbanec, *Multilateralna sigurnost informacijskih sustava, jedan od uvjeta povezivanja u Europske integracije*, Znanstvena konferenca o razvoju organizacijskih ved, Portorož, 03/2002.

[4] Hutinski Ž., *Zaštita u informacijskim sustavima, sinopsis predavanja za poslijediplomski studij "Informacijske znanosti"*, <ftp://ftp.foi.hr/nastava/postdipl/zastitais/> (02/2004.)

[5] Electronic Commerce Interest Group, <http://www.w3.org/ECommerce/> (02/2004.)

[6] Hartman, T., *Making Sense of E-signatures* <http://www.rkmc.com/article.asp?articleId=178> (02/2004.)

[7] http://www.businessweek.com/bwdaily/dnflash/june2000/nf00620f.htm?scriptFramed?scriptFramed

[8] Salkever, *What Do E-Signatures Mean for You?*, <http://www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html> (02/2004.)

[9] T.M.A. Lomas, *SET Protocol Description*, <http://www.cl.cam.ac.uk/Research/Security/resources/SET/intro.html> (02/2004.)

[10] -, *Secure Electronic Transactions Protocol*, <http://www.byte.com/art/9706/img/067csd2.htm > (02/2004.)

[11] *Webopedia* (online dictionary and search engine), <www.webopedia.com/; http://webopedia.internet.com/quick_ref/OSI_Layers.asp> (02/2004.)

[12] SSL.Com, <http://www.ssl.com/> (02/2004.)

[13] -, *Introduction to SSL*, <http://developer.netscape.com/docs/manuals/security/sslin/contents.htm> (02/2004.)

[14] Poslovni Forum, <http://www.poslovniforum.hr/> (02/2004.)

[15] Parkins, K., *What is Pretty Good Privacy?*, <http://www.heureka.clara.net/sunrise/pgpwhat.htm> (02/2004.)

[16] -, [RSA Security Inc.], *What is PGP?*, <http://www.rsasecurity.com/rsalabs/faq/5-2-6.html> (02/2004.)

[17] -, PGP documentation, <http://www.pgpi.org/doc/> (02/2004.)

[18] Narodne novine d.d., *Zakon o elektroničkom potpisu*, <http://www.mzt.hr/mzt/hrv/informacije/dokument/zakoni/0242.htm> (02/2004.)

[19] Privredna banka Zagreb d.d. - PBZCOM@NET, <http://com.pbz.hr/sigurnost.html> (02/2004.)

[20] *e-quality*, web newspaper of *Hrvatskog društva za kvalitetu*, <http://kvaliteta.inet.hr/e-quality> (02/2004.)

[21] *Pravilnik o certificiranju elektroničkog potpisa*, <http://www.mzt.hr/mzt/hrv/informacije/dokument/zakoni/1472.htm> (02/2004.)

[22] Elektronicko placanje – BROSURA, <http://staticweb.rasip.fer.hr/research/ecash/broshura/broshura.htm> (02/2004.)

[23] *Računovodstvo i financije*, časopis Hrvatske zajednice računovođa i financijskih djelatnika, Maurović, Lj., *Elektronički potpis - preduvjet pravne sigurnosti sudionika elektroničke trgovine,* 08/2001, No. 8.

[24] Franić, Z., *Potpis na kompjuterskom ekranu,* Poslovni svijet, 1996;382:15.

[25] Franić, Z., *Elektroničkim potpisom i Hrvatska napokon povezana s pravno uređenim kiberprostorom*, <http://www.vjesnik.hr/html/2002/02/21/Clanak.asp?r=gle&c=5>, (02/2004.)

[26] FINA, *Istraživanje posjećenosti hrvatskih Internet stranica*, < http://www.fina.hr/default.asp?ru=1&gl=200402230000002&sid=&jezik=1> (02/2004.)

[27] FER, ZEMRIS (Zavod za Elektroniku, Mikroelektroniku, Računalne i Inteligente Sustave), *Elektronički novac*, <http://sigurnost.zemris.fer.hr/emoney/> (02/2004.)

[28] Odsjek za europske ekonomske integracije, *Informacijsko društvo: Legislativa i regulativa u informacijsko komunikacijskoj tehnologiji*, <http://www.zg.hgk.hr/odsjeci/europintegr/prilozi/informacijsko_drustvo.htm> (03/2004.)

[29] Sun Microsystems, Inc., *Radius extension Guide*, <http://docs.sun.com/source/806-4252-10/contents.htm> (03/2004)

[30] Coulouris, G., J. Dollimore, T. Kindberg: *Distributed Systems, Concepts and Design, Second edition*, Addison-Wesley, USA, 1996.

[31] Juričić, T., *Usporedba ostvarenja RAID5 sustava na operacijskim sustavima Windows NT i Linux*, diplomski rad, Zagreb, rujan 2001., <http://sigurnost.zemris.fer.hr/RAID/juricic/> (02/2004.),

[32] -, ISDN router on a dics, <http://www.schumann.cx/isdn-router/> (03/2004.)

[33] Fli4l, the on(e)-disk-router, <http://www.fli4l.de/> (02/2004.)

[34] V. Čerić, M. Varga et al.: *Poslovno računarstvo*, Znak, Zagreb, 1998.

[35] V. Srića i suradnici: *Menedžerska informatika*, MEP Consult, Zagreb 1999.

[36] Šehanović, J., Ž. Hutinski, M. Žugaj: *Informatika za Ekonomiste*, Sveučilište u Rijeci, Pula 2002.

[37] Virtual Private Network Consortium, <http://www.vpnc.org/> (02/2004.)

[38] CNS Data Network, <http://www.net.berkeley.edu/> (02/2004.)

[39] RSA Security Inc., <http://www.rsasecurity.com/> (02/2004.)

[40] Digital certificates from thawte the global certificate authority, <http://www.thawte.com/> (03/2004.)

[41] CAcert.org, <http://www.cacert.org/> (03/2004.)

[42] VeriSign Inc., <http://www.verisign.com> (03/2004.)

[43] Hodges, J., *Some Directory-Service-oriented talks & panels...*, (02/2004.) <http://www.stanford.edu/~hodges/talks/index.html>

[44] MS Strategy for Lightweight Directory Access Protocol (LDAP), <http://www.microsoft.com/technet/prodtechnol/WinNTAS/plan/ldapcmr.mspx> (03/2004.)