SECURITY IN COMPUTER NETWORKS

Andreea Ionescu
The Academy of Economic Studies from Bucharest
Hyperion University from Bucharest
Calarasilor path, Number 169, Sector 3 Bucharest

Raul Serban
The Academy of Economic Studies from Bucharest
Hyperion University from Bucharest
Calarasilor path, Number 169, Sector 3 Bucharest

ABSTRACT

In this article it presents the electronic security of the computer networks. The electronic security refers to the totality of the policy recommendations and actions required to minimize the risk associated to perform electronic transactions, the risk refers to branches in the system, intrusion or theft of any means, technique or process used to protect information system. The confidentiality, integrity, availability, and compliance with laws, regulations and standards are fundamental security objectives, which are among the requirements of a business environment. The security requirements that must be fulfilled for e-business environment are: identification, authentication, accountability and audit. Security audit records dealing with the analysis of the activities performed if the protection system is in accordance with established security policies and procedures.

ISO (International Standards Organization) established the security services based on a set of security mechanisms that can be implemented in all protocols OSI (Open Standard Interconnection) to achieve integrity and protection of environmental resources for network communication. The main services defined by ISP are: authentication, access control, data confidentiality, data integrity, non-repudiation and auditing. To fulfill security services exist security mechanisms that can be used individually or in combination, such as: encryption, digital signatures, access control mechanisms (the list of access rights, passwords, access time test, data integrity mechanism.

Software resources mechanism for risk analysis systems are:

- OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation);
- COBRA (Consultative, Objective and Bi-functional Risk Analysis) - provides a framework for risk analysis based on ISO 17799 standard (BS 7799).

Among symmetric key cryptographic systems are mentioned: DES, Triple DES, IDEA, FEAL, RC2, RC4 and A5.

The main functions of a firewall are:
- the attack in force (brute force);
- masquerading;
- replay of the packets;
- message modification;
- unauthorized access via the Internet or web services that are based such as: e-mail, SMTP (Simple Mail Transfer Protocol);
- bombs and spams e-mails;
- deception by e-mail (e-mail spoofing);
- infection;
- trojan (trojan horse);
- virus;

The main purpose of the SSL is the secure and the connection between of two applications.

Appeal to notions of digital signatures and certification, which does not allow listening, eavesdropping or falsifying the information change between the two parts.

IPSEC is a set of application for services integration and Privacy authentication based cryptography IP. The Standard can be used to build virtual private networks (VPN) over the Internet.

PPP (Point to Point Protocol) uses features of the ISP dial-up. PPP it uses features of the ISP and the ISP dial-up.

PPP and IP packet standard serial lines transmissions between two points: for begin using two protocols.

- PAP (Password Authentication Protocol);
- CHAP (Challenge HandShake Authentication Protocol) based on encryption.

The firewall is the generic name of a component of a network that controls the traffic between the Personal Computer networks of organizations and external networks, for utilization of network policies.

The main functions of a firewall are:
- block the access of particular websites in the Internet; - limit the traffic of the public services of the organizations (taking into account IP address and ports);
- interdicts to some users the access of some servers and external networks;
- monitors communications between the internal network and external network;
- through encrypts the transmitted packets through VPN networks.

1. The degree of vulnerability A has the following consequences-conditional access of some bad intentioned users.
2. The degree of vulnerability B allows to local users in general to increase their privileges and to obtain the control over the system.
3. The degree of vulnerability C allows to users to alter indoor or outdoor machining processes.

Obvious, is the absence of independent sources stabilized power supply UPS (Uninterruptible Power Supply) which can lead to loss of files to work even damage computer systems in case of high frequency fluctuations or power supply and even certain licenses purchased for a single installation.

One of the biggest threats to information security in computer systems is the viruses into systems that infestation so called computer viruses. The general concept of computer virus is describing different types of attacks on computers alter or destroy computer data, but can cause malfunctions in the network by using its resources for self-production.

A computer virus is a malicious code a potential harmful piece of software that copies itself into other programs and modify them in order to failure.

A worm is an independent of the program. It produces by self-copying from one computer to another network in most cases. While a virus, a worm does not alter or destroy computer data, but can cause malfunctions in the network by using its resources for self-production. It’s multiply using a file transfer mechanisms, such as Internet or e-mail.

A Trojan horse (sometimes using the simple name Trojan) is a piece of code that hides inside a program and will run an operation hidden.

Spoofers represents a generic name given to programs that allow to a user using some artifices of calculations, have access to information in the system. In general, spoofers they are possibly by suing mechanisms that enable Trojan horse programs that allow access information.

A information in the system.

Hoax (Joker) are messages sent by e-mail with lose warning about existing virus and requires all persons known to be altered. The most behavior of malicious virus programs with “standard” can be grouped into several categories, depending on the “host” carrier. Viruses meet are:

1. file viruses;
2. boot viruses
3. macro viruses
4. script viruses
5. e-mail viruses

General Terms
ISO, OCTAVE, COBRA, DES, TRIPLE DES, IDEA, RC2, RC4, A5, IPSEC, PPP, PAP, CHAP, VPN, TROJAN, Spoofers, Hoax;

Keywords
File viruses; boot viruses; macro viruses; script viruses; e-mail viruses; chat and instant messaging viruses; e-mail viruses; chat and instant messaging viruses; security; authenticity; confidentiality; integrity; encryption.

1. INTRODUCTION
ISO 27002:2005 tells that “the Information is an asset which, like other important business assets, has value to the organization and therefore must be protected accordingly”.

Information can be found in various forms and means by which it is distributed or stored are different, so the information can be: stored electronic video display devices, printed or written on paper, presented orally in the conversation. Electronic security represents the total of policy recommendations and actions required to minimize the risk associated to perform electronic transactions, the risk refers to branches in the system, intrusion or theft or any means, technique or process used to protect information system.

Source or threat is any system vulnerability that can trigger accidentally or intentionally exploiting a certain system. When there is a vulnerability that can exploit a source of threat not represents a risk. A source of threat not represents a risk when there is a vulnerability that can exploit. Impact is a measure of the effect of an event. Risk is determined by the combination of likelihood and impact of an event, so that the result is expressed in different levels of risk “high”, “medium” or “low”. Control is the means and includes risk management policies, procedures, guidelines practices, organizational structures that can be administrative or technical.

Natural threats are floods, landslides, and avalanches earthquakes. Human threats are events that are caused by human beings. Examples of unintentional actions are: introduction of the error data are inadvertently delete a file and examples of actions deliberately made are: unauthorized access to confidential information, attacks or network loading applications programs to serve as support for attacks. Source of human threats are: hackers, crackers, computer criminals, terrorism, industrial espionage and staff within the company. The sources of human threats crackers personality rebellious are: intrusion system, disrupting function, unauthorized access to the system, code-breaking and/or modification of programs/data. Cybercrime such as: publishing illegal information, destruction of information, gaining revenue, unauthorized modification of data (threat: information corruption, destruction and computer fraud actions). Terrorism represents: assaults, exploitation, destruction, revenge (bomb, terrorism, information warfare, attack on the system (interruption service) and penetration system.

Industrial espionage and economic espionage is the competitive advantage. Staff within the company (corrupt, evil intentionally, negligently, poorly trained corrupt): revenge, intelligence, curiosity, financial gain (introducing false data corruption of information, introducing viruses into the system (viruses, logic bombs), sales of information.

Electronic signature addresses technologies, processes and human resources, not just devices and or applications. Human...
resources it is represented by: managers, owners, business partners, employees, contractors, service providers, customers and representatives of regulatory authorities.

Business processes are represented by reporting steps to meet business objectives, so common processes may include service management, reporting and incident management, change management, identity management and I.T. procurement.

Technology consists of: network infrastructure, software applications, components and physical security access devices. Networking infrastructure consists of: wired network, networks, data/voice, equipment, telecommunications and storage devices (software and hardware), communication equipment, connections Internet access services remotely;

- software applications;
- physical security components: video cameras, biometric access control, environmental control system (temperature, humidity).

Access devices such as: laptops and PDA.

Confidentiality, integrity, availability and compliance with laws, regulations and standards are fundamental security objectives, which are among the requirements of a business environment.

“Based on the above analogy, attributes of a secure and reliable network system include the following:

- secrecy (confidentiality);
- integrity (accuracy);
- denial of service (unavailability)”;[1]

1. Confidentiality is ensuring that information procedures and methods that are in transit or stored, be accessible only entities authorized to access those resources, prevent unauthorized access to information.

“Secrecy involves maintaining information confidentiality. This in itself means that hardware, software and data of computer system are accessible only authorized users. Access compromises the read-type privilege such as directory listing, file reading and printing.”[1].

2. Integrity is represented by procedures and methods to ensure that information that is in transit or stored, it cannot be changed, so that information is protected from alteration or unauthorized alteration or loss.

“Integrity involves maintaining information accuracy. This means preventing unauthorized users from modifying the system hardware, software or data. Such modification includes deleting, writing, creating, creating or changing attributes “[1].

3. Availability ensures that authorized entities have access to information resources when they need them, such as prevention of DOS attacks (Denial of Service). “Denial of service is the prevention of legitimate access to system hardware (e.g. CPU, printer), software (e.g. editor, compiler), data (e.g. in a database system), or the delaying of time critical operations (e.g. in real time applications).”[1]

4. Compliance with laws, regulations and standards applicable.

In the study “Trustworthiness in electronic commerce: the role of privacy, security, and site attributes” by France Belanger, Janine S. Hiller and Wanda J. Smith are presented the following ideas “While the growth of business-to-consumer electronic commerce seems phenomenal in recent years, several studies suggest that a large number of individuals using the Internet have serious privacy concerns, and the winning public trust is the primary hurdle to continued growth in e-commerce. This research investigated the relative importance, when purchasing goods and services over the Web of four common trust indices (i.e. (1) third party privacy seals, (2) privacy statements, (3) third party security seals, and (4) security features. The results indicate consumers valued security features significantly more than the three other trust indices. We also investigated the relationship between these trust indices and the consumer’s perceptions of a market trustworthiness. The findings indicate that consumers’ ratings of trustworthiness of Web merchants did not parallel experts’ evaluation of sites’ use of trust indices. This study also examined the extent to which consumers are willing to provide private information to electronic and land merchants. The results revealed that when making the decision to provide private information, consumers rely on their perceptions of trustworthiness irrespective of whether the merchant is electronic only or land and electronic. Finally, we investigated the relative importance of the three types of Web attributes: security, privacy and pleasure features (convenience, ease of use, cosmetics). Privacy and security features were of lesser importance than pleasure features when considering consumers’ intention to purchase. A discussion of the implications of these results and an agenda for future research and provided”. [2]

2. SECURITY OF COMPUTER NETWORKS-STANDARDS

Security requirements that must be fulfilled for e-business environment are: identification, authentication, accountability and audit.

Identification procedures and processes so that are necessary to establish a unique identity for all user or an entity with a business system so that identification allows accounting for all individual operations and prevents unauthorized access.

Authentication is the procedure for checking the identity of the entity requesting access to the business system, the process by which the system validates the begin information provided by the user entity.

Information classification determines the level of security required for a certain informational resources. For example, financial information or any other information that requires protection against unauthorized access and trade secrets.

In terms of security, the information is of two types:

1. The information used in business;
2. User information in the government;

The information used in business are: confidential, private, public and sensitive. Information used in the government are secret and top secret, confidential, restricted, sensitive but unclassified and classified.

Accountability is closely related with the security measures required by business users of the system who will be responsible for actions taken after connecting to the system.
Security audit records dealing with the analysis of the activities performed to determine if the protection system is in accordance with established security policies and procedures. The purpose of this audit is to identify security-related weaknesses or failures that can be corrected and controlled.

Business integrity, in order to maintain system integrity taking the following measures:

1. Separation of user data and processes;
2. Separating data and system processes;
3. Data protection and hardware changes, software protecting it;
4. Control operations and maintenance actions.

Data integrity is represented by data protection mechanisms against destruction or unauthorized access and registration mechanisms of changes.

Service reliability refers to the safe and easy way in which an authenticated user is able to access and use the system resources.

To maintain certain operational and efficient security system security documentation is required.

Security requirements are grouped according to the following areas:

1. Operational Security;
2. Technical Security;
3. Security management;

Operational security has the following characteristics:
- workspace control features: temperature, humidity, state substances, harmful;
- control power supply;
- access to data;
- distribution data in external environment;
- facilities for physical protection offices, data centers, computer rooms specially equipped for;
- case desktop, personal computers, laptops;

Technical security concerns:
- communication: routers, dial-up interconnection;
- access control;
- cryptographic systems;
- identification and authentication;
- the reuse of object;
- the audit of the system;

Security management refers to the process of establishing and maintaining a framework and manages structure and processes provide assurance that information security strategies are aligned and supported by business objectives are consistent with applicable laws and regulations by compliance policies and internal controls.

Security management aims occupations:
- allocation of responsibilities;
- ensure continuity of supported provided;

- response capability to incidents;
- periodic review of the way in which security controls;
- staff training in information technology, particularly in subdomain security;
- system of licensing and renewal;
- system for applying security plan;
- assessment of risk;

For each area of security requirements can act screening:
- physical control;
- technical control;
- administrative control;

Physical control has the focus IT environment protection. To ensure physical-control are needed:
- personnel security, lacks, cameras and uninterruptible power supplies;
- technical control refers to access control: authorization to use objects, data encryption;
- referenced administrative control: the security policy and security procedures implemented as a part of the security plan;

An example here it mentioned:
- administrative control over security policy;
- administrative control over security guidelines;
- administrative control over security;
- administrative control over security procedures;
- training in security;

Roles and responsibilities will be reported to the organization’s security for:
- manager is represented by the person responsible for implementing the security plan;
- security officer ensure that the IT system is implemented and executed in accordance with the security policy, assess vulnerabilities and establishes security measures;

The owner is represented by the person who is responsible for data protection (such as data owner) or information assets. General responsibilities of data owners are dividing levels of data classification defines how to access data and how they are protected.

The custodian deals with asset protection or data organization and beyond, its responsibility logical access control. Custodian it is called system security administration.

Technical security specialist is a member of the IT department and is trained to work with owners and those who own the data.

The user is represented by any person who is entitled to use the system resources so allocated to a user rights are consistent with the responsibility meet.

ISO (International Standards Organization) established the security services based on a set of security mechanisms that can be implemented in all protocols OSI (Open Standards
Interconnection) to achieve integrity and protection of environmental resources for network communication.

OSI reference architecture, defined by ISO 7498-2 refers to:
- define security services;
- define security mechanism;
- principles of organization-tiered security;
Association security mechanism security services;
The basic principles for organizing the security levels are:
- the number of security services that can be purchased to be minimal;
- security services can be used in protection systems several levels;
- security mechanisms should not duplicate functions of communication services;
- respect each level functional independency;
- will minimize system functionality based on trust;
- when protection is provided at a level based on security mechanisms at a lower level, it is necessary that no intermediate non violate this dependence;
- security services must be defined to allow expansion with new services;
The main services defined by ISO are: authentication, access control, data confidentiality, data integrity, non-repudiation and auditing.

To fulfill security services exist security mechanism that can be used individually or in combination, such as: encryption, digital signatures, access control mechanisms (the list of access rights, passwords, access time, access time test, data integrity mechanism.

ISO 2700 series was reserved by ISO for information security:
- ISO 2700 includes foundations and principles (including elements of ISO 13335 MICTS Part 1);
- ISO 27001 contains requirements ISO (Information Security Management System), has been revised BS 77992 (published in October 2005);
- ISO 27002 includes guide for information security practices, rename the ISO 17799 standard (published in 2007);
- ISO 27003, includes an ISMS implementation guide (includes items ISO 13335 MICTS Part 1);
- ISO 27004 is an ISMS standard measurement and metrics;
- ISO 27005-Risk Management (ISO 13335 includes elements MICTS Part 2);
- ISO 27006 accreditation is a guide for organizations ISMS certification registration (EA review 7/03);
British Standard Information Security, BS 7799, was published in 1999 in two parts:
- code of practice for information security management;
- requirements for information security implementation in accordance with this code of practice;
In 2000, the ISO (International Standard Organization) adopted the British Standard BS 7799 and published as an international standard known as ISO 17799, Code of Practice for Information Security Management. ISO 17799 standard identified 36 control objectives and 127 control items that were included in 10 categories of control.
The 10 categories of control of ISO 17799 are:
- security policy;
- business continuation planning;
- access control system;
- development and maintenance of the system;
- physical and environmental security;
- compliance;
- security personnel;
- security organization;
- computers and network-management;
- classification and control of information resources;
Accordingly BS 7799-2, implementing and information security management system (ISMS) requires completion of seven steps:
1. Define the ISMs policy and is made according to the directions, requirements and needs of organization;
2. Responsibilities and Resources-identify the persons involved in the responsibilities assigned to each system;
3. Risk management;
4. Selecting controls;
5. Applicability
4.. Implementation
The benefits of implementing an ISMS are:
1. Confidece business partners (suppliers, clients);
2. Business continuity;
3. Improving prevention systems and incident response;
4. Minimize risk, customers will access information;
5. Justification and cost optimization of costs required to implement security controls;
6. Demonstrate and management commitment to information security;
7. Demonstrate compliance with their security practices recognized standards;
8. Compliance with legal requirements, rules and legal regulations;
9. Ensuring that risks and controls are constantly reviewed;
The IT Governance Institute provides best practices for IT processes through publication to COBIT (Control Objectives for Information and Related Technology);
COBIT is processes structured in four areas:
- planning and organization;
- purchase and implementation;
- operation and support;
Monitoring and evaluation;
The basis of any security model are:
- security plan, which is part of the strategic business development plan.
Policy is the central component of the security plan. In determining policy is envisaged:
- shared value assets, how to access, permissions;
- consequences of loss of confidentiality or operational capacity;
- vulnerabilities that can be identified;
- existing threats;
- the likelihood of threats;
“A security threat has been defined as a “
Security policy shall specify the following aspects:
- security objectives of the organization;
- staff responsible for securing;
- involvement of the ensemble to ensure security: who will provide training in security such security will be integrated into the organizational structure.
To ensure the security objectives and archive a high level of protection, security plan will be developed and implemented by level:
- security application/business set of measures that address business-specific risks relate, first, security software used to develop business applications (web servers);
- security system: it can be implemented at the system command and control software functions;
- network security is part of a network design. Network security controls including firewalls, VPN (Virtual Private Network) and gateways.
- physical security: protection systems, devices and media for backup, including access controls, uninterruptible power resources, redundant communication lines.
- security organization: responsible for all aspects of the organization security plan, including security policies, training in security, business systems of the organization and planning for disaster recovery.
In order to achieve an effective protection system is necessary to go through stages:
- risk assessment;
- defining security policy;
- implementation;
- administration;
- audit;
For existing security policy steps will be taken:
1. analyze the major risks of the organization –to define procedures by which risks will be prevented as a result of a major disruption;
2. defines the security policy –treatment components that cannot be prevented malicious actions without improving protective measures;
3. establish an emergency plan if protective measures are default;
4. because of these problems can only be solved by defining a secure itewal a generality and the expenditure of money for certain activities, security policies and the expenditure of money for certain activities, finally accept some risks;
“A security threat has been defined as a “circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse” (Kalakota and Whinston, 1996). Security, then is the protection against threats. Under this definition, threats can be made either through network and data transaction attacks, or through unauthorized access by means of false or defective authentication. This definition must be tailored in order to be applicable to consumer transaction to acknowledge that consumer information has value. For consumers it must be recognized that (1) economic hardship encompasses damages to privacy (loss of information) as well as theft, for example of credit information (2) authentication issues for consumers will be reserved, as in whether the Web site is ‘real’ rather than whether the purchaser’s identity is real. This tailored definition explains the security threats from a consumer’s standpoint of business. Security in B2C electronic commerce is reflected in the technologies used to protect and secure consumer data. Security concerns of consumers may be addressed by many of the same technology protections as those of businesses, such as encryption and authentication. For purposes of this research, the application of specific security technologies is categorized as security features.
Our delineation of privacy and security is similar to the distinction that Hoffman et al (1999) use in identifying ‘environmental control’ as separate from ‘control over secondary use of information”, described above. Environmental control refers to consumer concerns with sharing, information online due to expectations of threats to online security including fear of hackers and informational theft” [2].
The risk analysis is a distributed business environment involves four basics tasks:
1. Identifying sources of the risk;
2. Risk-determining probability;
3. Determination the assets to be protected;
4. Action-cost assessment of the threat;
1. Identifying sources of the risk-classes of intruders->each class of intruders must be examined in the context of distributed environmental threat from accidental to intentional;
2. Establish a reasonable estimate risk probability allows an overview of existing risk;
3. Determination the assets to be changes in function the commercial profile or not a organization in cause; examples of assets that can be protected are: information, equipment, networks, such as e-mail;
4. Evaluation of the cost of an action of threat, there are basic types of costs are taken into account: the primary cost—the cost of replacing lost resources, reintroduction data in databases; secondary cost, last business, cost side, the negative effect on client’s business;
In the study “Security beliefs and barriers for novice Internet users” by Steven Furnell, Valleria Tsaganidi and Andy Phippen it presents “End-users are now recognized as being at increased risk in online scenarios, with a range of threats that seek to specifically target them and exploit their systems. Novice users are particularly likely to face difficulties in this context, as their unfamiliarity with the technology can limit their ability to recognize the threats and understand the required protection. This paper presents the results from a qualitative study, arising from detailed interviews conducted with 20 novice users in order to assess their views and experiences with Internet security. The findings reveal a general awareness of the existence of threats, but less appears unconcerned about the potential impacts of the problems. In other cases, they felt unable to address their concerns as a result of their lack of technical knowledge or obstacles posed by security tools.”[4]

Including adverse effects arising as a result of threat agents can include:

1. Loss of business due to the access to the confidential data, allowing competitors;
2. Compromised reputation and images;
3. The loss of business relationship, lack of trust;
4. The loss of goods, which can take many forms: money and equipment, service capabilities in public bad;
5. Loss of trade secrets, production and technology, by compromising such secrets can have dramatic effect on profit organization;

Software resources for risk analysis systems:
- OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation);
- COBRA (Consultative, Objective & Bi-functional Risk Analysis) –provides a framework for risk analysis based on ISO 17799 standard (BS 7799);

Passive attack actions:
1. Network analysis (network scan)
   - creation of a complete profile of the infrastructure network security –using a combination of tools and techniques for preparing catalogs of information about the internal network organization concerned;
   - spying network: network gathering information with the intention to analyze and exploit personal make available to any third party;
   - traffic analysis (listening channel)-is determined the nature of the traffic between defined host and by analyzing network time session, frequency, message size; are encrypted and the spying has no result;

2. TYPES OF ATTACKS-ENCRYPTION-ALGORITHMS

Active type attack actions:
1. The attack in force(brute force)-using of tools for detection/breaking passwords and gaining unauthorized access to a network of an organization;
2. Masquerading the entity presents a false identity to have access to secret data or network resources to which access is not allowed with his own entity;
3. The replay of the packets-the combination with the active passive attack, in passive mode are captured packets passing through a network and vulnerable and unprotected; those packets are inserted into network as if they are into another original message;
4. Message modification –refers to capturing a message for unauthorized changes or deletion( the entire message or part of it), change order or delay transmission of captured messages;
5. Unauthorized access via the Internet or web services that are based, such as: e-mail(SMTP-Simple Mail Transfer Protocol), telnet passwords transmitted in clear (from the client to server), change the association between IP address and the domain name, execution of the scripts on the client-side (e.g. Java applets) shows the danger, of being made a code from an arbitrary location on a client machine;

    1. Bombs and spams e-mails (e-mail bombing and spamming) the e-mail bombs consist in repeated transmission of the same message to a certain receiver. Spam represents a variant of the same message bomb is sent to hundreds or thousands of receivers. Those can overcome storage capacity of the recipient’s mailbox.
    2. Deception by e-mail (e-mail spoofing): A user receives an e-mail that appears to have a specific origin (sender) but in reality it is false (behind the message is another sender). By example e-mail claiming to come from the network administrator asking the recipient to change the password to one specified in the message.

    1. Trojan (Trojan horse) –hidden code that is executed whenever is running an authorized software in which it was infiltrated, opening a lot of virtual gates on the infected computer, allowing to hackers to enter in the system;
    2. Virus–represents a malicious code program that infects computer files by copying it alone in those files when they are loaded in memory;
    3. Worm–program that can destroy data or use operating abnormally processes, copying the one in your computer’s memory;
    4. Logic bomb-for execution requiring additional data such as programming the attack scheduling or modification data in a specified time;

1. A certain level of protection and security can be assured by one or more solutions:
   - the encryption –for data protection and passwords;
   - the access control;
   - the infrastructure based access-based on hard key (USB key);
   - authentication by digital signature and certificates-check who send data over the network;
   - authorization -prevent the improper access;
   - checking data integrity and authentication code of their;
   - packet filtering;
   - disabling services that aren’t necessary;
   - packet filtering;
-deactivation of the unnecessary services;

The encryption is the process for transformation the message from a form that can be readable-clear text-in an encoded form.

The encryption is generally used for:

1. Protection transit data through networks against interception and unauthorized manipulating;
2. Protection stored data on computers against visualization and unauthorized manipulation;
3. Protection stored data on computers against visualization and unauthorized manipulation;

1. To prevent and detect accidentally or intentional modification of the datas;
2. To verify authenticity transactions or documents;

The key like concept it refers usually to a information in a binary form, of a certain length, which it is used with a cryptographic algorithm for encryption and/or decryption.

1. At encryption key affects how data is changed.
2. At decryption, only the correct key can recover the original data.

Whether \( M = \text{message space}, \ C = \text{cryptogram space and} \ K = \text{key space}. \) A cryptographic system consists of:

- \( E_i : M \rightarrow C, \quad i \in K \) the transformation for encryption;
- \( D_j : C \rightarrow M, \quad j \in K \) the transformation for decryption;

With the property that for any encryption key such that \( i \) belongs to \( K \) there is a unique decryption key such \( j \) that belongs to \( K \) having the property \( D_j = E_i^{-1} \)

By substitution cipher we understand each letter or group of letters on the text source that are replaced by another letter or group of letters. Transposition cipher reorder text source.

For example if I have the text security for encryption and it is use the key number, it will result the chyper text “RESICAETUT”:

<table>
<thead>
<tr>
<th>C</th>
<th>I</th>
<th>F</th>
<th>R</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>S</td>
<td>E</td>
<td>C</td>
<td>U</td>
<td>R</td>
</tr>
<tr>
<td>I</td>
<td>T</td>
<td>A</td>
<td>T</td>
<td>E</td>
</tr>
</tbody>
</table>

The symmetric algorithms for encoding are of two types:

- block type algorithms-operating of the initial text block level bit;
- stream-type algorithms-operate on a bit (or byte) of the original text at a time;

In the study “UK ELECTRONIC COMMUNICATIONS ACT 2000-TAKE OF TIME FOR E-BUSINESS OR A MISSED OPPORTUNITY” by Mark Crichard appears “PART CRYPTOGRAPHY SERVICE PROVIDER” “Part I of the Act will, when brought into force, introduce a number of new measures relating to the provision of “cryptography support services”. This is a fairly broadly defined term of the Act, encompassing any service provided (to either or both senders and recipients of electronic communications or those storing electronic data) and which is designed to facilitate the use of cryptographic techniques for the purposes of:

(a) Securing that such communications or data can be accessed, or can be put into an intelligence form, only be certain persons;
(b) Securing that the authenticity or integrity of such communications or data is capable or being ascertained;

Under the Act the Secretary of State to establish a voluntary register of ‘approved’ cryptography support services supplier. This would extend to persons providing cryptography support services in the UK (or who are intending to do so), although such approval could also extend to such services provided outside the UK.

The idea behind this is to establish a statute-based accreditation scheme for ‘trusted service providers’ to improve consumer confidence. However, following the earlier consultation, the Government has decided not to implement these particular provisions yet, preferring instead to see how the industry’s attempts at self-regulation out” [3].

Among symmetric key cryptographic systems are mentioned: DES, Triple DES, IDEA, FEAL, RC2, RC4 and A5.

DES (Data Encryption Standard) represents a standard developed by International Business Machine. It operates on blocks of 64 bits and has a 56-bit key. DES was approved as a standard technique for encryption/decryption by the U.S. National Standardization Office (US National Bureau of Standards-NBS), the predecessor of NIST (National Institute of Standards).

Triple DES –is a symmetric-key cryptographic system that can hold a key of 112 bits and 16 parity bits and a key of 168 bits and 24 parity bits.

AES (Advanced Encryption Standard) represents the successor algorithm of DES.

IDEA-International Data Encryption Algorithm was developed by the year 1990 to replace DES (Data Encryption Standard) system. It uses blocks of 64 bit and keys of 128 bit. PGP (Pretty Good Privacy) is the most significant use of IDEA.

FEAL (Fast Data Encryption Algorithm) represents a family of algorithms that it utilizes blocks of 64 bits and keys of 64 bits.

RC2 and RC4 are algorithms with variable encryption key, between 40 and 128 bits. A5 represents a stream algorithm used to encrypt traffic from GSM network used widely throughout Europe.

DES is an algorithm based on block-type the message source (clear text) is divided in blocks of 64 bits and uses a 56–bit key generated randomly.

Given a plain text block of 64 bits (m1m2..m64) DES operates in 19 rounds:

- in the first round to create an initial permutation (IP), independent of the key, resulting in a block of 64 bit that is divided in two blocks, L0 the 32 bit from the left side and Ro the 32 bit from the right side;
-going 16 rounds, functionally independent, the previous result is the subject to a process of substitution, permutation and an exclusive OR operation (XOR) with the parameter key (each different round key Ki is used):

-in the penultimate round, the two groups of 32 binary digits recombine after the group left the 32 –bit has changed what) resulting with one of the right side, and in the penultimate round it starts an inverse permutation of the initial(IP-I), resulting a message on 64 binary encrypted cipher(c1c2…c64).

The advantages of the symmetric key encryption systems are:

-both encryption and decryption is done with the same key;

-transformation is performed quickly and easily due to the small number of calculations included in the same algorithm;

The disadvantages of the symmetric key encryption systems are:

-in a business environment the key distribution represents a problem;

-the other problem is the management of the keys;

The private key can not be used for signing electronic documents or the messages the mechanism is based on secret sharing;

In the case of cryptography with public key is ensuring data privacy, only the recipient can read the email, it only holds to private key to decrypt the messages.

But the recipient can not be sure that inbound messages emanating from those who claim that they have sent, everyone can use it for sending key.

Public key cryptography not replace secret key. The two techniques complement to provide a high level of security without diminishing speed and performance.

The dispersion functions (hash functions) have the fundamental role in the modern crypto-system and for creating abstract messages.

Hash functions have like input a message of arbitrary length and produce the fixed-length message, referred to as hash values, hash, hash or hash results.

Typically, it is the hash value 128 or 160 binary digits. When the hash function uses a private key as secondary input parameter, output depends on both teaches and key message and is called message authentication code MAC-Message Authentication Code.

The main characteristics of hash functions are:

-a message of any size generate a fixed size block of data and reduced, performing the same function on the same message hash will get the same result.

-the result of the hash is unpredictable, that a change in the message will cause a radical change hash value;

-is irreversible, for example is a way to get the message from the hash value;

To calculate summaries of messages are used the following scheme:

-MD2 (Message Digest) have the hash value is of 128 bits;
-MD4—the hash value is 128 bits;

-MD5—standard dispersion in the field, the value is 128-bit hash;

-SHA1 (Secure Hash Algorithm)—the hash value is 160 bits;

If the authentication of the received message is the main objective thus you proceed:

1. It manages in the first mode a summary of the first message by using an image of dispersion;
2. The summary is encrypted with the sender’s private key;
3. The summary is encrypted with the sender’s private key;
4. The encrypted message result represents digital signatures and can attach the message in the clear;
5. If the received message authentication is the main objective, I proceeded as follows:
   -it generates the first summary of the message with the private key by using a dispersion function;
   -summary encrypts the private key of the sender;
   -the encrypted result message is encrypted and we can attach digital signatures and message in clear.

Reception verification operation is performed as follows:

1. it will separate the digital signature of the message in plain text;
2. hash function is applied, the clear message is received and thus obtain a first snapshot;
3. the received digital signature with the sender’s public key, obtaining the second summary of the message;
4. the two previously—obtained summaries is compared. If the summaries are identical it can be clear that the message has not been altered and is from the real sender. Otherwise, the message content to be amended by the communication;

Public key infrastructure provides a technical framework (including protocols, services and standards) for:

-authenticating users;

-privacy;

-the data-integrity;

-non-repudiation;

-key management;

Public key infrastructure includes the following components:

-certification authority (a Certification Authority) is to issue and revoke digital certificates;

-registration authority (RA—Registration Authority) is to validate requests for issuing identity certificates and final entities;

The digital certificate represents an electronic data collection.

Public key infrastructure includes the following components:

-Deposits Certificates (Repository) stores and distributes certificates and certificate revocation lists (CRL—Certification Revocation List);

-End Entities (End Entity) represents users, devices and software applications that use digital certificates to implement security services;
The Certificate Authority has the following functions:
- generates certificates for end entities and certification authorities;
- maintains information about the status of certificates and certification revocation generated list;
- signs digital certificates and certificate revocation lists;
- periodically publish certificate revocation list;
- archives expired certificates;
A digital certificate is composed of the following elements:
- the certificate format version;
- the public key encryption;
- identifying information of the entity that has corresponding private key;
- period of validity of the certificate on which is operating;
- digital signature certification authority;
Electronic signature is the digital form of handwritten signatures (with the same features and capabilities (enables authentication of an electronic document));
Extended electronic signature is the signature while satisfying the following conditions:
- the signature is uniquely linked to the signature;
- to identify exclusively controlled by means of the signatory;
- is linked to data in electronic form which are reported so that any subsequent modifications is identifiable;
- the extended electronic signature is that signature realized that is supported with a certified electronic signature that practically is the only legal value;
At European, level CEN/ISS (European Committee for Standardization/Information Society Standardization System) WS/E-sign dealing with developing specifications for systems and devices used to create legally binding signatures.
Signature-creation software runs under an operating system on a hardware platform data (PC/PDA).
Secure Signature Creation Device contains data required signature, if the signature using asymmetric cryptographic algorithms, the device holds the private key, if the device is a smart card reader are required smart cards;
E-gate USB? Smart card was tested on the following operating systems: Microsoft Windows 98 (Second Edition), Windows ME, Windows 2000 SP4, Windows XP Professional (SP1). E-gate Smart Card requires the following resources: 1.33 MHz processor, RAM 32 mb, available USB.
PKI Systems are implemented in a lot of network protocol documentation:
- S/MIME (Secure/Multipurpose Internet Mail Extensions) was developed by RSA Data Security and is occupied with security in Internet mail messages using public key encryption.
- SET (Secure Electronic Transaction) is an open standard commercial area, with the ability to secure credit smart card transactions through Internet. It was developed by VISA, MasterCard, IBM. The protocol is based on digital certificates.
SSL (Secure Socket Layer) was developed by Netscape to secure the transfer of information between client-server applications such as the Internet. It represents a protocol independent from protocol and application.
It provides services of authentication, data compression, encryption and data integrity.
The main purpose of SSL is the secure and the connection between the two applications.
- appeal to notions of digital signatures and certification, which does not allow listening, eavesdropping or falsifying the information change between the two parts.
- IPSEC is a set of application for services integration and Privacy authentication based cryptography IP. The Standard can be used to build virtual private networks (VPN) over the Internet.
PPP (Point to Point Protocol) uses features of the ISP dial-up. PPP is use features of the ISP dial-up.
PPP and IP packet standard serial lines transmissions between 2 points: for begin using 2 protocols.
- PAP (Password Authentication Protocol) and CHAP (Challenge Hand Shaker Authentication Protocol) based on encryption.
“The increasing complexity of information and telecommunications systems and networks is reaching a level beyond human ability, mainly from the security assessment viewpoint. Methodologies currently proposed for managing and assuring security requirements fall short of industrial and societal expectations. The statistics about vulnerabilities and attacks show that the security, reliability and availability objectives are not reached and that the general threat situation is getting worse. With the deployment of Next Generation Networks-NGNs, the complexity of networks, considering their architecture, speed and amount of connections, will increase exponentially. There are several proposals for the network and security architecture of NGNs, but current vulnerability, threat and risk analysis methods should have some additional new characteristics, mainly regarding their adaptation to the continuous evolution of the NGNs. In addition, the application of security countermeasures will require technological improvements, which will demand further security analyses. This paper evaluates the current vulnerability, threat and risk analysis methods from the point of view of the new security requirements of NGNs. Then, the paper proposes to use autonomic and self-adaptive systems/applications for ensuring the security of NGNs.”[4]
The firewall is the generic name of a component of a network that controls the traffic between the PC network of organizations and external networks, for utilization of network policies.
The main functions of a firewall are:
- block the access of particular websites in the Internet;
- limit the traffic of the public services of the organizations (taking into account IP address and ports);
- interdicts to some users the access of some servers and services;
- monitors communications between the internal network and external network;
-through encrypts the transmitted packets through VPN networks;
-The firewall for filtration packets has functions for access control based on a hose can be treated (access of rules).
-The mechanism of filtration have the capacity of identification of the packets and specification of the mode in which those can be treated (accepted, ignored or refused);
-the rules after they actionned the filtration of packets are stored in tables configured by the administrator of the system or the officer of security;
-Firewall for filtered packets has two advantages:
-the speed – because the corresponded data to superior levels are examined;
The simplicity;
The rules for a firewall with the filtration of the packets (the IP address 193.232.3.0 is allocated to secure network):
The disadvantages of the firewall for encrypted packets:
-it cannot prevent attacks that exploit the vulnerability or functions to specified applications (doesn't examines datas of the superior levels);
-doesn't supports advanced schema for the authentication of users;
-are vulnerable to attacks by wich it uses the specified elements of the protocols stack of protocols TCP/IP, like the falsification of the levels of the address of the address of the network, routing by source, fragmentation of an IP packet;
-are susceptible to create of security by uncorresponent configuration;
The firewall with a complete monitored of the state is a filter of the packets that incorporates the necessary elements for creating a catalogue where are registered all the TCP connections solicited in the internal network;
The disadvantage is the difficulty of administration compared to other types of firewalls because their complexity.
The types of the firewall at level of application are:
-application level gateway or agent proxy;
-the circuit level gateway-realises a controlled connection (virtual circuit) between an intern host and another extern.
If on an internal network is installed a proxy, when it sends a request to a server through the Internet:
-the request from the host would be transmitted to the proxy server;
-the proxy server contacts the server on the Internet with the address, like the source addressess (not with the host that sends a request);
-the proxy server reception the data from the server on the Internet and transmitted the host that had it solicited;
The address IP of the internal host can’t be known out of the network;
The proxy servers registered the informations about the requests and the transfers like, after, can make an analysis of the access on the Internet.

The Intrusion Detection Systems are software and hardware components that:
- processing the events from the system to the network;
- monitorises the events from the system or the network;
- analysis the events;
- signals the security issues;

Honey posts are traps systems designates to attract a potential attacker to act on critical systems;
The advantages of honey posts are:
- directing an attacker to bait, not harm critical systems;
- collects information about the activity of the attacker;
- the actions attackers can be easily and extensively monitored and results can be used to refine models and improving protection systems;

Honey disadvantages posts are:
- legal implications for the use of these devices are not well defined;
- honey posts are not sufficiently provided for the use in the security technology;
- an expert attacker, are directed to a bait may become more aggressive in its distructive actions on organizational systems;
- a high level of expert necessary for administrators and security managers to control the installation and use of these systems;

A honeynet is a collection of interconnected posts honey to simulate a network infrastructure;
The advantages of intrusion detection systems are the following:
- intrusion detection;
- out intrusion activities;
- automated response;
- interface with other system in the system;
- the management in the security policy;

The disadvantages of intrusion detection systems are:
- limitations in defining policy;
- the application-level vulnerabilities;
- the means of access to applications that are bypassed security checks;
- limitations identification and authentication schemes;

The environmental complexity given that it reflects the business system will be placed; an autonomous system (Small Office/Home Office-SOHO), sometimes called a standalone autonomous system refers to a small company that includes various devices, laptops, telecommunication systems in a broadband network. The system is a very simple business environment.

Common practices accepted security for autonomous environments are:
- use of dedicated firewall Internet connection;
- use of personal products or autonomous systems;
-periodically applying the updates and patches for applications (antivirus software, web browser, email client) and operating system;

- web client product and e-mail to be configured to block the traffic/ messages that may contain distractive code;

-disabling unnecessary applications (personal web server, SNMP, messengers); systems/user who connect to wireless LAN that can connect to LAN network cable or uncabled;

-backup and recovery procedures;

-physical security procedures;

Instead a company has a complex IT environment and includes many systems with different architectures and network access can be achieved by several techniques. The complexity involves many interconnected applications, different protocols and multiple categories of users and access to different data classes.

The high IT environment environmental measures susceptibility of being attack. Vulnerability may exist in the system concept. The hackers will follow to attack the vulnerable elements of the system.

The accepted common practices for environments are:

-internal network segmentation through firewalls and other defensive techniques;

-centralized management system to restrict access by users;

-centralized management of security applications such as antivirus products;

-the auto-install patches and updates for operating systems and applications;

-restricting access to printer and multifunctional devices;

-centralized system for monitoring log files (logging);

-facilities for centralized backup and recovery;

The common accepted security practices for secure environments are:

-the number of applications by the system in is low (doesn’t combine too many application servers on the same system);

-if it is possible, it would be used an firewall application for each host;

-the number of users who will access the system will be limited to a minimum;

-authentication is required (token authentication, biometric authentication, smart card);

-management or remote access should be restricted, if used, the connection must be encrypted;

-updates, patches and security related applications and operating systems must be tested and filter unnecessary protocols;

-intrusion detection and log files will be monitored;

-tools for testing system vulnerabilities will be regularly used;

-the system administrators should be professional in the used technology;

Business environment may include multiple security zones, namely:

- uncontrolled area, such as the Internet is a global network connecting millions of computers and therefore cannot be controlled;

- controlled are such as; demilitarized zone for Internet, Intranet, restricted area and safe area;

- demilitarized zone for Internet (Internet DMZ) is generally controlled area containing components which customers directly communicate. It is a buffer between the Internet and internal network. Transportation between uncontrolled and a controlled area is classified as public;

In the study “Challenges for the security analysis of Next Generation Networks” are presented the requirements for a new and more effective security solution approach of NGNs. Due to the characteristics of the current and future security problems of NGNs, we argue that the current and future security problems of NGNs, we argue that the current standardization efforts may fall short of providing a comprehensive solution. The objectives of proposed solution approach are:

-Localization of the security problems, for ensuring their effective detection and mitigation;

-Information sharing among NGN among components, done according to need-to-know, segregation and fragmentation rules.

-Vulnerability, threat and risk analysis tools carrying out more effectively their assessments by exploiting real time information sharing;

-Creation and use of automatic and self-adaptive components to assure the security, reliability and availability of the systems and networks;

The main tools of the proposed solution are autonomic and self-adaptive applications/systems. They should enable the choice of the more appropriate security solution for each circumstance, resulting in the improvement of the security, availability of the application and network services. Future work should take advantage of the many research projects regarding autonomic and self-adaptive applications/systems active today e.g. ‘Autonomic Internet’, supported by the EC’s FP7 (http://ist-autoi.eu/autoi/; http://www.future-internet.eu/home.html).

The authors plan to work on reviewing and describing the security requirements for each stratum and security dimension of the NGN architecture, in the light of possible applications for autonomic and self-adaptive components.”[4]

Intranet is a commonly controlled area, which contains components that directly communicate;

-restricted area (production network), represented by one or more areas that can be designated as restricted, other supporting functions which access is strictly controlled and not allowed directly from an uncontrolled network. Network is limited by one or more firewalls websites;

-the safe-zone (network management) access is only available to a select group of authorized personnel;

PTP (Point-to-Point Tunneling Protocol) operates at level two (data link) and is based on PPP standard;

Thus, PPP allows extending private networks of companies, through some own tunnels in the infrastructure of the Internet;
PTP utilizes mechanisms offered by PPP protocol to maintain the connection, packet encapsulation and at the authentication of the users. For authentication PTP uses two protocols:

-CHAP (Handshake Authentication Protocol) the authentication protocol used to connect a user bears only offered by an Internet access provider. The CHAP periodically check to identify a client whenever the server will require the session to be performed.

-PAP (Password Authentication Protocol), for example the implementation of Windows 2000, the PPP frames are encrypted with MPE (Microsoft-Point-to-Point Encryption).

SSH is one of the most popular protocols used for opening a communication session on a remote computer. SSH encrypts all data automatically transmitted in the network, including passwords, binary files and commands for managing and automatically everything will be decrypted at the reception. Encryption is transparent: the user works normally, he is not interested in encrypting the messages sent over the network. Classification is done by threats that manifest the section:

“The following are some protocols currently being developed to deal with authentication and encryption on the WWW:

-SSL, Secure Sockets Layer [10, 11];

-SHTTP:http://www.commerce.net/information/standards/drafts-shttp.txt;

-Shen.http://www.w3.org/EN/WWW/Hand/secure-protocol.html;

-Kerberos protocol;

-secure electronic transaction (SET) (proposed by Visa and MasterCard);” [1]

Classification is done by threats that manifest section:

Authentication: target of a website is a method validation of the identity of a user, service or application.

Brute Force attack by automating the testing process to detect the user names, passwords, credit card numbers of the encrypted keys.

The authorisation: the attacks target of the web site is a way to determine if a user, service or application has the necessary permissions to perform the requested action.

Prediction credentials/session is a method for diversion of rights of another user or to pretend to be another user.

Insufficient authorization to access sensitive content or functions that should require more access control restrictions.

Insufficient Session Expiration allow to attacker to reuse previously allocated rights or session IDs for authorization.

-fixer refers sessions to the attacks on the abuse or exploitation connection users website.

When a user visits a website, it establishes a relationship of trust between the two sides. An attacker can use several techniques to exploit user trust. Forgery of content: tricking a user to certain content that appears on a website is legitimate and not from an external source. Websites scripting forcing a website to repeat executable malicious code that will load the user’s browser. Execution of commands refers to attacks designed to execute commands on remote websites. All websites are using forums of the websites for downloading data from users.

Often, the data provided by users are used to generate commands to receive some dynamic webpages. If the process is insecure, an attacker can change the order of execution.

Buffer Overflow attacks alter the flow of an application by overwriting a portion of memory.

Format String Attack alter the flow of an application by constructing LDAP commands from user-supplied input.

SQL injection: illegal building SQL queries from user-supplied input.

SSI injection (also called server site includes) the reference code in a web application that runs locally later by the web server.

XPATH injection builds a request from user input type – disclosures relate to attacks designed to elicit specific information system that hosts a website. Specific system includes software, version number and patch levels and or location backup and temporary files.

Logical attacks focuses on abuse and exploitation of web application logic flow application involves procedural logic flow used in order to achieve actions of recuperation of the password, accounts tenders and purchases are examples commerce application logic.

A website may require z user to perform a variety of steps to complete a particular action.

The attacker may be able to circumvent or to abuse by the harm a website and its users development of distributed web applications securely is a challenge.

In general, attention is focused on the following security requirements Authentication: identifying clients accessing the application.

Authorization’s controls provide access for clients.

Secure communication: messages remain private and aren’t changed by unauthorized entities.

NET Framework security system is governed by NSET usenet configurable rules called security policy.

Policy allows storing your end and administrator to adjust settings working conditions. The security policy defines four levels safety.

Policy level computer: a set of specific policies computers (Computer administrator).

User Policy: a set of policy defined by users defined by users for a single account login.

Detection and intrusion:

Since the set of preventive measures is not perfect, it is necessary to detect possible security breaches and to act to reduce their impact. Services included in this category are:

1.Auditing of security relevant events is a key operation in case of situations and to recover from security breaches. Security Audit is responsible for capturing, analyzing,
reporting, archiving and retrieving records the events and conditions of informatics solution.

2. Intrusion detection and screening policy insecurity is essential in making timely measures.

3. Integrity test is designed to determine whether or data recording system was compromised.

4. Restore security, if a security breach occurs, the system must be able to revert to what is known and trusted.

The study called “Secure communication for electronic business applications in mobile agent networks” by Woei-Jiunn Tsaur speaks about “the security of mobile agents and agent hosts in electronic business applications. We focus on the cryptographic, solutions for the confidentiality, integrity, authenticity, and non-repudiation in mobile agent networks environments. In order to protect the security of transactions in e-commerce, we propose an appropriate public key cryptosystem (PKC) for the mobile-agent based networks. The proposed PKC is constructed based on the elliptic curve cryptosystems. In addition, we further employ the integrated cryptosystems to design several security schemes for protecting mobile agents and agent hosts, such as the proxy signature, proxy authenticated encryption scheme and authentication scheme. The proposed schemes in this paper have the following advantages:

1. When verifying the validity of public key, it does not need to spend extra time to verify the signature in the digital certificate.

2. Verifying both a signature and the validity of public key can be concurrently fulfilled in a logical single step;

3. The security requirement of non-repudiation between customers and servers is achieved actually.

4. Both signing and encrypting a message can be concurrently accomplished in a logically single step.

5. A user can register only once to a system authority for many services.

6. The load of registration can be delegated to one trusted third party.

7. The host platforms do not maintain any database of user’s keys.

Furthermore, we also implement all of the proposed ECC-based self-certified public key cryptosystem and related security schemes to demonstrate our security requirements of confidentiality, integrity, authenticity and non-repudiation for protecting mobile agent networks in electronic business applications.”[6]

Vulnerability of systems can be defined as a weakness in the security system of an organization related to computer systems, which can be exploited by one or more threats, susceptibility to attack on the systems;

The key vulnerabilities in software systems and related hardware, network computers, storage data (hard disks or phones) electromagnetic radiation that can be intercepted, related to staff member (not only their employees, but management, the system administration and thirs parties who come into contact with the system). There is no system that is not vulnerable to natural disasters is a very serious problem for security and even continued operation of an organization.

There are the following classes of vulnerabilities:

1. Unauthorized access to resources;
2. Compromise of data confidentiality;
3. Unauthorized modification of data and application;
4. Blocking operation services (denial of services Dos);
5. Repudiation or denial of recognition of transactions made through networking;

The unauthorized access can be achieved by exploiting the following types of vulnerabilities:

1. The lack or effective mechanisms for authentication and authorization;
2. The proper management of passwords and the access rights;
3. Exploiting bugs (errors) uncorrected of existing applications running on networked systems;
4. Leaving unauthorized networked computers;
5. Lack of misuse of mechanisms to block the access in case of repeated attempts to connect;
6. No logging failed login attempts;
7. Use default access rights, or are generally to permissive users;

Compromising data confidentiality occurs when data is accessed, read or provided to a person who does not have this right. It occurs when someone obtain access to confidential information unprotected by proper cryptographic mechanisms or printed on paper. The main vulnerabilities that can be exploited for this proposes are:

- Improper configuration of access rights to files containing confidential information;
- Storage/transmission of confidential information no being encrypted; back-up storage place insufficiently protected;
- Printing unattended and improper handling of these children;

Unauthorized modification of data and applications:

1. Unauthorized modification of data and applications occurs when making additions, deletions or substitutions of unauthorized files or data stored in the package when they are sent over the network.
2. Modifications may be accidental or intentional and generally quite serious effects if not detected and corrected quickly;

The vulnerabilities that allow this type of attack are:

1. The lack of data integrity verification mechanisms;
2. The lack of tools to detect and protect against viruses;
3. Granting write access to users who do not generally need only read right;
4. The lack protection mechanisms for writing files;
5. Inadequate protection of transmission media;

Masquerade is attempting to claim that an entity is another to take its specific privileges. In the context of networks, masquerade involves elementary the ability to receive a message in the guide of legitimate recipient of the message and distinguish the sender to transmit messages to the destination. These attacks are done by intentionally changing addressing information in messages sent over the network or
via recording or replay network traffic and can be achieved by exploiting the following vulnerabilities:
1. Sending clear messages in the network;
2. Lack of tools to detect and protect against viruses;
3. Grant write access to users who do not normally need only read right;
4. Lack of protection mechanisms and writing files;
5. The lack of message authentication codes and digital signatures;
6. The lack of the mechanisms in real-time verification messages;

The blocking operation service (DOS denial of services):
A block function is a network service when that service can no longer perform tasks in an acceptable time. Blocking service operation can be achieved by exploiting the following vulnerabilities:
1. The sending clear messages in the network;
2. The lack of message authentication codes and digital signatures;
3. The lack of verification mechanisms in real-time messages;
4. The lack of timestamp to prevent replay attacks of messages;

Repudiation or denial of recognition of transactions made through the network creates serious damage to the parties involved (such as the situation of a bank check, denied coverage because no account, but simply because the bank has its authentication tools).

The degree of vulnerability A has the following consequences—unconditional access of some bad intentioned users.

The degree of vulnerability B allows to local users in general to increase their privileges and to obtain the control over the system.

The degree of vulnerability C allows to users to alter indoor or outdoor machining processes. Obvious, is the absence of independent sources stabilized power supply UPS (Uninterruptible Power Supply) which can lead to loss of files to work even damage computer systems in case of high-frequency fluctuations or power supply and—even certain licenses purchased for a single installation.

An actual classification is done vulnerabilities but to every organization, for each activity according to the impact it would have some threat that could exploit that vulnerability classification by levels determined following an operation called “vulnerability assessment”.

“Current Internet communications security is typically provided by the integration of secure transport functionality into client and server software. Two problems arise with this approach: Firstly, the use of integrated security services requires modification to the existing Internet applications, requiring re-development and re-deployment projects. Secondly, high-level security services such as authorization are not provided by secure transport protocols, requiring applications to rely on customized (and often insecure) mechanisms for the provision of such services. We propose a platform-independent system that uses proxy applications to provide both secure transport and authorization services transparently to existing and widely used technologies. We discuss the merits of our architecture in the context of the intended deployment environment: an Internet-based heterogeneous private network such as an extranet or Virtual Private Network (VPN). We show that our approach achieves its goals at the expense of introducing a minor degree of performance loss into overall client-server communications, yet we maintain that this performance loss is a minor expense in relation to the advantages of the system as a whole” [5].

The threat represents a potential cause because of an unwanted incident which may cause damage to a system or organization and its assets, exploiting existing vulnerabilities in the system or organization.

The threats generate unwanted incidents, events or accidents damaging effects can be very large impact on the organization. There are threats that cannot be eliminated, they can only be known and can take steps to avoid or minimize their effects.

The groups of information security threats can be grouped into three main categories.
1. Natural and physical disasters: earthquakes, floods and fires;
2. Legal information theft, financial fraud, unauthorized internal access, obedience phones, intercept messages, penetration systems, employee sabotage, theft, mobile computing devices(laptop computers), malicious;
3. Technological DOS (Denial of Service) due to traffic overloaded, loss of power supply, power surges or fluctuations frequency;

Natural and physical threats come from natural phenomena or other physical elements that interacts with computer systems or networks. May be started here earthquakes, floods, storms, lightning. It can work towards minimizing or even eliminating their threat. You can install warning devices in case of natural disasters or devices to eliminate their effect. People come from an accidental threat (unintentionally or intentionally). These incidents can cause havoc on computers because even negligence in handling various components, insufficient professional training, insufficient reading documentation, etc.

Because of in attention a user can destroy the transport support memory may overwrite data in a database or delete data which it considers unnecessary to understand not what is used. A system administrator (local area network) can modify the security level of a user or change or cancel the passwords to some vital information.

All people can come from intentional threats with ill will may be internal or external. Internal threats come from our employees who have access to information easier, with fewer barriers of the past and knowing some of the company’s security policy. External threats coming from - several categories, namely:
- the foreign - intelligence agencies;
- terrorists and terrorist organizations;
- the criminals;
- raiders;
- hackers and crakers;

Foreign intelligence agencies have every incentive to get hold of information on new technologies. High-tech manufacturing companies are targeted attacks coming from them. It is
necessary that these organizations use technology and highly sophisticated encryption software to protect information. Organizations terrorist watch especially where banks can extract funds for terrorist financing, the airlines to divert planes and take hostages and then negotiate a ransom or other demands, where NGOs can inform the police action, the government or international forces on them. Criminals are considered those who, with knowledge in computer science, using blackmail to extort money under threat of destruction of information systems target or disclosure of secrets. Organizations register their different daily information on storage media.

One of the biggest threats to information security in computer systems is the viruses into systems that infestation so called computer viruses. The general concept of computer virus is describing different types of attack on computers.

A computer virus is a malicious code, a potential harmful piece of software that copies itself into other programs and modifies them in order to failure.

This malicious code will launch the operations that will have an effect on data security in your computer. Malicious code is a met as a remedy, program vagabond, vandalized harmful or potentially harmful software. The malicious code will help to identify the virus by creating so-called virus signatures.

Because malicious code that exists in computer systems has different action due to the construction code, malicious code can be grouped into several categories: viruses, worms, Trojans, bombs, hidden or secret ways, spoofer’s, hoax, other types of malicious programs.

Malicious code can have behaviour to aggregate behaviour of several programs. In this category are included hybrid viruses. Because this behaviour is hard to define what category it belongs. Important classification but not protect against their installation and especially antivirus programs.

Virus itself is a piece of program code that copies itself into a large number of programs, so that a virus is an independent program. A virus executes its program code only the host program, it is submitted, it realised into execution. The virus can immediately reproduce and infect other computer programs, or wait, depending on how it was programmed, a specific date or event on which to multiply. Virus Friday (Friday 13 th Virus) to launch the any day of the year is Friday and was the number 13.

A virus can infect both internal memory and mobile devices introduced in computer viruses. Hence, it can spread memory media (floppy disk, CD ROMs, cassettes and tapes, pen drive and flash drive), network and modem connections. Many viruses spread by flexible discs.

A worm is an independent program. It reproduces by self-copying from one computer to another through network in most cases. Unlike a virus, a worm does not alter or destroy computer data, but can cause malfunctions in the network by using its resources for self-production. It’s multiply using file transfer mechanisms, such as Internet or e-mail.

The notion of worm was first introduced in 1975 by science fiction writer John Brunner in his book “The Shockware Rider”. The author describes a program named “tapeworm” that “lives (inside the computer, the computer multiplies the computer as long as there is a network connection). It was developed in the early ‘80s by researchers at the XEROX Research Center. The type worm designed to multiply from one computer to another. Definition of initiatives: a program it is found in one or more computers. “One significant example of worms which has attracted much media attention is the Internet Worm. The Internet Worm, which was activated on the evening of 2 November 1988, spread to thousands of systems on the Internet and brought them all down”. [1]

A Trojan horse (sometimes using the simple name Trojan) is a piece of code that hides inside a program and will run an operation hidden. A Trojan horse is the mechanism used to disguise a virus, worm or a secret door (BO). A Trojan horse is the mechanism used to install programs or destructive attack. The idea of using such programs comes from the mythology of the Trojan horse but left the gates of Troy and that the city was destroyed.

A Trojan horse will hide a popular program or a function call which creates suspicion user but will launch illegal operations. The user can throw an apparently harmless program but it has a built in unauthorized code.

Unauthorized functions performed by program code included can launch a virus or a worm.

The classic case of a Trojan horse attack is described by Dennis M. Ritchie. An attacker creates a program that captures passwords (password grabber). It displays on the terminal screen prompt: login. Once entered your username and password, they are taken the Trojan horse programs that certain copied or sent to a destination where they can be read. Login screen is displayed incorrectly and the user, thinking that he mistyped account or password, re-enter the known combination. Thus were captured user account password without it suspected.

There is a special category of Trojans that are created as intruments of destruction. This category includes PC Cyborg Trojan horse. It hides in a program that provides information about AIDS viruses.

After the system is installed, edit the AUTOEXEC.BAT file and will count how many times it turns the infected system. After a predefined number of starts, usually 90, the Trojan hides folders and encrypted files names on disk.

Another type of Trojan, distributed through Usenet network and through e-mail, called AOLGOLD will install an archive from a program like an improvement. Usenet but actually wipe the hard drive a number of directories including: C:\DOS, C:\WINDOWS, C:\WINDOWS\SYSTEM.

Other examples of Trojan horses:

- Whalck a Mole-of a game that contains an executable file and is an archive WinZap autoextractive which is a program that represents a distribution which for execution NetBus you launch each time the computer;
- BoSniffer is actually a tool that claims executable and unpack multiple files or run them in a remote and can include files to the commands and scripts, allowing attackers to create custom attacks in the system. Can operate under any name charge;
- Windows NT FPN WCLNT.DLL is a library that is installed on NT servers passwords NovelNetWare systems. This DLL intercepts password changes before being encrypted and written in SAM, allowing NetWare services to obtain a visible password. There are Trojan horses that not leave traces of their presence, not create detectable damage, may live forever in programs and can self-destruct before being detected.
A bomb is a type of Trojan horse to launch a virus, worm or other type of attack. A bomb can be a standalone program or a piece of code that will be installed by a developer who will work on a certain date or when certain conditions are met. Technically, there are two types of bombs: time and logic. A time bomb is activated when running a specific time of installation or when reaching a certain date. A logic bomb will act when they meet certain conditions imposed by the one who created it.

Other potentially harmful programs are: hidden paths, secret paths, spoofer and hoax.

Hidden Pathways (Trap Doors) are points of entry into the system software designers left intentional to test and monitor programs or, in case of refusal of access to debug subroutine can access. Trap doors are used during testing and the removed when the software is delivered to the user. Normally, an entry point type Trap Door is activated by the person who created it. But there are cases when these points are discovered and exploited by malicious people.

Secret keys (Back Office-BO) can be created using Trojan horses. The mechanism involves placing in the target computer in a program when then open the access roads to resources. It represents intruments of administration of distance for Windows 9.X. It was released in 1998, at the Congress of Security Issues and allows the administration and control almost completely from distance, including the possibility to add and remove registry keys, reinstalling the operating system, to send and receive files, to view passwords stored in cache, to initiate processes and create partitions file. BO can be configured to install and run in any file name.

A year after launch there is a new version of “Back Office 2000” which featured original, with two exceptions:

-both the client and the server runs on Windows NT/2000(not just Windows 9X);

-program dispose of a set of development tools that allow for customized variations extremely difficult to detect;

NetBus is another type of BO, a variant with faster and simpler interfaces than the original BO, but with better and efficient features such as the remote control chart. It is a very adaptable configuration between versions that circulate on the Internet.

Of operations that will be carried out it mentioned:
1. launch on operation to scan ports victim’s system;
2. retrieving cache passwords of applications;
3. printing;
4. located remote reboot( forcibly or fresh);
5. mouse diversion;
6. remote-spy of applications such as: Yahoo Messenger and AOL Instant Messenger
7. opening a web browser and go to a website user defined;

Spoof is a generic name given to programs that allow to a user using some artifices of calculations, have access to information in the system. In general, spoofer, they are possibly by suing mechanisms that will enable Trojan horse programs that allow access information.

Hoax (Joker) are messages sent by e-mail with lase warnings about existing virus and requiring all persons known to be altered. Sometimes these warnings contain attachments that are designed, apparently to stop or eliminate the alleged virus. Resending the message to other destinations makes the virus to multiply without its creator to design it to multiply.

Besides these sequences malicious code that may affect the security of computer systems is also met:

-bacteria;
-rats;
-crabs;
-crawling;
-salami-slices;

Bacteria are programs that do not create damage, but can simply copy them to lower the operating speed of the system. They can multiply in internal or external memory and thus limit its workspace.

Rates are a special category of programs that reproduce very quickly and very strongly affecting speed.

Crabs attack with predilection monitors computer systems. Desktop wallpaper images will be cropped or illegible.

They do not cause damage. There are known situations when these programs destroy physically computer equipment.

Creatures have the same structure and the same behaviour as worms.

Slicers cut small portions of data. A slice salami attack type will alter one or two decimal places in a file.

The life cycle of a computer virus:

As you can see, not evey malicious program is virus. However the name under which the computer virus is known and it annihilates programs are known under one name antivirus program.

For all “malicious programs” apparently behaves like a biological virus, received the generic name of computer virus.

Like biological viruses, computer virus needs a host to infect, to reproduce, to spread. This home consists of information stored on the memory media. Most viruses infect program files, in the case bears the name of the virus files. When the infected file, the virus carrier, is launched in the execution of a user who does not know the existence of infection, the virus code is autocharged computer’s internal memory is executed code, then look for another file that is infected and it copies itself to. Action of a computer virus is developed step by step, as allows:

1. Program containing the virus is launched in execution;
2. The virus code is loaded into internal memory (RAM);
3. Virus code execution is launched;
4. The virus copies itself into other programs;

2. VIRUSES-FILE, BOOT, MACRO, SCRIPT, E-MAIL, CHAT AND INSTANT MESSAGING

Computer virus life cycle resembles that of biological counterpart and depends on many factors, including:
aggressive virus, how to conceal it, its detection by the host’s vulnerability to viruses that, quality antivirus (antidata) and its actions. As in real life, correct information to people has a great contribution to eradicating it and to limit the consequences of viruses.

The life cycle of a virus include: creating, copying, pasting multiple computers, activation, detection, assimilation and destruction.

Mode of action of some computer viruses

The most behavior of virus malicious programs with “standard” can be grouped into several categories, depending on the “host” carrier. Viruses meet:

1. file;
2. boot;
3. macro;
4. script;
5. e-mail;
6. chat and Instant Messaging;

File viruses:

These viruses are the most common and most destructive category. File viruses sometimes called software viruses, malicious submit their software to a file.

When the program is launched into execution the virus copies itself to the shared memory computing system and launches its own program execution and carbonless destruction.

Need to distinguish between viruses that affect file type document files.

Action of a virus file is done in those successive steps:

1. The user launches the application execution. He does not know the file application is a virus;
2. Malicious virus code is loaded into the internal memory on the computer system. The virus takes over control of execution;
3. The virus copies itself into other file;
4. Virus launches program for which it was designed;
5. The host takes over execution;

Overwrite malicious host program early is not often used because in this way, the host program will function abnormally because after ending sequence of the virus inserted code will proceed to execute the host program a sequence which can lead blocking execution and create suspicion on proper operation of the computer;

Go to the end of the program viruses into the host supposedly at the top of the host to be an unconditional jump to the end of the file where the virus is attached malicious code.

After virus code is executed to jump back to the beginning of the the program host. In this way, the host program will work without lock. It done but in this case, an increase in file size which host the user can create suspicion cleaners will take action;

Viruses by overwriting the data resulting from the execution – host program is virus by inserting malicious code in the reserved data without affecting the operation of the program in this may. This malicious is harder to detect because it does not affect the size or content host program;

A file virus is considered to be static or polymorphic. A virus can “adapt” to certain conditions offered by the host computer or file. This virus is called adaptive virus. A file is considered to be static if during its existence, does not change the structure of the code. Code remains intact regardless of the number and extent of infection created.

File polymorphic viruses are able to change their “signature” when you multiply by a computer system to another. Because of this, these viruses are very difficult to detect, causing therefore the biggest disasters.

Overwriting viruses rewrite (overide) host program with their own program. In this way, the program did not have host and is functional.

The type viruses Entry-Point Obscuring use an ingenious method of infecting the host program. The host program will introduce only a small sequence of program that, when certain conditions, will launch the virus malicious code found in another location. Execution of the program will not involve host and execution expecting it to proper conditions to launch destructive program.

Company viruses do not directly attack the host file, but creates a copy which will launch the original instead. In this way, execute the original file formatting memory media be cloud and renamed format.com into format.exe. The latter file will actually contain the virus. Company may modify viruses and ways (paths) network access so as to give reference to cloned files.

The link viruses not only on a small scale change program content host. At the beginning of the program will be installing a host jump instruction (GOTO, JUMP) at location outside the host that will contain the virus code. The action is similar to that which describes in the modes of infection by jumping to the end host program or overwrite data from host program execution.

Viruses OBJ, LIB and source code are not spreading so great. They infect object modules (OBJ) compiler libraries (LIB) and source code of the host program. The utmost, however, file viruses affect executable file (with extensions exe, com).

The most known viruses in the file are: CASPER, CHERNOBYL, CRUNCHER, DIE-HARD2, Fun Love, Jerusalem, Junkie, Magistr, Natas, Nimda, OneHalf, Plagiarist and Vienna.

These viruses can infect the boot sector on flexible discs flare. On usually infects the MBR (Master Boot Record). Could be very destructive and lock the computer during system boot operation. They can also destroy all the information on disks, usually during system boot operation. They can also destroy the information on disks, usually from your hard drive. Currently there are over 100 known viruses, these viruses or boot options. Unlike other types of viruses, they have limited action due to action due to limiting the use of increasingly less flexible disc.

The only way a boot virus infection is to lead the operating system from a mobile storage medium containing a boot virus or pirated previrusated Windows. This support, in turn, they have limited action due to limiting the use of increasingly less flexible disc.
The only way a virus infection boot is to boot from a mobile storage medium containing a boot virus or pirated medium containing a boot virus a pirated Windows previrusated.

This supports in turn, they have limited action due to limiting the use of increasingly less flexible disc.

The only way a virus infection boot is to boot from a mobile storage media that contains a boot section virus or pirated Windows previrusated. This support in turn was infected computer that contains a boot sector virus.

When starting the computer computer system is running normally following actions, in the loading (boot):

- BIOS launch the instructions POST (Power On Self Test);
- The BIOS reads system configuration information refered to it in CMOS memory computing;
- BIOS examine the first sector on the hard disk master boot record on floppy disk;
- The BIOS passes control to the boot sequence or boot record MBR;
- The load examines partition table to determine how many logical disks containing physical disk;
- transfer the control file group system;
- the loading-drive system and the operating system is starting execution;

When the system is infected with a boot sector virus, the boot is changed significantly, like this:

- is launches the BIOS POST instructions;
- the BIOS read configuration information from CMOS memory computer system;
- BIOS examine the first sector of the hard disk master boot record or boot record area on floppy disk;
- the BIOS passes control to the MBR boot sequence or record that contains the virus code (virus);

Flexible malicious virus boot disk is done by overwriting the existing code in the boot sector. With that of the viruses;

Flexible malicious virus boot disk can be done in three ways:
1. Virus will overwrite the MBR code;
2. Virus will overwrite the boot sector;
3. Virus will change your boot sector to an address that will contain the virus code;
4. Virus will move, in most cases, the original boot sector into another disk free zone;

The virus will move in most cases, the original boot sector into another disk free zone. For this reason removing the virus and its effects on hard disks can be achieved by hidden DOS command FDISK/MBR executed from a bootable floppy disk, fully virus –free which contains this commands.

Once released into execution, the virus remains in memory and will infect resident flexible used discs.

This group of viruses has a different mode of action than other viruses of the same type, such as viruses due occupy the same area of the disk, MBR or boot sector viruses cannot exist more on a boot disk virus last installed it will delete the existing one disk.

The most famous boot viruses include: Frankenstein, KULROY-B., Matthew, Michelangelo, Parity, Stoned.

Macro Viruses

It is also called macro viruses. They infect files document type. Not to be confused with viruses that affect executable files. Macro viruses stand to take place as a way of spreading physical boot viruses. If the boot sector viruses spread through documents electronically transferred between users against boot sector, macro viruses aremore numerous, reaching a total nearly 5000. For document type affects file that are portable across different platforms-system can detect both for Windows and Macintosh systems. Paradoxically, the first macro virus called concept was contained in the documentation CDROM websites and software applications offered by Microsoft Windows 95 Software Complexity Test”, “Microsoft Office 95 and Windows 95 Business Guide” and “Snap on Tools for Windows NT CD”.

A macro virus will use the facility to create macro commands to facilitate its work, the virus will use their feature to spread and destructive their goal.

The virus exploits a self-application execution macro execution command macro virus containing malicious code can delete or edit portions of the text, delete or rename files, to multiply and create other types of damage.

Many virus copies itself normal.dot macro is launched in progress in Microsoft Word whenever a document is opened. In this way, the new document open will be infected.

Micro viruses affect DOC and DOT files with extensions created by Microsoft Word, XLS and XLW created with Microsoft excel, ADE, ADP, MDB and MDE created with Microsoft Power Point Access created with Microsoft Access SAM created Lotus Ami Pros CSC created Roler Photo Paint.

The prevalence of microviruses are those that affect Microsoft platforms, not because the platform is more vulnerable than others, but because most documents are created with it.

Operation of a macro virus is run step by step, thus to:

1. file document is opened using an dedicated application;
2. the document is loaded into memory. Loading into memory, with the document and macro execution. The virus is loaded into memory.
   -the virus will copy your own macro in standard initial template;
   -virus will copy your own macro is standard initial template;
   -virus -destructive program launches;
   -the most known macro viruses are: Atom, Colors, Concept, DMV, Format C, Gala, Hot, Melissia, Nuclear, Ppoint, Attach.

Macro Viruses

It also called macro viruses. They infect files document type. Not be confused with file viruses that affect executable files. Macro viruses stand to take place as a way of spreading physical boot viruses.

Against boot sector, macro viruses are more numerous, reaching a total nearly 5000. For document type affects files that are portable across different platforms-system can detect both Windows and Macintosh systems. Paradoxically, the first micro virus called concept was contained in the documentation CDROM websites and software applications offered by Microsoft Windows 95 Software Compatibility
A macro virus will use the facility to create macro commands to facilitate its work. The virus will use this feature to spread and destructive their goal.

The virus exploits a self-application execution macroexecution is launched automatically when the document is opened. Launched execution command macrovirus containing malicious code can delete or edit portions of the text, delete or rename files, to multiply and create other types of damage.

Many virus copies itself to the file normal.dat macro is launched in progress in Microsoft Word whenever a document is opened. In this way, the new new document open will be infected.

Micro viruses affect DOC and DOT files with extensions created by Microsoft Words, XLS and XLW created with Microsoft excels ADE, ADP, MDB, and MDE created with Microsoft Power Point Access created with Microsoft Access SAM created Lotus Ami Pros CSC created Roler Photo Paint. Operation of a macro that virus is run step by step, thus to:

1. file document is opened using an dedicated application;
2. the document is loaded into memory. Loading into memory, with the document and macro execution. The virus is loaded into memory;
3. the virus will copy your own macro in standard initial template;
4. virus will copy your own macro in standard initial template;
5. virus-destructive program launches;
6. the most known macro viruses are: Atom, Colors, Concept, DMV, Format C, Melissa, Nuclear, Ppoint, Attach.

Script viruses:

These viruses are created using scripting languages or scripting languages that are used to writing programs and operating systems to create Web pages.

The difference between scripting languages is that, from the programming languages C and Visual Basic scripts are less complex. The script is actually a program code written in a scripting language. Script instructions are creating increasingly more viruses with them.

VBS file contain intructions actually writes. Simply use a text editor to reach a Windows Notepad or Word Pad to write instructions and ultimately save the file with VBS. Launched execution file launches its destructive code. A script virus can easily modified using these tools. The result will be a new variant of the virus.

It can make the observation that a macro virus is actually a type of virus script, macro language as in currently scripting languages.

Activation of these viruses is done through Microsoft’s Windows Scripting Host Windows Operating Systems, or when a document containing the virus is opened or viewed.VBS or JavaScript, HTML, MIME, PHP.

E-mail viruses

E-mail represents the most used Internet application today. The benefits are obviously very high, but there are equally large reversal, because through e-mail are transferred the most informatics viruses. The possibility to use electronic e-mail by sending viruses was made by developments in technology. The first e-mail message was sent and received in clear text (plain text) without the possibility of being able to insert a virus in the post. Only that technique envolved when developing the transition from plain text to HTML e-mail, when where possible different writing fireworks (color, shape, size of characters).

An e-mail in HTML format is as a Web HTML page. And an HTML WebPage has incorporated ActiveX Controls and JavaScript applets that can contains malicious code. Viruses that are transmitted by e-mail are not actually viruses and script viruses standard acceptance. Another way is transmitting a virus is attaching the file in a plain text message.

For the spread of viruses through e-mail are used in main way three ways:

- by attachments, using Trojan horse technique;
- by incorporating malicious code in HTML;
- spreading the viruses by injected files at the text messages is the best way and most common used. If the recipient does not launch execution file containing the virus nothing happens.

But if you go to his execution when the code is executed destructive virus and the virus will accept operations for which it was designed, it will multiply and spread. Generally users who have minimal knowledge about viruses, it will open a file or sent unsolicited by an unknown person. But there are situations when the virus took address Address Book user to another user's known, but has computer viruses. And if the message contains an infected file that comes from a friend might be that the user opens it and infection to occur.

Trojan horse technique is used to hide malicious files. The vast majority of email users do not open files with the extension exe or com even if they come from a single source. And then the virus comes as Trojan horse, changing the extension to food the victim.

Extensions TXT and JGP are more reliable in this case. Files with these extensions can not contain viruses . Exe, jgp (you can see two extensions) can be opened by a careless or uninformed user and run the virus.

Security vulnerabilities exploited by viruses to multiply are present mainly in email programs for Microsoft Office Express and Microsoft Outlook and Internet Explorer. Transmission standard developed attachments emails automatically open attached messages. Transmission standard developed attachments emails automatically open attached messages. This allowed the creation of e-mails in HTML format that contains a malicious executable attachment. Internet Explorer read as one wrong attachment and opens automatically.

This type of attack is called MIME exploit (MIME operations. MICROSOFT has filled this gap security and email programs do not allow such attacks.

Incorporate malicious code in HTML email messages is done by writing JAVASCRIPT code. These code will run automatically when the message is viewed without further need for the infection to occur through infected attachments. Against infection with attachments when the user is not open the attachment and infection file not occur, this infection occurs, and infection occurs automatically when you view the message.
This method of propagation has the best chance of success, but requires advanced knowledge and incorporated code in e-mail. Because of this infection in this way is quite rare. In the category of e-mail viruses are distinguished: 666test, Babydona, Badtrans, BubbleBoy, FreeLink, Hard, Hybrys, KakWorm, Kletz, LoveLetter, Mellisa, Monopoly, MyLife, NakedWife, Nimda and VBS/SST.

Service chat conversation is provided by specialized servers in a subnet called Internet Relay Chat (IRC). This allows to or more users to discuss individual or group and change files between the new using a communication channel.

The users of a particular channel is called the new channel members. Transmission Protocol used is DCE (Direct Client to Client Protocol).

User can using a program such as MIRC(Microsoft Internet Relay Chat) to connect to a chat server and to initiate a group of discutions.

Using this environment created a virus to multiply and infect your computer in the network can in two distinct ways:

1. by transfer or infected files between users;
2. infection by transfer or infected files between users;
3. using IRC scripts;
Infection through infected file transfer between users is quiet simple.

The attacker sends a file to the target and this would be useful to the recipient. It can be a help file, a utility, a little game, a documentation file or image. Once the recipient opens the file sent virus will activate and will launch their destructive.

The infection using IRC scripts involves writing scripts that will contain instructions to be executed sequentially. Once accepted by the recipient or recipients, these scripts will automatically substitute similar files the target computer and will initiate the attack. The infection by transfer or infected files between users is quite simple to achieve. The attacker will send the target one file who wants to be useful recipient. Most infections happen when, following the attack, it will create the file in the current the folder mirc.ini script.ini or MIRC. They contain scripts and execute commands that have been projected.

Installation of these scripts and execute commands that have been projected. Installation of these scripts is possible if the auto-configured DCC-Get it on. Being active will accept all files sent by users in chat channels, respectively. For greater certainty, this option will be set to inactive.

The most known viruses IRC are: Acoragil, Back Office, Bat, Dmsetup, Flood, Phono, Goner, links, Millenium, pIRC Events, Script.ini, Simpsalapim, Stages.

Instant the Messaging programs used today, AOL Instant Messenger (AIMS), MSN Messenger, Windows Messenger, ICQ and Yahoo! Messenger are also subject to attacks.

Using this software, users can send instant messages and file as well. In this way can transmit viruses. Only, unlike other programs that allow and receive files over the Internet without user permission, here the user can accept or file that is designed for.

A computer that participate in instant messaging to the virus can not unless the user has given accept to download and user has given accept to download run or view a file that it is intended that contains the virus.

Instant messaging programs are generally used by people who really need this service and that time does not allow them to sit it unnecessary conversation. Messages are sent between users trust (most of them knowing the physical to the chat service, where often users of a channel are not known, and more dubious identities.

Viruses in this category have the characteristic that they are committed network IM service. If a virus is designed to work in a network of Yahoo! Messenger, it will work in MSN Messenger Network.

The most important viruses in this category Choke, Gender, Hello, Reeza, Stage. The most important viruses in this category Choke, Gender, Hello, Reeza, Stage.

Virus hoax

They are a special category of viruses that rely on creditul man who may become the target of an attack. E-mail or windows appear while browsing you like “You won a trip…”, “You have won a sum of…”, “Your computer has a virus…”, “Send these message to all your acquaintances and you get lucky…” with the invitation to allow or confirm with “Yes” are quiet common on the Internet. Sometimes this type of viruses, especially those that appear in Windows browsing works even when you choose the option No. For this reason, it is advisable to close the option Windows Close (X), from the Taskbar->Close, or by pressing ALT+F4 key pair.

The most important viruses in this category are: Blue Mountain Card, Good Time, Help, Rit Takes Guts to Say “Jesus”, MusicPanel (MP3), New Pictures of Family, New Ice Age, Pretty Park, Sulfinbk.exe, VeryBad, Mobbler, WTC Survivor Virus.

In the study “An economic mechanism for better Internet security” by Xia Zhao, Fang Fang and Andrew B Whinston is examined the Internet architecture and address security issues from an economic perspective. We propose a certification mechanism to induce SPs to exert collective efforts and improve Internet security. To be more specific, the proposed mechanism provides certified SPs incentives to deploy regulatory practices. We use a game-theoretic model to examine the efficiency of our mechanism. The result show that our mechanism can increase the efficiency for all Internet Service Providers. By providing SPs with appropriate incentives, our mechanism can create a better communication environment over the Internet.

The challenging issue is, who should be the certification provider? The certification provider can be a non-profit institution, such as Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a central authority with limited power in the essentially decentralized and neutral global network. However, its functions are restricted to running the addressing system, giving out blocks of unique identifiers to countries and private registries. Commentators have suggested ICANN should play an enhanced role in governing the unregulated Internet. By providing certification services, it introduces a soft regulation to the Internet, characterized by the fact that participation is voluntary, and participants choose their actions based on self-interest. The certification provider can also be a for profit organization. The previous analysis examines the certification provider’s profit and discusses its impact on the overall efficiency level.
One concern on our proposed mechanism is that if the certified network completely blocks inbound traffic sent from the non-certified network completely blocks inbound traffic sent from the non-certified network, then the overall network is suffer. Our result shows that blocking is an optional strategy in the separating outcome only if the value of communication Vis relatively low compared to the disutility caused by the malicious attack. In the pooling outcome, everyone will join the certified network and “blocking” is only a threat to those who deviate. Alternatively, we suggest the certified SPs consider strategies such as slowing down the incoming traffic sent from non-certified networks to deteriorate the non-certified SPs’ payoff. However, due to the network interdependency, the certifies SPs will also suffer from such a strategy. How to provide the certified SPs proper incentives to “punish” those non-certified ones deserves further study.

The paper characterizes the effectiveness of security practices using a simple parameter, x, representing the false negative. In most control settings, both false negative and false positives are used to describe the effectiveness of security practices. Since regulative practices generally outperform protective practices in reducing errors, the analysis and results considering both false positive and false negative will be similar.

The implementation of the certification mechanism may generate extra overhead to identify the service providers’ certification status. We ignored such an impact in our model by assuming that the size of overhead is negligible compared to the regular traffic. In situation that the assumption does not hold, we suggest the certification provider to adjust the subscription fee to accommodate the overhead cost. Although the overhead will create a deadweight loss which reduces the value of the certification mechanism, the loss is inevitable as no security mechanism is free. Giving the rising concerns on security, the overhead should not stop the implementation of the certification mechanism.

The main contribution of our paper is to propose a new incentive framework to the management of the network security. Compared to the current Internet infrastructure which is open to everyone and consequently leaves everyone exposed to the security risks, our vision of the Internet is one where all the active parties 9e.g. the service providers who cannot afford to make such an endeavor under certain conditions. Such a proposal may sound controversial from an idealistic point of view. However, it can induce those competent service providers to take more actions in safeguarding the Internet, providing the individual users a worry-free environment. Our analytical results prove that the framework produce efficiency for Internet communication”[7].

5. CONCLUSIONS

In conclusion, we have spoken in this article about the electronic security of the computer networks, that refers to the totality of the policy recommendations and actions required to minimize the risk associated to perform electronic transactions, the risk refers to the branches in the system, intrusion or theft of any means, technique or process used to protect the information system. The confidentiality, integrity, availability, compliance with laws, regulations and standards, that are fundamental security objectives, which are among the requirements of a business environment. The security requirements that must be fulfilled for e-business environment are: identification, authentication, accountability and audit. Security audit records dealing with the analysis of the activities performed if the protection system is in accordance with established security policies and procedures.

6. AUTHOR’S DESCRIPTION

Andreea IONESCU graduated from the Faculty of Cybernetics, Statistics and Economic Informatics of the Academy of Economic Studies in 2008 (Bachelor’s degree) and Master of E-Business in 2010. She is university assistant in computer science at The Faculty of Economic Studies at Hyperion University of Bucharest. She is currently a PhD candidate at Institute from Bucharest, in Economic Informatics Field. Her interest includes: e-commerce and project management.

Raul Serban has graduated the Faculty of Automatic, Electronics and Applied Informatics at Hyperion University from Bucharest in 2006 (Bachelor’s degree) and master at Hyperion University at the Faculty of Economic Science. He is currently a PhD candidate at the University from Pitesti at The Faculty of Exactly Sciences and Aplicable Informatics. His interests includes: e-commerce, databases and project management.

7. REFERENCES


