Analysis of security protocols in the information system

Claudia HLOPEANICOV
Academia Militară a Forţelor Armate
„Alexandru cel Bun”
mun. Chişinău, Republica Moldova
claudia.hlopeanicov@academy.army.md

***Abstract* – The standards are essential to ensure interoperabilitz protocols worldwide. They are divided into two categories: standard de facto and in law standards. De facto standards were not originally approved by any institution but they were adopted due to the spread and use them widespread. Instead, in law standards are approved from the moment of their creation by a competent international body.**

***Keywords* – security protocols, standard protocol, information system, information security.**

I. Introduction

The potential of the information society is growing due to technological development and multiple access routes. In this context, the good development of business security systems require an information system functional. The security management of information systems are a key factor in the effective exercise of an institution for the protection of data and conducting electronic transactions. They can be counted among the main tchnical means implemented of modern society institutions whose activities can not take place optimally withouta well developed system: antivirus, data backups, training on the importance of implementing security measures and prosecution.

Although the variety of crimes in the information society is high, even if it will be even greater as techology will progress, the following are the most common criminal offenses: computer fraud, false information, data or facts detrimental computer programs, computer sabotage, unauthorized access, unauthorized interception, software piracy, computer espionage, etc.

Within less than a generation, the information revolution and the introduction of computers in all spheres of life have caused many changes in modern society. The world is gradually turning into a global village, where there are no borders for business, communications and trade.

After choosing the transmission medium, be it in telegraph cables or an optical fiber, we need to establish a set of rules for its proper use, that defines how messages (data) are coded, how a transmission is started and ended, and so on. Must be avoided two types of errors: a set of rules that establish rules incomplete or contractory.

II. General Concepts

Expanding the use of computers in almost all areas of life and connecting computers into the international networks has made the crimes committed by or through the computer to be more diverse, more dangerous and more frequent in international environment. An analysis of the factors generating criminal actions showed that communication networks and modern computer have specific characteristics which are very useful for criminals and involves serious difficulties for potential victims as well as law enforcement (complex issues of systems security, diversity of hardware and software, lack of experience of many users, anonymity of communication, encryption and international mobility). Groups acting in the field organized crime, economic espionage and worldwide intelligence services already exploit these new criminal cyber actions. Many governments, business people, many users do not realize the danger to which are exposed by these new conditions of committing crime, nor cyber-crime protection significance, or technical and legal ways to counter the threat of criminals.

Information system means all data, information, information flows and information of circuits the treatment procedures and information designed to contribute to status and the institution’s objectivs.[1]

The role of information is to transmit information between different elements. For example, in an educational institution, the role is to ensure the information system of governing people with information to make important decisions or various other reasons. In the framework information system, most activities can be conducted with the help of computer technology.

[1] www.wikipedia.org

Information systems are threatened from both internally and externally. Could be well-intentioned people who are making different errors in operating or the malicious people, who sacrifice time and money to penetrate information systems. Among the technical factors that allow security breaks may be some errors of communication software, different computing or communications equipment faults. Also, lack of adequate training of the administrator, operators and users of systems increases the probability of security errors. The abuse of some systems (hacking and cracking) is also one of the major risk factors for informationa systems security.

The information security is a vital issue for all internet users, whether service providers whether users. The growing need for communication, on the one hand and the need for protection and information security on the other hand are two different and even opposing requirements that must be secured networks and information systems.

The information security has become one of the major components of the Internet. Relatively new field of information security is looking for technical solutions to resolve this apparent contradiction. Speed and efficiency of communication of „instant" documents and messages provides numerous opportunities for attacks in a modern society based on competitive economy.

And especially the nature of security should be an object of careful analysis in case of networks. Networks are complex assemblies of computers. It is verydifficult to obtain a complete scheme of all existing entities and operations at a time, so that networks are vulnerable to various types of attacks or abuse. Complexity is caused by geographical dispersion, sometimes international, of network components, involving several organizations in administration of a single network, existence of different types of computers and operating systems, existence of large number of entities. In the near future, computer networks will become an essential part of social and individual life. Activities of government, business, commercial, industrial and even personal activity depends from the correct functioning of network. As the personal computers can be connected from home in networks, a number of activities can be done by individuals. Should be considered data types that people can read, which are the other persons with whom they can communicate, to which programs they have access. More information stored in files become possible to correlate through the networks. This association to filles can have adverse consequences on individual/private character of information. Information is vulnerable to attack at any point in a network, from its introduction until the final destination. In particular, information is more susceptible to attack when passing through communication llines. Strong measures of access control based on password, operating systems protection schemes are making network communications lines more attractive for attacks than the host computer.

But using the services of e-mail, web, funds transfer, etc. is based on a feeling, often fake, of communications security that can convert potential earnings caused by easy access to information into major losses, due to theft of data or inserting false data. Information systems security can be characterized in a variety of ways.

In recent years major changes have occurred in the nature of security problems, both in terms of technical background and of business. Consequently, many assumptions about the traditional security technologies are no longer valid. Inability of knowing the depth and extend of these combined changes can only lead to solutions that aren't the most effective in security issue. For these reasons, the need of survival offers new techniques and perspectives for business in the security matter that are essential in searching for solutions. More over, the survival of infomation systems extends the narrow area of security, accessible only to experts in the field, to the perspective to risk management type, which requires the participation of the organization as a whole (executive management, security experts, experts in various types of applications of the organization, etc.) to protect critical systems of that organization against attacks, failures or accidents. So we can define the survival as the ability of a system to promptly fulfill its mission in the presence of attacks, failures or accidents.

III. Analysis Protocol Standards

By protocol means a set of rules that two entities that communicate between they must comply with for the exchange of information can take place. Through entity means any kind of device capable of transmitting and receiving information. Protocol sets out what will communicate, how to communicate and the moments in time when you communicate.

IPSec is a standard protocol of the Internet Engineering Task Force (IETF) that provides data authentication, integrity and confidentiality in time as data is transferred between two or more points in a communication IP based network.

IPSec protocols components are:

- Encapsulating Security Payload (ESP) – provides authentication, integrity and privacy against data theft, while providing message content protection. IPSec provides a framework for implement standard encryption algorithms such as SHA and MD5. The algorithm IPSec creats a unique and unchangeable identifier for eachpacket, equivalent with a fingerprint yhat can detect a potential changes. Packets that are not authenticated are canceled in addition and longer sent to the receiver. Furthermore, the ESP provides IPSec encryption services. ESP authentication is designed to contents of the packege and not to its header.
- Authentication Header.
- Internet Key Exchange (IKE).

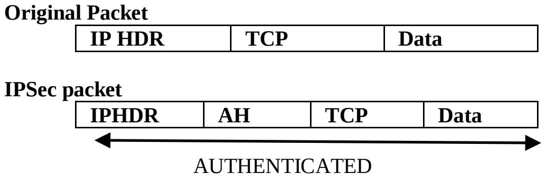

Fig.1 Comparison between an original IP packet header and an IP with IPSec packet.[2]

Introduces the concept of IPSec Security Association (SA) which is a logical connection between two devices that transfer data. A security association provides data protection for unidirectional traffic by using protocols defined by IPSec.

An IPSec tunnel consists of two unidirectional security associations that provide a protected full-duplex channel.

IPSec uses the IKE to facilitate and automate the installation and keys exchange between communicating parties. Using keys it ensure that only the sender and receiver of a message can access it. IPSec requires that the keys should be recreated or frequently updated, so that the sides need to communicate with each other securely.

Conclusions

We should mention that the new conditions related to the development of information society based on the use of global information networks, development of cross-border information exchange, globalization of the world economy system and increasing computerization needs the highlighting of factors did not previously represented significant threats. These factors make security of national interests in the field of information security to be an important element of its national security.

In conclusion, to address all security issues in network to be addressed two aspects of a network insider attacks and protection from outside attacks. Also, a computer network protection is achieved not only logically applications, but also physically, security protocols and equipment. Equipment, located in a public location, where access multiple categories of persons suspected attacks are more physically than those in locations with strict access control.

Good practice teaches us that the security policies to be applied at all hierarchical levels of a network of computers, not just at the level of access that match the end users. Also, use antivirus and firewall programs to protect computers and servers is needed at every level of the data network using security protocols.

As intitutions become more dependent on well functioning information systems security issue it is becoming increasingly important. New protocols and standards will emerge, new applications will be conceived, and our lives will be further changed and enhanced.

References

[1] J. Habraken, „Reţele de calculatoare pentru începători”, Editura BIC ALL, 2002.

[2] McClure Stuart, „Securitatea reţelelor”, Editura Teora, 2002.

[3] E. Stancu, „Terorism şi Internet”, revista „Pentru Patrie", nr. 12/2000, p. 26.

[4] D. Oprea, „ Sisteme informaţionale pentru afaceri”, Editura Polirom, 2002.

[5] R. Daniel Zatu, „Reţele de calculatoare în era Internet”, Editura Economică, 2002.

[6] D. Zaharie, „Proiectarea obiectuală a sistemelor informatice”, Editura DualTech, 2003.

[7] http://www.securitatea-informatica.ro.

[8] http://ro.wikipedia.org/wiki/Sistem_informatic

[9] http://ro.wikipedia.org/wiki/Securitatatea_(calculatoare).

[10] www.scibd.com.

[11] www.bitdefender.ro

[2] ***,”Securitatea datelor și sistemelor informatice”,Editor INDEX, http://www.scribd.com/doc/51394692/carte-tehn-info-INDEX-font-13. pag.186.