GLOBAL SECURITY MODEL

Radu PIETRARU[1]

Materialul îşi propune prezentarea unui model de securitate pentru o clasă particulară de sisteme şi anume sistemele de calcul conectate la Internet. Originalitatea modelului constă în abordarea ierarhică a securităţii pe trei nivele: nivel de securitate sistem stand-alone, nivel de securitate de reţea local-network şi nivel de securitate Internet; precum şi în selectarea şi prezentarea diferenţiată a mecanismelor de securitate specifice fiecărui nivel de securitate în parte.

The material aims to present a security model for a particular class of systems, systems connected to the Internet. The originality of the model is hierarchical approach of security on three levels: level stand-alone, level local network and level Internet; and in the selection and presentation of specific security mechanisms used in each security level.

Keywords: security, security model, Internet security

1. Introduction

The purpose of information security technology is [1] to enable an organization to fulfill its mission and objectives by implementing a system with careful consideration of technical risks present in the organization and its partners and customers.
Security can be detailed by the following security objectives [1]:
1. Availability (of systems and data for legitimate use). Availability is a requirement that aims to ensure that systems function properly and services are unavailable to authorized users.
2. Integrity (of systems and data). Integrity is the most important security objective after availability.
3. Confidentiality (of data and information system). Confidentiality is the requirement implies that private or confidential data are not disclosed to unauthorized persons.
4. Responsibility (individually). Accountability is the requirement implies that the actions of any entity can be uniquely associated with that entity.
5. Trust (the other four objectives were adequately insured). Trust is the basis for ensuring that security measures, technical and operational functions properly to protect information systems and processed.

[1] Lecturer, Department of Automatic Control and Industrial Informatics, University POLITEHNICA of Bucharest, Romania, e-mail: radup@aii.pub.ro

2. Server Security

A server is a system which provides the main service, one or more services to other hosts over a network. For example, a file server provides file sharing services, so users can access, modify, store and delete files.

Each system, including all server systems, must be protected from a potential impact on the system on loss of confidentiality, integrity or availability. Measures of protection (or security checks) can be divided into two categories. The first category of systems security weaknesses must be addressed. If a system is a well known weakness attackers can exploit and this is why the system must be repaired to remove or to mitigate the vulnerability. The second system should provide only strictly necessary functionality to each user and no one should have to provide functions that are not necessary. This principle is known as the minimum necessary privileges. A common problem related to security controls is often those that become more difficult to use systems by introducing additional security barriers. When ease of use is a requirement to seek mitigation of security controls (for example, if passwords must meet complexity tough and long, users need to remember long and complicated passwords, which is quite hard which leads to relaxation in the Finally, the check security). Choosing the optimal route between functionality, easy use and decent security level is a challenge for professional staff (for detailed planning of security see [2]).

Another fundamental principle stipulates use of multiple layers of security. – hierarchical protection. For example, a system can be protected from external attack by several controls, here including a network firewall, a system-level firewall and system protection level operating system. The reason for using several levels of protection is redundant protection offered by the hierarchical model. If the yield level and no longer protects the system against a particular type of attack, the next level of security can undertake this function. Combinations of network systems with local protection provide a complete and redundant protection against external attacks. There are certain steps necessary (steps) to design and implement a security server system. Before planning any security measure is essential to have a security policy. Following steps to implement security server system in accordance with general security policy, provides a rigorous foundation for implementing an effective security system and protection [3]:

- Planning and installation of operating system and other software components for server systems.
- Setting and implementing a security system in the operating system.
- Setting and implementing a security system to the application server system.

For systems that provide services such as web servers, database servers and name servers must implement specific security controls.

It is necessary to implement mechanisms for network protection (firewalls, packet filtering or proxy servers). Choosing the mechanisms necessary for a given situation depends on many factors: the location server client system (local area network, Internet, remote access VPN, etc.), location of the server network, type services and not least the type of threats to server address. Maintaining an acceptable level of security requires continuous surveillance and monitoring system operation and monitoring of the server operating system vulnerabilities and software systems used. The aim is to reduce the techniques presented risks associated with the system server. Using best practices lead to implementing a robust security system.

When trying to solve a problem of security is better to consider the following simple principles of security [4]:

Simplicity - security mechanisms (and computer systems in general) must keep a natural simplicity. Complexity is generating security vulnerabilities.

Reliability - if a failure occurs, the system must respond in a safe manner (reliable), for example, security controls must remain in operation - it is better to lose functionality than security.

Open design - security system should not be dependent on the secrecy of the implementation or its components.

Separation of privileges - the operational functions, as far as possible, must be separated and provide a granularity as fine. The concept should be applied to systems, software systems and users.

Acceptance - users should understand the need for security measures. This can be achieved through education and training.

Isolated mechanisms - when a function is implemented in the system is preferable that a process or service that has access to some resources not to send their credentials to interact with other mechanisms.

Time factor - indicating the time and effort required breaking a security system. Needs time and work the attacker must be greater than the (equivalent) and information system that will provide for success, discouraging an effort.

Records - records and logs should be maintained so that there is evidence of attack or compromise the system or network. This information can then help in securing the future of network and system by identifying methods and weaknesses exploited by the attacker.

3. Communications Security

This chapter aims to present two important aspects of network security: control mechanisms of network traffic (filtering communications) and

mechanisms for protecting information transmitted on the network (communications encryption). Both issues have an important role in the security system because the lack of security mechanisms in these directions can seriously compromise system security. Without the ability to control network traffic is impossible to ensure the integrity and system availability, and lack of mechanisms to protect information transmitted on the network can compromise the integrity and confidentiality.

Communications security, direct or indirect, is a care at least as high as the security server itself because the server functionality can be compromised as well as communications through compromise and compromises other existing functional levels. Compromise communications system can be communications interception, alteration or counterfeiting of currencies. Interception of communications can lead to loss of privacy and possible compromise of other functional levels (for example interception of login passwords). Alteration or falsification may compromise the confidentiality of communications (communication partners may send sensitive data to malicious entity impersonating the server), may compromise the protective role of communications server and can adversely affect operation of the other services offered by the server.

In terms of how interconnected the server can distinguish the following cases [5]:

- Server with a single connection. If the server is not providing transit service information (routing) but other types of services (web, mail, file server, etc.). Link can connect the server directly in a local network or Internet. In both cases serving area may be comprehensive (even if Internet connection is made through a local network does not mean that access to services is limited to the server). A single connection involving only need to secure their communications. Protection should be provided both when the connection is made via another network (local) in the case of a direct connection to the Internet and must be independent of external mechanisms available (there is a firewall of protection to the local network does not eliminate need their protection at server level).
- Server with multiple connections. This model assumes the existence of an interconnection or more server connections. These connections may be redundant in nature (it can interconnect with the same group receiving - this case is identical in terms of the need for security with the previous model - a server with a single connection), can be functional in nature, other (groups receiving different - Local network / Internet for example) communications transit officials or not (the server may have the role of routing information between the two groups or not). If the server has the

role of router communication between different groups is necessary for its security functions to expand the transit information.

There are several issues that arise in communication security system:

- Protection against communications to be provided without permission. This level of security as the service meets the firewall - wall protection - and provides filtering of communications after a defined policy. This level of security is needed both in the model with a single connection, and certainly the model with multiple connections.
- Protection against unauthorized attempts to access server resources - attempts to work around the filter level communications. This level of security, known as IDS - Intrusion Detection System, involving analysis of real-time communications and detect attempts to breach the security policy defined. It preventive security level and applies to both models of connectivity.

4. Global Security Model

Global security model aims to summarize the technical aspects of security. Global model is organized on three levels defined by the degree of interconnection of the system:

- Stand-alone security model - no connectivity systems
- Local-network security model - complete with details of security issues related to limited connectivity to a local topology.
- Internet security model - explores the problems that arise when exposure outside the system through the Internet.

The three security levels are not independent of each other as security concerns is addressed hierarchically, each filling level security measures by adding to the previous set of threats and corresponding security measures with new types of risk scenarios. All three security levels overlapping and forms the global security model.

Stand-alone security model aims to summarize the issue of security of computer systems ignoring the threats that come from connecting to its network. The first category of security measures for this level refers to the physical protection system. Access to the system must be controlled to prevent unauthorized physical access to the system. This mechanism should be implemented at the organizational level (with access rules in the area of the system) and physical layer (the access control system in the room, case of the system, video surveillance). The next important mechanism is intended to protect information stored on a file system. The operating system should provide a mechanism for access rights to files and directories (file system type NTFS or extfs for example) allowing discretionary access to information based on access

rights. An additional level of protection it provides encrypted file system (CFS, EncFS) that allow expansion beyond the operation of security information storage device in the system. File protection information can also include protection for system errors that can lead to accidental loss of data integrity by journalized file systems (ext3, JFS, ReiserFS) or redundancy mechanisms of information storage (RAID) that allow reconstruction of data in the case of an error.

Implementing a secure access to the system is through a mechanism of authentication and authorization of users. Usually this is done through a password system but can be implemented and additional measures based on biometric information and identifying hardware key (token device). Authentication mechanism allows users to accurately identify and implement mechanisms to allow control of access rights to information and computer system resources. Authentication mechanism must not allow rejection of responsibility carry out operations. The security control should be implemented at operating system and, if necessary, at the level of applications.

Safety mechanisms on equipment availability (redundant equipment operation): redundant data storage (RAID storage arrays), redundant power supply system (source room processing), alternative electricity supply system (independent sources - UPS), Pipelines multiple system, Multiple processing units Multiple peripheral.

Installing sites against malicious code prevent the introduction into the system, accidental or deliberate, of them. Control portable storage media help to protect against the spread of malicious code and prevent stealing of information from the system. Control of storage media can be radically, by disabling the corresponding peripheral, or selectively by implementing a security policy that only certain users have the right to use certain storage media.

Ensure integrity of system files and user files should implement a backup mechanism to make regular saving all the important information in a system separate from system storage medium (tape, optical discs and external magnetic media). Making backups can provide information in the system recovery after destruction of equipment or an alteration of the information. Work on his system and user activity may be supervised by a mechanism for recording (logging) special operations. These records will be stored in a series of logs to be part of the file system. Surveillance mechanism should allow: handling system, diagnostics business applications, tracking and identification of user activity. Implementation of security does not end with the definition, installation, configuration and operation of security mechanisms.

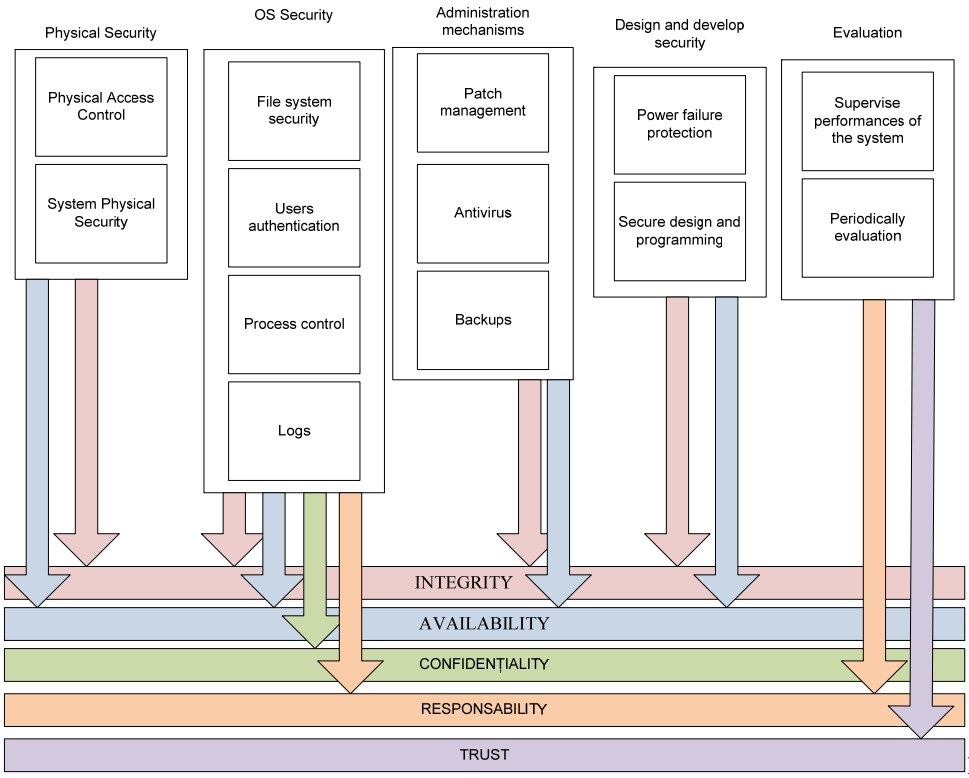

Fig.1 Stand-alone security model

Local-network security model aims to add an additional level of security issues that is networking system. In this level the question is only a limited connectivity, local area network level. This limitation means that entities - communication partners - the network are known, there is a certain level of trust between the system and they, by default security threats will have an extreme character.

Connect the network system would create two new categories of problems:

- Protection of information transmitted on the network, even if talk of a local area network in which all participating partners are reliable, certain information is likely to have a sensitive nature and require a degree of protection.
- Protecting the network services system, because the overall security model addresses the server systems, their implicit role in a local network, is to provide specific services to other computing systems (application servers, database servers, network authentication services).

New threats emerged at this level can be divided into two classes:

- Threats posed by networking:
- Threats to network services (see [6], [7], [8], [9]).

Security communications network could be implemented at two levels: physical security - ensuring availability and integrity of the media, and logical security of data transmission - ensuring integrity and confidentiality of information in transit. Transmission security involves protecting the natural environment of the lines of communication, where traditional networks and protect the logic of communication, where wireless networks. Quality network services that can disrupt the availability of such communications and the availability of network services must be ensured through specific mechanisms. The fall of communication channels can be avoided by implementing redundant interconnection topologies, it prevents the loss of availability of network communications.

Logical secure data transmission implies the implementation of mechanisms to prevent interception (recording) and interpretation (recovery) information transmitted over the network. This is achieved through the use of network equipment that does not work on-site broadcast packet (use of equipment switch and not hub) and using, if necessary, encoded communication protocols (encryption of messages or packages). Network services can be protected mainly by a properly configured specific (dependent on the type of service), a strong authentication mechanism (taken from the operating system or their own) and a careful monitoring of network connections. Authentication mechanism is responsible for correct identification of users and linking them to the rights they hold and use the default service in processing information. In addition to mechanisms to reduce the risk of threats to network-type impersonation (strong authentication mechanisms) should be implemented mechanisms to ensure availability of network services by protecting against DoS attacks. To prevent this will require a mechanism to monitor the connections - a system similar to those IDPS who are able to filter legitimate connections to the parasite. All special events related to networking and operation of network services must be recorded in log files. The log files must be reviewed and any incident of malicious network data must be recorded and documented. Analysis of dangerous events in the network must be part of the surveillance system. Regular evaluation should include operation of the network (in terms of system) and operation of network services.

The last level of global security model, Internet security model, introduces the issue of connecting to external systems through the Internet. Because high connectivity, threats are diversifying, the risk increases and the identities of the attackers are completely unknown. This final level of security finalizes the global security model leading to the complete security model.

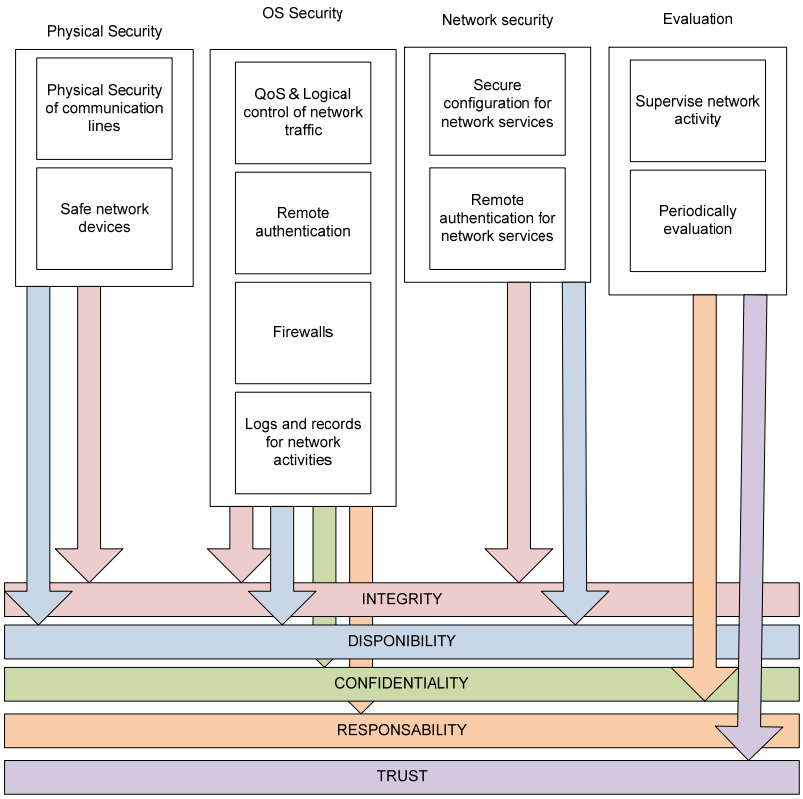

Fig. Fig. 2. Local network security model

Internet security threats to the system have two major issues:

- Threats present if previous levels have a greater security risk due to global conjuncture.
- Availability of communications and network services depend on network sectors that can not be controlled directly.

These issues imply new security mechanisms:

- Protection system and network which belongs to penetration attacks and DoS-type attacks by installing firewalls and IDPS systems.
- Protection communication network through the implementation of encryption mechanisms communications network segments that cross uncertain.

In addition to these mechanisms need to be implemented tougher security mechanisms on the remote user authentication and security mechanisms specific Internet services (e-mail security service, web, dns, etc.). Given the much higher traffic information and dynamic operation connected to the Internet surveillance

systems of records shall be assisted by automated tools for analysis of events to report a summary of work to alleviate the burden (for more details see [10]).

6. Conclusions

Introducing comprehensive model has been gradually on the basis of three security levels defined in the model: level stand-alone, local model network and the Internet model. The first levels of model is currently a rare model describing security mechanism of an isolated system without network connection, but allow focus on security mechanisms of the system without introducing the complexity of the network to external threats. The second level introduces the risk induced model of network threats but limited source of threats to the context of a local network without exposure to the Internet environment. In this level can easily identify security mechanisms rudiments of the next level, but they are presented in such a way that allows a more relaxed approach to specific security controls. The last level generalized set of threats present in the previous global model and allowing filling its application on the server systems connected to the Internet. The three levels represent a hierarchical structure and allow the gradual application in designing and implementing a security system.

Global security model has been validated in practice through an implementation of an Internet server that is managed by the author of this article. The system is used as an Internet server in the Department of Automatic Control and Industrial Informatics with the functions of the router, DNS server, web server and mail server for aii.pub.ro domain. System runs CentOS Linux and has implemented all the security mechanisms presented in the global security model. The system is in continuous operation for three years and allowed theoretical improvement and validation of global security model in practice.

R E F E R E N C E S

[1] *G. Stoneburner,* Underlying Technical Models for Information Technology Security, 2001
[2] *M. Swanson, J. Hash, P. Bowen*, Guide for Developing Security Plans for Federal Information Systems, 2006
[3] *K. Scarfone, W. Jansen, M. Tracy*, Guide to General Server Security, 2008
[4] *Matt Curtin*, Developing Trust: Online Privacy and Security, 2001
[5] *J. Wack, K. Cutler, J. Pole*, Guidelines on Firewalls and Firewall Policy, 2002
[6] *M. Tracy, W. Jansen, M. McLarnon*, Guidelines on Securing Public Web Servers, 2002
[7] *M. Tracy, W. Jansen, S. Bisker*, Guidelines on Electronic Mail Security, 2002
[8] *A. Singhal, T. Winograd*, Guide to Secure Web Services, 2006
[9] *R. Chandramouli, S. Rose*, Secure Domain Name System (DNS) Deployment Guide, 2006
[10] *K. Kent, M. Souppaya*, Guide to Computer Security Log Management, 2006.