CONSIDERATIONS ABOUT COMPUTER NETWORKS SECURITY UNDER VARIOUS OPERATING SYSTEMS

Nicolae Radu MARSANU[1]
PhD, University Professor , Department of Computer Science
Academy of Economic Studies, Bucharest, Romania

e-mail: radumarsanu@ie.ase.ro

Claudiu SICHITIU[2]
Graduated of the Bucharest Academy of Economic Studies, Faculty of Cybernetics, Statistics and Economic Informatics, 2010.
He follows the Economic Informatic master courses.

e-mail: claudiu.sichitiu@gmail.com

George SICHITIU[3]
Graduated of the Bucharest Academy of Economic Studies, Faculty of Cybernetics, Statistics and Economic Informatics, 2010.
He follows the Economic Informatic master courses.

e-mail: george.sichitiu@gmail.com

Abstract: Importance of security issues in computer networks has increased with the expansion of electronic data processing and transmission via the network. When operating on confidential information, it is important that the benefits of sharing and communication of a computer network to be supported by substantial security facilities. This is essential given that computer networks have come to be used including the development of banking, shopping or fees. Following the implementation of security mechanisms in a computer network, information can not be accessed or intercepted by unauthorized people (or curious, possibly even malicious) and will prevent falsification of information transmitted or illegal use of certain services.

Keywords: computer network security, protection, open system, encryption, MS Windows 7, UNIX, Mac OS X, firewall

1. Introduction

The security of computer networks means usually, integrity, availability, reliability and best possible protection of resources. Most times there is no total protection solutions, each implementing of a computer networks security are a compromise between efficiency, cost and settlement operations. A well-secured system can hamper current operations traffic and also it is more expensive then others. Security should be conceived as an inclusive property of a computer system that is embedded in an environment [1]. Security management objective is to eliminate or minimize the vulnerabilities of the computer.

Computer network security protection covers all computer and network connected together [18]. A computer network is a set of computers and other devices interconnected through communication media, thus ensuring the sharing of a large number of users of all physical resources (disks, printers, scanners), logical (system or application programs) and information (databases, files) available to all connected computers. A computer network consists of two or more devices connected to allow the exchange of information [4]. A computer network should primarily ensure connectivity between multiple computers. For a private network, it may be sufficient to connect two computers to each other directly, and users may, for example, transfer files from one computer to another. But, for Internet, the network must be built so that it can grow to a level to cover the whole world [9].

Technologies that are used for a computer networks have grown dramatically in recent years and the need for interoperability became evident. It had developed a new path for communication between computer systems. An open system is a system based on a common design of a network architecture and supported by a suite of protocols. Open architecture system (open system) maximizes the opportunity for interoperability [15]. OSI (Open System Interconnection) reference model is based on a proposal developed by ISO (International Standards Organization), as a first step in standardizing the various protocols, model is called ISO / OSI-RM (Open Systems Interconnection Reference Model), as it relates to interconnection open systems. OSI model has helped to change the image of computer networks. Is the most discussed and the most mentioned model for a network architecture. However there is no computer network based on this model [6].

One of the most important thing in a computer network is the protocols that are used. A protocol is a set of rules that define how data is formatted and processed into a computer network [15]. If a computer network architecture is open, not only one vendor has the technology for it and control principle and its development. Anyone who has access to it and he can model software and hardware architecture based on that network. The architecture of TCP / IP (Transmission Control Protocol / Internet Protocol) is used in Internet. TCP is able both to transmit and receive simultaneous data streams, even though this may seem opposed to the basic concept of data transmission in many based computer network technologies [14].

Because the need for a increasingly mobility and connectivity, wireless communication has seen a boom in recent years. Spread of mobile devices (laptop computers, PDAs and smartphones) which is largely led to the development of wireless communication technologies, but they were not the only engine. Computers connected by wireless networks are characterized as having a low bandwidth, high latency and unpredictable availability and stability, unlike wired computer networks. In addition, all these features range from device to device and from network to network [19]. Wireless perspective is very appealing.

2. Security threats to computer networks

In the first decades of their existence, computer networks were used by researchers in universities to send e-mails and by corporations employee to share printers. In these circumstances, the security was not so important. But now, when millions of ordinary citizens using the network for banking operations, purchases and tax payments, network security is a major potential problem. Network security problems can be divided in four interconnected areas: privacy, authentication, integrity and non-repudiation.Confidentiality refers to keeping information away from unauthorized users. Authentication is determining the identity of the person. Non-repudiation involving signatures and integrity checks to ensure accuracy and data protection [10].

Internet was designed to create standards for communication between computers. Internet supports data transfer trough a mechanism called Protocol. Protocols are rules stereotipizate, very detailed, explaining exactly how to change a set of messages. Communication between computer networks is called *internetworking*. The Internet as we know it today is essentially the largest and ultimate computer network, spread across the globe [15].

Security policy of a computer networks should define the approach to be tackle when pursuing a suspected intrusion. Procedures that deal with this type of problem must be clearly specified. A large number of questions about security must be made before an incident happen, so that must responses be as clear and objective. A security policy is a set of rules and procedures that have potential impact and limiting freedoms and, of course, individual security levels of all users. Security policies are very important in system security plan [8], [13].

National Computer Security Center (NCSC) of National Security Agency (NSA) of USA has published a series of documents that define the criteria for classification of trusted and security systems. These criteria represent the frame to develop security systems. Well known "Orange Book" defines seven classes trusted systems:

- Class D - minimum protection - systems that have been evaluated, but have decided not to bring equipment or software for a higher security level;
- Class C1 - discretionary protection - placing the control system only as they need and maintain separation of data users;
- Class C2 - protection of access control - systems which implement access control in C1 class and record actions by user authentication procedures (login);
- Class B1 - type security protection - systems that implement a formal model of political and security;
- Class B2 - structured protection - a system that includes all of the class B1 and it is expected that all topics and articles relating to systems;
- Class B3 - areas of security - systems that meet requirements for monitoring and include administrative intrumente security mechanisms and the ability to signal relevant current events;
- Class A1 - design verification - similar systems in class B3, but with additional architectural features and design requirements associated with formal specification and verification techniques.

3. Models and methods of protecting computer networks and data

For network security is important to implement specific mechanisms based on the physical level (Physical Protection of transmission lines), followed by procedures to block access to the network (firewalls), application of techniques to encode data (encryption) , specific method for the protection of such communication between application processes running on different computers on the network. Security mechanisms also could be related to: preventing violation of security, limiting the damage caused by security violation as they occur and offset their consequences [1], [7].

Cryptographic algorithms are only one piece of the puzzle when it needs to securing a computer network. Using encryption algorithms increases every day as more information becomes digitally encoded and published on the Internet. All this information must be secure with the best encryption method [18]. The main methods of protecting computer networks and data are encryption schemes, digital signatures, digital seals, digital envelope, software protection and security review [11].

An important issue in designing software that will operate, control and secure information system and computer network is the security model that the system or network will be based. Security model implements security policy, which was chosen and implemented by designers of system and computer network [18]. To protect against unauthorized access to computers in a network there are several solutions: using firewalls and secure the network area, authentication and authorization access, creating of secure communication channels, etc.. The main methods of securing a computer network are: firewalls, authentication and authorization external access, NIS service, SSL protocol, S-HTTP protocol, PCT protocol, IP-level security, Secure Shell (SSH). A firewall is a system placed between the internal network (intranet) and external network (internet). The main role is to protect the intranet in accordance with certain rules and criteria that can be set by configuration. The simplest form of protection wall is shown in Figure 1.

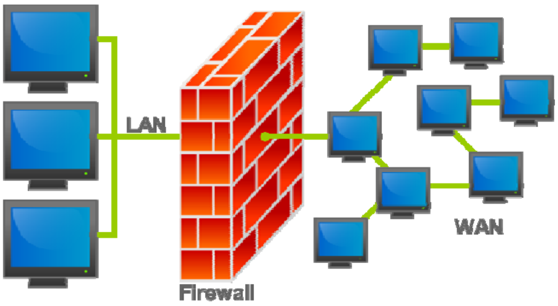


Fig. 1. – Simple form of a firewall

4. Computer networks security under various operating systems

An operating system (OS) is a set of system software programs in a computer that regulate the ways application software programs use the computer hardware and the ways that users control the computer. A computer being secure depends on a number of technologies working properly. A modern operating system provides access to a number of resources, which are available to software running on the system, and to external devices like networks via the kernel. Network services include offerings such as file sharing, print services, email, web sites, and file transfer protocols (FTP), most of which can have compromised security. At the front line of security are hardware devices known as firewalls or intrusion detection/prevention systems. At the operating system level, there are a number of software firewalls available, as well as intrusion detection/prevention systems. Most modern operating systems include a software firewall, which is enabled by default. A software firewall can be configured to allow or deny network traffic to or from a service or application running on the operating system. Therefore, one can install and be running an insecure service, such as Telnet or FTP, and not have to be threatened by a security breach because the firewall would deny all traffic trying to connect to the service on that port.

MS Windows

MS Windows operating systems have been criticized many times because of the two major weaknesses: the security and reliability. Reliability of an operating system is usually quantified by the time of working without having problems. Unfortunately, MS Windows tends to become unstable after a period of time, unlike other operating systems. Of all desktop operating systems, Windows has a reputation as the most vulnerable to viruses, worms, trojans and other attacks of this kind. Some parts of the MS Windows vulnerability is because it's database of users is very large. MS Windows has many security holes that are found and exploited by malicious people. While Microsoft is vigilant in its efforts to fix these security holes, its developers are always one step behind hackers, and while users waits for security patches their computers are vulnerable [17].

Versions of MS Windows was originally designed for use on a single computer without a network connection, and did not have security features built from begining [20]. However, MS Windows NT and its successors were designed for security (including network security) and multi-user computers, but were not originally designed with an advanced Internet security, since they were first developed in the early 1990s, Internet use was not widespread. Microsoft releases security patches through Windows Update service approximately once a month, although critical updates are available at shorter intervals of time when necessary. While MS Windows 9x operating system series functionality offered to have profiles for multiple users, they had no concept of access privileges, and also does not allow simultaneous access, so that the concept of multi-user was rather false one. On the other hand, they have implemented only partial memory protection. Series of MS Windows NT operating systems, by contrast, were well implemented multi-user functionality, and an absolute memory protection. However, a lot of benefits that made a multi-user system, highly tuned operating system, were canceled because, before MS Windows Vista and MS Windows 7, the first user account created during setup process was an administrator account, which was also default for the next newest accounts. Although MS Windows XP had limited accounts, most home users had fewer rights set for new accounts (because of the large number of programs which unnecessarily required administrator rights). Therefore most users hade accounts on a computer with administrative rights all the time. MS Windows Vista and MS Windows 7 solves this problem by introducing a system of privilege User Account Control. When a person is authenticated from a standard user, a session is created and is assigned a process that contains only basic privileges. In this way, the new session is impossible to make changes that would affect the entire system.

An attack that should be considered when using wireless technology is the threat of data interception. The interception of data, one of the main advantages of wireless technologies, paradoxically, lead to one of its biggest weaknesses. Because wireless transmissions are sent by air to the target device, any system set up correctly in broadcast radio can also receive these messages. Thus, the devices should not be in the computer network can receive transmissions. Expanding computer network through wireless technology has also increased the area of attack by malicious users. Some methods of ensuring security of computer networks connected by wireless technology are: Protected Access WPA, WEP, 802.1x authentication, etc [12].

UNIX

UNIX operating system with TCP / IP suite for communication and NFS file system is a convenient solution to form a complete operating system in a computer network. Many years before, Dennis Richie said about UNIX security: "It was designed from the outset to be secure. It was designed with the characteristics required to make security services. In other words, Unix can be secured, but any particular system of UNIX may not be secure when it is delivered. Unix has a sophisticated security system that controls user access to files, change the system database and system resources.

Currently there are many techniques that were used to secure computer networks with UNIX operating systems:

- use encryption to protect against violation of access rights;
- strengthening the operating system and applications against attackers;
- physical isolation of system vulnerability;
- firewalls implementing;
- development of advanced authentication systems not based on IP address or hostname;
- development of system traps to detect potential attackers;

In MS Windows operating systems, the user has often and management rights and this can create security problems. Linux operating systems is a clear distinction between the system administrator rights and use rights system. Therefore, only one user has full administrative rights. This is one special user called root. Root has full rights in Linux operating system. He can make configuration, can change how the system starts operating, grant partial rights to other users etc.

Because everything in UNIX is represented as a file, it means that to be able to communicate two UNIX computers on the same network, those must be able to share files. Sharing files is a useful way to distribute information to many users, whatever of their connection to the network. NFS (Network File System) is the method of sharing files between UNIX computers. It is a standard but has some security issues. NFS enables filesystems physically residing on one computer to be used by other computers on the network, and to show users on remote stations like any other local drives.

One of the most powerful and widely used authentication service is Kerberos Authentication Server. Kerberos is a set of protocols that can be used to authenticate access to a computer. It allows network users to communicate in order to reveal the identity and to authenticate, preventing lines of listening situations. Kerberos data encryption performed secrecy. Also, Kerberos provides real-time authentication in an insecure distributed environment.

Advantages of computer network security under UNIX

Unix system's strengths are numerous. It is highly configurable, is well understood by many programmers in the security industry and is the most remarkable existing operating system. Many researches are devoted to understanding and repair any security problems that might arise. Unix is considered a very stable and high performance operating system. In addition, because it was designed to run on multiple hardware platforms (including IBM and

SGI servers) and many versions of these platforms, that can support high data rates required for any firewall that supports a network of computers. It is also immune to the need of restart the computer after the configuration changes, which never happens in Windows NT systems.

Disadvantages of computer network security under UNIX

Problems arise when inexperienced Unix administrators do not know how to install the firewall and disable many vulnerable programs and services (but potentially valuable to a non-firewalled system) which are enabled by default. Many of these vulnerable programs and services (*called daemons*) are configured to run in the security context of root, they can create an attacker with full access to the system once they have exploited vulnerable components. A UNIX *daemon* is a program that works in the background and perform services or functions useful for all users. These programs have been called "daemons" because their operations are hidden from user. Disabling them its relatively simple. Administrators easily delete or rename scripts that activate their start up, or comment code lines from *inetd.conf* configuration file.

Mac OS X

Security is available for different levels in the operating system Mac OS. Mac security architecture must be understood in light of its overall architecture of network security. There are two main network protocols used on the Mac today: AppleTalk and TCP / IP. In general the local AppleTalk provides services that are not available on the Internet: print, share files with other machines on the same network, and applications from homegroup. TCP / IP provides several services globally, including Internet services such as email and websites access. TCP / IP also provides services that have traditionally been available only on AppleTalk, including file sharing and related programs (AppleScript and Apple Events) on the Internet or intranet.

Mac OS X has a reputation of being an operating system easy to use, reliable and very safe.Core operating system Mac OS X is UNIX-based and includes powerful features memory protection that contributes to a low incidence of errors and failures. Also inherits a strong foundation in UNIX witch tends to limit the number of security holes and any damage that can be made by hackers. Another factor that ensures a better security is the small number of viruses that have been developed for attacks against Mac OS X, because most attacks were directed to other operating systems like Windows [17].

In Mac OS X, Apple has implemented a security strategy that is central in operating system design. Security strategy aims: open-source based, security default settings, modern security architecture, innovative security applications, rapid response. Mac OS X security model has four layers. Layers are not independent so that an attacker can exploit a weakness in a single layer of protection offered to pass over one or all four layers. The four-layer security model of the operating system Mac OS X are: physical security, security of Open Firmware, login passwords, user accounts. Figure 2 below shows the network security architecture when Open Door products are included. The lower layer presents two main protocols, AppleTalk and TCP / IP. Even if the AppleTalk protocol is local and is not accessible through the Internet, security remains a concern in many environments.

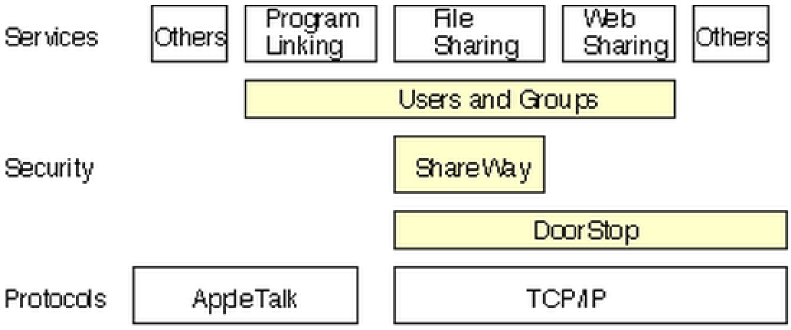


Fig. 2 Macintosh networks security architecture

Advantages of computer network security under Mac OS X

Because Mac operating system is open-source (open source) and Unix based, OS X offers the same advanced security features like other Unix systems. Also, because the operating system core is open source, you can make improvements on it to solve security bugs and add new features. In addition, most implementations OS X Server are based on the Unix components such as Apache Web Server, MySQL database server and Sendmail e-mail. There is a widespread thinking that running a firewall on a Mac is usually safer because most crackers are not familiar with Mac technology. Though there are some reports showing vulnerability in applications running on a Mac, some of them even show the weaknesses of the operating system. There are also easy to configure firewall services. BrickBouse is a user interface API firewall built into Mac OS.

Disadvantages of computer network security under Mac OS X

Significant weaknesses are actually the opposite side of strengths from a Mac operating systems. Because the system is not very known yet, there are many vulnerabilities that waits to be discovered by hackers, who could make a serious attempt to enter the system, especially in areas that are not public for users (eg graphic support areas). Also, because a Mac server has only a limited number of options developed into a firewall API, administrators may feel that they lack something, such as the ability to customize the API to include additional security features, such sophisticated intruders detection. Although some existing open source solutions provide these features, there is no company to produce an enterprise version of a firewall product for OS X [2].

5. Microsoft Windows 7 security

MS Windows 7 is the latest desktop operating system from Microsoft, which was built on the strengths and weaknesses of its predecessor, MS Windows XP and Windows Vista. In addition to basic system enhancements and new services, MS Windows 7 provides more security functionality, enhanced auditing, monitoring capacity and the ability to encrypt personal data and remote connections. MS Windows 7 also has recently developed internal improvements to protect the internal system such as Kernel Patch Protection, Service Hardening, Data Execution Prevention, Address Space Layout Randomization, and required levels of integrity. MS Windows 7 is designed to be used safely. First was developed frameworks Microsoft's Security Development Lifecycle (SDL) and it was designed to support the Common Criteria requirements, enabling it to carry out Evaluation Assurance Level (EAL) certification, which fulfil Federal Information Processing Standard - FIPS).

MS Windows 7 was built on the foundation of MS Windows Vista security, although improvements have occurred several places such as Group Policies, User Account Control (UAC), BitLocker and Windows Firewall. In addition they have opened several new features such as BitLocker To Go AppLocker and [18].

Firewall Windows Firewall was introduced in MS Windows Vista a step forward from MS Windows XP. Thus, with this major change it became a serious competitor in the market for firewall software. Overall of MS Windows 7's firewall is only slightly better then the one from MS Windows Vista. It has support for filtering outgoing traffic and it also can analyze traffic for all applications in a bidirectional way.

DirectAccess DirectAccess is a new feature may be significant long-term. Using different softwares becomes increasingly complex, and DirectAccess provides easier access to them. This means that there will be no need to make a VPN connection, because this new component do this automatically. This allows a remote machine to remain connected in a business network for as long as it exist an interoperable connectivity.

BitLocker BitLocker is a full disk encryption component included in Ultimate and Enterprise versions of MS Windows Vista and MS Windows 7, also in MS Windows Server 2008 and MS Windows Server 2008 R2 platforms. It is designed to protect data on a hard disk using encryption. It use default encryption technology AES (Advanced Encryption Standard) in CBC mode on 128-bits, combined with the Elephant diffuser for additional disk encryption specific security not provided by AES.

BitLocker To Go BitLocker To Gois an extension of the application BitLocker that supports encryption for detachable hard drive, such as flash memory and USB sticks. BitLocker To Go is only available to Enterprise and Ultimate versions of Microsoft Windows 7. To enable BitLocker To Go, insert a removable hard drive into your computer, and right click on the icon appeared in My Computer and choose the option "Turn on BitLocker".

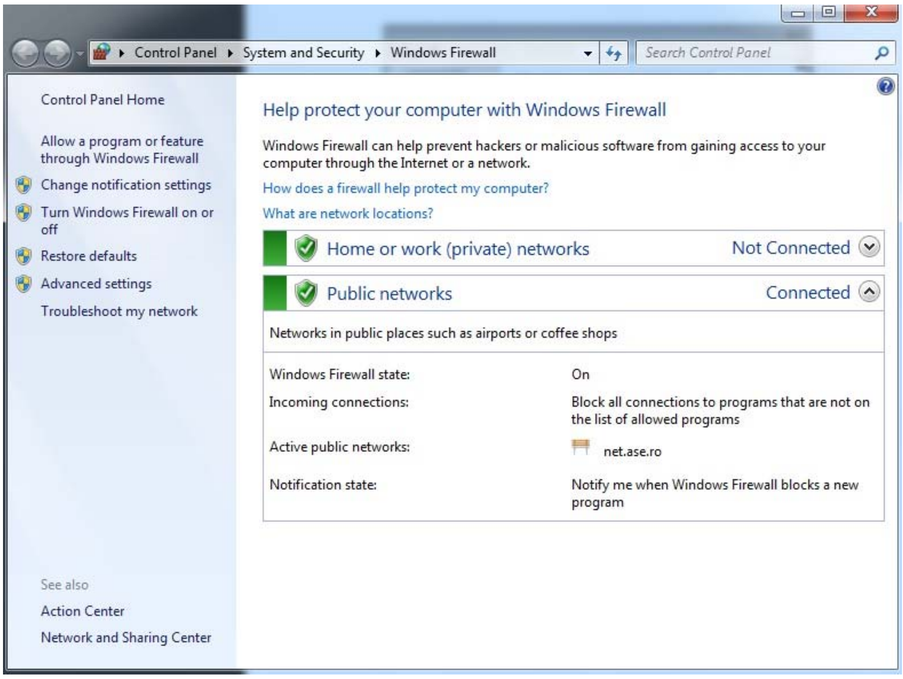
User Account Control - aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system. In other words, a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved beforehand or the user explicitly authorizes it.

AppLocker - a set of Group Policy settings that evolved from Software Restriction Policies, to restrict which applications can run on a corporate network, including the ability to restrict based on the application's version number or publisher

Action Center - In MS Windows 7 security-related options were collected in Action Center, an application that replaces the center of security (Security Center) which is found in MS Windows XP and MS Windows Vista. Action Center is designed to work with third-party firewall, antivirus and antispyware programs, and programs implemented in MS Windows 7 (Windows Firewall and Windows Defender), but also with those available, such as Microsoft Security Essentials. The first line of defense in computer security is to protect from attacks from outside. After the computer is connected to the Internet, it becomes just another node on a wide global network. A firewall provides a barrier between your computer and network that is connected by preventing the entry of unwanted traffic while allowing clear passage for authorized connections. The firewall in MS Windows 7 is enabled by default for all connections, and provide protection even from starting the computer [3].

Using Windows Firewall in different computer network locations

Firewall for MS Windows 7 maintains a separate profile (that is, a complete collection of settings, including rules for different programs, services and ports) for each of the three network location types: area, private and public. Windows Firewall is Control Panel application that provides a simple interface for monitoring the status of firewall and routine tasks such as allowing access to a program or firewall blocking all incoming connections [18]. Like Windows Defender, Windows Firewall can be found in Control Panel. To open the Windows Firewall such as in Figure 3 go to Start Menu > Control Panel > System and Security> Windows Firewall.


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	net.ase.ro
Notification state:	Notify me when Windows Firewall blocks a new program

Fig. 3 Windows Firewall shows status and settings for each network connected.

Microsoft Security Essentials

Microsoft Windows 7 does not provide an antivirus program. If a user installs an antivirus program that is recognized and accepted by the Action Center. Microsoft, however, provides MSE (Microsoft Security Essentials), a free security program. It protects against viruses, spyware, trojans and malicious software. It can be free downloaded from *www.microsoft.com/security_essentials* and its installation makes Windows Defender automatically disable [5].

Managing access to resources in a computer network

In any computer network, there are resources to which users should have access to them. Sharing is a process that allows users access from a computer network a certain resource located on a computer. A share network provides a single location to manage data shared by several users. Sharing also provides, that an administrator can install an application once and manage it from one location. You can control user access by assigning permissions to share folders. Sharing permissions are less complex than NTFS permissions (New Technology File System) and can be applied only folders (unlike NTFS permissions that can be applied to both folders and files) [16].

6. Conclusions

Computer network security protection covers all computers connected to the network and devices connected to the network. General attributes that define security are: confidentiality, integrity, authentication, non-repudiation. For network security is important to implement specific mechanisms based on the physical level (physical protection of transmission lines), continuing with the procedure that block access to the network (firewalls), application of techniques to encode data (encryption) , specific method for the protection of such communication between application processes running on different computers on the network. Cryptographic algorithms are only one piece of the puzzle when it comes to securing a computer network. Using encryption algorithms increases every day as more as information becomes digitally encoded and published on the Internet. All this information must be secure and the best method is encryption. Given that there may be interest so many of "breaking" of a computer network, it is obvious that the designers of its hardware and software resources must take serious measures to protect against malicious attempts. Protection methods that can stop "enemies" may be useless or having a very limited impact on some opponents – that they are devoted and with considerable material possibilities.

References

1. Biskup, J. **Security in Computing Systems: Challenges, Approaches and Solutions,** Ed. Spring-Verlag Berlin Heidelberg, 2009, pp. 6
2. Brenton, C., Hunt, C. **Mastering Network Security**, 2nd Edition, Ed. Sybex, 2004
3. Craig, S., Bott, E., Siechert, C. - *Windows 7 Inside Out*, Published by Microsoft Press, 2010, pp. 498-531
4. Dean, T. **Network+ Guide to Networks**, 5th Edition, Ed. Course Technology, 2010, pp. 2-10
5. Fehily, C. **Microsoft Windows 7: Visual QuickStart Guide**, Ed. Peachpit Press, 2010, pp. 381-390
6. FitzGerald, J., Dennis, A. **Business Data Communications and Networking**, Ed. John Wiley & Sons, 2009, pp. 366-417
7. Kizza, J.M. **A Guide to Computer Network Security**, Ed. Springer, 2009, pp. 43-56
8. Kizza, J.M. **Computer network security**, Ed. Springer, 2005, pp. 178-179

9. Mârşanu, R., Reveiu, A., Constantinescu, R., Alecu, F., Ion, A.M., Bologa, R., Botha, I., Vespan, D., Velicanu, A. **Calculatoare**, Editor Tribuna Economică, 2009, pp. 371-384
10. Mârşanu, R. **Servicii de securitate a rețelelor de calculatoare WLAN**, Revista Tribuna Economică nr.15 din 14 aprilie 2010, pp. 30-32
11. Mârşanu, R **Vulnerabilități în rețelele de calculatoare WLAN**, Revista Tribuna Economică nr.19 din 12 mai 2010, pp. 32-34
12. Mârşanu, R **Niveluri și aspecte în securitatea rețelelor de calculatoare**, Revista Tribuna Economică nr.23 din 9 iunie 2010, pp. 29,30
13. McNab, C. **Network security assessment**, Editia a 2-a, Ed. O'REILLY, 2007
14. Miller, P. *TCP/IP* **The Ultimate Protocol Guide**, Vol. 1, Ed. BrownWalker Press, 2009, pp. 534-535
15. Nell, D., Lewis, J. **Computer Science Illuminated**, Ed. Jones and Bartlett Publishers, 2009, pp. 505, 524
16. Panek, W., Wentworth, T. **Mastering, Microsoft Windows 7 Administration**, Ed. Sybex, 2010, pp. 391
17. Parsons, J.J., Oja, D. **New Perspectives on Computer Concepts**, Ed. Course Technology, 2010, pp. 198-201
18. Singh, B. **Network Security and Management**, Ed. Prentice-Hall of Indita Private Limited, 2007, pp. 10-17, 34-38,
19. Stallings, W. **Cryptography and Network Security: Principles and Practice**, Ediția a 5-a, Ed. Pearson Education, 2010, pp. 529
20. http://www.microsoft.com

[1] **Radu MARSANU** is professor at Computer Science Department, Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies Bucharest. He has graduated Faculty of Cybernetics, Statistics and Economic Informatics in 1978 and he holds PhD diploma in 1993. He is the author of 42 books and university courses in the domain of informatics, the last published book being *COMPUTERS* in December 2009. For the *PERSONAL COMPUTERS Architectural Elements* book, he won the prize *Book of the year 2001* in informatics domain. In 2007, he received from graduates of the Faculty of Cybernetics, Statistics and Economic Informatics, diploma of excellence in teaching activities for exceptional specialized knowledge. His scientific research activity include over 43 articles and studies published in the journals of international scientific conferences or in professional journals rated by CNCSIS, indexed in international databases, among them two articles are ISI rated. He participated in 38 research projects as director (two projects) or as team member. He is member of the Informatic National Commission of the Ministry of Education Research Youth and Sports from 1995, president of the Commission to National Olympiade in Informatics, member of the Commission for the selection the members of Romania olympic team at international competitions, member of INFOREC and UPI professional associations. Areas of professional competence are: Computer Science and Networks, Operating Systems, Economic Informatics, Technology of Databases, Technology of Web applications, Management information systems, E-learning, E-commerce.

[2] **Claudiu SICHITIU** has graduated of the Bucharest, Academy of Economic Studies, Faculty of Cybernetics, Statistics and Economic Informatics in 2010. He follows the Economic Informatic master courses. His research interests include computer networks security, economic informatics and object-oriented programming. Main capabilities and skills: advanced programming in C/C++, C#, Java, SQL ORACLE, PL/SQL.

[3] **George SICHITIU** follows actual the Economic Informatics master courses. He is graduated of the Academy of Economic Studies in Bucharest**,** the Faculty of Cybernetics, Statistics and Economic Informatics in 2010. His areas of interests are computer science and networks, software programming, database technology, operating systems. Main capabilities and skills: programming in C, C++, C#, Java, computer network, project management.