SECURITY OF COMPUTER NETWORKS IMPLEMENTED IN UNIVERSITIES AND BUSINESS ENVIRONMENT

Andreea IONESCU*

Abstract. *This article talks about the main aspects of security in computer networks implemented in universities and business environment. To achieve integrity and protection of environmental resources for network communication, ISO (International Standards Organization) has established the security services based on a set of security mechanisms that can be implemented in all protocol OSI (Open Standard Interconnection).The computer network is a combination of hardware, software and cables (optical and classical), that together allow to several computers to communicate with each other. Computer networks are of the following types: Personal Area Network, Local Area Network, Home Area Network, Storage Area Network, Campus Area Network, Metropolitan Area Network, Wide Area Network, Enterprise Private Network, Virtual Private Network and Global Area Network. There are also computer network that does not use cables (no optical, no classical) for transmitting information between its components, infrared and radio waves, which are called wireless networks (wireless), so allowing these networks to be mobile and easy to use. In this scientific article, I made research on the network of computers from Hyperion University, where I work as assistant in computer science and I presented different methods of security of computers used in laboratories of research by students and teachers from Hyperion University.*

Keywords: *security, computer networks, PAN, LAN, HAN, SAN, CAN, MAN, WAN, EPN, VPN, GAN.*

1. Introduction

In the past, computers were located in data centers, where users could run their programs. Today, more interconnected computers in different office, buildings or geographical areas are called computer networks. A network of computers designates a lot of interconnected computers able to

* The Hyperion University from Bucharest, 169, Calea Calarasilor Street, Bucharest, Romania, 030615, The Academy of Economic Studies from Bucharest, andreeaionescu252011@yahoo.com

communicate among themselves in order to exchange information or sharing more resources. The advantages of networking are: access to resources, increased reliability, saving money and environment strong communication. There are the following types of computer networks: PAN, LAN, HAN, SAN, CAN, MAN, WAN, EPN, VPN and GAN. The scientific article “Improving the security of industrial networks by means a formal verification” demonstrates that “Computer networks are exposed to serious security threats that can even have catastrophic consequences from both the points of view of economy and safety if such networks control critical infrastructures, such as for example industrial plants. Security must be considered as a fundamental issue starting from the earlier phases of the design of a system, and suitable techniques and tools should be adopted to satisfy the security –related requirements. The focus of this paper is on how formal methods can help in analyzing the standard cryptographic protocols used to implement security-critical services such as authentication and secret keys distribution in critical environments. The analysis of the 802.11 shared key authentication protocol by S3A, a fully automatic software tool that is based on a formal approach, is illustrated as a case study, which also highlights the peculiarities of analyzing protocols based on a wireless channel.” [1]

2. Experimental (Theory, Modeling)

Classification of computer networks

Computer networks are divided into: LAN, MAN, WAN, PAN, GAN, SAN, EPN, VPN. Relatively small networks with more than a few hundred computers in the same building directly connected networks are called Local Area Network. A wireless LAN (based on radio) is called WLAN-Wireless LAN. Thus, the scientific article “Security Framework for Wireless Sensor Networking-Review” demonstrates that “Due to the significant advances in miniaturization, low power circuit design but reasonably efficient to carry the sensitive information through wireless communication, wireless sensor network (WSN) have attracted attention a lot in recent years. WSN’s are being used in many applications like health monitoring, military purposes, and home automation. Since WSN suffer from many constraints including lower processing power, low power life, small memory and wireless communication channel, security becomes the main concern to deal with such kind of networks. Due to these well accepted limitations, WSN is not able to deal with traditional cryptographic

algorithms. This paper gives an overview of cryptographic frameworks designed so far and also a comparison of existing schemes is tabled."[2]

WAN-Wide Area Network means the geographically wide area networks, such as between two cities on a country, a continent, or even worldwide.

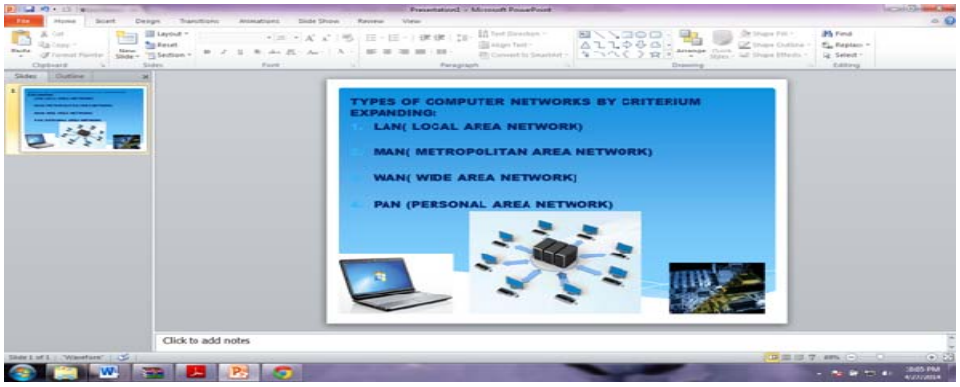

Figure 1. Types of computer networks after the criterion distance.

Definition of computer network

What is exactly a computer network?

A computer network or a data network represents a telecommunications network which allows computer to exchange data. Networked computing devices pass data each to each other along data connections in computer networks. In a computer network, the connections (network links) between nodes are established with wireless media or using cable media. Internet represents the best-known computer network. In a computer network, devices that originate, route and terminate the data are called nodes. Nodes of a computer network are: personal computers, laptops, phones, web servers and networking hardware. Two such devices are called to be networked together when one device is able to exchange information and data with each other, if they have or not a direct connection to each other. The applications supported by computer networks are: World Wide Web, printers, fax machines, shared use of application and storage server, use of e-mail and instant messaging applications.

Network topology

The physical layout of a network is less important than the topology that interconnects network nodes. The majority of diagrams that describe a

physical network are topological, not geographic. The symbol on those diagrams denotes network nodes and network links.

Network links

In a computer network, the communication media used to link devices to form a computer network are of the following type: optical fiber (fiber optic communication), electronic cable (Home PNA, power line communication and radio waves (wireless networking). In the OSI Model the communication media are defined at layer 1 and 2-the physical layer and the data link layer. IEEE 802.3 or represents a family of communication media between networked devices over Ethernet. What makes Ethernet? Ethernet exactly transmits data over fiber and copper cables. IEEE 802.11(Wireless LAN standard) uses radio waves or other use infrared signals as a transmission medium. Power lines communications uses to transmit data a building's power.

Wired technologies

The following technologies are classified from slowest to fastest transmission speed:

Twisted pair wire represents the most widely medium for all telecommunication. Twisted –pair cable consist of cooper wires which are twisted into pairs. The computer network cabling (wired Ethernet-such as IEEE 802.3) consists of 4 pairs of cooper cabling, that can be used for data transmission and voice transmission. The transmission speed varies from 2 million bits per second to 10 billion bits per second. UTP (Unshielded Twisted Pair) and Shielded Twisted Pair (STP) represent twisted pair cabling. For local area network is used coaxial cable for cable television, office buildings and other worksites. To create a high-speed local area network, ITU-T G.hn technologies uses existing home wiring such as: power lines, coaxial cable and phone lines. What is an optical fiber? An optical fiber is exactly a glass fiber, which carries pulses of light that represent data. Advantages of optical fibers over metal wires are immunity from electrical interference and very low transmission loss. What can do optical fibers? Optical fibers may simultaneously carry multiple wavelengths of light that increases the rate that data can be sent and also enable data rates of up to trillions of bits per second. The optical fibers can be used for undersea cables to interconnect continents and for long runs of cable carrying very high data rates. In a business, price represents a main factor distinguishing wired-and wireless technology.

There are more types of Wireless technologies are of the following types: terrestrial microwave, communications satellite, radio and spread spectrum technologies.

1. The terrestrial microwave-communication uses Earth –based transmitters and receivers resembling satellite dishes. The terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. The relay stations are spaced to 48 km (30 mi) apart.

2. The communications satellites-the satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. Where are located the satellites? The satellites are stationed in the space, in geosynchronous orbit 35400 (22000 mi) above the equator. They are capable of receiving and relaying voice, TV signals and data. Also cellular and PCS systems are using several radio communications technologies.

3. The radio and spread spectrum technologies –wireless local area networks use a low-frequency radio technology and a high-frequency radio technology similar to digital cellular. To enable communication between multiple devices in a limited area are used wireless LANs spread spectrum technology. The IEEE 802.11 standard defines a common flavor of open standard wireless radio-wave technology known as Wi-Fi. The free-space optical communication is using a visible or invisible light for communications. The line-of-sight propagation in the most cases, is used, that limits the physical positioning of communicating devices. The scientific article "Wireless mesh network security: A traffic engineering management approach" demonstrates "The wireless mesh network (WMN) is an emerging multihop, heterogeneous, easily scalable and low cost network. The architecture of the WMN is a connectionless-oriented, mobile and dynamic traffic of routed packets. The mesh infrastructure environment easily forms multiple chains of wireless LANs (WLAN) coupled with the simultaneous multihop transmission of data packets from peripherals via mobile gateways to the wireless cloud. WMN operates as an access network to other communication technologies. This exposes the WMN to numerous security challenges not only in the mesh transmission operation security but also in the overall security but also in the overall security against foreign attacks. We surveyed and identified the security vulnerabilities in Internet Protocol (IP) broadband networks, the security challenges in the routing layer of the WNM and explored new concepts to solving security challenges in WMN using traffic engineering (TE)

security resolution mechanisms. We analyzed the advantages, comparative strengths and weakness in the use of traffic engineering based on simulation results and evaluations."[3]

The exotic technologies

In time, there have been various attempts of transporting data through exotic media:

IP over AVIAN Carriers was a humorous April fool's Request for Comments, issued as RFC 1149 was implemented in 2001 in real life. The extending of Internet to interplanetary dimensions is done via radio waves.

Network nodes

Starting from the physical communications media described here, the network compromise additional basic system building blocks, such as: hubs, repeaters, routers, bridges, modems, switches, network interface controller (NICs) and firewalls.

The network interfaces

A network interface controller (NIC) represents a computer hardware that provides a computer with the ability to access the media transmission and it has the ability to process low-level network information. For example I give in this context the NIC that may have a connector for accepting a cable, or an aerial for wireless transmission and reception with the associated circuit. In Ethernet computer networks, each computer network has a unique MEDIA ACCESS CONTROL (MAC) address-usually stored in the controller's permanent memory. The Institute of Electrical and Electronic Engineers (IEEE) to avoid address conflicts between networks devices; it maintains and administers MAC address uniqueness. An Ethernet MAC address has the size of six octets, so that the three most significant octets are reserved to identify NIC manufacturers and these manufacturers, using only their assigned prefixed, uniquely assign the three least-significant octets of every Ethernet interface they produce.

The repeaters and hubs

What is a repeater? A repeater represents an electronic device that receives a network signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction and the signal can cover longer distances without degradation. In twisted pair, Ethernet configurations repeaters are required

for cable that runs longer 100 meters. Repeaters can be tens or even hundreds of kilometers apart with fiber optics. What is a hub? The hub represents a repeater with multiple ports. The repeaters work on the physical layer of the OSI model. The repeaters require a small amount of time to regenerate the signal and this can cause a propagation delay, which affects network performance. Many network architectures limit the number of repeaters that can be used in a row, such as the Ethernet 5-4-3 repeaters. The repeaters are used for long distance links such as undersea cabling.

The bridges

What are bridges? A network bridge connects and filters traffic between two network segments at data link layer (layer 2) of the OSI model to form a single network, so it breaks the network's collision domain and maintains a unified broadcast domain. The network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient computer networks. Bridges are of the following types:

1. The Local Bridges connect directly LANs.
2. The Remote Bridges are used to connect a WAN (Wide Area Network) links between LANs. The remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
3. The wireless bridges can be used to join LANs or to connect remote devices to LANs.

The Switches

A network switch represents a device that forwards and filters OSI layer 2 between ports based on the MAC addresses in the packets. A switch is different from a hub because it only forwards the frames to the physical ports involved in the communication rather than all ports connected. The switch it can be thought of as a multi-port bridge. It learns to associate physical ports to MAC addresses by exam the addresses source of received frames. In the case of an unknown destination is targeted, the switch broadcasts to all ports but the source. In normal mode the switches have numerous ports, facilitating a star topology for devices and cascading additional switches. The multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The switch is often used loosely to include devices such as bridges and routers, as well as devices that may distribute traffic based on load or based on application content, I give in this context for example a Web URL identifier.

The Routers

What is a router? A router represents an internetworking device that forwards packets between networks by processing the routing information included in the packet of datagram-an example is the Internet protocol information from layer 3. The routing information is processed in conjunction with the routing table. To determine where to forward packets a router uses its routing table(a destination in a routing table includes a “null”, also known as the “black hole” interface so it can go into it, however, no processing is done for said data.

The Modems

What are modems? Modems are used to connect network nodes via wire not originally, designed for digital network computer traffic, or for wireless. For doing this, one or more frequencies are modulated by the digital signal to produce an analog signal that can be tailored to give to required properties for transmission. The modems are used for telephone lines, using a Digital Subscriber Live technology.

Firewalls

What are firewalls? A firewall represents a network device for controlling network security and access rules. Typically firewalls are configured to reject access requests from unrecognized sources while allowing actions from recognized one. The firewalls play in a network computer the vital role of growing security in parallel with the constant increase in cybernetic attacks. The scientific article “Improving cloud network security using the True-Rule Firewall” tells “In this study, we aim to identify the limitations of the currently used firewalls(Listed-Rule firewalls) and have found disadvantages including: (1) possibility of shadowed rule that causes the problematic network security and functional speed;(2) rule switching that changes the meaning of the rules entailing the problematic network security;(3) possibility of redundant rules that entails the problematic speed; (4) designing that the needs to place the bigger rule after smaller rules, which cause the designing difficulty; and (5) sequential rule processing that causes the problematic speed.

Furthermore, we have proposed the Tree-Rule firewall that demonstrates none of the above-mentioned limitations. The Tree-Rule firewall utilizes rules in a tree data structure, and forwarding decision of an input packet based on the rules with follow the tree structure so that the

decision on the packet becomes faster. The Tree-Rule firewall has been tested and compared with IPTABLES on LAN and we found that the Tree-Rule gives better performance."[4]

Network structure

The network topology represents the layout or organizational hierarchical of interconnected nodes of a computer network. Different network topologies can affect throughput and reliability is more critical often. Having many technologies, such as bus networks, a single failure can cause to fail entirely. The robustness of a computer network is given by the big number of interconnections, but the more expensive is it to install.

Common layouts

The common layouts are: a bus network, a star network, a mesh network and a tree network.

The bus network means that all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.

The star network means all nodes that are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.

The ring network means that each nod is connected to its left and right neighbor node, so that all nodes are connected and that each node can reach each other node by traversing nodes left-or right. FDDI (Fiber Distributed Data Interface) made use of such topology.

The mesh network means that each node is connected to an arbitrary number of neighbors in such a way that there is at least one traversal from any node to other. In a tree network all nodes are arranged hierarchically. Important here is the fact that the physical layout of the nodes in a network reflect the network topology. A good example is that of FDDI (Fiber Distributed Data Network), where the network topology is a ring (actually the counter-rating rings), but the physical topology is often a star, because all neighboring can be routed via central physical location.

Overlay network

An overlay network represents a virtual computer network that is built on top of another network. In the overlay network, nodes are

connected by virtual or logical links. In an overlay network, each link corresponds to a path, perhaps through many physical links, in the underlying network. Topology of the overlay network may (and often does) differs from that of the underlying one. We present an important example – many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet. The overlay networks have been around since the invention of networking when the computer systems were connected over telephone lines using modems, before any data network existed. The Internet itself is a striking example of an overlay network.

At first, the Internet was built as an overlay on the telephone network. Today, at the network layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network. However, the overlaying network, is composed of a mesh-like interconnect of sub-networks interdicts a table (actually a map) indexed by keys. The overlay networks also have been proposed as a way to improve Internet routing, such as, the example is through quality of service guarantees to achieve higher-quality streaming media. Previous proposals as the following examples IP Multicast, DiffServ and IntServ have not seen wide acceptance largely because they require modification of all routers in the network. An overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. I can say that the overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination. Akami Technologies manages an overlay network that an overlay network that provides reliable, efficient content delivery (a kind of multicast). The Academic research includes end system multicast resilient routing and quality of service studies, among others.

COMMUNICATIONS PROTOCOLS

The communications protocols are: HTTP, TCP, IP, POP3, UDP and IP.

The scientific article “Presentation of various types of electronic business available on the Internet, Advantages, Disadvantages, Key Requirements and Security Implementation Model of an Electronic

Business" demonstrates "The development of the electronic business that is found on the Internet supposes the usage of the standards like:

- TCP/IP (Transmission Control Protocol/Internet Protocol) is represented by the communication between TCP and IP. These were the first networking protocols defined in these standards;
- On the Internet TCP/IP is the communication protocol and it is used for communication between computers; also we can say that:
- TCP/IP defines the way in how electronic devices are connected on the Internet and how data should be transmitted between them;
- The protocols that are found inside TCP/IP standard are:
- TCP (Transmission Control Protocol) it is used for the communication between applications;
- UDP (User Datagram Protocol) it is used for simple communication between applications; it is included in the Internet Protocol Suite, the principal set of network protocols used on the Internet;
- IP (Internet Protocol) this is used for communications between computers; now we have IPV4 (Internet Protocol Version 4) and his successor IPV6;
- ICMP (Internet Message Protocol) this is a used for errors and statistics and also for supervising and diagnosis the problems from the network;
- DHCP (Dynamic Configuration Protocol) represents a network protocol of computers used by hosts (DHCP clients) that assign IP addresses and other information of configuration the network in a dynamic way;
- HTML (Hypertext Markup Language) represents a form of markup oriented presentation of text documents on one page, using the specialized software called HTML user agent.
- HTTP IETF (Internet Engineering Task Force) has coordinated the development of the HTTP which represents an application protocol for distributed, collaborative and hypermedia information systems. HTTP is the most commonly used methods for accessing information on the Internet that are stored on the World Wide Web. The HTTP protocol is the default text protocol for WWW. If a URL does not contain the part of the protocol, it is considered as HTTP. HTTP requires that the destination computer runs a program that understands the protocol and sent to the destination file can be an HTML (Hypertext Markup Language), a graphics file, sound, animation or video, an executable program on that

server and a publisher the text. According to OSI classification HTTP protocol for application level and the implementation and its evolution is coordinated by the W3C (World Wide Web Consortium).”[5]

The Internet layering system or TCP/IP model and its relation to common protocols often layered on top of it. The communication protocol represents a set of rules for exchanging information over network links. In a protocol stack, each protocol leverages the services of the protocol below it. HTTP running over TCP over IP over IEEE 802.11/TCP is an important example of a protocol stack. Ethernet represents a family of protocols used in LANs, described by a set of standards together called IEEE 802 published by the Institute of Electrical and Electronic Engineers. Ethernet has a flat addressing scheme and it operates mostly at levels 1 and 2 of the OSI model. Today, for home users, the most well know member of the protocol family is IEEE 802.11, otherwise a Wireless LAN (WLAN).The complete protocol IEEE 802 suite provides a diverse set of networking capabilities. MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol, IEEE 802.11Q describes VLAN’s and IEEE 802.1X it defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs and it is also found in WLANs-it is what the home user sees when the user has to enter a wireless access key.

INTERNET PROTOCOL SUITE

TCP/IP or the Internet Protocol Suite is the foundation of all modern networking. The Internet Protocol Suite offers connection-less as well as connection-oriented services over an inherently unreliable network crossed by data-gram transmission at the Internet Protocol (IP) level. The protocol suites at this core defines the addressing, identification, and routing specifications for Internet Protocol Version 4 (IPv4) and for IPv6, the next generation of the protocol that has a much enlarged addressing capability.

SONET/SDH

SONET (Synchronous Optical Networking) and SDH (Synchronous Digital Hierarchy) represent standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. These protocols were originally designed to transport circuit mode

communications from a variety of different sources primarily to support real-time, uncompressed circuit switched voice encoded in PCM (Pulse Cod Modulation) format. SONET/SDH was the obvious choice for transporting ATM (Asynchronous Transfer Mode) frames. Asynchronous Transfer Mode represents a switching technique for telecommunications computer networks, which uses asynchronous time-division multiplexing and encodes data into small, fixed-cells. ATM is different from other protocols such as Internet Suite Ethernet that uses variable sized packets or frames and has similarity with both circuit and packet switched networking. Asynchronous Transfer Mode is similar to with both circuit and packet switched networking. This thing is a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as video and voice. ATM use a connection oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

GEOGRAPHIC SCALE

By the characterization centralized by its physical capacity or its organizational purpose a network can be classified. Using the network, including user authorization and access rights, differ accordingly.

PERSONAL AREA NETWORK

A personal area network (PAN) represents a computer network used for communication among computer and different information technological devices close to one person. Devices that are used in personal area network are: fax machines, printers, personal computers, telephones, video game consoles, PDA’s and scanners. Personal Area Network includes wireless and wired devices. A wired PAN is constructed with USB and Firewire connection and a Wireless PAN is formed from technologies like Bluetooth and infrared communication.

LOCAL AREA NETWORK

What is a Local Area Network? A Local Area Network represents a computer network that connects computers and devices in a limited geographical area such as: school, home, office building and closely positioned group of buildings. Wired LAN’s are based on Ethernet technology, but newer standards such ITU-G provides a way to create a wired LAN existing wiring, such as power lines, telephone lines and

coaxial cables. The main characteristics of a Local Area Network are: higher data transfer rates, limited geographic range and lack of reliance on leased lines to provide connectivity. The IEEE 802.3 Local Area Network technologies operate at data transfer rates up to 100Gbit/s. A Local Area Network is connected to a Wide Area Network using a router. The scientific article “Research of Network Security Assessment Quantization Based on Mobile Agent” shows to readers that “As the security situational assessment widely applying to the computer network field, scholars have designed and implemented a large number of network security situational assessment methods. However, most works are based on local area network and single host, which is hardly to meet the demand of large-scale network security assessment. In this paper, we based on quantitative hierarchical network security situational assessment model, introduced the mobile agent technology, designed the distributed computing for large-scale network and evaluated the whole network security situation for future prediction.”[6]

HOME AREA NETWORK

What is a home area network? The home area network represents a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers, laptops and accessories, such as printers and mobile computing devices. The most important function is sharing of Internet access, often a broadband service a cable TV or digital subscriber.

STORAGE AREA NETWORK

What is a storage area network? A storage area network represents a dedicated network that provides access to consolidated, block level data storage. Storages Area Network are primarily used to make storage devices, such as tape libraries, disk arrays and optical jukeboxes accessible to servers so that the devices appear like locally attached devices to the operating system. A storage area network typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The complexity and cost of Storage Area Networks dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium sized business environments.

CAMPUS AREA NETWORK

What is a campus area network? The campus area network (CAN) is made up of interconnection of local area networks within a limited geographical area. The switches and the routers (networking equipment) and optical fiber, cooper plant, Cat 5 cable (transmission data) are owned by the campus owner (a university, enterprise and government). A university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls. The backbone network represents a part of a computer network infrastructure that provides a path of exchange of information between different sub-networks and Local Area Networks. The backbone network can tie together sub-networks, diverse networks within the same building, across different buildings or over a wide area network. The most excellent example is a large company that might implement a backbone network to connect departments that are located around the world. The network backbone is formed from the equipment that ties together the departmental networks. The critical factors that must take into account when designing a network backbone are: network performance and network congestion. In normal way, the backbone network's capacity is greater than that of the individual networks connected to it. The most significantly example of a backbone network is the Internet backbone, which represents a set of wide area networks (Wide Area Networks) and core routers that ties together all computer networks interconnected to the Internet.

METROPOLITAN AREA NETWORKS

What is a metropolitan area network? The metropolitan area network represents a large computer networks that usually spans a city or a large campus.

WIDE AREA NETWORK

What is a wide area network? The wide area network (WANs) represents a computer network which covers a large geographic area such as: a city, a country and spans different distances. A Wide Area Network uses a communications channel that combines many media such as: cables, telephone lines and air waves. The Wide Area Network often makes the usage of transmission, which facilitates by common carriers, such as

telephones companies. The Wide Area Network technologies in generally way that function at the lower three layers of the OSI reference model: the physical layer, the data link layer and the network layer.

ENTERPRISE PRIVATE NETWORK

An enterprise private network represents a computer network that a single organization builds to interconnect its offices locations (examples: shops, production sites, head offices and remote offices), so they can share computer resources.

VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) represents an overlay computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks(for example, the Internet) instead of by physical wires. Where appropriate, the data link layer protocols of the virtual network are said to be tunneled through the larger computer networks. One common application is secure communication through the public Internet but a VPN need not have explicit security features, such as content encryption or authentication. Virtual Private Networks (VPNs) can be used to separate the traffic of different user communities over an underling network with strong security features. The virtual private network may have best-effort performance, or may have a defined service level agreement (SLA) between the Virtual Private Network customer and the Virtual Private Network service provider. A VPN has a topology more complex than point-to-point.

GLOBAL AREA NETWORK

What is a global area network? The Global Area Network represents a computer network used for supporting mobile across an arbitrary number of Wireless Local Area Networks, satellite coverage the areas and so on. In the mobile communications the key challenge is handling off user communications from one local coverage area to the next. The IEEE Project 802 involves a succession of terrestrial wireless Local Area Networks.

ORGANIZATIONAL SCOPE

The computer networks are typically managed by the organizations that own them. The private enterprise network may use a combination of

extranets and intranets. They provide the network access to the Internet, which has no only a single owner and permits virtually unlimited global virtually unlimited connectivity.

INTRANETS

What represents an intranet? An intranet represents a set of computer networks that are under the control of a single administration entity. An intranet uses the IP protocol and IP-based tools like web browsers and file through the intermediate of applications. The administrative entity limits the usage of the intranet to its authorized users. An intranet represents the internal Local Area Network of an organization. An intranet typically has at least one web server to provide users with organizational information. On a local area network, an intranet represents an intranet, which is also anything behind the router.

EXTRANET

What is an extranet? An extranet represents a computer network that is also under the administrative control of a single organization and supports a limited connection to a specific external network. The best example is that of an organization, which may provide access to some aspects of its intranet to share data with its customers and business partners. The others entities aren't necessarily trusted from a security standpoint. The network connection to an extranet is often implemented via Wide Area Network technology. The internetwork represents the connection of multiple computer networks via a common routing technology using the routers.

INTERNET

The largest example of internetworking is the Internet. It represents a global system of interconnected, academic corporate, governmental, public and private computer network. The Internet is based on the networking technologies of the Internet Protocol Suite. Also the Internet represents the successor of the Advanced Research Projects Agency Network (ARPANET), which was developed by DARPA of the United States Department of Defense. The Internet represents the communications backbone underlying the World Wide Web (WWW). The participants in the Internet, use a diverse array of methods of several hundred document

and opened standardized protocols that are compatible with the Internet Protocol Suite and a addressing system(IP addresses), administered by the Internet Assigned Number Authority and address registries. Large enterprises and service providers exchange information about the reach of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

The scientific article “Presentation of various types of electronic business available on the Internet, Advantages, Disadvantages, Key Requirements and Security Implementation Model of an Electronic Business” demonstrates that “The Internet represents a whole infra-structure, services, users and resources. It also refers to:

- Backbones->high-speed networks that have been made to interconnect other networks in: North America, Europe, South America, Asia;
- Regional networks that connect universities and colleges;
- Commercial networks providing access to main communication network subscribers and their networks of commercial organizations for internal use but are connected to the Internet;
- Local Networks refers to a campus network;

Networks available on the Internet are:

- the Intranet represents a communication system performance of an organization;
- VAN (Value Added Network) private networks for the exchange EDI (Electronic Data Interchange) between business partners(e.g. National Bank of Romania has its own communication network RCD);
- VPN (Virtual Private Network) is a logic network which combines several technologies of the private networks and for establishing connections and networks to ensure security in transit unsafe;
- grid computing used for connecting computer networks around the world, to create and use a global computing environment;
- grid network technology offers the opportunity to meet a wide variety of resources including supercomputers, storage systems, data sources and special classes of devices distributed geographically, to be used as a single computing resources;
- grid computing is another step in process of virtualization started by: the process of partitioning a single system virtual machine;

- virtualization homogenous resource virtualization applied to both servers and the central processing and storage resources, networks and application sometimes;
- virtualization enterprises especially for distributed organizations;
- virtualization outside the organization Internet communication information, integrating information through collaborative networks;
- grid computing is a mean of integrating various technologies and solutions to fulfilling a goal". [5]

DARKNET

DARKNET represents an overlay network, typically running on the Internet, which is only accessible through specialized software. A DARKNET represents anonymous network where connections are made only between trusted peers to sometimes called "friends", using ports and non-standards protocols. DARKNET are different from the distributed peer-to-peer networks like sharing is anonymous (that means, IP addresses aren't shared publicly) and that's way the users can communicate with little fear of governmental on corporate interference. The Internet represents a global system of interconnected governmental, corporate, academic, public and private computer networks and it is based on the networking technologies of the Internet Protocol Suite. It represents the successor of the Advanced Research Project Agency Network (ARPANET).

3. Results

For example in the Hyperion University from Bucharest exist laboratories of computer science, physics, and others, where students from different faculties study and make their hours at different disciplines and use the computers that are on different laboratories to make their researches. Laboratories of research from the Hyperion University from Bucharest are:

1. In A Building there are:
   a. At the second floor exists the Laboratory of Numerical Methods, Microcontroller, Microprocessor Systems and Signal Processing;
   b. At the third floor there is ->CAD/CAM Systems, ASDN and Programming and Automatic.

c. At the fourth floor there is: 4.5 The laboratory of Applied Informatics, Databases, Engineering Programming and Algorithm Design.
d. At the sixth floor there is 6.8 Meeting Automatic Sampling systems, Measurements and Traducers and Automatic System Engineering;
e. At the seventh floor exist: 7.2 The Physics I-The Laboratory of Physics and Thermal Phenomena-Physics I (Mechanics Physics), 7.3 Mechanics Physics and Physics I and 7.4 Theoretical and Mathematics Physics.

2. In B building there are also the following laboratories of research:
a. The Laboratory for Innovative Technology for the Faculty of Exact Sciences;
b. The Laboratory of Automatic Control and Applied Information;
c. The Laboratory for Control Systems or IRA (Automatic Control Engineering).

To protect information, data on the computers we have like measurements of security the following implemented methods:

1. On different computer from the laboratories of research there is an antivirus program and a firewall that protects data and information stored on the computers.

2. At the level of router there is a firewall, which implements its functions: limits the traffic of the public services of the organizations (taking into account IP address and ports), blocks the access of particular websites in the Internet, monitors communication between the internal network and external network, encrypts the transmitted packets through VPN networks, it interdict to some users to access of some servers and external networks;

3. In laboratories of research exists Deep Freeze, which represents a method of freezing partition C. All data from computers are storage on D partition.

4. Another form of protection is ESET Live Scan, which represents a method of virus scanning.

5. If the student follows the path-> My Computer->System and Security->System->System Protection ->System Restore, he will discover that the System Restore is active and represents a restore point created, which represents another form of protection. On the partition D exist hidden files.

4. Discussion

As the reader studies this article he discovers all concepts of security networks implemented in universities and business environment. What business environment means? It refers to online websites of B2C (Business to Consumer) like: http://www.amazon.com, http://ebay.com, http://emag.ro where the reader can access the products online and buy what he likes. Here are many forms of security of the networks via the Internet. The scientific article "Security in computer networks" demonstrates "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, which are fundamental security objectives, 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 policy and procedures."[7]

5. Conclusions

In conclusion, in this scientific paper I presented: types of network computers from literature in computer science and different methods of security and protection of computers from the laboratories of research from Hyperion University.

REFERENCES

[1] I. C. Bertolotti, L. Durante, P. Maggi, R. Sisto, A. Valenzano, *Improving the security of industrial networks by means of a formal verification*, Computer Standards & Interfaces, **29,** pp. 387-397, 2007;

[2] G. Sharma, S. Bala, A. K. Verma, *Security Frameworks for Wireless Sensor Network-Review*, Procedia Technology 6, pp. 978-987, 2012;

[3] O. E. Muogilim, K-K Loo, R. Comley, *Wireless mesh network security: A traffic engineering management approach*, Journal of Network and Computer Applications, **34,** 478-491, 2011;

[4] Xiangjian He, Thawatchai Chomsiri, Priyadarsi Nanda, Zhiyan Tan, *Improving cloud network security using the True-Rule Firewall*, Future Generation Computer Systems, Volume **30,** 2014, pp. 116-126;
[5] A. Ionescu, R. Serban, *Presentation of various types of electronic business available on the Internet, Advantages, Disadvantages, Key Requirements and Security, Implementation Model of an Electronic Business*, Volume **2,** No. **3,** pp. 179-196, 2012;
[6] C. Xiaorong, L. Su, L. Minxuan, *Research of Network Security Situational Assessment Quantitization Based on Mobile Agent*, Physics Procedia, Volume **25,** 2012, pp. 1701-1707;
[7] A. Ionescu, R. Serban, *Security in Computer Networks*, International Journal of Data & Network Security, Volume **1**, No. **3,** pp. 63-84, 2012;
[8] F. Nastase, *Computer networks*, ASE Publishing, Bucharest, 2005, pp. 13-19;
[9] F. Baicu, A. M. Baicu, *Audit and Security of Computer Systems*, Victor Publishing, Bucharest, 2006;
[10] A. Ionescu, Dissertation paper: *Development of an electronic business using technologies PHP and MySQL –BCOMPUTERS*, ASE, Bucuresti, 2010;
[11] http://www.nastasef.ase.ro/fisiere/IEafaceri_electronice/cap7_AE_Securitatea.pdf
[12] Courses of electronic commerce
[13] http://en.wikipedia.org/wiki/Computer_network