NETWORK SECURITY

Christos Douligeris and **Panayiotis Kotzanikolaou**
Department of Informatics, University of Piraeus, Greece

Keywords: Security, Confidentiality, Integrity, Availability, Threats, Attacks, Security Service, Security Mechanism, IPSec, Firewall, IDS, VPN, cryptography

Contents

Summary

The wide deployment of several networks such as the Internet, 3G networks, enterprise networks, WiFi networks and Bluetooth networks to name just a few, has made networking a common task. However, the social, economical, commercial and ethical aspects of the various network applications have raised several security considerations deriving from network usage. This article is concerned with network security issues. First, the concepts related with information security and networks are presented and the goals of network security are analyzed. The concepts of threats, vulnerabilities and risks are briefly explained and some basic categories of network security threats and attacks are described. Security in networks is accomplished through security services. These services are described along with several widely used network security mechanisms which are commonly used to implement the security services. Finally, the differences in the security requirements of wireless networks in contrast with fixed networks are briefly explained in the last section of this article.

1. Introduction

This chapter discusses network security. Computer networks are analyzed and discussed in the previous related chapters. Based on the previous terminology, this chapter describes the security issues in computer networks. A broad definition of *network security* can be constructed by defining its two components, security and networks.

Security is a term which has been given a wide variety of definitions. According to dictionary definitions, *security is the freedom from danger or anxiety*. Among others, security is also defined as: (1) *A situation with no risk, with no sense of threat,* (2) *The prevention of risk or threat,* and (3) *Assurance, sense of confidence and certainty.*

1.1. Security in Information Technology

In traditional information theory, security is described through the accomplishment of some basic security properties, namely *Confidentiality*, *Integrity* and *Availability* of information. Confidentiality is the property of protecting the content of information from all users other than those intended by the legal owner of the information. The non-intended users are generally called unauthorized users. Integrity is the property of protecting information from alteration by unauthorized users. Availability is the property of protecting information from non-authorized, temporary or permanent withholding of information.

Other basic security properties are the *Authentication* and the *Non-repudiation*. Authentication is divided into peer-entity authentication and data-origin authentication. Peer-entity authentication is the property of ensuring the identity of an entity (also known as 'subject'), which may be a human, a machine or another asset such as a software program. Data-origin authentication is the property of ensuring the source of the information. Finally, non-repudiation is the property of ensuring that principals that have committed to an action cannot deny that commitment at a latter time. Detailed treatment of security properties can be found in several security standards, such as the ISO/IEC 7498-2 and the ITU-T X.800 security recommendation.

In a practical Information Technology approach, security involves the protection of information *assets*. In a traditional Information Technology risk analysis terminology, an asset is an object or resource, which is "worthy" enough to be protected. Assets may be:

- *physical* (*e.g.* computers, network infrastructure elements, buildings hosting equipment),
- *data* (*e.g.* electronic files, databases) or
- *software* (*e.g.* application software, configuration files)

The information assets must be protected by security *threats*. A security *threat* is any event that may harm an asset. When a security threat is realized, then an IT system or network is under a security *attack*. The *attacker* or *threat agent* is any subject or entity that causes the attack. Of course an asset may be threatened by various threats and each threat has a different threat level against each asset. An example of a threat agent in a computer network is a malicious outsider (external user) who attempts to bypass security measures and access the network. A threat which may be caused by such an attacker is unauthorized access to network resources.

A security *vulnerability* is any characteristic in a system, which makes one or more assets more vulnerable to threats. In the above example of a threat, a security vulnerability which exposes the system to unauthorized access is the lack or the misconfiguration of access controls. If access to the network is not properly controlled with well configured mechanisms, then it will be easier for a possible attacker to gain unauthorized access into the system and the network is more vulnerable to intrusion attacks.

The *impact* of the threat measures the magnitude of the loss that would be caused to the asset or asset owner if the threat were realized against it. The magnitude of loss is closely related with the operational or business value of the attacked asset.

The combination of threats, vulnerabilities and assets provides a quantified and/or qualified measure of the likelihood of threats being realized against assets, as well as the impact caused due to the realization of a threat. This measure is known as the *security risk.*

The protection of assets can be achieved through several security *mechanisms.* A security mechanism is any type of measure, (technical, procedural, legal etc) which may protect an asset from security threats, reduce their vulnerability and more generally reduce the level of security risks. A security mechanism may be:

- *Preventive*, if its goal is to prevent the realization of a security attack. Such mechanisms mainly reduce the threat level of security attacks.
- *Detective,* if its goal is to detect a security attack as fast as possible and thus restrict the consequences of the attack. These mechanisms mainly reduce the vulnerability level of security attacks.
- *Recovery,* if its goal is to recover the system after a security attack in the shortest possible time. These mechanisms mainly reduce the impact level of security attacks.

Thus, the security mechanisms provide capabilities that reduce the security risk of a system. Note that system and network security does not rely solely on technical security mechanisms. In almost every information system and network, procedural and organizational measures are generally required in addition to technical mechanisms, in order to accomplish the desired security goals.

1.2. Computer Networks

A *computer network* or simply a network is a collection of connected computers. Two or more computer systems are considered as connected, if they can send and receive data from each other through a shared access medium. The communicating entities in a computer network are generally known as *principals*, *subjects* or *entities.* These principals can be further divided into *users, hosts* and *processes.*

- A user is a human entity, responsible for its actions in a computer network.
- A host is an addressable entity within a computer network. Each host has a unique address within a network.
- A process is an instance of an executable program. It is used in a client/server model, in order to distinguish between the client and the server processes.

- A client process is a process that makes requests of a network service.
- A server process is a process that provides a network service, for example as daemon process running continuously in the background on behalf of a service

In order to formalize the way that networking is performed, *network reference models* have been developed, which group similar functions into abstractions known as *layers*. Each layer's functions can communicate with the same layer's functions of another network host. On the same host, the functions of a particular layer have interfaces to communicate with the layers bellow and above it. This abstraction simplifies and properly defines the necessary actions for networking.

The *International Standards Organization* (ISO) *Open Systems Interconnection* (OSI) Reference Model defines seven network layers, as well as their interfaces. Each layer depends on the services provided by its intermediate lower layer all the way down to the physical network interface card and the wiring. Then, it provides its services to its immediate upper layer, all the way up to the running application. The network layers in the ISO/OSI Reference Model are the following (from the lowest to the highest): 1) The *Physical Layer,* 2) The *Data Link Layer,* 3) The *Network Layer,* 4) The *Transport Layer,* 5) The *Session Layer,* 6) The *Presentation Layer* and 7) The *Application Layer*. The X.200 recommendation of the ITU-T is aligned with the ISO/IEC 7498-1 standard. More details on network reference model can be found in *Models and Layered Protocol Organization*.

Each reference model needs a suite of network *protocols* in order to implement the functions of each layer. Generally, a network protocol is a well-defined specification which allows network hosts to communicate in a particular and predefined way. From a point of view, protocols define the "syntax" of the communication. By properly combining protocols in protocol stacks, the layers of network reference models can be implemented and allow network communication. It needs to be noted that not all protocol suites include all the seven layers of the ISO/OSI model. The most popular protocol suite, the Transmission Call Protocol/ Internet Protocol (TCP/IP), has five layers. There are no Presentation and no Session layers; the functions of these layers are incorporated in the layers above and below. Although detailed description of the TCP/IP is given elsewhere, it is important to understand how it works, in order to understand network security.

A network is considered as a *wired* or *fixed* network if the access medium is some kind of physical cable connection between the computers, such as a copper cable or a fiber optic cable. On the other hand, a network is considered as a *wireless* network, if the access medium relies on some kind of signaling through the air, such as RF communication. A network can also be divided according to its geographical coverage. Depending on its size, a network can be a Personal Area Network (PAN), a Local Area Network (LAN), a Metropolitan Area Network (MAN) or a Wide Area Network (WAN).

1.3. Telecommunication Networks

A telecommunication network is a collection of connected links, which allow messages to pass from one part of the network to another, through the intermediate links. In the general term, computer networks may be considered as telecommunication networks. However, the term telecommunication networks are basically used to describe telephone networks. These include fixed networks, such as the Public Switched Telecommunication Network (PSTN), which is globally used for wire-line telephone communications. They also include mobile networks, such as the Global System for Mobile communications (GSM), which is the most common cellular phone network, or the next generation Unified Mobile Telecommunication System (UMTS) network. The GSM is considered as second-generation (2G) mobile network, while UMTS is considered as a third generation (3G) mobile communication network.

The General Packet Radio Service (GPRS) is a service that provides packet radio access for GSM users as a step towards the third-generation telecommunication networks. GPRS reserves radio resources only when there is data to be sent. In this way it enables the efficient provision of a variety of packet-based services to the mobile subscribers of second generation networks. GPRS attempts to reuse the existing GSM network elements as much as possible, in order to effectively build a packet-based mobile cellular network.

UMTS is a realization of 3G networks, intending to establish an integrated system that supports different operating environments. Users have seamless access to a wide range of new telecommunication services, such as high data rate transmission for high-speed Internet applications, independently of their location. Thus, mobile networks are a natural extension of the wired Internet computing world, enabling access for mobile users to multimedia services that already exist for non-mobile users and fixed networking.

Security in telecommunication networks has in general the same requirements as in computer networks, concerning the required security services and mechanisms, which are discussed in the following sections. However, the security design in telecom networks shall take into consideration several aspects and differences, such as the closed nature of telecom networks in comparison with the open nature of the Internet, the wireless access of mobile telecommunication networks and the end-user mobility, the particular security threats, the type of information to be protected, and the complexity of the network architecture. The radio transmission is by nature more vulnerable to eavesdropping, than fixed-line transmission. The user mobility and the universal network access certainly provoke security treats. As the telecommunication networks are converging towards IP-based communications (*e.g.* in the GPRS and UMTS) and as computer (information) and telecommunication networks are getting more and more interconnected, a holistic approach towards network security must be followed.

1.4. The Goals of Network Security

Regardless of the access medium and the coverage of a network, *network security* can be considered through the achievement of two security goals: *computer system security* and *communication security*.

- The goal of *computer systems security* is to protect information assets against unauthorized or malicious use, as well as to protect the information stored in computer systems from unauthorized disclosure, modification or destruction.
- The goal of *communications security* is to protect information during its transmission through a communication medium, from unauthorized disclosure, modification or destruction.

In order to achieve the goals of network security in any network, the following steps must be followed:

1. *Define the assets to be protected and the perimeter of the network.* Before implementing any security measures, the assets of the network must be identified and assessed. Furthermore, the perimeter of the network to be protected must be defined, in order to distinguish the internal or private network from the external or unreliable network.
2. *Define the possible security threats and attacks*. After the network assets and the network perimeter have been defined, the possible security attacks that threat the network must be defined and evaluated. This will help in focusing on the protection from the most possible threats. In this process it is very important to consult specialized Internet sites that focus on network security and security threats, either of proprietary products or from security threats and vulnerabilities databases.
3. *Evaluate the security risks and define the desired security level*. The following step is to evaluate the examined threats in conjunction with the existing vulnerabilities and assets. This can be performed by using a risk analysis methodology. Then, after the risks against network security have been identified, the desired security level must be defined, in order to set up the suitable security measures.
4. *Define security policies that formally set up the desired security level*. The desired security level must then be formalized through network security policies. These policies are a formal way to define what security services must be provided, in order to reach the network security goals and to reduce the risk to the desired and acceptable level.
5. *Define the security services and implement the proper security mechanisms*. The security services define what security properties must be maintained in each part of the network, such as authentication and access control. The security mechanism defines the way that will implement the functionality of the defined security services. More details about network security services and mechanisms are provided in the following sections. Note however that the apart from the technical security mechanisms, other non technical security measures are also defined in order to achieve the desired security level that is formally described in the security policies. These non-technical measures are mostly security procedures.
6. *Periodically assure that the proper security policies, services and mechanisms are in place*. Although the security threats may have been properly recognized and security policies may enforce the desired security level with security mechanisms and controls, it is important to periodically assure that everything is set up correctly. Problems may arise due to new security threats and vulnerabilities, new security needs or attenuation of the existing security

mechanisms. The period that each of the above must be examined differs, since due to technology changes it is usually required to examine the security mechanisms more frequently than the security policies or services, or the desired security level.

-
-
-

Bibliography

Douligeris C. and Serpanos D. (eds) (2006). *Network Security: Current Status and Future Directions.* Wiley – IEEE. [This book is a collection of surveys related with all the aspects of network security].

Douligeris C. and Mitrokotsa A. (2004). *DDoS attacks and defense mechanisms: classification and state-of-the-art.* Computer Networks (44), 643-666, Elsevier. [This work provides a survey on several attacks and defense mechanisms for Distributed Denial of Service attacks in networks].

Menezes A. J, van. Oorschot P. C, Vanstone S. A. (1997). Handbook of Applied Cryptography, CRC Press. [This handbook is a major source of information on applied cryptography].

Peltier T.R. (2001). Information Security Risk Analysis, Auerbach Publications, 2001. [This book describes methodologies on information risk analysis and security policies for systems and networks].

International Standardization Organization (1994). *Information Processing Systems – Open Systems Interconnection – Part 1: Basic Reference Model*, ISO/IEC 7498-1: 1984, also ISO/OSI 7498-1: 1994. [This ISO standard describes the basic reference model for networks].

International Standardization Organization (1989). *Information Processing Systems – Open Systems Interconnection – Part 2: Security Architecture*, ISO/IEC 7498-2: 1989. [This ISO standard describes the security architecture for OSI networks].

International Telecommunication Union (1991). *Security Architecture for Open Systems Interconnection for CCIT Applications*, Recommendation ITU-T X.800, 1991.

International Telecommunication Union (1994). *Information Technology – Open Systems Interconnection – Basic Reference Model: The basic model*, Recommendation ITU-T X.200, 1994.

International Telecommunication Union (1995). *Information Technology – Open Systems Interconnection – Lower Layers Security Model*, Recommendation ITU-T X.802, 1995.

International Telecommunication Union (1994). *Information Technology – Open Systems Interconnection – Upper Layers Security Model*, Recommendation ITU-T X.802, 1994.

Biographical Sketches

Christos Douligeris received the Diploma in Electrical Engineering from the National Technical University of Athens in 1984 and the M.S., M.Phil. and Ph.D. degrees from Columbia University in

1985, 1987, 1990, respectively. He has held positions with the Department of Electrical and Computer Engineering at the University of Miami and currently he is affiliated with the Department of Informatics, University of Piraeus in Greece. He has served in technical program committees of several conferences. His main technical interests lie in the areas of performance evaluation of high speed networks, neurocomputing in networking, resource allocation in wireless networks and information management, risk assessment and evaluation for emergency response operations. He was the guest editor of a special issue of the IEEE Communications Magazine on ‘‘Security for Telecommunication Networks’’ and he is preparing a book on ‘‘Network Security’’ to be published by IEEE Press/ John Wiley. He is an editor of the IEEE Communications Letters, a technical editor of IEEE Network, and a technical editor of Computer Networks (Elsevier).

Panayiotis Kotzanikolaou was born in Athens, Greece in 1974. He received his BSc in Computer Science from the University of Piraeus, Greece in 1998 and his PhD in 2003 from the same university. Currently he is affiliated with the Greek Regulatory Authority for the Assurance of Information and Communication Security and Privacy. His research focuses on cryptography and security for mobile agents, distributed systems, intelligent networks, ad hoc networks and sensor networks. He has served as a technical committee member and as a reviewer for various security conferences and as a reviewer for journals in the area of information and communication security.