Security Framework Design Intended for Networked Devices

Byungjoo Park*

Department of Multimedia Engineering, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
**Correspondent Author: Byungjoo Park* (bjpark@hnu.kr)*

Abstract

As more organizations and businesses are using computer networks and the Internet, the need for a secure computing environment must also be increased. A secure computing environment must consist of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, and distribution of computing resources. This paper presents a security framework for securing computer networks, to guide organizations, businesses and individuals to prevent information leak or being passed to unauthorized users.

Keywords: *computer networks, security issues, access control, cryptography*

1. Introduction

The need for a secure computing environment must be tightened as more and more organizations and businesses are using computer networks and the Internet. A secure computing should be taken care of IT Professionals not as an optional component anymore when considering the use of computing resources. Security must be integrated into every system of the computing environment. It must consist of the provisions and policies adopted by the network administrator of an organization to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

Every applications entailed in a computing environment must be incorporated with security, as these applications will be used by people who expect the security and privacy of their data. Security must cover a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among organizations, businesses, and individuals.

This paper presents a security framework for securing computer networks, to guide organizations, businesses and individuals to prevent information leak or being passed to unauthorized users. For these purpose, they must define a proper and effective security policies and standards in place in the organization in accordance with laws and regulations, aside from technology to safeguard their resources against unauthorized access.

The rest of this paper is organized as follows: Section 2 explains the overview of related literatures; Section 3 outlines the security framework design for securing networked devices; and the concluding remarks in Section 4.

2. Related Technologies

2.1 Computer Networks

The interconnection of computers and other devices using a communication channel to allow sharing of resources and information is referred to as a computer network. It is a group of devices connected to each other, wherein at least one device is able to send or receive data to or from a remote device [1].

Computer networks can be classified according to the medium used to transport the data, communications protocol used, scale, topology, benefit, and organizational scope. The rules and data formats for exchanging information in a computer network are known as the communications protocols that provide the basis for network programming.

2.1.1 Wired Technologies

Wired networks make use of Ethernet cables and network adapters to interconnect components. To connect more devices into the network, it generally requires a central device such as hubs, switches, or routers [2].

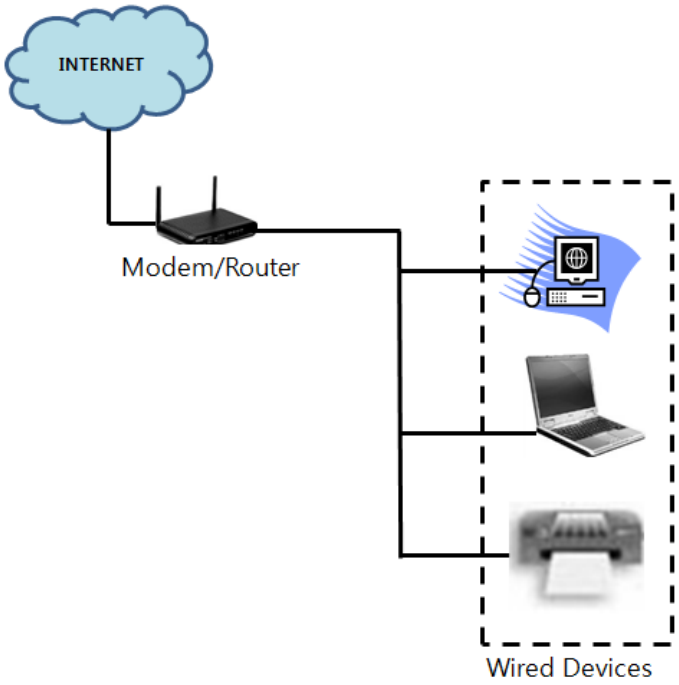

Figure 1. Wired Networks

2.1.2 Wireless Technologies

Any type of computer network that is not connected by any kind of cables is referred to as Wireless Networks. It utilizes a transmitter (e.g. wireless router or access point) that is hardwired to an Internet connection. The other computers or wireless devices are connected

through this access point that acts as a gateway to interconnect these devices in the network and to the Internet [3].

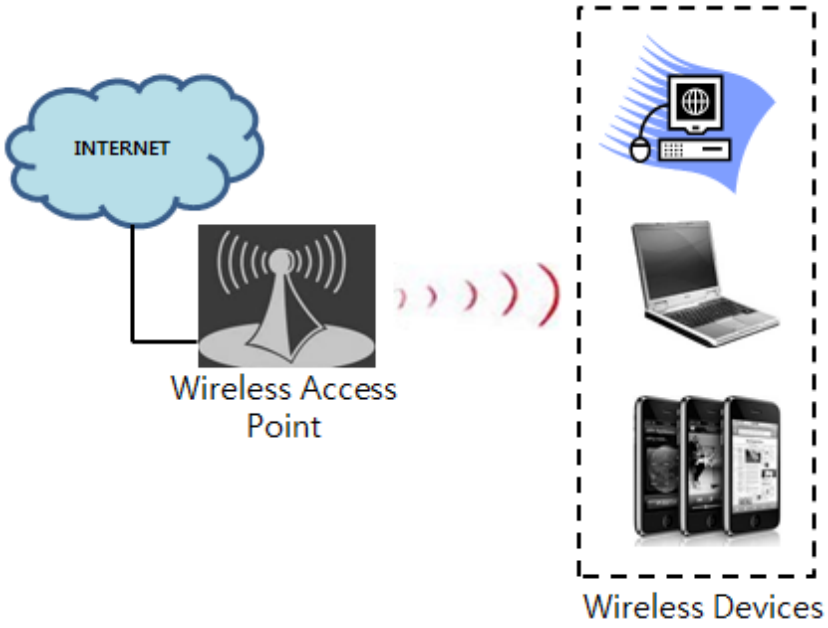

Figure 2. Wireless Networks

2.2 Cryptography

Cryptography refers to the art of information protection. The method used for protection is information transformation called encryption into a coded form with the use of keys. It is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient know, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses [4].

2.2.1 Symmetric-key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher [4].

2.2.2 Public-key Cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair

are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages [6].

3. Security Framework Design for Networked Devices

Security techniques that lead for the design of a security framework of networked devices include encryption, identification, authentication, access control, and other techniques. Protection against network attacks must be designed to withstand the attack and not necessarily to prevent the attack to happen.

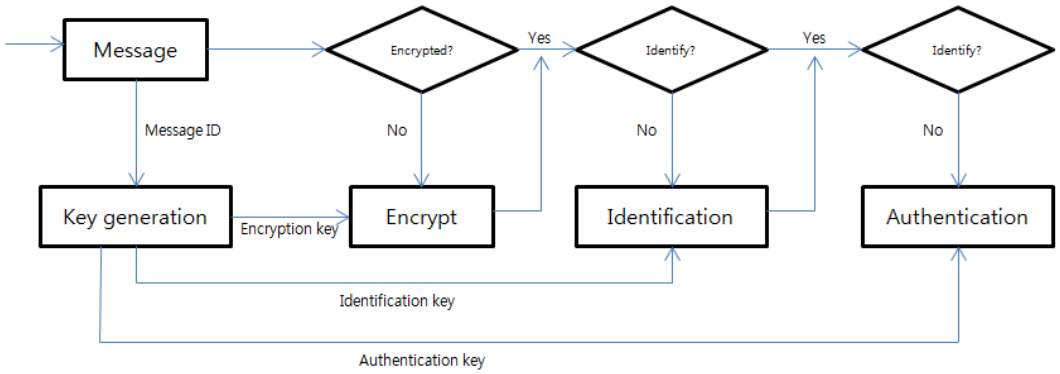

Figure 3. Communication Framework for a Secured Computer Network

In order to prevent security issues from adversary attacks or from malicious mis-configuration, it is essential that devices or computers connected in the network should only accept connections or control messages from valid sources.

The essential services of access control to computer networks must include authorization, identification and authentication, access approval, and accountability [5]:

- authorization is to specify what a user or a group of users can and cannot do;
- identification and authentication enforces that only legitimate users or group of users within the organization can log on to a system;
- access approval is to grant access during operations, by association of users with the resources that they are allowed to access based on the authorization policy;
- accountability identifies what a user (or all users associated with a current user) did.

Figure 3 shows a communication framework designed for a secure channeling of network resources within a computer network. The framework includes cryptography

techniques, and identification and authentication techniques (I and A) for restricting the control access of users of the network.

A proper application of cryptographic techniques enhances the network security against a wide variety of attacks. Cryptographic techniques can provide confidentiality (encryption) of communication between devices, authentication of the identities of the devices, and can ensure that it will be detected if the data being communicated is changed during transit.

To ensure the security and integrity of the computing resources being shared in a computer network, access control policies is included. Identification and Authentication is the secure identification of the network users. Identification is the method for recognizing the user requesting access and authentication. A user or an entity needs to have a unique ID for identification. Example of identifying a living person is through biometrics.

Authentication refers to methods to ensure that message sources are properly identified by the network devices with which they communicate. It is the process of confirming if the user or a message is authentic or true. It is also known as verifying a person's identity. Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems [5].

Furthermore, a written secure network policy covering authorize use and security access is necessarily important for every organization. A typical security policy document could include the following sections:

- Purpose
- Scope
- Policy
- Responsibilities
- Enforcement
- Definitions
- Revision History

Security policies included in the network policy must be thoroughly reviewed. The previously discussed techniques can be incorporated in the Network Security policy of an organization.

4. Conclusions

This paper presents a security framework for securing computer networks, to guide organizations, businesses and individuals to prevent information leak or being passed to unauthorized users. Organizations must consider that technology is not the only issue for information security in computer networks. A secure computing environment must

consist of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, and distribution of computing resources.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024401, 2011-0026286, 2012-0007273).

References

[1] http://en.wikipedia.org/wiki/Computer_network.
[2] http://en.wikipedia.org/wiki/Local_area_network.
[3] http://en.wikipedia.org/wiki/Wireless_network.
[4] http://en.wikipedia.org/wiki/Cryptography.
[5] http://en.wikipedia.org/wiki/Access_Control#Access_Control_Techniques.
[6] http://en.wikipedia.org/wiki/Public-key_cryptography.