# Chapter 3.1
# Current Network Security Technology

**Göran Pulkkis**
*Arcada Polytechnic, Finland*

**Kaj Grahn**
*Arcada Polytechnic, Finland*

**Peik Åström**
*Utimaco Safeware Oy, Finland*

## INTRODUCTION

Network security is defined as "a set of procedures, practices and technologies for protecting network servers, network users and their surrounding organizations" (Oppliger, 2000, Preface). The need for network security is caused by the introduction of distributed systems, networks, and facilities for data communication. Improved network security is required because of the rapid development of communication networks. Network security is achieved by using software- and hardware-based solutions and tools.

## BACKGROUND

This article gives a topical overview of network security technologies, that is, the topics are not covered in detail, and most topics are briefly introduced and left for further study. The main objective is to present "state-of-the-art" network security technologies and to stimulate discussion about related skills and education needed by network users, IT professionals, and network security specialists.

DOI: 10.4018/978-1-61350-323-2.ch3.1

## PROTECTION AGAINST MALICIOUS PROGRAMS

Malicious software exploits vulnerabilities in computing systems. Malicious program categories are (Bowles & Pelaez, 1992):

- **Host Program Needed:** Trap door, logic bomb, Trojan horse, and virus.
- **Self-Contained Malicious Program:** Bacteria and worm.
- **Malicious Software Used by an Intruder after Gaining Access to a Computer System:** Rootkit.

Threats commonly known as adware and spyware have proliferated over the last few years. Such programs utilize advanced virus technologies for the reason to gather marketing information or display advertisements in order to generate revenue (Chien, 2005).

Modern malicious programs (including adaware and spyware) employ anti-removal and stealth techniques as well as rootkits to hide and to prevent detection. Rootkits conceal running processes, files, or system data. This helps an intruder to maintain system access in a way, which can be extremely difficult to detect with known security administration methods and tools. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris, and versions of Microsoft Windows. A computer with a rootkit on it is called a rooted computer (Hoglund & Butler, 2005; Levine, Grizzard, & Owen, 2006).

The ideal protection is prevention, which still must be combined with detection, identification, and removal of such malicious programs for which prevention fails. Protection software is usually called antivirus software, which is characterized by generations (Stephenson, 1993):

- **First Generation:** Simple scanners searching files for known virus "signatures" and checking executable files for length changes.
- **Second Generation:** Scanners using heuristic rules and integrity checking to find virus infection.
- **Third Generation**. Memory resident "activity traps" identifying virus actions like opening executable files in write mode, file system scanning, and so forth.
- **Fourth Generation:** Software packages using many different antivirus techniques in conjunction.

Anti-adware/spyware modules are usually integrated in these software packages.

Protection levels of modern antivirus software are:

- **Gateway Level Protection:** Consists of mail server and firewall protection. Viruses are detected and removed before files and scripts reach a local network.
- **File-Server-Level Protection:** Consists of server software. Viruses are detected and removed even before network users access their files/scripts.
- **End-User-Level Protection:** Consists of workstation software. Viruses undetected in outer defense lines are detected and removed. However, this level is the only antivirus protection level for data communication, which is end user encrypted.

All levels should be combined to achieve depth in antivirus defense. Virus definition databases should be automatically and/or manually updated.

Examples of antivirus and anti-spyware software are Ad-Aware, F-Secure Internet Security, and Norton AntiVirus.

## FIREWALL TECHNOLOGY

Firewalls protect computers and computer networks from external security threats. Firewalls fall into four broad categories (Stallings, 2006):