IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB9159

Chapter I

Network Security Software

Göran Pulkkis
Arcada Polytechnic, Finland

Kaj J. Grahn
Arcada Polytechnic, Finland

Peik Åström
Arcada Polytechnic, Finland

ABSTRACT

This chapter is a topical overview of network security software and related skills needed by network users, IT professionals, and network security specialists. Covered topics are protection against viruses and other malicious programs, firewall software, cryptographic software standards like IPSec and TLS/SSL, cryptographic network applications like Virtual Private Networks, secure Web, secure email, Secure Electronic Transaction, Secure Shell, secure network management, secure DNS and smartcard applications, as well as security administration software like intrusion detectors, port scanners, password crackers and management of network security software management. Tools and API's for security software development are presented. A four-level network security software skill taxonomy is proposed and implications of this taxonomy on network security education is outlined. University and polytechnic level network security education is surveyed and the need for inclusion of network security software development skills in such education is pointed out.

INTRODUCTION AND BACKGROUND

The steadily growing international computer network user community needs an expanding staff of well educated network security professionals to guarantee the reliability of the global IT infrastructure of computer nodes in wired and wireless networks. Network security tools are usually software tools. Network security professionals should know these tools, how to use and develop them, and know what kind of network security they can provide.

In accordance with Oppliger (1999, preface) we define network security as "a set of procedures, practices and technologies for protecting network servers, network users and their surrounding organizations." Network security software (computer programs) covers the area defined above. In order to give a more structured picture of network security software, the material has been organized into the following topics:

- Protection against malicious programs
- Firewall software
- Cryptographic software
- Security administration software
- Security software development
- Network security software skill levels
- Network security software skills in higher education

The text gives a topical overview of network security software: 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" of network security software and to discuss related skills and education needed by network users, IT professionals, and network security specialists.

PROTECTION AGAINST MALICIOUS PROGRAMS

Malicious software exploits vulnerabilities in computing systems. In Bowles and Pelaez (1992) is presented a taxonomy, in which malicious programs are divided into two categories:

1. *Host program needed*
   - **Trap door**

     A trap door is a secret entry point bypassing normal authentication procedures to a program. Trap doors have for many years been used legitimately in program development for debugging and testing purposes. Malicious use of trap doors is a serious security threat.