Current Network Security Systems

Göran Pulkkis
Arcada Polytechnic Helsinki, Finland

Kaj Grahn
Arcada Polytechnic Helsinki, Finland

Peik Åström
Arcada Polytechnic Helsinki, 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 based tools, that is, network security software (Pulkkis, Grahn & Åström, 2003).

BACKGROUND

This article gives a topical overview of network security software, 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" of network security software and to stimulate discussion about 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. Malicious program categories are (Bowles & Pelaez, 1992):

- *Host program needed*
  - **Trap door**
  - **Logic bomb**
  - **Trojan horse**
  - **Virus**
- *Self-contained malicious program*
  - **Bacteria**
  - **Worm**

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 (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**
  Antivirus software packages using many different antivirus techniques in conjunction.

Examples of recent advanced antivirus techniques are *generic decryption* (*GD*) and *digital immune system (DIS)* technology (Stallings, 2000, Chap. 9).

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.

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

FIREWALL SOFTWARE

Firewalls protect computers and computer networks from external security threats. Firewall types are:

- **Packet-filtering router**, which applies a software and/or hardware implemented filtering rule set to each incoming/outgoing IP packet and then forwards or discards the packet. Most TCP/IP routers support basic user defined filtering rules. A packet-filtering firewall can also be a stand-alone network link device, for example, a computer with two network cards.
- **Application-level gateway (proxy server)**, which acts as an application level traffic relay. A typical application level gateway is a protocol oriented proxy server on a network link, for example, an HTTP proxy, a SMTP proxy, a FTP proxy, and so forth. An HTTP proxy is also a Web page cache for Web usage through the proxy.
- **Circuit-level gateway**, which typically relays TCP packets from one connection to another without examining the contents.

CRYPTOGRAPHIC SOFTWARE

Cryptographic network security software consists of secure network applications and secures network system software.

Software for Secure Network Level Data Communication

Secure network level data communication is based on the Internet Protocol Security (IPSec) protocol. Two computers in the same TCP/IP network implement end-to-end security through the network, when IPSec software is installed and properly configured in both computers. IPSec provides two operation modes:

- **Transport mode**, where original IP headers are used
- **Tunnel mode**, where new IP headers are created and used to represent the IP tunnel endpoint addresses. IPSec is usually embedded in Virtual Private Network (VPN) software. VPN provides secure LAN functionality in geographically distributed network segments and for Internet connected computers. Fundamental VPN types are:
- **Access VPN**, a secure connection to a LAN through a public TCP/IP Network
- **Connection VPN**, a secure remote connection between two logical LAN segments through a public TCP/IP network.

IPSec and VPN functionality is included in Windows 2000/XP. Commercial VPN software products are F-Secure VPN+™, Nokia VPN, Cisco Security VPN Software, and so forth. Open source IPSec and VPN software is also available (Linux, 2003).

Middleware

Middleware is a software layer between the network and the applications for providing services like identification, authentication, authorization, directories, and security (Internet2 Middleware, 2004). Shibboleth (2004) is an example of open source authentication and authorization middleware. Commercial security middleware based on the SHH protocol is presented in SSH Tectia Solution (2004).

Software for Secure Transport Level Data Communication

Many network applications are based on the IETF Transport Layer Security (TLS) standard. The TLS/SSL protocol is based on an established client-server TCP connection. Then both computers execute the SSL Handshake Protocol to agree on the cryptographic algorithms and keys for use in the actual data communication (Stallings, 2000, p. 214). TLS/SSL versions of common application level TCP/IP protocols are available (see Table 1).

VPN solutions can also be implemented using the TLS/SSL protocol and executed on the transport level. This technology, called SSL-VPN provides VPN functionality to geographically distributed network segments and for Internet connected computers using a standard Web browser. A commercial SSL-VPN software product is presented in Symantec™ (2004).

Web Security

Basic Web security features are access level security and transaction level security. Access level security is provided with firewalls which guard against intrusion and unauthorized use. Transaction level security requires protocols for protecting the communication between a

Table1. Secure application level protocols based on TLS/SSL (Oppliger, 2000, p.135)

Secure protocol	Port	Description
HTTPS	443	TLS/SSL protected HTTP
POP3S	995	TLS/SSL protected POP3
IMAPS	993	TLS/SSL protected IMAP4
SMTPS	465	TLS/SSL protected SMTP
NNTPS	563	TLS/SSL protected NNTP
LDAPS	636	TLS/SSL protected LDAP