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.

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):

- **Packet-Filtering Router:** 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):** Acts as an application level traffic relay, that is, traffic is filtered based on specified application rules. 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.
- **Circuit-Level Gateway:** Typically relays TCP packets from one connection to another without examining the contents. Traffic is filtered based on specified session rules such as when a session is initiated by a recognized computer.
- **Stateful Multilayer Inspection Firewall:** Traffic is filtered at three levels, based on a wide range of specified application, session, and packet filtering rules.

CRYPTOGRAPHIC TECHNOLOGY

Cryptographic network security technology consists of network security applications, network security system software, and cryptographic hardware.

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:** Original IP headers are used.
- **Tunnel Mode:** 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:** Secure connection to a LAN through a public TCP/IP Network.
- **Connection VPN:** 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 (Openswan Portal, 2006).

Middleware

Middleware is a software layer between the network and the applications for providing services like identification, authentication, authorization, directories, and security (Internet2 Middleware Initiative [I2-MI] Portal, 2006). Shibboleth is an example of open source authentication and authorization middleware (Shibboleth Project Portal, 2006). Commercial security middleware based on the SHH protocol is SSH Tectia Solution (2006).

Secure-Transport-Level Data Communication

Many network applications are based on the IETF transport layer security (TLS) standard (Dierks & Rescora, 2006). 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. 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.