

ANNEXES

ANNEX 1. GLOSSARY

ANNEX 2. HANDBOOK BIBLIOGRAPHY

ANNEX 3. ELECTRONIC RESOURCES

ANNEX 4. ORGANIZATIONS

ANNEX 5. PRINT RESOURCES

ANNEX 1. GLOSSARY

802.11

802.11 is a set of developing IEEE standards for wireless local area networks (WLAN). The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society. For further information on the IEEE and the IEEE Computer Society, see <http://standards.ieee.org> and <http://www.computer.org/>.

Information about definitions and functional requirements for 802.11 may be found in this document: http://grouper.ieee.org/groups/802/11/Documents/DocumentArchives/1992_docs/1192091.DOC

Access

The ability to enter a secured area and, in the case of accessing a computer, to read, write, modify, or use any of the computer's system resources.

Access authorization

Permission granted to users, programs, or workstations.

Access control

A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access. Security policies should be supported by access control, which assist in the prevention of unauthorized use of any of a company's system resources either externally (by an intruder) or internally (by an employee who should not have access).

Accountability

Ensuring that activities on supported systems can be traced to an individual who is held responsible for the integrity of the data.

Assurance

A level of confidence that the information system architecture mediates and enforces the organization's security policy.

Attachment

An attachment is a method by which text and images can be sent via e-mail. Any non-text file (a program or a picture or a video) is converted ("encoded") into a printable form and inserted into the text message. Anything stored in your computer is composed of zeros and ones. Encoding, in its simplest form, would send the zeros and ones as printable characters.

Attack

An assault on system security from an intelligent threat; a deliberate attempt to evade security services and violate the security policy of a system.

Audit

The independent collection of records to access their veracity and completeness.

Audit trail

An audit trail is a documented record of events allowing an auditor (or security administrator) to reconstruct past system activities, it may be on paper or on disk. In computer security systems, it is a chronological record of when users log in, how long they are engaged in various activities, what they were doing, whether any actual or attempted security violations occurred.

Authentic signature

A signature, particularly a digital signature, that can be trusted because it can be verified.

Authenticate

In networking, to verify the identity of a user, device, or any other system entity.

Authentication

The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authorization

Granting officially approved access rights to a user, process, or program in accordance with a company's security policy. Usually authorization is completed after the user is authenticated. The user may then be authorized for various levels of access or activity.

Availability

The portion of time a system can be use for productive work.

Backdoor

A way to bypass the normal login security and gain control of a computer without necessarily obtaining the owner's consent. If a backdoor is installed on a network-attached computer, a person anywhere on the Internet may be able to gain control of the computer without your knowledge or approval. A backdoor need not have malicious intent; e.g. operating systems are sometimes shipped by the manufacturer with privileged accounts for use by field service technicians or the vendor's maintenance programmers. However, they may also be used for intrusion by unauthorized persons. Also known as a "trap door".

Backup

The process of copying computer files to some other location either on the computer, or on storage devices that may be separated from the computer. Backups allow you to recover data in the event that the originals are no longer available, for reasons ranging from accidental deletion to physical damage, theft, or other loss.

Bandwidth

Capacity of a network or data connection, often measured in kilobits per second (kbps) for digital transmissions.

Buffer Overflow

A software bug that occurs when a program moves data into a space in memory, but there is not enough room in memory to store that data. The program may discard characters to try to make space for the new data. Destroying these characters can cause all sorts of problems, and often can allow things to happen which affect the integrity or security of the program. Buffer overflows can be avoided (if you are programming) by checking that there is sufficient spaced in memory before doing a move.

Bulletin board

Allows users from the Internet to write or read messages posted by other users and to exchange programs and files.

CERT

The Computer Emergency Response Team was established at Carnegie-Mellon University after the 1988 Internet worm attack named Morris.

Compromise

Violation of a company's system security policy by an intruder that may result in the modification, destruction, or theft of data.

Computer crime

Any form of illegal act involving electronic information and computer equipment.

Computer fraud

A computer crime that an intruder commits to obtain money or something of value from a company (or individual). Often, all traces of the crime are covered up. Computer fraud typically involves modification, destruction, theft, or disclosure of data.

Confidentiality

Ensuring that sensitive data is limited to specific individuals (external and internal) or groups within an organization. The confidentiality of the information is based on the degree to which an organization must protect its information – for example, registered, proprietary, or nonproprietary.

Conflict-of-interest escalation

A preset procedure for escalating a security incident if any members of the security are suspect.

Contingency plan

A security plan to ensure that mission-critical computer resources are available to a company in the event of a disaster (such as an earthquake or flood). It includes emergency response actions, backup operations, and postdisaster recovery.

Control

A protective action that a company takes to reduce its risk of exposure.

Cookie

A file that is written to or read from your hard disk at the request of a remote web site. The web site requests that the file be written and reads it later. As a simple

example, if you tell a web site what your username is, it can request that this information be written to your disk. When you go back to that web site, it reads the cookie and knows what your username is. Cookies may be used to generate profiles of web usage habits and, in some cases, may infringe on personal privacy.

Countermeasure

An action that a company takes to reduce threats to a system. A countermeasure can be a hardware device, software package, procedure, and so on.

Cracker

Someone who tries to break the security of, and gain access to, someone else's system without being invited. (See also hacker).

Cryptography

The mathematical science that deals with transforming data to render its meaning unintelligible, prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form.

Data-driven attack

A form of attack that is encoded in innocuous-seeming data executed by a user or other software to implement an attack. Data-driven attacks are a serious concern even to protected systems because they may get through firewalls in data form and launch an attack on the system behind the firewall.

Data Encryption Standard (DES)

An encryption standard developed by IBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Data integrity

The assurance that a company's data has not been exposed to modification or destruction either by accident or from malicious acts.

Decode

Conversion of encoded text to plain text through the use of a code.

Decrypt

Conversion of either encoded or enciphered text into plain text.

Dedicated

A special purpose device. Although it is capable of performing other duties, it is assigned to only one.

Defense in depth

The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

Denial of service

A Denial-of-Service attack is when computers on the Internet are bombarded with (garbage) messages to such a great extent that they spend all of their time responding to these messages. Real user traffic can no longer get through.

Domain Name Server spoofing

Assuming the Domain Name Server (DNS) name of another system by either corrupting the name service cache of a victim system or compromising a domain name server for a valid domain.

E-mail bombs

Code that when executed sends many messages to the same address for the purpose of using up disk space or overloading the e-mail or Web server.

Easy access

Breaking into a system with minimal effort by exploiting a well-known vulnerability, and gaining superuser access in less than 30 seconds (a piece of cake for an intruder).

Eavesdropping

Passive secret wiretapping i.e. without the knowledge of the originator or the intended recipients of the communication.

E-mail

The computer-based equivalent of postal mail – e(lectronic)-mail. Properly addressed e-mail can be sent and received by anyone connected to the Internet. From the perspective of the Internet, all e-mail is composed of printable text (ASCII) messages.

Encryption

The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm). Encryption is a way to disguise information so that it cannot be read easily, except by the intended recipient. In the simplest case, there is a “key” that is used to disguise that information. It can only be read after being decrypted, and to decrypt it, you would need to know the proper “key”.

End-to-end encryption

Encryption at the point of origin in a network, followed by decryption at the destination.

Environment

The aggregate of external circumstances, conditions, and events that affect the development, operation, and maintenance of a system.

Escalation

The procedure of reporting (and passing responsibility for resolving) a security breach to a higher level of command. See also, “Internal escalation,” “External escalation,” and “Conflict-of-interest escalation.”

External escalation

The process of reporting a security breach to an individual or group outside the department, division, or company in which it occurred. Once a problem is escalated, responsibility for resolving that problem is either accepted or shared with the party to whom the problem is escalated.

Extranet

Extranet refers to extending the LAN via remote or Internet access to partners outside your organization such as frequent suppliers and purchasers. Such relationships should be over authenticated link to authorized segments of the LAN and are frequently encrypted for privacy.

Fault tolerance

A design method that ensures continued systems operation in the event of individual failures by providing redundant systems elements.

File compression

File compression is a means of storing or transmitting a

large quantity of text, images, or code. Even entire archives may be compressed; in fact, this is a standard backup procedure. Examples of compressed archives include “zip” and “tar” files which can contain very bulky information in a dense form. They are “unzipped” and individual files may be called up through fairly simple processes. There are a number of vendors and some freeware available for file compression.

Firewall

A security system that controls traffic flow between networks. Several configurations exist: filters (or screens), application relays, encryption, demilitarized zones (DMZ), and so on. Firewalls have two forms: a firewall may be software program running on your computer or it may be a separate piece of hardware that watches what is being sent and received over a network. Firewalls can block transmissions that are unexpected or disallowed. They can also control communications between you and the outside world.

Gateway

A bridge between two networks.

Global System for Mobile Communications (GSM)

GSM is an open, non-proprietary system that is constantly evolving. GSM satellite roaming has extended service access to areas where terrestrial coverage is not available.

Global Positioning System (GPS)

Used primarily for navigation, this satellite-based system maps the location of various receivers on Earth.

Hacker

Someone with an interest in computers who enjoys experimenting with them. The term has also come to mean a person with malicious intentions who gathers information on computer security flaws and breaks into computers without the system owner’s permission, although the term cracker is more appropriate for an exclusively negative connotation. (See also Cracker).

Hacking

In general, writing code for computers. In a security context, the term often is used to mean exploiting system vulnerabilities to gain unauthorized access.

HTML

HyperText Mark-up Language tells a web browser or mail program how to display text and images. It can also give other instructions to the browser/mail program. A mark-up language allows commands or instructions embedded in the text to be displayed and printed. An example of a mark-up language is:

This sentence is <<Start Bold>>very<<End Bold>>
short.

When the sentence is displayed, the words within the << >> are taken as instructions on what to do. As a result, most of the sentence would be displayed as: This sentence is very short.

Identification

Recognizing users on a company's system by using unique names.

Identity theft

Identity theft is when someone gathers enough information about you to convince others (such as banks, stores or governments) that they are you.

Incident-response procedures

Formal, written procedures that detail the steps to be taken in the event of a major security problem, such as a break-in. Developing detailed incident-response procedures before the occurrence of a problem is a hallmark of a well-designed security system.

Insider attack

An attack originating from inside a protected network.

Internal escalation

The process of reporting a security breach to a higher level of command within the department, division, or company in which the breach occurred.

Internet

A web of different, intercommunicating networks funded by both commercial and government organizations. The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The

first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of open networks in the late 1980's required a new model of communications. The amalgamation of many types of systems into mixed environments demanded better translator between these operating systems and a non-proprietary approach to networking in general. Telecommunications Protocol/Internet Protocol (TCP/IP) provided the best solutions to this.

Internet Engineering Task Force (IETF)

A public forum that develops standards and resolves operational issues for the Internet.

Internet Service Provider (ISP)

The company through which an individual or organization receives access to the Internet. Typically, ISPs provide e-mail service and home-page storage in addition to Internet access. Some ISPs also provide offsite data storage and backup services.

Intranet

A company's internal network.

Intruder

An entity that gains or attempts to gain access to a system or system resources without having authorization to do so.

Intrusion detection

A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection System (IDS)

A system dedicated to the detection of break-ins or break in attempts either manually via software expert systems that operate on logs or other information available on the network.

International Standards Organization (ISO)

A group that sets standards for data communications.

ISP

The company through which an individual or organization receives access to the Internet. Typically,

ISPs provide e-mail service and home-page storage in addition to Internet access. Some ISPs also provide offsite data storage and backup services.

Key

In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected software.

Keyboard logger

A program that captures everything that is typed on a keyboard. The data can be written to disk or sent to someone else via the Internet. If a keyboard logger is installed on a computer, everything that is entered on the computer, including usernames and passwords, can be captured, just as if someone was looking over your shoulder while you typed!

Least privilege

Designing operational aspects of a system to operate with a minimum amount of system privilege. This design reduces the authorization level at which various actions are performed and decreased the chance that a process or user with high privileges may be caused to perform unauthorized activities resulting in a security breach.

Local Area Network (LAN)

An interconnected system of computers and peripherals, LAN users share data stored on hard disks and can share printers connected to the network.

Logging

The process of storing information about events that occurred on the firewall or network.

Log processing

How audit logs are processed, searched for key events, or summarized.

Log retention

How long audit logs are retained and maintained.

Logic bomb

A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.

Network computer architecture

A computing architecture in which components are dynamically downloaded from the network into the client device for execution by the client. The Java programming language is at the core of network computing.

Network-level firewall

A firewall in which traffic is examined at the network protocol packet level.

Network worm

A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability. A network worm may attack from one system to another by establishing a network connection. The worm is usually a self-contained program that does not need to attach itself to a host file to infiltrate the networks.

Open Source

Programs that are distributed in source format under conditions that allow free modification and distribution. Since the source code is available, people can see how it works and are able to change it. The authors of Open Source code often encourage other programmers to participate in the further development of the programs. Open Source also includes software that is given away for free and many Open Source programs, both free and for sale, offer functionality that is similar to proprietary programs that may cost a substantial amount of money. Sometimes Open Source programs are incorporated into fee-based programs in special licensing arrangements. See www.opensource.org and www.fsf.org for additional information.

Operating system

System software that controls a computer and its peripherals. Modern operating systems, such as Unix, Linux, and Windows XP handle many of a computer's basic functions.

Password

A secret code assigned to a user, known by the computer system. Knowledge (and entry) of the user ID and password is often used to authorize that user to access system resources

Password cracker

A software program containing whole dictionaries that tries to match user passwords.

Password sniffing

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Penetration

Successful, repeatable, unauthorized access to a protected system resource.

Penetration test

A system test, often part of system certification, in which evaluators attempt to circumvent the security features of the system and penetrate various layers of systems resources.

Perimeter-based security

The technique of securing a network by controlling access to all entry and exit points of the network.

Permissions

The authorized actions a subject can perform with an object (i.e. read, write, modify, or delete).

Personal Identification Number (PIN)

A sequence of numbers or letters that serve to authenticate a user to a system or service. A PIN is similar to a password, but generally pertains to completing financial transactions (bank or credit card accounts) or physical access to a location rather than access to computing resources.

Point of Contact (POC)

The person or persons to whom users and/or system administrators should immediately report a break-in or suspected security breach. The POC is the information-system equivalent of a 911 emergency line.

Policy

Organizational- level rules governing acceptable use of computing resources, security practices, and operational procedures.

Privacy

The protection of a company's data from being read by unauthorized parties. Safe guards such as encryption can provide a level of assurance that the integrity of the data is protected from exposure.

Private Key

The element of a public/private key pair that is kept secret by the key pair owner. The private key is used to decrypt messages that have been encrypted by the corresponding public key. It is also used to construct a digital signature – the document to be signed is hashed using a secure hash algorithm and then the hashed value is encrypted using the private key; this process forms the digital signature.

Protocols

Agreed-upon methods of communications used by computers.

Public Key

The element of a public/private key pair that can be known by anyone. The public key is used to encrypt information that is to be intelligible only to the holder of the corresponding private key. It is also used to decrypt a digital signature in order to compare the decrypted digital signature and the hashed value of the signed document.

Reliability

The probability that a system will adequately accomplish its tasks for a specific period of time, under the expected operating conditions.

Remote Access

The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks to access network applications and information.

Risk

The probability that a particular vulnerability of a system will be exploited, either intentionally or accidentally.

Risk Analysis: The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets and identifies controls that need improvement.

Salami Slice

A hacker method for the acquisition of funds. A database of account information is copied. Then on a later date all accounts are charged a minimal amount, so as not to arouse suspicion.

Scalability

The ability to expand a computing solution to support large numbers of users without having an impact on performance.

Security audit

An independent professional security review that tests and examines a company's compliance with existing controls, the results of which enable an auditor to recommend necessary changes in security controls, policies, and procedures.

Security procedures

A set of detailed instructions, configurations, and recommendations to implement a company's security policy.

Server

The control computer on a local area network that controls software access to workstations, printers and other parts of the network.

Smart card

A credit card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Snapshot

A copy of what a computer's memory (primary storage, specific registers, etc.) contains at a specific point in time. Like a photograph. A snapshot can be used to catch intruders by recording information that the hacker may erase before the attack is completed or repelled.

Snooping tool

A program used by an intruder to capture passwords and other data.

Social engineering

An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user to attempt to gain access to systems illicitly.

Spam

(Used as verb, e.g. to spam someone) To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. (Used as a noun: spam) electronic "junk mail."

Spoof

To gain access to a system by masquerading as an authorized user.

Stateful evaluation

Methodology using mixture of proxy or filtering technology intermittently, depending on perceived threats (or the need for speed).

Token

In authentication, a device used to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held devices similar to pocket calculators or credit cards.

Total Cost of Ownership (TCO)

A model that helps IT professionals understand and manage the budgeted (direct) and unbudgeted (indirect) costs incurred by acquiring, maintaining, and using an application or a computing system. The TCO normally includes training, upgrades, and administration as well as the original purchase price.

Threat

Any item that has the potential to compromise the integrity, confidentiality, and availability of data.

Tiger team

A group of professional security experts employed by a company to test the effectiveness of security by trying to break in.

Time bomb

A program inserted into software by an intruder that triggers when a particular time is reached or an interval has elapsed.

Trap door

A way to bypass the normal login security and gain control of a computer without necessarily obtaining the owner's consent. If a backdoor is installed on a network-attached computer, a person anywhere on the Internet may be able to gain control of the computer without your knowledge or approval. A backdoor need not have malicious intent; e.g. operating systems are sometimes shipped by the manufacturer with privileged accounts for use by field service technicians or the vendor's maintenance programmers. However, they may also be used for intrusion by unauthorized persons. Also known as a "back door."

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.

Two-Factor Authentication:

Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors," just as he/she must have an ATM card and a Personal Identification Number (PIN) to retrieve money from a bank account. In order to be authenticated during the challenge/response process, users must have this specific (private) information.

Universal Resource Locator (URL)

Universal Resource Locator – a generalized address to locate something in the Internet. Examples are <http://www.infodev.org> and <mailto:infodev@worldbank.org>

User

Any person who interacts directly with a computer system.

User ID

A unique character string that identifies a user.

User identification

User identification is the process by which a user identifies himself to the system as a valid user. This is not the same as authentication, which is the process of establishing that the user is who he says he is and has a right to use that system.

User interface

The part of an application that the user works with directly. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

Username/password

A name and a secret password that identifies a user to a computer system or a web site.

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a private connection between two machines that sends private data traffic over a shared or public network, the Internet. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.

Virus

Code that is embedded into a computer program. When the program is executed, the viral code wakes up. Once active, a virus can replicate itself, post messages, destroy data, or degrade system performance.

Virus signature

Characteristic marks of a virus that are tracked and fought by security service software vendors. Security patches are provided routinely by the most active software vendors, including McAfee, Norton (specifically their security tools including virus protection and firewalls), and Microsoft, which is working to secure flaws in its systems and programs.

Vulnerability

A flaw or weakness in a system's design, implementation, or operation that can be exploited by an intruder to violate the system's security policy.

Wireless Equivalent Protocol (WEP)

Wireless Equivalent Protocol. It was designed to be implemented over WLANs to offer the same security features as a physical wire: confidentiality, access control, and data integrity.

Wireless Local Area Network (WLAN)

A wireless network that corresponds to wireless laptops or other mobile devices.

Wiretapping

An attack that intercepts and accesses data and other information contained in a flow in a communication system. Originally, the term applied to a mechanical connection to an electrical conductor. It now refers to reading information from any medium used for a link or even directly from a node, gateway or switch.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively, leading to a denial-of-service on that network, or networks.

ANNEX 2. HANDBOOK BIBLIOGRAPHY

This Annex covers resources that were used and cited in the main text of this document. Additional resources will be listed in Annexes 3, 4, and 5.

Practical Unix & Internet Security, by Simson Garfinkel, Gene Spafford, and Alan Schwartz (O'Reilly & Associates, Inc.: CA, 2003)

Web Security, Privacy & Commerce, by Simson Garfinkel with Gene Spafford (O'Reilly & Associates, Inc.: CA, 2002)

IT Security: Risking the Corporation, by Linda McCarthy, Forward by Gene Spafford (Prentice Hall PTR: NJ, 2003)

PART 1

The future of global policy making site :
<http://www.markle.org/globalpolicy/index.html>
Includes the DOT Force Roadmap and the Louder Voices Study.

Digital Opportunity Taskforce (DOT) reports:
<http://www.dotforce.org/teams>
Includes material on eStrategies:
http://www.dotforce.org/reports/documents/65/E-Strategies_e.pdf

See also plans for the International e-Development Resource Network:
<http://www.dotforce.org/teams/IeDRNBusinessPlan.ppt>

Government guidelines for the development of the information society:
http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.shtml

OECD Electronic Commerce site:
<http://www.oecd.org/EN/home/0,,EN-home-29-nodirectorate-no-no-no-29,00.html>

OECD Electronic Commerce for Development Study (2002)
<http://www.oecd.org/EN/document/0,,EN-document-273-nodirectorate-no-15-36384-29,00.html>

OECD eGovernment:
<http://www.oecd.org/EN/about/0,,EN-about-301-nodirectorate-no-no-no-13,00.html>

OECD ICT policy:
<http://www.oecd.org/EN/home/0,,EN-home-40-nodirectorate-no-no-no-29,00.html>

Global Internet Policy Initiative:
<http://www.gipiproject.org/>

Center for Democracy and Technology:
<http://www.cdt.org/> and also the eGovernment handbook pages, completed in collaboration with infoDev: <http://www.cdt.org/egov/handbook/>

From the text footnotes for Part 1:

DOT-Force, <http://www.dotforce.org/about/>

Draft Declaration of Principles, World Summit on the Information Society, Document WSIS03/PCIP/DT/4(Rev.3)-E.

Moore, Paxson, Savage, Shannon, Staniford and Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy*, Vol. 1, No. 4, July/August 2003, pp. 33-39.

PART 2

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society. For further information on the IEEE and the IEEE Computer Society, see <http://standards.ieee.org> and <http://www.computer.org/>

Information about definitions and functional requirements for 802.11 may be found in this document: http://grouper.ieee.org/groups/802/11/Documents/DocumentArchives/1992_docs/1192091.DOC

The Unicode standard was developed to produce international software and to process and render data in most of the world's languages. The following paper presents the background of the

development of this standard among vendors and by the International Organization for Standardization (ISO). The paper describes the design goals and principles. It also discusses how an application handles Unicode text. It concludes with a description of some approaches that can be taken to support Unicode and a discussion of Microsoft's implementation. Microsoft's decision to use Unicode as the native text encoding in its Windows NT (New Technology) operating system is of particular significance for the success of Unicode.

<http://research.compaq.com/wrl/DECarchives/DTJ/DTJB02/DTJB02SC.TXT>

Additional material on the technical aspects of security may be found at the following links:

The Sans Institute Reading room:

http://www.sans.org/rr/catindex.php?cat_id=48

<http://www.securityfocus.com>

<http://www.sysinternals.com> offers a variety of freeware utilities for monitoring system usage and handling other aspects of systems security.

<http://www.deter.com/unix/index.html> is a Unix security page.

<http://msgs.securepoint.com> contains mailing lists for a number of popular security tools.

http://www.cert.org/tech_tips/unix_configuration_guidelines.html offers Unix configuration guidelines from CERT.

http://www.cert.org/tech_tips/win_configuration_guidelines.html offers Microsoft Windows configuration guidelines from CERT.

<http://www.cert.org/security-improvement/modules/m09.html> covers CERT guidelines on detecting signs of intrusions.

<http://sites.inka.de/lina/freefire-l/index.en.html> is a link to the FreeFire project for free security software.

<http://www.counterpane.com/log-analysis.html> contains advice and how-to's on analyzing system logs.

PART 3

The Human Development Report 2001: Making New Technologies Work for Human Development" (UNDP: NY, 2001).

See a number of works by Glaessner, Kellermann, and McNevin including "Electronic Safety and Soundness: Securing Finance in a New Age, Public Policy Issues (October 2003). This Monograph is the culmination of efforts over the past three years and builds upon a series of papers. These include: "Electronic Security: Risk Mitigation in Financial Transactions" (May 2002, June 2002, July 2002), "Electronic Finance: A New Approach to Financial Sector Development?" (2002), and "Mobile Risk Management: E-Finance in the Wireless Environment" (May 2002). All papers are available at: www.worldbank1.org/finance (click on E-security).

Further material on research projects and security management products is available at the IT Governance Institute (ITGI): www.itgi.org.

For information on the cases and programs, see the Information Systems Audit and Control Association at: www.isaca.org. One such study featured the country of Uruguay which might be of particular interest to readers of this handbook: http://www.isaca.org/ct_case.htm.

COBIT (<http://www.isaca.org/cobit.htm>, or <http://www.itgi.org>) is an open source product that provides a reference framework on e-Security for management, users, and IS audit, control, and security practitioners. The latest communication from ISACA will give you a good overview of current and future developments of the Association: Volume 8 2003 of Global Communiqué: <http://ISACF:RESEARCH4@www.isaca.org/@member/gcmm/gcv034.pdf>

Due to the rise in security incidents globally, a number of consulting firms have been producing reports on IT in an international context. See, for example, Ernst &

Young recently released the 2003 Global Information security survey:

[http://www.ey.com/global/download.nsf/US/TSRS_Global_Information_Security_Survey_2003/\\$file/TSRS_Global_Information_Security_Survey_2003.pdf](http://www.ey.com/global/download.nsf/US/TSRS_Global_Information_Security_Survey_2003/$file/TSRS_Global_Information_Security_Survey_2003.pdf)

Information on security issues including survey data on incidents and organizational responses may be found at the Sans Institute: www.sans.org.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. For further information on a wide range of security issues, see www.infragard.net.

A second organization focused on a wide range of threats to individual. State and national security is the newly formed Department of Homeland Security in the United States. The new department's first priority is to protect the nation against further terrorist attacks. Component agencies will analyze threats and intelligence, guard U.S. borders and airports, protect U.S. critical infrastructure, and coordinate the response of the country for future emergencies. DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions. See, www.dhs.gov.

The FBI has recently published a survey on computer crime: see www.gocsi.com for the main Computer Security Institute website and http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf for the Survey itself.

The ICC is an international body whose membership includes developing countries, the group is engaged with research and exchanges on ICT issues such as, e-Commerce, e-security, privacy, and law in the context of the Internet. The ICC web site and related pages may be found at: http://www.iccwo.org/home/menu_electronic_business.asp

The following are several examples of recent work performed by the ICC:

a) Electronic Signatures Directive – review and response to the European Commission review of the Electronic Signatures Directive, which was submitted to the European Commission in September 2003.

b) Draft Privacy Toolkit - The Draft Privacy Toolkit develops the broad approach of ICC to the regulation of personal data and suggests the best way to protect privacy while allowing business to function effectively and continue to innovate.

c) Draft ICC policy statement on employee privacy, data protection and human resources - This draft policy statement sets out ICC's positions on the key issues relating to data protection and human resources, and provides recommendations for government policy in this area.

d) Draft E-terms - E-terms 2004 is ICC's new self-regulatory legal instrument on electronic contracting. The document has been prepared by an informal drafting group. In its current form, the draft model clause is a focused instrument that addresses three identified issues: (i) contract formation; (ii) confidentiality issues; (iii) evidential value of electronic records. The clause is limited to issues that are specific for the electronic medium. Thus, E-terms 2004 must be read in the context of existing conventional contract regulations and rules.

Federal Information System Control Manual (FISCAM) offers technical and policy information at: www.gao.gov/special.pubs/ai12.19.6.pdf

The International Standards Organization (ISO) develops standards for the information technology sector worldwide. Its code of practice for information security management, ISO/ IEC 17799, transforms the British Standard BS 7799, which has been adopted in many countries, into an International Standard and it is expected to become the reference document for codes of good practice to ensure secure and trustworthy e-commerce. See documents posted at www.iso.org.

ADDITIONAL LINKS FOR PARTS 3 AND 4: FOCUS ON INTERNATIONAL BUSINESS ISSUES CASES AND LEGISLATION

1) Implementing e-Government - being ready:

<http://www.audit.nsw.gov.au/guides-bp/e-govt-BPG.pdf> is an excellent and simple checklist for governments to implement e-government (20 pages). Of interest: chapters on privacy, security, and technology and information management (Audit Office of New-South Wales, Australia)

2) Case studies on protecting critical infrastructure through network security may be found at:

<http://www.itu.int/osg/spu/ni/security/index.html>. Korea and Brazil are featured in the Country Examples.

3) "The government's guidelines for the development of the information society", Minister for Innovation and Technologies, Rome, June 2002 is an excellent example on a government approach to setting up a plan for ICT security. See also,

http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf

which contains an executive summary on Italy's national plan for ICT security.

4) Reference to Global ICT Policy Themes, Issues and Venues, including security and privacy may be found at: <http://www.markle.org/globalpolicy/> The organization focuses on enabling meaningful participation by developing-nation stakeholders and features an implementation team on local policy participation from the G8 digital opportunity task force, June 2002

5) THE ITU site contains a collection of links to policy and regulatory web sites:

<http://www.itu.int/osg/spu/ni/security/links/policy.html>
There are also links for development and e-strategy issues:

<http://www.itu.int/ITU-D/e-strategy/internet/>

The World e-Trust memorandum of understanding:

http://www.itu.int/ITU-D/e-strategy/MoU/world_e.html, and e-Business: A Technology Strategy for Developing Countries:

<http://www.itu.int/ITU-D/e-strategy/publications-articles/wmrcjune00/ntoko.html>

2003 Australian Computer Crime and Security Survey

Canadian Criminal Code, Part VI, Invasion of Privacy and Part IX, Offences against rights of property.

Claessens Stijn, Glaessner Thomas and Klingebiel Daniela, "E-Finance in Emerging Markets: Is Leapfrogging Possible?"

Commission of the European Communities: Network and Information Security: Proposal for A European Policy Approach- Brussels, June 6, 2001.

Commission of the European Communities: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime – eEurope 2002, Brussels, January 26, 2001.

Department of Justice, Canada:

www.canada.justice.gc.ca/en/cons/la_al/index.html#toc: Lawful Access – Consultation Document.

Dr Chae, Kijoon, "Introduction to Critical Network Infrastructures," May 20-22, 2002, Seoul, Korea.

Dr Lim, Chaeho, "Creating Trust in Critical Network Infrastructures: Korean Case Study." May 20-22, 2002, Seoul.

European Union Directive 2000/31/EC - on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

European Union Directive 97/33/EC – on Interconnection in Telecommunications.

European Union Directive 2002/58/EC – on privacy and Electronic Communications.

Glaessner, Thomas, Kellerman Tom, and McNevin, "Electronic Security: Risk Mitigation in Financial Transactions -Public Policy Issues," June 2002, The World Bank.

Global Dialogue "E-Security: Risk Mitigation in the Financial Sector," The World Bank, Integrator Group, September 25, 2002

Goodman E., Seymour, Hassebroek B., Pamela, King, Davis and Ozment, Andy, "International Coordination to Increase the Security of Critical Network Infrastructures," May 20-22, 2002, Seoul.

Harrop, Mike, "Creating Trust in Critical Network Infrastructures –Canadian Case Study," May 20-22, 2002, Seoul, Korea.

International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) – Lead Study Group 17 on Communications and Systems Security (www.itu.int/ITU-T/) .

Internet Security Alliance – Common Sense Guide for Senior Managers – Top Ten Recommended Security Practices, July 2002.

Keck, Richard and Satola, David, "Entering the Grid Computing Marketplace – A Primer of Key Legal Issues," April 1, 2003.

Kellerman, Thomas, "Mobile Risk Management: E-finance in the Wireless Environment," The World Bank, May 2002.

McCullagh, Declan, "Will Canada's ISPs become spies?" CNET News.com, August 27, 2002.

Monetary Authority of Singapore – Technology Risk Management Guidelines for Financial Institutions – February 28, 2003.

Official Journal of the European Communities – Council Resolution on a common approach and specific actions in the area of network and information security, January 28, 2002.

Official Journal of the European Communities – Council Resolution on the Implementation of the eEurope 2005 Action Plan, February 18, 2003.

OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Privacy Amendment Act of Australia (Private Sector) - Act 2000

"Security of Internet Enabled Wireless Devices," Wireless Task Force Findings, National Security Telecommunications Advisory Committee, January 2003.

Shaw, Robert, "Creating Trust in Critical Network Infrastructures: The Case of Brazil." May 20-22, 2002, Seoul.

The National Strategy to Secure Cyberspace, President's Critical Infrastructure Board, United States, September 2002.

"Wireless Security," Wireless Task Force Report, National Security Telecommunications Advisory Committee, January 2003.

PART 4

Once source on privacy is the annual survey by EPIC and Privacy International, "Privacy and Human Rights 2003" (Sept. 2003)
<http://www.privacyinternational.org/survey/phr2003/>

See also, the Global Privacy Report - a lengthy report on privacy conditions around the world, funded by the Japanese Ministry of Public Management, Home Affairs, Posts and Telecommunications., August 14, 2003
<http://joi.ito.com/joiwiki/PrivacyReport>

Links to anti-spam laws and organizations all around the world, as well as to articles in law journals analyzing the problem in more depth may be found at:
<http://www.spamlaws.com/>

WIPO has published a summary of intellectual property legislation in WIPO Member States, available at
<http://www.wipo.org/about-ip/en/ipworldwide/index.html>.

From the text footnotes for Part 4:

<http://www.usdoj.gov/04foia/privstat.htm>

A more extensive, although dated, discussion of legal issues in the U.S. can be found in *Computer Crime: A Crimefighter's Handbook* (O'Reilly). The book is out of print, but used copies are available.

The Global Internet Policy Initiative has a host of resources on the full range of policy issues affecting ICT development: <http://www.internetpolicy.net>.

The National Strategy to Secure Cyberspace [United States], February 2003
<http://www.whitehouse.gov/pcipb/>

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
http://www.ocipep.gc.ca/home/index_e.asp. For descriptions of how various other countries have responded to critical infrastructure protection, see "International Critical Information Infrastructure Protection Handbook," edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

The U.K.'s Home Office has created a National Infrastructure Security Coordination Centre (NISCC) to coordinate critical infrastructure protection issues, provide alerts and attack response assistance, and facilitate public-private relationships to protect infrastructure. Within NISCC, there is a Computer Emergency Response Team, known as UNIRAS. An Electronic Attack Response Group (EARG) is also within NISCC to provide assistance to critical infrastructure organizations and government departments that suffer an attack. UNIRAS will provide an early warning and alert service to all UK businesses. The NISCC website (<http://www.niscc.gov.uk>) provides detailed information on the British government's approach.

Under Australian law, Executive Agencies are non-statutory bodies established by the Governor-General when a degree of independence within the governmental structure is needed and when the functions of the agency require a government-wide approach. The head of an Executive Agency is appointed by, and directly accountable to, a Minister, in this case the Minister for Communications, Information Technology and the Arts. See: http://www.noie.gov.au/Projects/confidence/Protecting/nat_agenda.htm.

International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies

and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

For descriptions of how various other countries have responded to critical infrastructure protection, see International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002): <http://www.isn.ethz.ch/crn>.

United States Presidential Decision Directive 63: Critical Infrastructure Protection, May 22, 1998
<http://www.fas.org/irp/offdocs/pdd-63.htm>. See also PDD 62: <http://www.fas.org/irp/offdocs/pdd-62.htm>.

E.O. 13228, Establishing the Office of Homeland Security and the Homeland Security Council, October 8, 2001, <http://fas.org/irp/offdocs/eo/eo-13228.htm>; E.O. 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001: <http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>.

The National Strategy to Secure Cyberspace, Feb. 14, 2003, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

The National Strategy to Secure Cyberspace was supplemented by *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released March 4, 2003, http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf. Both of these documents are implementing components of *The National Strategy for Homeland Security*, issued by the White House on July 16, 2002.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency*, Feb. 11, 2003, COM(2003) 63 final, 2003/0032 (COD): http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf

Council resolution of 28 Jan. 2002; European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions*

- *Network and Information Security: Proposal for a European Policy Approach*, June 6, 2001, COM (2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm

European Commission, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee on the Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Jan. 26, 2001, COM(2000) 890 final, <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>

Homeland Security Act,
<http://www.whitehouse.gov/deptofhomeland/analysis/>

Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, <http://csrc.nist.gov/policies/FISMA-final.pdf>.

Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, <http://csrc.nist.gov/policies/FISMA-final.pdf>.

Thomas J. Smedinghoff, "The Developing U.S. Legal Standard for Cyber-security," Baker & McKenzie, Chicago, <http://www.bmck.com/e-commerce/us%20cyber-security%20standards.pdf>;

In the United States, the Securities and Exchange Commission has brought actions against corporations that insufficiently protected their computer systems from unauthorized access. See *SEC v. National Business Communications Corp.*, SEC Litig. Release No. 11223, Sept. 19, 1986, SEC Litig. Release No. 11229, Sept. 26, 1986. *In the Matter of Material Sciences Corporation*, SEC Litig. Release No. 41930, Sept. 28, 1999.

Sarbanes-Oxley Act of 2002, Pub. Law 107-204.

<http://www.aicps.org>; <http://www.isaca.org>.

As is made clear throughout this handbook, there is a growing body widely accepted computer security standards, ranging from the Organization for Economic Cooperation and Development (OECD) Guidelines for the

Security of Information Systems to the information security standards adopted by non-governmental standards bodies. See generally, Michael Nugent, *It Can't Happen Here*, Wall Street Technology Association, Ticker, A Technology Magazine For Industry Profession (2003), http://www.wsta.org/publications/articles/0402_article03.html

Carol A. Siegel, Ty R. Sagalow, Paul Serritella, *Cyber-Risk-Management Technical and Insurance Controls for Enterprise-Level Security*, Security Management Practices, pg. 42, (September/October 2002). http://www.gsu.edu/~accrss/Security_and_Business_Risk.pdf.

NIST's Computer Security Resource Center (CSRC) publishes information on a broad range of security topics, including cryptographic standards and applications, security testing, security research, system certification and accreditation guidelines, return on security investments, small business computer security, and federal agency security practices. <http://csrc.nist.gov/>. NIST publications are available at <http://csrc.nist.gov/publications/index.html>.

National Security Agency, *Security Recommendation Guides*, <http://nsa1.www.conxion.com/>.

CERT/Coordination Center, Software Engineering Institute, Carnegie Mellon University, <http://www.cert.org/>.

European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach*, June 6, 2001, COM(2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm.

Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, Commission of the European Communities, Feb. 11, 2003, COM(2003) 63 final, 2003/0032 (COD), http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf.

"Protecting Developing Economies from Cyber Attack – Assistance to Build Regional Cyber-security Preparedness," APEC Media Release, Mar. 18, 2003, http://www.apecsec.org.sg/whatsnew/press/PressReL_ProtectgFromCyberAttack_180303.html.

<http://www.ncs.gov/NSTAC/attf.html>

The American Bar Association's Privacy & Computer Crime Committee has published a detailed report covering cybercrime in depth. Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003, <http://www.abanet.org/abapubs/books/cybercrime/>.

UN General Assembly, Resolution 55/63, *Combating the criminal misuse of information technologies*, Dec. 4, 2000, http://www.nvk2000.ru/apec/documents/International_Agreements/55-63_English.pdf

UN General Assembly, Resolution 56/121, *Combating the criminal misuse of information technologies*, Jan. 23, 2002, <http://ods-dds-ny.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement>.

The treaty, ETS no. 185, is online at <http://conventions.coe.int/treaty/EN/cadreprincipal.htm> along with an extensive Explanatory Report.

Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Aug. 27-Sept. 7, 1990, report prepared by the Secretariat, UN publication, Sales No. E.91.IV.2, chap I. For the text of these recommendations, see United Nations Commission on Crime Prevention and Criminal Justice, Report on the Eighth Session, Apr. 27-May 6, 1999, E/CN.15/1999/12, <http://www.un.org/documents/ecosoc/docs/1999/e1999-30.htm>.

UN, *International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime*, <http://www.uncjin.org/Documents/EighthCongress.html>.

Report of UN Economic and Social Council's Commission on Crime Prevention and Criminal Justice effectively summarizes UN and other international work in the

cybercrime and cyber-security area. *Effective measures to prevent and control computer-related crime*, E/CN.15/2002/8, Report of the Secretary-General, United Nations, Economic and Social Council, Commission on Crime Prevention and Criminal Justice, Eleventh Session, Vienna, Apr. 16-25, 2002, <http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>.

Gramm-Leach Bliley Act, 15 USC, Subchapter 1, § 6801.

"Appendix B to Part 570—Interagency Guidelines Establishing Standards for Safeguarding Customer Information," Part III, <http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>.

"Financial Institutions and Customer Data: Complying with the Safeguards Rule," <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>

Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484-94, May 23, 2000, (codified at 16 C.F.R. Part 314), <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.

Technology Risk Management Guidelines for Financial Institutions, Monetary Authority of Singapore, Draft Nov. 11, 2002, <http://www.mas.gov.sg/display.cfm?id=94D063CD-5EB6-4636-82B5A725F9F6E9F5>.

45 CFR §160, 162, 164; <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>

HIPAA, 42 U.S.C. Section 1320d-2(d)(2).

Linda A. Malek and Brian R. Krex, "HIPAA's security rule becomes effective 2005," *The National Law Journal*, Mar. 31, 2003 at B14.

http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Article 4(1), Official Journal L 201/37, July 31, 2002, at 37-47 (replacing EU

Directive 97/66/EC), http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett.

Security Breach Information Act (SB 1386), added to the California Civil Code as Section 1798.29; Keith Poulsen, "California disclosure law has national reach," SecurityFocus Online, Jan. 6, 2003, <http://online.securityfocus.com/news/1984>. Other disclosure proposals have been put forth in the U.S. See [Michael Vatis, Testimony before the House Government Reform Committee, April 8, 2003; Sen. Bennett's proposal.

PART 5

<http://news.cnet.com/news/0-1005-200-4523277.html>

<http://www.wired.com/news/technology/0,1282,34496,00.html>

<http://www.microsoft.com/technet/security/bulletin/MS01-017.asp>

Forum of Incident Response and Security Teams, the worldwide consortium of major computer incident response groups. Visit <http://www.first.org> for more information. ISS reported a security problem to 11 vendors in December 1999, then released the information about the vulnerability to the press in February 2000. For further information, see <http://www.cnn.com/2000/TECH/computing/02/04/shop.glitch.idg>

"Dos and Don'ts of Client Authentication on the Web," USENIX and MIT Technical Report 818, by Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster

ANNEX 3. ELECTRONIC RESOURCES

There is a certain irony in trying to include a comprehensive list of electronic resources in a printed document. Electronic resources such as Web pages, news-groups, and mailing lists are updated on an hourly basis; new releases of computer programs can be published every few weeks.

We thus present the following electronic resources with the understanding that this list necessarily cannot be complete nor completely up to date. What we hope, instead, is that it is useful. By reading it, we hope that you will gain insight into places to look for future developments in computer security. Along the way, you may find some information you can put to immediate use.

Mailing Lists

There are many mailing lists that cover security-related material. We describe a few of the major ones here. However, this is not to imply that only these lists are worthy of mention! There may well be other lists of which we are unaware, and many of the lesser-known lists often have a higher volume of good information.

Never place blind faith in anything you read in a mailing list, *especially* if the list is unmoderated. There are a number of self-styled experts on the net who will not hesitate to volunteer their views, whether knowledgeable or not. Usually their advice is benign, but sometimes it is quite dangerous. There may also be people who are providing bad advice on purpose, as a form of vandalism. And certainly there are times where the real experts make a mistake or two in what they recommend in an off-hand note posted to the net.

There are some real experts on these lists who are (happily) willing to share their knowledge with the community, and their contributions make the Internet a better place. However, keep in mind that simply because you read it on the network does not mean that the information is correct for your system or environment, does not mean that it has been carefully thought out, does not mean that it matches your site policy, and most certainly does not mean that it will help your security. *Always* evaluate carefully the information you receive before acting on it.

A Big Problem With Mailing Lists

The problem with all these lists is that you can easily overwhelm yourself. If you are on lists from two response teams, four vendors, and another half-dozen general-purpose lists, you may find yourself filtering several hundred messages a day whenever a new general vulnerability is discovered. At the same time, you don't want to unsubscribe from these lists, because you might then miss the timely announcement of a special-case fix for your own systems.

One method that we have seen others use with some success is to split the mailing lists up among a group of administrators. Each person gets one or two lists to monitor, with particularly useful messages then redistributed to the entire group. Be certain to arrange coverage of these lists if someone leaves or goes on vacation, however!

Another approach is to feed these messages into Usenet newsgroups you create locally especially for this purpose. This strategy allows you to read the messages using an advanced newsreader that will allow you to kill message chains or trigger on keywords. It may also help provide an archiving mechanism to allow you to keep several days or weeks (or more) of the messages.

Finally, most security mailing lists offer the option of subscribing to a daily digest of the list. Digest subscribers usually receive a single message each day that contains all of the day's messages. Managing these digests can be easier than sorting through each individual message as they arrive. Of course, you may learn about new vulnerabilities several hours later than other system administrators — or attackers.

Response Teams and Vendors

Many of the incident response teams (listed in Appendix E) have mailing lists for their advisories and alerts. If you can be classified as one of their constituents, you should contact the appropriate team(s) to be placed on their mailing lists.

Many vendors also have mailing lists for updates and advisories concerning their products. These include computer vendors, firewall vendors, and vendors of security software (including some freeware and

shareware products). You may wish to contact your vendors to see if they have such lists, and if so, join. To subscribe to Microsoft's Security Notification Service mailing list, for example, visit the Microsoft Profile Center at <http://register.microsoft.com/regsys/pic.asp> and register.

Major Mailing Lists

These are some of the major mailing lists.

Bugtraq

Bugtraq is a full-disclosure computer security mailing list. This list features detailed discussion of UNIX security holes: what they are, how to exploit them, and what to do to fix them. This list is not intended to be about cracking systems or exploiting their vulnerabilities (although that is known to be the intent of some of the subscribers). It is, instead, about defining, recognizing, and preventing use of security holes and risks. To subscribe, sign up at <http://www.securityfocus.com>. Note that we have seen some incredibly incorrect and downright bad advice posted to this list. Individuals who attempt to point out errors or corrections are often roundly flamed as being "anti-disclosure." Post to this list with caution if you are the timid sort.

SecurityFocus also runs several other mailing lists that cover areas of security (such as IDS, honeypots, or viruses) or specific flavors of Unix (such as Linux or Sun systems). A particularly interesting list is "incidents" which is for reporting actual attacks and break-ins. SecurityFocus is owned by the Symantec Corporation

NTBugtraq

A full-disclosure computer security mailing list for Microsoft Windows NT-based systems (including Windows 2000 and XP). Non NT-based releases are off-topic for this list. In other ways, it resembles the Bugtraq list. Subscribe at <http://www.ntbugtraq.com>.

CERT-advisory

New CERT/CC advisories of security flaws and fixes for Internet systems are posted to this list. This list makes somewhat boring reading; often the advisories are so watered down that you cannot easily figure out what is actually being described. Nevertheless, the list does have its bright spots. Send subscription requests to

majordomo@cert.org. Put "subscribe cert-advisory" in the message body.

Archived past advisories are available at <http://www.cert.org/nav/alerts.html>.

Computer underground digest

A curious mixture of postings on privacy, security, law, and the computer underground fill this list. Despite the name, this list was not a digest of material by the "underground"—it contained information about the computing milieu. Unfortunately, it stopped publishing in 2000, and it is unclear if the list will ever resume. This list was available as the newsgroup *comp.society.cu-digest* on the Usenet; the newsgroup was the preferred means of distribution. The list is archived at numerous places around the Internet, including its home page: <http://sun.soci.niu.edu/~cudigest/>

Firewalls

The Firewalls mailing list, which is hosted by the Internet Software Consortium, is a primary forum for folks on the Internet who want to discuss the design, construction, operation, maintenance, and philosophy of Internet firewall security systems. To subscribe, visit <http://www.isc.org/services/public/lists/firewalls.html>.

The Firewalls mailing list is usually high volume (sometimes more than 100 messages per day, although usually it is only several dozen per day). To accommodate subscribers who don't want their mailboxes flooded with lots of separate messages from Fire-walls, a digested version of the list is also available, and the list is archived on the web site.

Firewall-Wizards

The firewall-wizards mailing list is a moderated list focused not only on the design and implementation of firewalls but also other network security topics. You can subscribe (or browse the archives) at <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>.

RISKS

RISKS is officially known as the ACM Forum on Risks to the Public in the Use of Computers and Related Systems. It's a moderated forum for discussion of risks to society

from computers and computerization. RISKS is also distributed as the *comp.risks* Usenet newsgroup, and this is the preferred method of subscription. If you don't get Usenet (and don't want to read it via <http://groups.google.com>), you can send email subscription requests to RISKS-Request@cs.sri.com with the word "subscribe" in the body.

Back issues are available through Google (as above) or from <http://www.risks.org>

SANS Security Alert Consensus

Security Alert Consensus is a weekly digest of alerts and announcements from several other security mailing lists and vendors. Subscriptions can be customized to include only those operating systems for which you are responsible. Subscribe at <http://www.sans.org>.

Usenet Groups

There are several Usenet newsgroups that you might find to be interesting sources of information on network security and related topics. However, the unmoderated lists are the same as other unmoderated groups on the Usenet: repositories of material that is often off-topic, repetitive, and incorrect. Our warning about material found in mailing lists, expressed earlier, applies doubly to newsgroups.

comp.security.announce (moderated)

Computer security announcements, including new CERT/CC advisories

comp.security.unix

UNIX security

comp.security.misc

Miscellaneous computer and network security

comp.security.firewalls

Information about firewalls

comp.virus (moderated)

Information on computer viruses and related topics

comp.admin.policy

Computer administrative policy issues, including security

comp.protocols.tcp-ip

TCP/IP internals, including security

comp.unix.admin

UNIX system administration, including security

sci.crypt

Discussions about cryptology research and application

sci.crypt.research (moderated)

Discussions about cryptology research

comp.risks (moderated)

As described above

microsoft.public.security,

microsoft.public.win2000.security,

microsoft.public.windowsxp.security_admin

Microsoft hosts dozens of Usenet groups for its operating systems and applications, include several devoted specifically to security.

WWW Sites

There are literally thousands of WWW pages with pointers to other information. Some pages are comprehensive, and others are fairly narrow in focus. The ones we list here provide a good starting point for any browsing you might do. You will find most of the other useful directories linked into one or more of these pages, and you can then build your own set of "bookmarks."

CIAC

The staff of the CIAC keep a good archive of tools and documents available on their site. This archive includes copies of their notes and advisories, and some locally developed software:
<http://ciac.llnl.gov>

CERIAS

CERIAS (Center for Education and Research in Information Assurance and Security), the successor to COAST (Computer Operations, Audit, and Security Technology) is an inter-disciplinary center in information security research and education at Purdue University. It functions with close ties to researchers and engineers in major companies and government

agencies. CERIAS focuses on real-world research needs and limitations.

From a purely historical perspective, this represents what may be the oldest, and longest-running Internet archive of security tools and reference materials. Created in 1989 as an ftp-only site, the archive started as a collection of anti-virus tools and gradually expanded to include scanners, firewalls, and documents of all kinds. The site transitioned through gopher and WWW servers, and from a personal archive (Spafford's) to the COAST Laboratory archive, to the current CERIAS archive. For its first decade the site was generally believed to be the largest archive of security material on the Internet.

Over the last few years, the archive and hotlist have diverged somewhat, and fewer items are currently stored there than before. (Many of the commercial sites have resources to pay a staff to maintain more comprehensive archives.) Nonetheless, the current archive contains many items of historical interest, a large collection of useful tools and documents, including items not carried elsewhere, and items that are produced by CERIAS and CERIAS partners. There are also extensive lists of pointers to organizations and resources.

<http://www.cerias.purdue.edu/infosec/>
<ftp://ftp.cerias.purdue.edu>

FIRST

The FIRST (Forum of Incident Response and Security Teams) Secretariat maintains a large archive of material, including pointers to WWW pages for other FIRST teams: <http://www.first.org>

NIST CSRC

The National Institute of Standards and Technology's Computer Security Division maintains a comprehensive archive of documents and tools. This is a trusted, useful site for documentation, standards, and software. <http://csrc.nist.gov/index.html>

Insecure.org

Home of the **nmap** portscanning tool, the Insecure.org web site links to archives of many important mailing lists and other security information: <http://www.insecure.org>

NIH

The WWW index page at NIH provides a large set of pointers to internal collections and other archives: <http://www.alw.nih.gov/Security/>

Software Resources

This appendix describes some of the tools and packages available on the Internet that you might find useful in maintaining security at your site. Although this software is (or was) freely available, some of it is restricted in various ways by the authors (e.g., it may not be permitted to be used for commercial purposes or be included on a CD-ROM, etc.) or by the U.S. government (e.g., if it contains cryptography, there may be constraints on export or use in certain locales). Carefully read the documentation files that are distributed with the packages. If you have any doubt about appropriate use restrictions, contact the author(s) directly.

Although we have used most of the software listed here, we can't take responsibility for ensuring that the copy you get will work properly and won't cause any damage to your system. As with any software, test it before you use it!

Some software distributions carry an external PGP signature. This signature helps you verify that the distribution you receive is the one packaged by the author. It does not provide *any* guarantee about the safety or correctness of the software, however.

Because of the additional confidence that a digital signature can add to software distributed over the Internet, we strongly encourage authors to take the additional step of including a stand-alone signature. We also encourage users who download software to check several other sources if they download a package *without* a signature.

Crossplatform Tools

Kerberos

Kerberos is a secure network authentication system that is based upon private key cryptography. The Kerberos source code and papers are available from the Massachusetts Institute of Technology. Contact: MIT Software Center
W32-300
20 Carlton Street
Cambridge, MA 02139
(617) 253-7686

You can use anonymous FTP to transfer files over the Internet from: <ftp://athena-dist.mit.edu/pub/kerberos>
Kerberos is integrated into Microsoft Windows 2000 and later releases.

nmap

nmap is the port scanner of choice for both attackers and defenders. It can perform a wide variety of TCP, UDP, and ICMP scans (including various "stealth scans" that attackers might use to disguise their activities), and has a sophisticated ability to "fingerprint" operating systems and determine their vendor and version remotely. It is available from:
<http://www.insecure.org>

OpenSSH

OpenSSH is a free software implementation of the Secure Shell protocol (versions 1 and 2) for cryptographically-secured remote terminal emulation, command execution, and file transfer. It is developed and maintained by the OpenBSD project, but the "portable" version compiles and runs on most Unix systems and several other operating systems. There are also several good free software SSH clients for Windows, including PuTTY. Disable the telnet daemon before you connect your system to a network; install OpenSSH (or another SSH server) if you need to be able to connect to your system over the network. You can get OpenSSH at:
<http://www.openssh.org>

OpenSSL

OpenSSL is a free software implementation of the Secure Sockets Layer (versions 2 and 3) and Transport Layer Security (version 1) protocols. It provides libraries for these protocols that are commonly required by other

server software (such as web servers). It also provides a command line tool for generating cryptographic certificate requests, certificates, signatures, and random numbers. OpenSSL is available from:
<http://www.openssl.org>

Snort

Snort is a powerful open source packet sniffer and network intrusion detection system. Its IDS ruleset is regularly updated, enabling it to parse the TCP/IP packets that it monitors in real time, and report suspicious traffic. Get *Snort* from:
<http://www.snort.org>

Tripwire

Tripwire, written by Gene H. Kim and Gene Spafford of Purdue University, is a file integrity checker, a utility that compares a designated set of files and directories against information stored in a previously generated database. Added or deleted files are flagged and reported, as are any files that have changed from their previously recorded state in the database. Run Tripwire against system files on a regular basis. If you do so, the program will spot any file changes when it next runs, giving system administrators information to enact damage-control measures immediately.

You can get the freeware version of Tripwire from:
<http://www.tripwire.com/downloads/>

Unix Tools

chrootuid

The *chrootuid* daemon, by Wietse Venema, simplifies the task of running a network service at a low privilege level and with restricted file system access. The program can be used to run WWW and other network daemons in a minimal environment: the daemons have access only to their own directory tree and run with an unprivileged user ID. This arrangement greatly reduces the impact of possible security problems in daemon software.

You can get *chrootuid* from:
<ftp://ftp.porcupine.org/pub/security/index.html>
<ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/chrootuid/>

portmap

The *portmap* daemon, written by Wietse Venema, is a replacement program for Sun Microsystem's *portmapper* program. Venema's *portmap* daemon offers access control and logging features that are not found in Sun's version of the program. It also comes with the source code, allowing you to inspect the code for problems or modify it with your own additional features, if necessary.

You can get *portmap* from:

<ftp://ftp.porcupine.org/pub/security/index.html>
<ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/portmap/>

Portsentry

The *portsentry* program is a proactive defense against portscans that may precede an attack. *portsentry* listens on a unused TCP/IP ports and takes action when outsiders attempt to establish connections to one or more monitored ports. Actions can include adding the scanning host to */etc/hosts.deny*, adding the scanning host to a packet-filtering firewall, or running other arbitrary commands. *portsentry* is available at:
<http://sourceforge.net/projects/sentrytools/>

Swatch

Swatch, by Todd Atkins of Stanford University, is the Simple Watcher. It monitors log files created by *syslog*, and allows an administrator to take specific actions (such as sending an email warning, paging someone, etc.) in response to logged events and patterns of events.

You can get Swatch from:

<http://www.oit.ucsb.edu/~eta/swatch/>
<ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/swatch>

tcpwrapper

The *tcpwrapper* is a system written by Wietse Venema that allows you to monitor and filter incoming requests for servers started by *inetd*. You can use it to selectively deny access to your sites from other hosts on the Internet, or, alternatively, to selectively allow access.

You can get *tcpwrapper* from:

<ftp://ftp.porcupine.org/pub/security/index.html>
ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/

Tiger

Tiger, originally written by Doug Schales of Texas A&M University (TAMU), is a set of scripts that scan a UNIX system looking for security problems. Tiger was originally developed to provide a check of the UNIX systems on the A&M campus that users wanted to be able to access off-campus. Before the packet filtering in the firewall would be modified to allow off-campus access to the system, the system had to pass the Tiger checks. Tiger was dormant from 1994-1999, but is once again being actively maintained and updated.

You can get Tiger from:

<http://www.tigersecurity.org>

trimlog

David Curry's *trimlog* is designed to help you to manage log files. It reads a configuration file to determine which files to trim, how to trim them, how much they should be trimmed, and so on. The program helps keep your logs from growing until they consume all available disk space.

You can get *trimlog* from:

<ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/trimlog/>

wuarchive ftpd

The *wuarchive* FTP daemon offers many features and security enhancements, such as perdirectory message files shown to any user who enters the directory, limits on number of simultaneous users, and improved logging and access control. These enhancements are specifically designed to support anonymous FTP.

You can get the daemon from:

<http://www.wu-ftp.org>

Windows Tools

Antivirus software

There are many fine antivirus products produced by companies that regularly issue updated virus lists. It is less important which antivirus product you choose than that you choose one, and use it consistently. The best products offer real-time antivirus protection as a background service, rather than just virus scanning on demand.

Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (BSA) is a security-checking application for Windows NT 4 and later systems. It performs a variety of checks on the local system or on remote systems under your administrative control, including checking for updated security patches, password quality, filesystem configuration, auditing, and application-specific checks for IIS and SQL Server. Highly recommended as the first tests to run – if it can't pass this, you've got problems.

Get it from:

<http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp>

Microsoft IIS Lockdown Wizard

IIS, the Windows web server, has repeatedly been the source of system compromises. If you don't choose to replace it completely with Apache (<http://httpd.apache.org>) or another web server, at minimum you should run this Wizard, which disables unnecessary components and tightens security of the IIS installation and configuration. Get it from:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43955>

ANNEX 4. ORGANIZATIONS

Here we have collected information on a few useful organizations you can contact for more information and additional assistance.

Professional Organizations

You may find the following organizations helpful. The first few provide newsletters, training, and conferences. FIRST organizations may be able to provide assistance in an emergency.

Association for Computing Machinery (ACM)

The Association for Computing Machinery is the oldest of the computer science professional organizations. It publishes many scholarly journals and annually sponsors dozens of research and community-oriented conferences and workshops. The ACM also is involved with issues of education, professional development, and scientific progress. It has a number of special interest groups (SIGs) that are concerned with security and computer use. These include the SIGs on Security, Audit and Control; the SIG on Operating Systems; the SIG on Computers and Society; and the SIG on Software Engineering.

The ACM may be contacted at:

ACM Headquarters
One Astor Plaza
1515 Broadway
17th Floor
New York, New York 10036-5701
+1-212-869-7440

ACM has a US Public policy committee that comments on pending legislation affecting security, privacy, and usability. Many of the items they are concerned with should also be of concern to those interested in security.

<http://www.acm.org/usacm/>

The ACM has an extensive set of electronic resources, including information on its conferences and special interest groups. The information provided through the

World Wide Web page is especially comprehensive and well organized:

<http://www.acm.org>

American Society for Industrial Security (ASIS)

The American Society for Industrial Security is a professional organization for those working in the security field. ASIS has been in existence for 40 years and has 32,000 members worldwide as of 2002. Its 25 standing committees focus on particular areas of security, including computer security. The group publishes a monthly magazine devoted to security and loss management. ASIS also sponsors meetings and other group activities. Membership is open only to individuals involved with security at a management level.

More information may be obtained from

<http://www.asisonline.org> or:

American Society for Industrial Security
1625 Prince Street
Alexandria, Virginia 22314-2818
+1-703-519-6200
<http://www.asisonline.org/>

www.cisecurity.org

Cisecurity is a useful source of security information, checklists, and tools for Unix and Windows.

Computer Security Institute (CSI)

The Computer Security Institute was established in 1974 as a multiservice organization dedicated to helping its members safeguard their electronic data processing resources. CSI sponsors workshops and conferences on security, publishes a research journal and a newsletter devoted to computer security, and serves as a clearinghouse for security information. The Institute offers many other services to members and the community on a for-profit basis. Of particular use is an annual *Computer Security Buyer's Guide* that lists sources of software, literature, and security consulting.

You may contact CSI at <http://www.gocsi.com> or:

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
+1-415-947-6320

Electronic Frontier Foundation (EFF)

EFF advocates and litigates on issues related to civil liberties and freedom on the Internet. Although its concerns are considerably broader than security, EFF maintains an interesting archive of privacy- and security-related documents at <http://www.eff.org/Privacy>. EFF can be contacted through that web site, or:

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110-1914
+1-415-436-9333

Electronic Privacy Information Center (EPIC)

EPIC is a public interest research center that studies electronic privacy issues. EPIC litigates and advocates for privacy and civil liberties. EPIC's web site is <http://www.epic.org>, or it can be contacted at:

1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
+1-202-483-1140
Email: info@epic.org

High Technology Crimes Investigation Association (HTCIA)

The HTCIA is a professional organization for individuals involved with the investigation and prosecution of high-technology crime, including computer crime. There are chapters throughout the U.S., and in many other countries. Information is available via the WWW page or through regular mail or phone:
<http://htcia.org>

HTCIA, Inc.
1474 Freeman Dr.
Amissville, VA 20106
+1 540-937-5019

Information Systems Security Association (ISSA)

The ISSA is an international organization of information security professionals and practitioners. It provides education forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members. They publish a magazine and sponsor conferences and workshops. Chapters are present throughout the U.S. and around the world.

For more information about ISSA, contact:

ISSA Headquarters
7044 S. 13th Street
Oak Creek, WI 53154
+1-414-768-8000
+1-800-370-ISSA

ISSA has a WWW page at:

<http://www.issa.org>

Information Systems Audit and Control Association (ISACA)

The ISACA is an international organization of information security management, audit and consulting professionals and practitioners. It provides education forums, publications, professional certification and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members. They publish a magazine and sponsor research, conferences and workshops. Chapters are present throughout the U.S. and around the world.

For more information about ISSA, contact:

ISACA Headquarters
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
+1-847-253-1545
+1-847-253-1443

ISACA has a WWW page at:

<http://www.isaca.org>

International Information Systems Security Certification Consortium, Inc.

The (ISC)² is an international organization that supervises the CISSP and SSCP professional certifications. The Certified Information Systems Security Professional and Systems Security Certified Practitioner designations are widely accepted as standard levels of certification of those working in security. The organization requires certificants to subscribe to a professional code of conduct and to undergo continuing education after passing the initial tests.

More information can be found on the WWW site or via mail.
<http://www.isc2.org>

(ISC)² Services
P.O. Box 1117
Dunedin, FL 34697
USA
+1.888.333.4458

(ISC)² Europe Operations
Nestor House
London UK EC4V 5EX
+ 44 (0) 20 7779 8030

(ISC)² Asia Operations
17/F., Printing House
Central Hong Kong
+852 2111 6612

The Internet Society

The Internet Society sponsors many activities and events related to the Internet, including an annual symposium on network security. For more information, contact the Internet Society:
<http://www.isoc.org>

You may also contact the Society's US or European headquarters:

1775 Wiehle Ave., Suite 102
Reston, VA 20190-5108
+1-703-326-9880

4, rue des Falaises
CH-1205 Geneva
Switzerland
+41-22-807-1444
Email: info@isoc.org

IEEE Computer Society

With nearly 100,000 members, the Computer Society is the largest member society of the Institute of Electrical and Electronics Engineers (IEEE). It too is involved with scholarly publications, conferences and workshops, professional education, technical standards, and other activities designed to promote the theory and practice of computer science and engineering. The IEEE-CS also has special interest groups, including a Technical Committee on Security and Privacy, a Technical Committee on Operating Systems, and a Technical Committee on Software Engineering. More information on the Computer Society may be obtained from:

IEEE Computer Society
1730 Massachusetts Avenue N.W.
Washington, DC 20036-1992
+1-202-371-0101

The Computer Society has a set of WWW pages starting at:
<http://www.computer.org>

The Computer Society's Technical Committee on Security and Privacy has a number of resources, including an online newsletter:
<http://www.ieee-security.org/>

IFIP Technical Committee 11

The International Federation for Information Processing, Technical Committee 11, is devoted to research, education, and communication about information systems security. The working groups of the committee sponsor various activities, including conferences, throughout the world. More information may be obtained from:

<http://www.ifip.org>
(Follow the links for security or for TC 11.)

Systems Administration and Network Security (SANS)

SANS conducts workshops and conferences around the U.S. to provide continuing education in various aspects of system administration and security. This includes training in intrusion detection, firewalls, and general security. The organization also provides various on-line newsletters and alerts, plus some self-paced instruction. More information can be found on their WWW site.

<http://www.sans.org>

USENIX/SAGE

The USENIX Association is a nonprofit education organization for users of UNIX and UNIX-like systems. The Association publishes a magazine, sponsors numerous conferences, and has representatives on international standards bodies. The Association sponsors an annual workshop on UNIX security and another on systems administration, plus many conferences with security-related information.

SAGE stands for the Systems Administrators Guild. It is a special technical group of the USENIX Association. To join SAGE, you must also be a member of USENIX.

Information on USENIX and SAGE can be obtained from:

USENIX Association
2560 Ninth Street
Suite 215
Berkeley, CA 94710
+1-510-528-8649
office@usenix.org

The USENIX WWW page is at:
<http://www.usenix.org>

U. S. Government Organizations

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (formerly the National Bureau of Standards) has been charged with the development of computer security standards and evaluation methods for applications not involving the Department of Defense (DoD). Its efforts include research as well as developing standards. More information on NIST's activities can be obtained by contacting:

NIST Computer Security Division
100 Bureau Drive
Mail Stop 8930
Gaithersburg, MD 20899-8930
+1-301- 975-2934
<http://www.nist.gov>

NIST operates the Computer Security Resource Center:
<http://csrc.nist.gov/>

National Security Agency (NSA)

The NSA maintains lists of evaluated and certified products, as well as technical information about security, especially cryptography. Linux users may be interested in the NSA Secure Linux program, a set of kernel patches that enhances Linux security. NSA also operates the National Cryptologic Museum in Maryland, and has an online museum of cryptology. The NSA web site is <http://www.nsa.gov>.

Also available from the site are a number of helpful configuration guides for common operating systems and routers. These guides provide helpful tips on changing default configurations to support better security and control.

Emergency Response Organizations

The Department of Justice, FBI, and U.S. Secret Service organizations listed below investigate violations of the federal laws related to fraud, theft, and the misuse of computer resources. The various response teams that comprise the Forum of Incident and Response Security Teams (FIRST) do not investigate computer crimes per se, but provide assistance when security incidents occur; they also provide research, information, and support that can often help those incidents from occurring or spreading.

Note that Federal agencies often have field (local) offices where you can get more personal contact, although not all field offices are staffed by personnel with the same level of training as those at headquarters offices. You can check your phone directory for local numbers: look under "US Government."

Department of Justice (DOJ)

10th & Constitution Ave., NW
Criminal Division, (Computer Crime & Intellectual Property Section)
John C. Keeney Building, Suite 600
Washington, DC 20530
+1-202-514-1026
<http://www.cybercrime.gov>

Federal Bureau of Investigation (FBI)

In addition to the NIPC, the FBI also runs the Infraguard — a set of regional cooperative efforts uniting the FBI and local businesses to protect against computer crime. The Infraguard links may be found on the NIPC WWW pages.

National Infrastructure Protection Center
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001
+1-202-323-3205
<http://www.nipc.gov>

U.S. Secret Service (USSS)

Financial Crimes Division
Electronic Crime Branch
U.S. Secret Service
Washington, DC 20223
Voice: +1-202-435-7700
http://www.ustreas.gov/ussf/financial_crimes.shtml

Forum of Incident and Response Security Teams (FIRST)

The Forum of Incident and Response Security Teams (FIRST) was established in March 1993. FIRST is a coalition that brings together a variety of computer security incident-response teams from the public and private sectors, as well as from universities. FIRST's constituents comprise many response teams throughout the world. FIRST's goals are to:

- Boost cooperation among information technology users in the effective prevention of, detection of, and recovery from computer security incidents
- Provide a means to alert and advise clients on potential threats and emerging incident situations
- Support and promote the actions and activities of participating incident response teams, including research and operational activities
- Simplify and encourage the sharing of security-related information, tools, and techniques

FIRST sponsors an annual workshop on incident response that includes tutorials and presentations by members of response teams and law enforcement.

FIRST incorporated in mid-1995 as a nonprofit entity, and migrated FIRST Secretariat duties away from NIST.

The Secretariat can be reached at:
FIRST Secretariat
First.Org, Inc.
PMB 349
650 Castro Street, Suite 120
Mountain View, CA 94041
Email: first-sec@first.org
<http://www.first.org/>

FIRST consists of a large number of member organizations. Check online for the most up-to-date list

of members. If you have a security problem or need assistance, first attempt to determine which of these organizations most clearly covers your operations and needs. If you are unable to determine which (if any) FIRST group to approach, call any of them for a referral to the most appropriate team.

Most of these response teams have a PGP key with which they sign their advisories or enable constituents to report problems in confidence:

<http://www.first.org/rep-info/>

Most teams have arrangements to monitor their phones 24 hours a day, 7 days a week.

Computer Emergency Response Team Coordination Center (CERT/CC)

One particularly notable FIRST team is the CERT® Coordination Center, which serves all Internet sites. CERT grew from the computer emergency response team formed by the Advanced Research Projects Agency (ARPA) in November 1988 (in the wake of the Internet Worm and similar incidents). The CERT/CC charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research into improving the security of existing systems. Their WWW archive (*<http://www.cert.org>*) contains an extensive collection of alerts about past (and current) security problems. Contact CERT at:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
+1-412-268-7090 (24 hour hotline)
Email: cert@cert.org

ANNEX 5. PRINT RESOURCES

There have been a great many books, magazines and papers published on security in the last few years, reflecting the growing concern with the topic. Trying to keep up with even a subset of this information can be quite a chore, whether you wish to stay current as a researcher or as a practitioner. Here, we have collected information about several useful references that you can use as a starting point for more information, further depth, and additional assistance.

We have tried to confine the list to a small set of accessible and especially valuable references that you will not have difficulty finding. A few of the references we have left in for historical reference as much as for any other reason. We've provided annotation where we think it will be helpful.

If you are interested in building your security bookshelf, we advise you to visit a bookstore, see the booksellers at a security conference, or read the reviews of books in security-related venues. The field is moving quickly. Just as you keep up with bugs and patches, it is important to maintain your currency with the literature!

UNIX Security References

These books focus on UNIX computer security.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical Unix and Internet Security, 3rd Edition*. Cambridge, MA: O'Reilly and Associates, Inc., 2003.

Grampp, F. T., and R. H. Morris. "UNIX Operating System Security," AT&T Bell Laboratories Technical Journal, October 1984. This is the original article on UNIX security and remains worth reading.

Wood, Patrick H., and Stephen G. Kochan. *UNIX System Security*, Carmel, IN: Hayden Books, 1986. A good treatment of UNIX System V security prior to the incorporation of TCP/IP networking. This book is of mainly historical interest.

Windows Security References

Norberg, Stefan. *Securing Windows NT/2000 Servers for the Internet: A Checklist for System Administrators*. Cambridge, MA: O'Reilly and Associates, 2002. An excellent hardening guide for Windows NT-based systems that will be used to provide Internet services.

Anderson-Redick, Stacey. *Windows System Policy Editor*. Sebastopol, CA: O'Reilly and Associates, 2000.

Other Security References

The following books and articles are of general interest to all practitioners of computer security.

Computer Crime and Law

Freedman, David H., and Charles C. Mann. *@Large*; NYC, NY, 1997. A story about a huge computer crime spree caused entirely by two people. This incident spawned the FBI Computer Crime Squad, some FIRST teams, and the writing of the Tripwire tool at Purdue.

Icove, David, Karl Seger, and William VonStorch, *Computer Crime: A Crimefighter's Handbook*, Sebastopol, CA: O'Reilly & Associates, 1995. A popular rewrite of an FBI training manual; dated, but with some worthy material.

Power, Richard. *Tangled Web*. Indianapolis, IN, Que, 2002. A collection of stories of cybercrime and investigation. Cites a number of statistics to give a snapshot of the problem.

Computer-Related Risks

Leveson, Nancy G. *Safeware: System Safety and Computers. A Guide to Preventing Accidents and Losses Caused by Technology*. Reading, MA: Addison Wesley, 1995. This textbook contains a comprehensive exploration of the dangers of computer systems, and explores ways in which software can be made more fault tolerant and safety conscious.

Neumann, Peter G. *Computer Related Risks*. Reading, MA: Addison & Wesley, 1995. Dr. Neumann moderates the Internet RISKS mailing list. This book is a collection of the most important stories passed over the mailing list since its creation.

Computer Viruses and Programmed Threats

Communications of the ACM, Volume 32, Number 6, June 1989 (the entire issue). This whole issue was devoted to issues surrounding the Internet Worm incident.

Ferbrache, David. *The Pathology of Computer Viruses*. London, England: Springer-Verlag, 1992. This was probably the best all-around book on the technical aspects of computer viruses, although it doesn't cover macro viruses.

Denning, Peter J. *Computers Under Attack: Intruders, Worms and Viruses*. Reading, MA: ACM Press/Addison-Wesley, 1990. A comprehensive collection of readings related to these topics, including reprints of many classic articles. Historical interest.

Hoffman, Lance J., *Rogue Programs: Viruses, Worms and Trojan Horses*. New York, NY: Van Nostrand Reinhold, 1990. A comprehensive collection of readings on viruses, worms, and the like. More historical interest.

The Virus Bulletin. Virus Bulletin CTD. Oxon, England. An international publication on computer virus prevention and removal. This is an outstanding publication about computer viruses and virus prevention. It is likely to be of value only to sites with a significant PC population, however. The publication also sponsors conferences that have good papers on viruses. <http://www.virusbtn.com>.

Cryptography Books

Denning, Dorothy E. R. *Cryptography and Data Security*. Reading, MA: Addison-Wesley, 1983. The classic textbook in the field. Now out of print but worth having.

Garfinkel, Simson. *PGP: Pretty Good Privacy*. Sebastopol, CA: O'Reilly & Associates, 1994. Describes the history of cryptography, the history of the program PGP, and explains the PGP's use.

Hinsley, F.H., and Alan Stripp. *Code Breakers: The Inside Story of Bletchley Park*. Oxford, England: Oxford University Press, 1993.

Hoffman, Lance J. *Building in Big Brother: The Cryptographic Policy Debate*. New York, NY: Springer-Verlag, 1995. An interesting collection of papers and articles about the Clipper Chip, Digital Telephony legislation, and public policy on encryption. Of some historical interest.

Kahn, David. *The Codebreakers*. New York, NY: Macmillan Company, 1972. The definitive history of cryptography prior to the invention of public key.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second edition*. New York, NY: John Wiley & Sons, 1996. The most comprehensive, unclassified book about computer encryption and data-privacy techniques ever published.

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. NY: Anchor Books, 2000. A very readable and up-to-date treatment of the history and principles of cryptography.

Wayner, Peter. *Disappearing Cryptography*; Boston, MA: Academic Press, 1996. Good coverage of steganography.

Cryptography Papers and Other Publications

Association for Computing Machinery. "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy." Report of a Special Panel of the ACM U.S. Public Policy Committee location: USACM, June 1994. (URL: http://info.acm.org/reports/acm_crypto_study.html)

Diffie, Whitfield. "The First Ten Years of Public-Key Cryptography." *Proceedings of the IEEE* 76 (1988): 560-76. Whitfield Diffie's tour-de-force history of public key cryptography, with revealing commentaries.

Diffie, Whitfield, and M.E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory* IT-22 (1976). The article that introduced the concept of public key cryptography

Lai, Xuejia. "On the Design and Security of Block Ciphers." *ETH Series in Information Processing 1* (1992). The article describing the IDEA cipher.

LaMacchia, Brian A. and Andrew M. Odlyzko. "Computation of Discrete Logarithms in Prime Fields." *Designs, Codes, and Cryptography*. (1991);, 46–62.

Lenstra, A.K., H. W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard. "The Number Field Sieve." *Proceedings of the 22nd ACM Symposium on the Theory of Computing*. Baltimore MD: ACM Press, 1990, 564–72.

Merkle, Ralph. "Secure Communication Over Insecure Channels." *Communications of the ACM 21* (1978): 294–99 (submitted in 1975). The article that should have introduced the concept of public key cryptography.

Merkle, Ralph, and Martin E. Hellman. "On the Security of Multiple Encryption." *Communications of the ACM 24* (1981): 465–67.

Merkle, Ralph, and Martin E. Hellman. "Hiding Information and Signatures in Trap Door Knapsacks." *IEEE Transactions on Information Theory 24* (1978): 525–30.

Rivest, Ron, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." *Communications of the ACM 21* (1978).

General Computer Security

Amoroso, Edward. *Fundamentals of Computer Security Technology*. Englewood Cliffs, NJ: Prentice-Hall, 1994. A very readable and complete introduction to computer security at the level of a college text.

Anderson, Ross. *Security Engineering*; NYC, NY: John Wiley & Sons, 2001. A comprehensive book on end-to-end system design with security in mind.

Bace, Rebecca. *Intrusion Detection*; Indianapolis, IN: Macmillan, 2000. An excellent book on the history and structure of intrusion detection systems for hosts and networks.

Computers & Security. This is a journal published eight times each year by Elsevier Press, Oxford, England. (Order from Elsevier Press, +44-(0) 865-512242.) It is one of the main journals in the field. This journal is priced for institutional subscriptions, not individuals. Each issue contains pointers to dozens of other publications and organizations that might be of interest, as well as referenced articles, practicums, and correspondence. The URL for the WWW page is included in "Security Periodicals."

Gasser, Morrie. *Building a Secure Computer System*. New York, NY: Van Nostrand Reinhold, 1988. A solid introduction to issues of secure system design. Most of the principles still aren't followed in modern systems (unfortunately).

Gollmann, Dieter. *Computer Security*; Chichester, UK, John Wiley & Sons, 1999. A good survey textbook, widely used in academic settings.

Hunt, A. E., S. Bosworth, and D. B. Hoyt, eds. *Computer Security Handbook, 3rd edition*. New York, NY: Wiley, 1995. A massive and thorough collection of essays on all aspects of computer security.

Pfleeger, Charles P and Shari Lawrence Pfleeger. *Security in Computing*. Englewood Cliffs, NJ: Prentice-Hall, 3rd edition, 2002. Another good introduction to computer security.

Russell, Deborah, and G. T. Gangemi, Sr. *Computer Security Basics*. Sebastopol, CA: O'Reilly & Associates, 1991. An excellent introduction to many areas of computer security and a summary of government security requirements and issues.

Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, 2000.

Thompson, Ken. "Reflections on Trusting Trust" *Communications of the ACM*, Volume 27, Number 8, August (1984). This is a "must-read" for anyone seeking to understand the limits of computer security and trust.

Viega, John and Gary McGraw. *Building Secure Software*; Indianapolis, IN: Pearson/ Addison-Wesley, 2002. An excellent book about how to code secure software, and the pitfalls of haphazard coding and deployment.

Wood, Charles Cresson, et al. *Computer Security: A Comprehensive Controls Checklist*, New York, NY: John Wiley & Sons, 1987. Contains many comprehensive and detailed checklists for assessing the state of your own computer security and operations. Out of print, but a valuable reference if you can find one used.

Network Technology and Security

Cheswick, Bill, Steve Bellovin, and Aviel Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition*. Reading, MA: Addison-Wesley, 2003. The second edition of the classic book on firewalls. This book will teach you almost everything you need to know about how firewalls work. The first edition text is largely available online for free, as well, at <http://www.wilyhacker.com/1e/>.

Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly & Associates, 2nd edition, 2000. A great how-to book that describes in clear detail how to build your own firewall.

Comer, Douglas E. *Internetworking with TCP/IP*. 3rd Edition. Englewood Cliffs, NJ: Prentice Hall, 4th edition, 2000. A complete, readable reference that describes how TCP/IP networking works, including information on protocols, tuning, and applications.

Garfinkel, Simson. *Web Security, Privacy, and Commerce*, 2nd Edition. Cambridge, MA: O'Reilly and Associates, Inc. 2002.

Garman, Jason. *Kerberos – The Definitive Guide*. Cambridge, MA: O'Reilly and Associates, Inc, 2003. Provides full coverage of Kerberos in Windows 2000 and Unix environments.

Hunt, Craig. *TCP/IP Network Administration*. Sebastopol, CA: O'Reilly & Associates, 3rd edition, 2002. This book is an excellent system administrator's overview of TCP/IP networking (with a focus on UNIX systems), and a very useful reference to major UNIX networking services and tools such as BIND and send-mail.

Kaufman, Charles, Radia Perlman, and Mike Speciner. *Network Security: Private Communications in a Public World*. Englewood Cliffs, NJ: Prentice-Hall, 2nd edition, 2002.

Stallings, William. *Cryptography and Network Security: Principles and Practices*. Englewood Cliffs, NJ: Prentice Hall, 2003. A good introductory textbook.

Security Products and Services Information

Computer Security Buyer's Guide. Computer Security Institute, San Francisco, CA. (Order from CSI, 415-905-2626.) Contains a comprehensive list of computer security hardware devices and software systems that are commercially available. The guide is free with membership in the Institute. The URL is at <http://www.gocsi.com>.

Understanding the Computer Security "Culture"

All of these describe views of the future and computer networks that are much discussed (and emulated) by system crackers.

Brunner, John. *Shockwave Rider*. New York, NY: A Del Ray Book, published by Ballantine, 1975. One of the first descriptions of a computer worm.

Dreyfus, Suelette. *Underground*; Australia, Reed Books, 1997. A book about the exploits of several Australian hackers relatively early on. Some of the story is incorrect, however, as the author failed to contact all parties to verify the facts.

Gibson, William. *Burning Chrome, Neuromancer, Count Zero, Mona Lisa Overdrive, Virtual Light, Idoru, All Tomorrow's Parties*. New York, NY: Bantam Books Cyberpunk books by the science fiction author who coined the term "cyberspace."

Hafner, Katie and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York, NY: Simon and Schuster, 1991. Tells the stories of three hackers—Kevin Mitnick, Pengo, and Robert T. Morris.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. New York, NY: Dell Books, 1984. One of the original publications describing the "hacker ethic."

Littman, Jonathan, *The Fugitive Game: Online with Kevin Mitnick*. Boston, MA: Little, Brown, 1996. A year prior to his capture in 1995, Jonathan Littman had extensive telephone conversations with Kevin Mitnick and learned what it is like to be a computer hacker on the run. This is the story.

Shimomura, Tsutomu, with John Markoff. *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It*. New York, NY: Hyperion, 1995. On Christmas Day, 1994, an attacker broke into Tsutomu Shimomura's computer. A few weeks later, Shimomura was asked to help out with a series of break-ins at two major Internet service providers in the San Francisco area. Eventually, the trail led to North Carolina, where Shimomura participated in the tracking and capture of Kevin Mitnick. This is the story, written by Shimomura and Markoff. Markoff is the journalist with The New York Times who covered the capture.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. This book is available in several places on the WWW; <http://www-swiss.ai.mit.edu/~bal/sterling/contents.html> is one location; other locations can be found in the COAST hot-list.

Stoll, Cliff. *The Cuckoo's Egg*, Garden City, NY: Doubleday, 1989. An amusing and gripping account of tracing a computer intruder through the networks. The intruder was later found to be working for the KGB and trying to steal sensitive information from U. S. systems.

Varley, John. "Press" Enter. Reprinted in several collections of science fiction, including *Blue Champagne*, Ace Books, 1986; *Isaac Asimov's Science Fiction Magazine*, 1984; and *Tor SF Doubles*, October, Tor Books, 1990.

Vinge, Vernor. *True Names and Other Dangers*. New York, NY: Baen, distributed by Simon & Schuster, 1987.

UNIX System Administration

Albitz, Paul and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly & Associates, 4th edition, 2001. An excellent reference for setting up DNS nameservers.

Bolsky, Morris I., and David G. Korn. *The New Kornshell Command and Programming Language*. Englewood Cliffs, NJ: Prentice-Hall, 2nd edition, 1995. This is a complete tutorial and reference to the ksh—the only shell some of us use when given the choice, and the inspiration for the POSIX shell standard used by bash and others.

Kernighan, Brian, Dennis Ritchie and Rob Pike. *The UNIX Programming Environment*. Englewood Cliffs, NJ: Prentice-Hall, 1984. A nice guide to the UNIX philosophy and how to build shell scripts and command environments under UNIX.

Nemeth, Evi, Garth Snyder, Scott Seebass, and Trent R. Hein. *UNIX System Administration Handbook. 3rd Edition*. Englewood Cliffs, NJ: Prentice-Hall, 2000. An excellent reference on the various ins and outs of running a UNIX system. This book includes information on system configuration, adding and deleting users, running accounting, performing backups, configuring networks, running sendmail, and much more. Highly recommended.

Welsh, Matt, Kaufman, Lar, Dalheimer, Matthias K., and Dawson, Terry. *Running Linux (4th edition)*. Sebastopol, CA: O'Reilly & Associates, 2002.

Wall, Larry, Christiansen, Tom, and Orwant, Jon. *Programming perl (3rd edition)*, Sebastopol, CA: O'Reilly & Associates, 2000. The definitive reference to the Perl scripting language. A must for anyone who does much shell, awk, or sed programming or would like to quickly write some applications in UNIX.

Windows System Administration

O'Reilly and Associates has a series of helpful books on Windows system administration, including *Windows NT TCP/IP Network Administration* (Craig Hunt and Robert Bruce Thompson, 1998), *Managing the Windows 2000 Registry* (Robichaux, 2000), *DHCP for Windows 2000* (Neall Alcott, 2001), *DNS on Windows 2000, 2nd Edition* (Matt Larson and Cricket Liu, 2001), *Windows 2000 Administration in a Nutshell* (Mitch Tulloch, 2001), and *Windows Server 2003 in a Nutshell* (Mitch Tulloch, 2003).

Security Periodicals

Computer Audit Update

Computer Fraud & Security Update

Computer Law & Security Report

Computers & Security

Elsevier Advanced Technology
Crown House, Linton Rd.
Barking, Essex I611 8JU
England
Voice: +44-81-5945942
Fax: +44-81-5945942
Telex: 896950 APPSCI G

North American Distributor:
P.O. Box 882
New York, NY 10159
Voice: +1-212-989-5800

<http://www.elsevier.nl/catalogue/>

Computer Security Alert

Computer Security Journal

Computer Security Buyers Guide

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
Voice: +1-415-905-2626

<http://www.gocsi.com>

Disaster Recovery Journal

PO Box 510110
St. Louis, MO 63151
+1 314-894-0276

<http://www.drj.com>

InfoSecurity News

West Coast Publishing, Inc.
161 Worcester Road, Suite 201
Framingham, MA 01701

<http://www.scmagazine.com>

Information Security

85 Astor Ave, Suite 2
Norwood, MA 02062

<http://www.infosecuritymag.com>