Information Security Resources: A Selected Annotated Bibliography

Daniel S. Dotson

ABSTRACT. The article contains selected resources in the area of information security and its related topics, covering the majority of resources published within the past five years. Serials, Web sites, monographs, and conference proceedings are described. Serials and conferences are described as a whole, with examples of topics recently addressed. Books and Web sites are described with important features and examples of topics covered are pointed out. While a majority of the resources are mainly written with the needs of computer professionals in mind, some of the resources target general users or users from other disciplines.

Introduction

The security of information stored electronically is an increasingly important topic as news of hackers, data theft, and security holes in software and operating systems seems to have become more common and as national security has become a topic of great importance.

Several terms and phrases are used to describe or are related to security in the realm of computer technology. Information security, information assurance, cryptography, cryptology, computer security, and network security are just a few of those. This selected annotated bibliography lists recent and historical works on a variety of information security topics. The resources are in a variety of formats and include serials, articles, Web sites, monographs (which include manuals, dictionaries, and handbooks), and conference and workshop proceedings.

This bibliography is designed as a guide to valuable information security resources that would be of use to librarians who deal with this topic area. It may also be a useful list of resources for professionals or individuals needing information security resources.

Starting Points

Some other useful guides to information security resources are available. This section highlights guides from the literature that are excellent sources on information security resources.

Balas, Janet L. 2003. "Security in the Library–Technology Brings a New Twist to an Old Problem." *Computers in Libraries* 23, no. 5: 28-30, http://www.epnet.com/ (accessed June 26, 2006).

This guide was written by a systems librarian with security issues in libraries in mind. The article provides an overview of important Web resources on security, including sites from government, Microsoft, institutes, and also sites that are library oriented.

Balas, Janet L. 2005. "Close the Gate, Lock the Windows, Bolt the Doors: Securing Library Computers." *Computers in Libraries* 25, no. 3: 28-30, http://www.epnet.com/ (accessed June 26, 2006).

> While on similar topics, most of the resources discussed in this article differ from the other recommended guide by this author. This article mentions some sites specific to certain vendors and operating systems (such as Linux, Microsoft, Apple, and Cisco), news resources, and more.

Kinkus, Jane F. 2002. "Computer Security." *Issues in Science & Technology Librarianship* no. 36, http://www.library.ucsb.edu/istl/ (accessed June 19, 2006).

> This article gives an overview of a wide variety of computer security resources on the Web and includes short descriptions of the sites. The resources are divided into categories such as general information, consumer information, biometrics, antivirus, security policies, and more.
>
> In addition to the abovementioned guides, the September 26, 2003 (volume 13, number 33) issue of CQ Researcher contains articles on government issues in cybersecurity. The issue has a short bibliography on page 815 that gives a list of books, reports, studies, and articles mentioned and a longer list of resources (labeled, "The Next Step: Additional Articles from Current Periodicals") on pages 816 through 819 that has articles grouped by topic.

Serials

Serials contain some of the most recent and varied information on information security topics. Information often appears in serials well before monographs. ISSN, current publisher, previous title, frequency, serial type, and beginning year of publication were verified through Ulrich's Periodicals Directory (online version).

Computer Fraud & Security
ISSN 1361-3723, Elsevier, Newsletter

Published since 1979, this monthly serial, formerly known as Computer Fraud & Security Bulletin, offers general information and news about computer security. Recent topics include phishing, an ISP collecting information for law enforcement, Al Qaeda, security incidents and threats, and the theft of millions of credit card numbers. An events calendar is found near the end of each issue.

Computers and Security
ISSN 0167-4048, Elsevier, Journal (Academic/Scholarly)

This refereed Elsevier publication started in 1982 and publishes eight issues yearly. Issues typically begin with a short article on a timely topic and a longer article on a security topic, both by the editor-in-chief. Following these sections are articles on several security topics, a calendar of events, and then refereed articles. The topics cover a wide range of issues and the scope, authors, and referees are international. Recent articles address such topics as trusted computing, worms, book recommendations, studying attacks, and authentication.

Designs, Codes, and Cryptography
ISSN 0925-1022, Springer, Journal (Academic/Scholarly)

Published since 1991, this monthly journal has information on various design, coding, and cryptography topics. Recent article topics include binary fingerprinting codes, Web metering, and binary codes.

EDPACS: The EDP Audit, Control & Security Newsletter
ISSN 0736-6981, Auerbach Publications, Newsletter

Published since 1973, this monthly newsletter focuses on a wide range of computer security topics. Recent articles cover spyware, IT governance, implementing an information security awareness program, and user authentication.

IEEE Security and Privacy
ISSN 1540-7993, IEEE Computer Society, Magazine (Trade)

This bimonthly magazine began publication in 2003. Each issue addresses various computer and security topics, beginning with an introductory brief article written by an editor. Readers are invited to write letters to the magazine. The scope is international. News, legal issues, conferences, threats to computer security, methods to insure security, standards, book reviews, and education are recent topics.

IEEE Transactions on Dependable and Secure Computing
ISSN 1545-5971, IEEE Computer Society, Journal (Academic/Scholarly)

This quarterly journal began publication in 2004. Recent topics include achieving privacy in trust negotiations, DDoS flooding attacks, secure group communication, and automated online monitoring of distributed applications.

IEEE Transactions on Information Forensics and Security
ISSN 1556-6013, IEEE Computer Society, Journal (Academic/Scholarly)

This new quarterly journal began publication in 2006. Topics in the first two issues include facial expression recognition, signature verification, personal authentication using 3-D finger geometry, biometrics, iris-based identification, and image hashing.

Information Management & Computer Security
ISSN 0968-5227, Emerald Group Publishing, Journal (Academic/
Scholarly)

Published since 1992, this journal produces five issues per year and was formed by the merger of *International Journal of Information Resource Management* (UK) and *Computer Control Quarterly* (Australia). Recent articles address biometric technologies, IT project failures, managing security vulnerabilities, knowledge management, and auditing in an e-commerce

perspective.

Information Security
ISSN 1096-8903, TechTarget, Magazine (Trade)

In publication since 1997, this monthly magazine covers various aspects of information security. Recent articles focus on such security aspects as network intrusion prevention, software, patches, viruses, and data protection.

Information Security Technical Report
ISSN 1363-4127, Elsevier, Journal (Academic/Scholarly)

Published since 1996, this quarterly journal addresses advances in information security. Recent articles broach such topics as identity management, malware, Web services security, and security topics at various companies.

Information Systems Security
ISSN 1065-898X, Auerbach Publications, Journal (Trade)

Published since 1991, this bimonthly journal was preceded by *Journal of Information Systems Security* and covers various information security
topics. Recent articles focus on wireless security, spam, small business network security, firewall topologies, bots, and biometric systems.

International Journal of Information Security
ISSN 1615-5262, Springer, Journal (Academic/Scholarly)

In publication since 2001, this semiannual journal focuses on such topics such as Web privacy, security protocols, authentication, and public-key encryption.

Journal of Cryptology
ISSN 0933-2790, Springer, Journal (Academic/Scholarly)

This quarterly journal began publication in 1988 and covers various information security and cryptology topics. Recent article topics touch on issues such as storage, transfer of data, retrieval of information, security attacks, and algorithms and models.

Network Security
ISSN 1353-4858, Elsevier, Newsletter

Published since 1994, this monthly newsletter addresses topics regarding network security. Recent articles address issues such as Blackberry security, vulnerabilities of specific products, internal security threats, bot networks, and biometrics. An events calendar is usually near the end of the journal.
Security Management
ISSN 0145-9406, The American Society for Industrial Security, Magazine (Trade)

This monthly magazine, in publication since 1957, focuses on a variety of security topics, including computer technology. Some recent topics in the area of information security include viruses, IT security, and data protection.

Security: The Magazine for Buyers of Security Products, Systems and Service
ISSN 0890-8826, BNP Media, Magazine (Trade)

Published since 1964, this monthly magazine covers various security topics and is not limited to topics regarding computer technology alone. Recent topics of articles include operating systems, database management, mobile devices, and biometrics.

Articles

This section contains information about 10 articles from a variety of serials (not limited to the titles from the previous section). While most of the articles are from the past few years, an example of an article discussing information security from 1948 is included to indicate that the topic has been around since before computers became common.

Chesla, Avi. "Information Security: A Defensive Battle." *Information Systems Security* 12, no. 6 (2004): 24-32, http://search.epnet.com/ (accessed March 17, 2006).

This article compares network security with a real-life battlefield (soldiers, defense strategies, etc.). The author uses military analogies to explain different levels of network security, methods used for security, communication, leadership, and examining one's defenses. The comparison of network security with military defensive measures is an excellent analogy and gives readers a context they can understand.

Condon, E.U. "Science and Security." *Science* 107, no. 2791 (1948): 659-665, http://www.jstor.org/ (accessed March 17, 2006).

Some may think that information security is a topic that is a fairly recent concern, but this article from 1948 shows that the topic has been around for at least fifty years, although not always focused on computers. The author discusses subjects such as the tradition of science to share knowledge in the face of World War II and the post-War era, where perhaps the most closely guarded information involved the atomic bomb. Scientists had to face new requirements, such as clearance, to gain access to certain data. The article also mentions problems in keeping some material too secure, such as not knowing where to find needed information within one's own organization or whether or not you are duplicating something already done.

Jain, Anil K., Arun Ross, and Sharath Pankanti. "Biometrics: A Tool for Information Security." IEEE Transactions on Information Forensics and Security 1, no. 2 (2006):125-143, http://ieeexplore.ieee.org (accessed June 26, 2006).

Instead of using passwords, biometrics may be used to ensure security. Such methods include verification through matching facial features, fingerprints, irises, keystrokes, hand

geometry, signature, and voice. The advantages and disadvantages of these different methods are mentioned in addition to examples of how some of these methods are being used.

Rebbapragada, Narasu. "All-in-One Security." *PC World* 24, no. 7 (2006):100-112, http://www.epnet.com/ (accessed June 26, 2006).

Ten security suites are ranked and rated on various factors, including detection and cleanup of malware and adware, firewall abilities, speed, design, and such added features as parental controls and instant messenger compatibility. The author describes the importance and quality of various features of the suites.

Ruiu, Dragos. "Learning From Information Security History." IEEE Security & Privacy 4, no. 1 (2006):77-79, http://ieeexplore.ieee.org (accessed June 26, 2006).

This article gives some historical information about security issues, including important events and points of interest. The article especially focuses on conferences the author has hosted and examines the topics discussed for trends. The author concludes that security problems are likely to get worse as perpetrators become more sophisticated.

Ryan, Julie J.C.H. "Information Security Tools and Practices: What Works?" IEEE Transactions on Computers 53, no. 8 (2004):1060-1063, http://ieeexplore.ieee.org (accessed March 17, 2006).

Designed as a guide for small businesses, this article looks at effective tools and practices to insure information security. Surveys were sent to small businesses to gather their major concerns (corruption of data, such as viruses, being at the top). The surveys were examined to see if certain practices or tools (or their lack of use) correlated in any way to security incidents.

Sendze, Monique. "The Battle to Secure Our Public Access Computers." *Computers in Libraries* 25, no. 1(2006):10-16, http://www.epnet. com/ (accessed June 26, 2006).

This article is a good overview of computer security issues in a library. The author discusses problems, solutions, tools, and policies in her public library system. A major topic is the balancing of security with accessibility, an important topic to most libraries.

Tolone, William et al. "Access Control in Collaborative Systems." *ACM Computing Surveys* 37, no. 1 (2006): 29-41, http://portal.acm.org (accessed June 26, 2006).

The focus of this article is balancing the need of access in a collaborative system (such as groupware or shared documents) with the need to provide security. Various security methods and their advantages and disadvantages are mentioned.

Trim, Peter R.J. "Managing Computer Security Issues: Preventing and Limiting Future Threats and Disasters." *Disaster Prevention & Management* 14, no. 4 (2005): 493-505.

This article goes over computer security issues faced by businesses and focuses on management issues rather than technical details. Statistics are used to drive home the point that

security is a problem and that management not only needs to take it seriously, but needs to make sure that policies, procedures, and personnel are a part of the security framework.

Zeller, Tom, Jr., "Cyberthieves Silently Copy as You Type." *The New York Times*, February 27, 2006, http://web.lexis-nexis.com (accessed June 26, 2006).

When accessing your bank or credit card account online, someone may be examining your keystrokes to determine your user information via keylogging programs. Incidents in Brazil and Miami illustrate that the problem is an international one and that security problems face both individuals and businesses. Such security incidents are making it into major newspapers.

Web Sites

Web sites provide valuable and up-to-date information on a variety of information security topics. Since many subjects are timely and require the need for information to be readily available, Web sites are valuable resources. The sites are managed by a variety of organizations, including societies, government agencies, businesses, educational institutions, and non-profit agencies.

CERIAS: http://www.cerias.purdue.edu/

The Center for Education and Research in Information Assurance (CERIAS) is located at Purdue University and specializes in education and research in the area of information security and assurance. The site has information about research projects, news and events, educational materials at all levels, and training information and resources. Other features include the Bibtex Paper Archive (papers on a variety of security topics), the CERIAS Hotlist (a large database of links organized by categories and topics), and an FTP archive (containing software, tools, standards, and more).

CERT Coordination Center: http://www.cert.org/

This site is produced by the Carnegie Mellon Software Engineering Institute, and according to the site, it was the first computer security incident response team. The major categories on the site are vulnerabilities, incidents, and fixes (view and report incidents and look for fixes), security practices and evaluations (improving security), survivability research and analysis (recent research, workshops, and trends in security), and training and education (courses offered for managers and technical personnel). The main page has recent news, a site search box, and links to other resources such as publications, CERT statistics, and more.

Computer Security Resource Center: http://csrc.nist.gov/

This is the Web site for the Computer Security Resource Center at the National Institute of Standards and Technology's Computer Security Division. The site has information on vulnerabilities, practices, publications (such as guidelines and standards), annual reports, focus areas, links to Computer Security Division news, and links to other resources. Links to services for the federal government, vendors, and users are also provided.

IEEE Computer Society Information Assurance: http://ieeeia.org/

IEEE offers this site on information assurance. Information is available on standards, conference proceedings, and workshops. The site provides links to IEEE groups (IEEE Information Assurance Standards Committee, IEEE Technical Committee on Security and Privacy, and IEEE Task Force on Information Assurance), standards (IEEE, ISO, IFIP), and other useful sites for those interested in information security.

Industry and Sectors Information Security: http://www.dti.gov.uk/sectors/ infosec/index.html

This site targeting businesses is from the Information Security Policy Team of the United Kingdom's Department of Trade and Industry. Information about legislation, business advice, publications, and select outside links is available.

Information Assurance Advisory Council: http://www.iaac.org.uk/

The Information Assurance Advisory Council brings together people from the corporate, public policy, law enforcement, and research community to address information assurance topics. The site offers tips, news (general, legislation, press releases, articles, conference papers, and interviews), information about meetings and workshops, and general information about the organization. A member intranet area with resources is also available.

Information Assurance Center: http://www.issl.iastate.edu/

The Information Assurance Center at Iowa State University is home to over 24 faculty members from various departments on campus and provides courses and a master's degree in Information Assurance and a graduate certificate program. The center also offers other educational and outreach opportunities. The site offers information about projects, labs doing special research, faculty and their research interests, and news about the center.

Information Assurance Technology Analysis Center: http://iac.dtic. mil/iatac/

The Information Assurance Technology Analysis Center, from the Department of Defense, is designed to provide a central point for information about information assurance technology. The site includes news, information on products, and links to other sites. Some areas and services are limited to Department of Defense personnel.

Information Security: http://infosecuritymag.techtarget.com/

The Web site for Information Security, also available as a print magazine, includes information on Windows security problems, viruses, and other security issues. The site has an archive of its articles back to 2000 and of selected articles back to 1998. White Page articles (some linking outside the site) written by outside companies are available on various subjects. Users may be asked to sign up to download an article, but the site also gives an abstract. A search engine searches both the site and the articles.

Information Security Forum: http://www.securityforum.org/html/_frameset.htm

Here is the Web site for the Information Security Forum (ISF), an association of over 260 companies and public organizations. The site offers access to free downloads and the ISF Standard (of good information security practice). Members gain access to a variety of tools and publications. Links to a membership list, list of projects, and information about the ISF's world congress are available.

Information Society: http://www.europa.eu.int/scadplus/leg/en/s21012.htm

This page links to English-language information about European Union rules and regulations, network security, data protection, and other useful information.

Microsoft Security: http://www.microsoft.com/security/default.mspx

This Microsoft Web site offers links to the most recent Windows Security Updates and security updates for other Microsoft products. The site also has information about recent security incidents such as viruses, worms, and hackers. Advice on how to keep one's computer secure is also offered. Information is categorized by the level of user (home users, IT professionals, developers, and businesses). Links to outside Web sites and to other useful features (such as chat, Webcasts, and newsgroups) are also provided.

National Information Assurance Partnership: http://niap.nist.gov/

The National Information Assurance Partnership (NIAP) was created to meet security testing needs of users and producers of information
technology. This Web site provides criteria, configuration guides, validated products, products being evaluated, protection profiles, briefings, events, and links to other organizations.

National Information Assurance Training and Education Center: http://niatec.info

This center is a consortium of academic, industry, and government organizations. The site has a variety of resources, including seminal papers and talks, information on virus tools, scholarship information for students, links to outside resources (including member sites), and links to a wide variety of publications (including journals, books, databases, government documents, and industry documents). Some publications are available in PDF directly from the Web site.

The National Security Agency/Central Security Service: http://www. nsa.gov/

The National Security Agency/Central Security Service is responsible for the U.S. government's information security needs. The site provides information and links about various security topics, agency information, government policies and legal information, and historical information (including information about the National Cryptologic Museum). The Research section provides valuable resources, including reports and presentations, links, and contacts.

Security-enhanced Linux is a major topic in this section and is covered by several reports and presentations as well as having its own dedicated page.

The SANS Institute: http://www.sans.org/

This Web site for the SANS (SysAdmin, Audit, Network, Security) Institute focuses on information security training and certification. The main page has a list of training opportunities, with several categories that may be offered at various locations worldwide as well as onsite. The site also offers information on webcasts, resources, projects, newsletters, sample policies, and other valuable information. A "top twenty" list takes the user to what the site sees as the top 10 Windows and top 10 UNIX vulnerabilities.

Security Portal for Information System Security Professionals: http:// www.infosyssec.com/ This site has hundreds of links to various topics, organizations (both national and international), news, ALT News Groups, mailing lists, a wide variety of search engines, virus alerts, anti-virus vendors, chat rooms, security alerts, vendor-specific alerts and patches, online tools, and recommended links. Search engines are provided that search a variety technology-oriented Web sites. These search engines can be used on the site itself, without having to link out to other Web sites. An open directory is available, with links sorted by language as an option.

Monographs

Monographs are able to go into extensive detail on information security topics. The monographs covered in this section cover a variety of topics. Some address information security as a whole, while some focus on a specific aspect. Some items target those working in the area of information security, while others are written with another field or the general reader in mind. While the majority of the monographs are published in the past five years, a few examples of earlier works are included.

Bidgoli, Hossein, ed. *Handbook of Information Security.* Hoboken, NJ: Wiley, 2005.

This handbook consists of three volumes, each with its unique index, but with the table of contents for all volumes. Each article has its own table of contents to its sections, a glossary of terms, cross-references to other topics, black and white images (photographs, diagrams, charts, etc.), and references. Some entries even recommend works to see for further information.

> Vol. 1: Key Concepts, Infrastructure, Standards, and Protocols
> Vol. 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations
> Vol. 3: Threats, Vulnerabilities, Prevention, Detection, and Management

Boone, J. V. *A Brief History of Cryptology.* Annapolis, MD: Naval Institute Press, 2005.

This history of cryptology mentions some of the earliest methods of security of information, such as the uses of cryptography in ancient Egypt, Leon Battista Alberti's cipher in

Renaissance Italy, and Polygraphia (published in Germany in 1518), the first book on cryptography. The vast majority of the history of cryptology (and the majority of the book's content) is related to its uses for modern inventions, such as the telegraph, telephone, and later radio, computers, and satellites. Appendix A contains a brief introduction to concepts of cryptology.

Bosworth, Bruce. *Codes, Ciphers, and Computers: An Introduction to Information Security.* Rochelle Park, NJ: Hayden Book Co., 1982.

Over two decades old, this book shows that information security is hardly a new topic. It begins with methods for codes and ciphers employed before computers and moves into methods of using these and other devices for computer security.

Bruen, Aiden A. and Mario Forcinito. *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century.* Hoboken, NJ: Wiley-Interscience, 2005.

This handbook covers the three topics listed in its title. The first part starts with historical background on cryptography and moves into fundamentals, methods of cryptography, different types of attacks, and practical issues. The second part deals with Information Theory and explains information (storage, transmission, etc.) mathematically. The third part focuses on using error correction in order to give better results.

Calabrese, Thomas. *Information Security Intelligence: Cryptographic Principles and Applications.* Clifton Park, NY: Delmar Learning, 2004.

Calabrese addresses such issues as security planning, risks and risk assessment, legal issues, planning, cryptography, viruses, worms, and other information security issues. Appendices include user labs and experiments, TCP/IP fundamentals, and a NIPC Cybercrime Reporting Form.

Easttom, Chuck. *Computer Security Fundamentals.* Upper Saddle River, NJ: Pearson Prentice Hall, 2006.

This book has an overview on a variety of computer security topics. It begins with the topic of cyber crime and security, which includes terminology, legal issues, security resources, and types of threats. Other chapters address security topics such as malware, Internet fraud and cyber crime, industrial espionage, cyber terrorism and information warfare, and security hardware and software. The appendices contain valuable information about educational opportunities, security resources, and sample security documents.

Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code.* Boston: Elsevier Butterworth Heinemann, 2005.

This guide goes into details of malicious code such as protection and prevention, responses to incidents, and the future of malicious code. The third chapter covers historical

information and includes famous incidents. The appendix of the guide contains a valuable list of security resources.

Fugini, Mariagrazia, and Carlo Bellettini. *Information Security Policies and Actions in Modern Integrated Systems.* Hershey, PA: Idea Group Pub., 2004.

Covering recent trends in information security, this book includes digital certificates, smart card applications, privacy on the semantic web, digital rights management, authentication, cryptography, authorization frameworks, and privacy. The issues presented are global and indeed most of the chapters have authors from outside the United States (mainly from Italy and Germany).

Furht, Borivoje, and Darko Kirovski, eds. *Multimedia Security Handbook.* Boca Raton, FL: CRC Press, 2005.

This handbook contains 26 chapters on various topics in multimedia security and focuses on security for formats other than text, including images, videos, 3-D models, and audio. The book covers security measures such as watermarking, fingerprinting, authentication, filtering adult images, and encryption. One chapter focuses on digital rights management issues for video formats.

Gattiker, Urs E. *The Information Security Dictionary: Defining the Terms that Define Security for E-Business, Internet, Information, and Wireless Technology. The Kluwer International Series in Engineering and Computer Science; SECS 767. 1st ed.* Boston: Kluwer Academic Publishers, 2004.

Gattiker offers definitions of various concepts in information security. Some definitions are short, while others go into detail for several pages and may include tables or diagrams. The valuable tables and figures found in the text are also listed in the table of contents. Appendices contain recommended sources that may be useful to users, including print resources, tools, Web resources, and standards. Cross-references to other terms are found throughout the dictionary.

Howlett, Tony. *Open Source Security Tools: Practical Applications for Security. Bruce Perens' Open Source Series.* Upper Saddle River, NJ: Prentice Hall, 2005.

This book, which includes a CD, offers information on open-source security tools for Windows, UNIX, and Linux. In the preface to the book, there is a handy chart listing various security tools and whether they're available on CD, for Windows, for UNIX/Linux, and the page number on which the tool can be found. The first chapter gives a general security overview. The following chapters describe tools in a specific area, such as operating systems tools, firewalls, encryption tools, etc. The appendices contain information on licenses, commands, common port numbers, sample forms, and a large appendix (over a hundred pages) covering Nessus plug-ins.

Kabatiansky, G., G. Kabatiansky, E. Krouk, and S. Semenov. *Error Correcting Coding and*

Security for Data Networks: Analysis of the Superchannel Concept. Chichester, West Sussex; Hoboken: England; NJ: John Wiley & Sons, 2005.

This title covers various aspects of coding data networks. Security topics are addressed in an entire chapter and include public-key cryptography, code-based cryptosystems, and code-based signatures.

Kairab, Sudhanshu. *A Practical Guide to Security Assessments.* Boca Raton, FL: Auerbach Publications, 2005.

After beginning with an overview of information security, the book moves into how to use a security assessment in the information security program of an institution. Such topics as planning, gathering information, evaluating processes and technology, and running a risk analysis are covered. The last two chapters in the book mention standards and legislation regarding information security. The book has 17 appendices, covering such varying topics as employee termination, administration of user IDs, HIPAA security, and questionnaires.

Kruegel, Christopher, Fredrik Valeur, and Giovanni Vigna. *Intrusion Detection and Correlation: Challenges and Solutions. Advances in Information Security; 14.* New York: Springer, 2005.

Intrusions and attacks are major concerns for computer professionals. This book covers aspects of intrusion detection, such as methods of avoiding attacks and alerts to attacks when they occur.

Merkow, Mark S. and Jim Breithaupt. *The Complete Guide to Internet Security.* New York, NY: AMACOM, 2000.

The title says it all. This book covers a wide variety of topics, beginning with foundations and fundamental elements and moving on to topics such as network security and hacking (including tools hackers use), security enforcement, national and international security-testing standards, physical security, cryptography, and resources for maintaining security as a long-term goal. Appendices provide information such as a sample security policy, recommended Web sites, security specialists, readings, and a glossary. Diagrams and examples are found throughout the book.

Nestler, Vincent J. et al. *Computer Security Lab Manual.* Boston: McGraw-Hill Irwin, 2006.

This practical manual on learning about computer security focuses mostly on networks and covers both Linux and Windows. The book begins with a section on getting users to know how networks actually work, followed by sections on threats to networks, preventing threats, and detection and response. Labs that make the reader actually apply the topic to a real network comprise the majority of the book. The labs include time estimates and screen shots.

Peltier, Thomas R. *Information Security Policies and Procedures: A Practitioner's Reference. 2nd ed.* Boca Raton, FL: Auerbach Publications, 2004.

Part 1 of this book covers designing and implementing security policies and procedures (including doing research and using focus groups), choosing an editor, the format and layout of documents, developing standards and procedures, and how to sell your final documents to those who will be affected by them. Part 1 ends with appendices containing sample documents. Part 2 is a reference guide to information security and includes an overview, fundamental issues, security tools used, employee responsibilities, processing information, and information security program administration.

Peltier, Thomas R., Justin Peltier, and John Blackley. *Information Security Fundamentals.* Boca Raton, FL: Auerbach Publications, 2005.

This book begins with an overview of information security and goes into types of threats, the structure of an information security program, policies, classifying information into various categories, confidentiality, copyright, access control, physical security, risk analysis and management, and business continuity planning. Other useful features include a glossary, chapter summaries, and illustrations.

Purser, Steve. *A Practical Guide to Managing Information Security. Artech House Technology Management and Professional Development Library.* Boston, MA: Artech House, 2004.

The book begins with a chapter that addresses issues in information security. The second chapter addresses general management techniques. The third goes into details about security tools. The rest of the book ties all these issues together in describing how actually to go about managing security through making policies, processes, etc.

Tipton, Harold F. and Micki Krause. *Information Security Management Handbook. 5th ed.* Boca Raton, FL: Auerbach, 2003. (Volume 1) Tipton, Harold F. and Micki Krause. *Information Security Management Handbook. 5th ed.* Boca Raton, London: Auerbach, 2005. (Volume 2)

The fifth edition of this title, which includes two volumes (published separately), contains hundreds of pages of valuable information on information security. One hundred and sixty-three topics in the first volume are broken into 10 areas: (1) access control; (2) telecommunications; (3) network and internet security; (4) information security management; (5) application program security; (6) cryptography; (7) enterprise security architecture; (8) operations security; business continuity planning; (9) law, investigation, and ethics; and (10) physical security. The second volume contains 41 topics in 10 areas similar to the first volume. Both volumes contain indexes and information about the editors and contributors to the volumes.

Wylder, John. *Strategic Information Security.* Boca Raton, FL: Auerbach Publications, 2004.

The book begins with a general introduction to information security. The rest of the chapters are divided into three sections. The Organizational Issues section addresses setting up a security organization and includes information about personnel. The Risk Management Topics section addresses such topics as networks, risk reduction strategies, and authentication. The Information Security Principles and Practices section includes continuity planning, monitoring,

auditing and testing, and outsourcing. The appendix is a page of recommended resources.

Conference and Workshop Proceedings

Conference proceedings are important works for researchers and practitioners. The following proceedings cover topics in information security, one having been active for over a quarter century.

ACM Conference on Computer and Communications Security

Published by ACM Press, the items in the proceedings are mainly from people working in the United States, although some international participants have papers included. Recent topics include access control, anonymity, authentication, crypto protocols, cryptographic tools, cryptography, denial of service, intrusion detection, keys, network security, operating systems, peer-to-peer networks, privacy, and sensor networks. Many proceedings contain a keynote address and invited talks.

ACM Symposium on Access Control Models and Technologies

This symposium covers a variety of topics in the area of access control. Topics in recent proceedings include video surveillance databases, trust-based authorization, secure collaboration, privacy control, access control for XML documents, access control policy implementation, verification, and constraints.

Advances in Cryptology–CRYPTO: International Cryptology Conference

Published by Springer as part of its Lecture Notes in Computer Science, this conference has met for over 25 years. This international conference covers a variety of cryptology and computer security topics. Many volumes have an invited talk (some more than one). Topics in past proceedings include authentication, ciphers, cryptanalysis, crypto-systems, encryption, foundations, keys, protocols, secret sharing, signatures, and zero-knowledge.

Advances in Cryptology–EUROCRYPT: International Conference on the Theory and Applications of Cryptographic Techniques

While this conference is held yearly in Europe, its participants are from across the globe. These proceedings are published in Springer's Lecture Notes in Computer Science series. Recent topics include algorithms, anonymity, ciphers, cryptanalysis, elliptic curves, encryption, foundations, hash functions, multiparty protocols, signatures, and voting schemes.

Computer Security Applications Conference

This yearly conference from the Applied Computer Security Associates, (which held its twenty-first meeting in 2005), has its papers since 1998 available online at http://www.acsac.org/ (also available from IEEE). Recent topics include a minimal-complexity secure GUI, Ticket-based Address Resolution Protocol (TARP), securing e-mail archives, graphical passwords,

stealth breakpoints, worm detection, and using predators to combat worms and viruses.

Computer Security–ESORICS European Symposium on Research in Computer Security

These proceedings are published by Springer as part of the Lecture Notes in Computer Science series. This conference, while held in Europe, has worldwide contributors. Recent topics covered include access control, authentication, confidentiality, data entanglement, dynamic constraints, electronic commerce, electronic voting, encryption, fingerprints, inference control, intrusion detection and prevention, mobile agents, privacy, and smart cards.

Computer Security Foundations Workshop (IEEE)

This workshop covers foundational issues of information security. Recent topics in its proceedings include information flow, protocols, declassification, denial of service, intrusion detection, authorization, and access control.

IEEE Symposium on Security and Privacy

This symposium has information security and privacy issues as its focus. Recent topics include intrusion detection, authentication, sensor networks, attacks and defenses, cryptography, static analysis, and network security.

Information and Communications Security: International Conference, ICICS: Proceedings

These proceedings are published by Springer as part of the Lecture Notes in Computer Science series. Topics in recent proceedings include access control, attacks, cyber-attack simulation, databases, denial-of-ser-vice attacks, encryption sticks, fingerprinting, key management, mobile agent security, oblivious transfer, signatures, and watermarking.

Information Security and Privacy: Australasian Conference, ACISP

Published by Springer as part of its *Lecture Notes in Computer Science* series, this conference has been meeting since 1996. Examples of topics addressed include access control, authentication, cryptoanalysis, key management, network security, protocols, secret sharing, and signatures.

Conclusion

Information security topics are major issues and a vast amount of information is available both online and in print. These resources are just some of the places those needing information on the constantly changing topics in information security can go to for guidance.