REFERENCES on COMPUTER

and INFORMATION SYSTEMS SECURITY,

and on CRYPTOGRAPHY

Compiled and Annotated
by
Charles Abzug, Ph.D.

ABRAMS, MARSHALL D.; JAJODIA, SUHIL; & PODELL, HAROLD J. (EDITORS; 1995). *Information Security: An Integrated Collection of Essays.* Los Alamitos, CA: IEEE Computer Society Press. QA76.9.A25I5415 1995; 005.8--dc20; 94-20899; ISBN 0-8186-3662-9. IEEE Computer Society Press Order Number 3662-01; IEEE Catalog Number EH0397-0.

AMOROSO, EDWARD G. (1994). *Fundamentals of Computer Security Technology.* Englewood Cliffs, NJ: PTR Prentice-Hall. QA76.9.A25A46 1994; 005.8--dc20; 93-43586; ISBN 0-13-108929-3. $57.00

BARR, THOMAS H. (2002). *Invidation to Cryptology.* Upper Saddle River, NJ: Prentice Hall. Z103.B34 2002; 652.'8--dc21; 2001036589; ISBN 0-13-088976-8.

BAUER, FRIEDRICH L. (1997). *Decrypted Secrets: Methods and Maxims of Cryptology.* New York, NY: Springer-Verlag. QA76.9.A25B38513 1997; 96-037583; ISBN 3-540-60418-9. $39.95

BEKER, HENRY; & PIPER, FRED (1982). *Cipher Systems: The Protection of Communications.* New York, NY: John Wiley & Sons. QA76.9.A25B39 1982; ISBN 0-471-89192-4. $79.00

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

BEUTELSPACHER, ALBRECHT (1994). *Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without any Arcane Skullduggery, but not Without Cunning Waggery, for the Delectation and Instruction of the General Public.* (Transformation from German into English Succored and Abetted by J. Chris Fisher. Washington, DC: Mathematical Association of America. QA76.9.A25B49 1994; ISBN 0-88385-504-6. $34.00

Beutelspacher provides a delightfully written and very readable summary of the principles of cryptology in a manner that is less mathematically challenging than most other books on the subject. While there are some students in the class who have a sufficiently deep mathematical background to be able to tolerate a more detailed description than is provided in Beutelspacher, it is expected that the great majority will find the level of this book appropriate. Anyone preferring a more heavily mathematical treatment of the subject is urged to pursue any of a number of superb texts, such as Douglas Stinson's *Cryptography: Theory and Practice*, or Friedrich Bauer's *Decrypted Secrets.* Some older books, such as Beker and Piper's *Cipher Systems,* and Dorothy Denning's *Cryptography and Data Security,* are also very good, but might not cover some of the very interesting modern developments such as double-key cryptography and digital cash.. A detailed historical account of the field can be found in any of several books published by David Kahn, of which *The Code-Breakers* is probably the best and most comprehensive example. A slightly annotated bibliography of cryptologic and other technical INFOSEC references is available for your inspection and reading pleasure (see below).

BISHOP, DAVID (2003). *Introduction to Cryptography with Java Applets.* Sudbury, MA: Jones and Bartlett Publishers. QA76.9.A25 B565 2003; 005.8—dc21; 2002034167; ISBN 0-7637-2207-3.

BRASSARD, GILLES (1988). *Modern Cryptology. A Tutorial.* New York: Springer-Verlag, *Lecture Notes in Computer Science,* G. Goos & J. Hartmanis, eds. Z103.B72 1988. ISBN 0-387-96842-3.

BRAUN, CHRISTOPH (1995). *UNIX System Security Essentials.* Reading, MA: Addison-Wesley Publishing Company. QA76.76.D63B735 1995; 94-031241; ISBN 0-201-74775-3. $21.95

BRUCE, GLEN; & DEMPSEY, ROB (1997). *Security in Distributed Computing: Did You Lock the Door?* Upper Saddle River, NJ: Prentice-Hall PTR. QA76.9.A25D454 1997; 005.8--dc20; 96-33404; ISBN 0-13-189208-4.

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

BRUNNER, JOHN (1975). *The Shockwave Rider.* New York, NY: Ballantine Books. PR6052.R855 74-23861; ISBN 0-345-24853-8-150.

CASTANO, SILVANA; FUGINI, MARIAGRAZIA; MARTELLA, GIANCARLO; & SAMARATI, PIERANGELA (1995). *Database Security.* Reading, MA: Addison-Wesley Publishing Company. QA76.9.D314S55 1994; 005.8—dc20; 94-26279; ISBN 0-201-59375-0.

CHAPMAN, D. BRENT; & ZWICKY, ELIZABETH D. (1995). *Building Internet Firewalls.* Sebastopol, CA: O"Reilly & Associates.

CHESWICK, WILLIAM R.; & BELLOVIN, STEVEN M. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Reading, MA: Addison-Wesley Publishing Company. TK5105.875.I57C44 1994; 005.8--dc20; 94-10747; ISBN 0-201-63357-4. $23.16

COHEN, FREDERICK B. (1995). *Protection and Security on the Information Superhighway.* New York: John Wiley & Sons, Inc. QA76.9.A25C59 1995; 005.8--dc20; 94-40488; ISBN 0-471-11389-1.

CURRY, DAVID A. (1992). *UNIX System Security: A Guide for Users and System Administrators.* Reading, MA: Addison-Wesley Publishing Company, Inc. QA76.9.A25C87 1992; 005.4'3--dc20; 91-43652; ISBN 0-201-56327-4 (hardcover).

DAVIES, D.W., & PRICE, W.L. (1984). *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer.* New York: John Wiley & Sons. TK5105.D43 1989;

DEAVOURS, CIPHER A.; MELLON, GREG; & KAHN, DAVID A., editors (1998). *Selections from Cryptologia: History, People, and Technology.* Artech House Telecommunications Library. ISBN 0890068623. $83.00

DENNING, DOROTHY E. (1983). *Cryptography and Data Security.* Reading, MA: Addison-Wesley Publishing Company. QA76.9.A25D46 1982; 001.64'028'9; 81-15012; ISBN 0-201-10150-5.

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

DENNING, PETER J., EDITOR (1990). *Computers Under Attack. Intruders, Worms, and Viruses.* New York: ACM Press; and, Reading, MA: Addison-Wesley Publishing Company. QA76.9.A25C667 1990; 006.8--dc20; 89-18537; ISBN 0-201-53067-8. $20.76

DEMPSEY ET AL. *Security in Distributed Computing.* Upper Saddle River, NJ: Prentice Hall.

ELECTRONIC FRONTIER FOUNDATION, JOHN GILMORE, editor (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design.* O'Reilly & Associates. ISBN 1565925203. $23.96

FIERY, DENNIS (1994). *Secrets of a Super Hacker, by The Knightmare.* Port Townsend, WA: Loompanics Unlimited. QA76.9.A25K62 1994; ISBN 1-55950-106-5.

FITES, PHILIP; JOHNSTON, PETER; & KRATZ, MARTIN (1992). *The Computer Virus Crisis. Second edition.* New York, NY: Van Nostrand Reinhold. QA76.76.C68F57 1992; 005.8--dc20; 91-21163; ISBN 0-442-00649-7.

FITES, PHILIP; & KRATZ, MARTIN P.J. (1993). *Information Systems Security. A Practitioner's Reference.* , New York, NY: Van Nostrand Reinhold. QA76.9.A25F536 1993; 005.8--dc20; 93-15895; ISBN 0-442-00180-0.

FORD, WARWICK (1994). *Computer Communications Security.* Upper Saddle River, NY: Prentice Hall. QA76.9.A25F65 1994; 005.8—dc20; 93-11666; ISBN 0-13-799453-2.

FORD, WARWICK; & BAUM, MICHAEL S. (1997). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Upper Saddle River, NJ: Prentice-Hall PTR. QA76.9.A25F66 1997; 658.8'4—dc21; 96-7695; ISBN 0-13-476342-4.

GARFINKEL, SIMSON; & SPAFFORD, GENE (1991). *Practical UNIX Security.* Sebastopol, CA: O'Reilly & Associates. QA76.9.A25G37 1991; ISBN 0-937175-72-2.

GARDNER, MARTIN (1984). *Codes, Ciphers and Secret Writing.* Dover Publications. ISBN 0486247619. $3.16

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

GARRETT, PAUL (2001). *Making, Breaking Codes: An Introduction to Cryptology.* Upper Saddle River, NJ: Prentice Hall. QA268.G37 2001; 652'.—dc21; 00-042742 ISBN 0-13-030369-0.

GASSER, MORRIE (1988). *Building a Secure Computer System.* New York, NY: Van Nostrand Reinhold. QA76.9.A25G37 1988; 005.8; 87-27838; ISBN 0-442-23022-2.

HAFNER, KATIE; & MARKOFF, JOHN (1991). *Cyberpunk. Outlaws and Hackers on the Computer Frontier.* New York: Simon & Schuster. QA76.9.A25H34 1991; 364.1'68--dc20; 91-11598; ISBN 0-671-68322-5; ISBN 0-671-77879-X (pbk); ISBN 0-684-818620.

HARNOIS, ALBERT J. (1991). *EDP Auditing: A Functional Approach.* Englewood Cliffs, NJ: Prentice-Hall, Inc. HF5667.12.H37 1991; 657.45'0285--dc20; 90-26781; ISBN 0-13-224684-8.

ICOVE, DAVID, SEGER, KARL, & VONSTORCH, WILLIAM (1995). *Computer Crime: A Crimefighter's Handbook.* O'Reilly & Associates, Inc. ISBN: 1-56592-086-4.

COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK was derived from an FBI training manual on the prevention and investigation of computer crimes. It delivers a wide-ranging, non-technical overview of computer system vulnerabilities, threat assessment, and the law. Covering the gamut from unlawful intrusion to poisoning of computer operations staff, this book provides an excellent introduction to threat assessment and security procedures for protecting an organization from computer crime. Unlike most computer security books aimed at system administrators, this one is written from the perspective of law enforcement, and describes what to do before, during, and after a computer crime is discovered. The book is divided into five parts. The first part of the book describes vulnerabilities, threats, and countermeasures, with equal emphasis given to the human components of a system as well as technical issues. The section on Social Engineering is well illustrated, if a bit too short, and some of the more obscure possibilities for covert channels and compromising emanations are well covered. The discussion suffers from a lack of references to documented attacks (see below), and a somewhat confusing explanation of the differences between Trojan Horses, viruses, worms, and logic bombs. Chapter 5, on risk assessment, nonetheless is excellent. Physical, personnel, and communications security are covered in the remainder of Part II. One exposure that I thought was not mentioned highly enough is the vulnerability of backup media to theft. "Dumpster diving" is discussed in some detail (together with a humorous and totally unnecessary diagram). I would have liked to see references given for many of the examples of computer crimes scattered throughout the book. Some of the descriptions edge toward hyperbole; more complete references would allow the reader to pursue further information if needed. Two of the appendices, written by John Gales Sauls and Michael G. Noblett, are liberally referenced. Part III of the book is the most unusual. It is essentially a checklist for the professional investigator who needs to collect and preserve evidence of a computer crime. Much detail is presented on the identification and preservation of anything even remotely related to a criminal investigation (within the bounds of the required search warrant, of course). Appendix D contains the full text of an actual search warrant used in an investigation in 1994, which makes for fascinating reading. It is interesting to compare these chapters with the Foreword, in which

Chris Goggans describes a search of his home by the U.S. Secret Service in 1990. Part IV contains the text of laws covering computer and communications security in the United States at the level of Federal and State courts. The text of a proposed computer crime law from Ghana is also included, for completeness. Appendices list books, organizations, electronic resources and governmental agencies responsible for computer security. These appendices are not nearly as detailed as those provided in COMPUTER SECURITY BASICS, by Deborah Russell and G.T. Gangemi, Sr. (ISBN: 0-937175-71-4), another book published by O$Reilly & Associates. Together, the two books complement one another perfectly.

- - - Review written by Joe Loughry, Distributed Systems Department, First Interstate Bank, on: Mon, 28 Aug 95

JACOBSON, ROBERT V. (1990). *The PC Virus Control Handbook. A Technical Guide to Detection, Identification, Disinfection, and Investigation. Includes Model Policy and Procedures.* San Francisco: Miller Freeman Publications. ISBN 0-87930-194-5.

KAHN, DAVID (1967). *The Codebreakers: The Story of Secret Writing.* New York, NY: MacMillan Publishing Company. Z103.K28 1967; 63-16109; ISBN 0-02-560460-0.

KANE, PAMELA (1994). *PC Security and Virus Protection: The Ongoing War Against Information Sabotage.* New York, NY: Henry Holt & Company, Inc. QA76.9.A25K34 1994; 005.8--dc20; 94-14134; ISBN 1-55851-390-6 $39.95

KAUFMAN, CHARLIE; PERLMAN, RADIA; & SPECINER, MIKE (1995). *Network Security: Private Communications in a Public World.* Englewood Cliffs, NJ: PTR Prentice-Hall. QA76.9.A25K38 1995; ISBN 0-13-061466-1. $48.00

Excellent coverage of the application of cryptography within various network communications protocols.

KIPPENHAHN, RUDOLF; translated by OSERS, EWALD (1999). *Code Breaking: A History and Exploration.* Overlook Press. ISBN 0879519193. $20.97

KONHEIM, A.G. (1981). *Cryptography: A Primer.* New York: John Wiley & Sons. Z103.K66; $115.00

KYAS, OTHMAR (1997). *Internet Security: Risk Analysis, Strategies and Firewalls.* Boston, MA: International Thomson Computer Press. ISBN 1-85032-302-X. $34.95

Originally written 13 Feb 2002, last revised 06 Sep 2004

LOBEL, JEROME (1986). *Foiling the System Breakers. Computer Security and Access Control.* New York: McGraw-Hill Book Company. QA76.9.A25L6 1986; 005.8; 85-24161; ISBN 0-07-038357-X.

MARKS, LEO (1999). *Between Silk and Cyanide: A Codemaker's War 1941-1945.* Free Press. ISBN: 0684864223. $19.25

MAYO, JONATHAN L. (1990). *Computer Viruses. What They Are, How They Work, and How to Avoid Them.* Windcrest Books (McGraw-Hill). QA76.76.C68M33 1989; 005.8--dc20; 89-33481; ISBN 0-8306-9582-6 (hardcover), 0-8306-3382-0 (pbk).

MENEZES, ALFRED J; VAN OORSCHOT, PAUL C; & VANSTONE, SCOTT A. (1997). *Handbook of Applied Cryptography.* Boca Raton, FL: CRC Press. QA76.9.A25M463 1996; 0005.8'2—dc21; 96-27609; ISBN 0-8493-8523-7.

NATIONAL RESEARCH COUNCIL (1991). *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press. QA76.9.A25C6663 1990; 005.8--dc20; 90-22329; ISBN 0-309-04388-3.

NATIONAL SECURITY AGENCY (1996). *Information Systems Security Products and Services Catalog.* Available from: ***National Security Agency, ATTN: V211 (Business Relations Office), 9800 Savage Road, Fort George G. Meade, MD 20755-6000 (Telephone 800-688-6115).*** For sale by: ***Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402 (Telephone 202-512-1800).***

NICHOLS, RANDALL K. (1999). *ICSA Guide to Cryptography.* New York, NY: McGraw-Hill. QA76.9.A25N53 1999; 98-36563; 005.8--dc21; ISBN 0-07-913759-8.

NEWTON, DAVID E. (1997). *Encyclopedia of Cryptology.* Abc-Clio. ISBN 0874367727. $65.00

O'SHEA, G. (1991). *Security in Computer Operating Systems.* Manchester and Oxford, England: NCC Blackwell Limited. QA76.9.A25O84 1991; 005.8; ISBN 0-85012-812-9.

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

PIPKIN, DONALD L. (1997). *Halting the Hacker: A Practical Guide to Computer Security.* Upper Saddle River, NJ: Prentice-Hall, Inc. QA76.9.A25P56 1997; 005.8--dc21; 96-46381; ISBN 0-13-243718-X (alk. paper).

PFLEEGER, CHARLES (1989). *Security in Computing.* Upper Saddle River, NJ: Prentice Hall. QA76.9.A25P45 1989; 005.8--dc19; 88-12411; ISBN 0-13-798943-1.

PFLEEGER, CHARLES (1996). *Security in Computing. Second edition.* Upper Saddle River, NJ: Prentice Hall PTR. QA76.9.A25P45 1996; 005.8--dc20; 96-32910; ISBN 0-13-337486-6.

PURSER, MICHAEL (1993). *Secure Data Networking.* Norwood, MA: Artech House, Inc. TK5105.5.P87 1993; 005.8--dc20; 93-7161; ISBN 0-89006-692-2.

RUSSELL, DEBORAH; & GANGEMI, G.T., SR. (1991). Computer Security Basics. Sebastopol, CA: O'Reilly & Associates. QA76.9.A25R8 1991; ISBN 0-937175-71-4.

SCHNEIER, BRUCE (1994). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York, NY: John Wiley & Sons. QA76.9.A25S35 1993; 005.8'2--dc20; 93-2139; ISBN 0-471-59756-2.

SCHNEIER, BRUCE (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second edition.* New York, NY: John Wiley & Sons. QA76.9.A25S35 1996; 005.8'2--dc20; 95-12398; ISBN 0-471-11709-9.

Schneier provides a thorough, comprehensive coverage of the entire field. In the 1996 edition, quite a few errors from the earlier edition are corrected.

SCHWARTAU, WINN (1994). *Information Warfare. Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press. QA76.9.A25S354 1994; 302.2--dc20; 94-2412; ISBN

SHIMOMURA, T.; WITH MARKOFF, J. (1996). *Takedown.* New York, NY: Hyperion Press.

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

SIMONDS, FRED (1996). *Network Security: Data and Voice Communications.* New York: McGraw-Hill. QA76.9.A25.S35 1996; 005.8--dc20; 95-30723; ISBN 0-07-057639-4 (HC); ISBN 0-07-057634-3 (PBK).

SINGH, SIMON (1999). *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography.* Doubleday. ISBN 03859495315. $17.47

SMITH, RICHARD E. (1997). *Internet Cryptography.* Boston, MA: Addison-Wesley. TK5102.94.S65 1997; 005.8'2—dc21; 97-13773 ISBN 0-201-92480-3.

SMITH, MARTIN (1993). *Commonsense Computer Security. Your Practical Guide to Information Protection. Second edition.* New York: McGraw-Hill Book Company. QA76.9.A25S64 1993; 658.4'78--dc20; 93-9060; ISBN 0-07-707805-5.

STALLINGS, WILLIAM (1995). *Protect Your Privacy: A Guide for PGP Users.* TK5102.85.S73 1995; 005.8'2--dc20; 94-41526; ISBN 0-13-185596-4.

STALLINGS, WILLIAM (1998). *Cryptography and Network Security. Principles and Practice.* Upper Saddle River, NJ: Prentice-Hall. TK5105.59.S713; 005.8—dc21; 98-15676; ISBN 0-13-86907-0.

STALLINGS, WILLIAM (2003). *Cryptography and Network Security. Principles and Practice. Third Edition.* Upper Saddle River, NJ: Prentice-Hall. TK5105.59.S713; 005.8—dc21; 98-15676; ISBN 0-13-091429-0.

STERLING, BRUCE (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York, NY: Bantam Books. HV6773.2.S74 1992; 364.1'68--dc20; 92-17496; ISBN 0-553-08058-X.

STINSON, DOUGLAS R. (1995). *Cryptography: Theory and Practice.* Boca Raton, FL: CRC Press. QA268.S75 1995; ISBN 0849385210. $49.95

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

STOLL, CLIFFORD (1989). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. First edition.* New York, NY: Doubleday. UB271.R92H477 1989; 364.1'68'0973--dc20; 89-7808; ISBN 0-385-24946-2.

TRAPPE, WADE; & WASHINGTON, LAWRENCE C. (2002). *Introduction to Cryptography with Coding Theory.* Upper Saddle River, NJ: Prentice Hall. QA268.T73 2001; 005.8'2--dc21; 2001036652 ISBN 0-13-061814-4.

VAN DER LUBBE, JAN C.A. (1998). *Basic Methods of Cryptography.* Cambridge, England: Cambridge University Press. ISBN: 0521555590. $30.95

War Games. Movie about a teenager who played havoc with a NORAD computer.

WHITE, GREGORY B., FISCH, ERIC A., & POOCH, UDI W. (1996). *Computer System and Network Security.* Boca Raton, FL, and New York, NY: CRC Press. QA76.9.A25W45 1995; 005.8--dc20; 95-4905; ISBN 0-8493-7179-1.

WRIXON, FRED B. (1998). *Codes, Ciphers and Other Cryptic and Clandestine Communication: 400 Ways to Send Secret Messages from Hieroglyphs to the Internet.* Black Dog & Leventhal Pub. ISBN 1579120407. $17.98

ZIMMERMANN, PHILIP (1995). *The Official PGP User's Guide.* Cambridge, MA: MIT Press, ISBN 0-262-74017-6. $14.95.

World-Wide Web Sites

www.drsolomon.com
www.drsolomon.com/virus/enc/end.htm
www.geocities.com/SiliconValley/9433
www.cyber.com/papers/
www.datafellows.com/v-descs/
www.datarescue.com/avpbase/

Originally written 13 Feb 2002, last revised 06 Sep 2004

References on INFOSEC and Crypto

www.metro.ch/avpve/
www.symantec.com.avcenter.vinfodb.html

FTP Sites

ftp.gate.net/pub/users/ris1/acvfaq/zipcomp.virus
cs.ucr.edu/pub/virus-l/vlfaq200.zip
ftp.gate.net/pub/users/ris1/word.faq
usit.net/pub/lesjones/good-times-virus-hoax-faq.txt

Newsgroups

comp.security.firewalls
comp.virus
alt.comp.virus
various 2600 or hacker newsgroups
NOTE: Check out for Frequently-Asked Questions (FAQ) first; newsgroup members are annoyed at getting the same questions over and over again.

Please mail your suggestions for additions or changes to this list to: Abzugcx@JMU.edu

Originally written 13 Feb 2002, last revised 06 Sep 2004