References

[Adfa 1995] Australian Defense Force Academy. Operating System Lab Notes, URL: http://www.cs.adfa.oz.au/teaching/studinfo/csa2/OSLabNotes/node11.html

[Amoroso 1999] Amoroso, E.G., *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response*, Intrusion.net, 1999

[Anderson 1972] Anderson, J.P., et al., "Computer Security Technology Planning Study," Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC), ESD-TR-73-51 Vol. 1, 1972

[Anderson 1980] Anderson, J.P., "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Fort Washington, PA, April 1980.

[Bace 2000] Bace, R.G., *Intrusion Detection*, Macmillan Technical Publishing, 2000.

[Bace 2001] Bace, R. and P. Mell, "NIST Special Publication on Intrusion Detection Systems," National Institute of Standards and Technology, draft document, February 2001.

[Bell Labs 2002] Bell Labs, URL: http://www.bell-labs.com/history/unix/tutorial.html

[Bevier 1989] Bevier,W.R., "Kit: A Study in Operating System Verification," *IEEE Transactions on Software Engineering,* Vol. 15, No. 11, November,1989.Vo l. 15, No. 11, November,1989.

[Bellovin 1991] Bellovin S. and Merritt, M., Limitations of the Kerberos Authentication System, Proceedings of the USENIX Winter 1991.

[Brand 1990] Brand R., Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery. CERT 0.6, June 1990.

[Bruneau 2001] Bruneau, G., "The History and Evolution of Intrusion Detection", October 13, 2001, URL: http://rr.sans.org/intrusion/evolution.php

[CC 1998] *Common Criteria for Information Technology Security Evaluation,* version 2.0, CCIB-98-026, Common Criteria Implementation Board, May 1998.

[CC 1999] *Common Criteria for Information Technology Security Evaluation,* version 2.1, Common Criteria Implementation Board, December 1999.

[CER 1992] Computer Emergency Response Team, Internet Security for Unix System Administrators, Presented at AARNet Networkshop, December 1992.

Cisco Systems 2000] Networkers 2000, Intrusion Detection and Prevention Product Jpdate Session 2505, URL: http://www.cisco.com/networkers/nw00/pres/2505.pdf

Caelli 1991] Caelli W., Longley D., and Shain M., Information Security Handbook, Stockton Press, 1991.

COV 1990] Minutes of the First Workshop on Covert Channel Analysis. IEEE Cipher. ,os Angeles. CA, July 1990.

CSSC 1993] *The Canadian Trusted Computer Products Evaluation Criteria,* Version .0e, Canadian System Security Centre, January 1993.

Curry 1990] Curry D., Improving the Security of your Unix System, ITSTD-721-FR-90-21, SRI International, April 1990.

Dean 1996] Dean, D., E.W. Felten and D.S. Wallach, "Java Security: From HotJava to Netscape and Beyond," *Proceedings of the IEEE Symposium on Security and Privacy.* Oakland, CA, May 1996.

Denning 1976] Denning, D.E., "A Lattice Model of Secure Information Flow." *Communications of the ACM,* Vol. 19. No. 5, pp. 236243, May 1976.

[Denning 1982] Denning, D.E., *Cryptography and Data Security,* Addison Wesley, Reading, Massachusetts, 1982.

[Denning 1987] Denning, D.E., "An Intrusion Detection Model," *IEEE Transactions on SoftwareEngineering,* Vol. 13, No. 2, February 1987.

[De Paoli 1998] De Paoli, F., A. dos Santos and R.A. Kemmerer, "Web Browsers and Security," in Mobile Agents and Security, G. Vigna, Ed., *Lecture Notes in Computer Science*, Vol. 1419, pp. 235-256, Springer-Verlag, June 1998.

[DoD 1983] *Department of Defense Trusted Computer System Evaluation Criteria,* Computer Security Center Standard, CSC-STD-001-83, 1983, in December 1983 released as a DoD standard, DOD 5200.28-STD.

[DTI 1989] DTI Commercial Computer Security Centre, "Overview of Documentation," Vol. 1, version 3.0, February 1989.

[Ellison 1992] Ellison C., RESULTS: challenge login devices, Usenet newsgroup sci.crypt, 6 October 1992.

[Enterasys Networks 2000] "Dragon Intrusion Detection Solutions", URL: http://www.enterasys.com/ids/

armer 1990] Farmer, D. and E.H. Spafford, "The COPS Security Checker System," *roceedings of the Summer 1990 Usenix Conference,* Anaheim, CA, June 1990.
C 1992] *Federal Criteria for Information Technology Security*, Draft, Vol. 1, National stitute of Standards and Technology and the National Security Agency, December 992.

IP 1977] Federal Information Processing Standards Publication 46, Data Encryption tandard, National Bureau of Standards, U.S. Department of Commerce, January 1977.

orrest 1996] Forrest, S., S.A. Hofmeyr, A. Somayaji, and T.A. Longstaff, "A Sense of elf for Unix Processes," *Proceedings 1986 Symposium on Security and Privacy,* akland, CA, IEEE, New York. pp. 120-128. May 1996.

raim 1983] Fraim, L., "Scomp: A Solution to the Multilevel Security Problem, *omputer,* Vol. 16, No. 7, pp. 26-34, July 1983.

Goguen 1982] Goguen, J. and J. Meseguer,"Security Policies and Security Models," *roceedings 1982 Symposium on Security and Privacy,*Oakland, CA, IEEE, NewYork, p. 1120, April 1982.

Gold 1979] Gold, B.D., R.R. Linde, R.J. Peeler, M. Schaefer, J.F. Scheid, and P.D. Vard, "A Security Retrofit of VM/370," *Proceedings of the National Computer onference,* Vol. 48, AFIPS Press Montvale, N.J., 1979.

Guttag 1978] Guttag, J., E. Horowitz, and D. Musser, "Abstract Data Types and oftware Validation," *Communications of the ACM*, Vol. 21, No. 12, pp. 10481064, ecember 1978.

Hebbard 1980] Hebbard, B., et. al., "A Penetration Analysis of the Michigan Terminal ystem," *ACM Operating Systems Review*, Vol. 14, No. 1, January 1980.

Haigh 1987] Haigh, J.T., R.A. Kemmerer,J.McHugh, and W.D. Young, "An Experience Jsing Two Covert Channel Analysis Techniques on a Real System Design," *IEEE ransactions on Software Engineering*,Vol. SE13, No. 2, February 1987.

Hoare 1972] Hoare, C.A.R., "Proof of Correctness of Data Representations," *Acta nformatica*, Vol. 1, pp. 271-281, 1972.

Hu 1991] Hu, W.M., "Reducing Timing Channels with Fuzzy Time," *Proceedings of he 1991 Symposium on Research inSecurity and Privacy,Oakland*, California, May 1991.

IDA 1987] Institute for Defense Analysis memorandum reports, M-379 through M-384, DA, Alexandria, VA, October 1987.

Ilgun 1995] Ilgun, K., R.A. Kemmerer and P.A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection System," *IEEE Transactions on Software*

Engineering, Vol. 21, No. 3, March 1995.

Innella 2001] Inella, P., "The Evolution of Intrusion Detection Systems", November 16, 2001, URL: http://online.securityfocus.com/infocus/1514

ITS 1990] *Information Technology Security Evaluation Criteria (ITSEC)*, Netherlands National Comsec Agency, Hague, The Netherlands, May 1990.

Javitz 1994] Javitz, H.S. and A. Valdes, "The NIDES Statistical Component Description and Justification," Technical Report, SRI International, Menlo Park, CA, March 1994.

Karn 1993] Karn P., Haller N., and Walden J., S/Key One Time Password System, anonymous ftp from thumper.bellcore.com, July 1993.

Karger 1991] Karger, P.A. and J.C. Wray, "Storage Channels in Disk Arm Optimization," *Proceedings of the 1991 Symposium on Research inSecurity and Privacy*, Oakland, California, May 1991

Kohl 1990] Kohl J., Neuman B., and Steiner J., The Kerberos Network Authentication Service, MIT Project Athena, Version 5 Draft 3, October 1990.

Kemmerer 1983] Kemmerer, R.A., "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels." *ACM Transactions on Computer Systems*, Vol. 1, No. 3, August 1983.

Kemmerer 1990] Kemmerer, R.A., "Integrating Formal Methods into the Development Process," *IEEE Software*, pp. 3750, September,1990.

Kemmerer 1994] Kemmerer, Richard A. "Computer Security," 1153-1164. *Encyclopedia of Software Engineering.* New York, NY: John Wiley and Sons, 1994.

Karn 1993] Karn P., Haller N., and Walden J., S/Key One Time Password System, anonymous ftp from thumper.bellcore.com, July 1993.

Kim 1992] Kim G. and Spafford E., README file from Tripwire system, anonymous ftp from cert.org, November 1992.

Lampson 1973] Lampson, B.W., "A Note on the Confinement Problem," *Communications of the ACM,* Vol. 16, pp. 613-615, October 1973.

Linde 1975] Linde, R.R., "Operating System Penetration," *Proceedings of National Computer Conference,* Vol 44, AFIPS Press, Montvale, N.J., 1975.

Lindqvist 1999] Lindqvist, U., and P.A. Porras, "Detecting Computer and Network Misuse with the Production-Based Expert System Toolset (P-BEST)," *Proceedings of the IEEE Symposium on Security and Privacy,* Oakland, CA., May 1999.

[Lunt 1988] Lunt, T.F., "Automated Audit Trail Analysis and Intrusion Detection: A Survey," *Proceedings of the llth National Computer Security Conference,* Baltimore, MD, Oct. 1988.

[Lampson 1973] Lampson, B.W., "A Note on the Confinement Problem," *Communications of the ACM,* Vol. 16, pp. 613615, October 1973

[Linde 1975] Linde, R.R., "Operating System Penetration," *Proceedings of National Computer Conference*, Vol. 44, AFIPS Press, Montvale, N.J., 1975.

[Lippmann 1999] Richard P. Lippmann; Evaluating Intrusion Detection Systems: The 1998 DARPA Off- line Intrusion Detection Evaluation. Proceedings of DARPA Information Survivability Conference & Exposition (DISCEX), Hilton Head, South Carolina, 25-27 January 2000. Los Alamitos, CA: IEEE Computer Society, 1999: Vol. 2, 12-26.

[Lippmann 2000] Richard P. Lippmann, David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman, Evaluating Intrusion Detection Systems: the 1998 DARPA Off-Line Intrusion Detection Evaluation, in Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX), Vol. 2, IEEE Press, January 2000.

[Lippmann 2000a] Lippmann, Richard et al. "The 1999 DARPA Off-line Intrusion Detection Evaluation", URL: http://www.ll.mit.edu/IST/ideval/pubs/2000/1999Eval-ComputerNetworks2000.pdf, 2000.

[Lipner 1975] Lipner, S.B., "A Comment on the Confinement Problem," *Proceedings of the Fifth Symposium on Operating Systems Principles*, The University of Texas.

[McAuliffe 1990] McAuliffe, N.J., L.J. Schaefer, D.M. Wolcott, T.K. Haley, N.L. Kelem and B.S. Hubbard, "Is Your Computer Being Misused? A Survey of Current Intrusion Detection System Technology," *Proceeding of the Sixth Computer Security Applications Conference,* Dec. 1990.

[McCauley 1979] McCauley, E. and P. Drognowski, "KSOS: The Design of a Secure Operating System," *Proceedings of the National Computer Conference,* AFIPS Press, June 1979.

[Millen 1976] Millen, J.K., "Security Kernel Validation in Practice," *Communications of the ACM,* Vol. 19, pp. 243-250, May 1976.

[MIS 2002] Management Information Systems, "Detecting an Intrusion", URL: http://www.eng.ufl.edu/home/mis/security/detection.html

[Morris 1979] Morris, R. and K. Thompson, "Password Security: A Case History," *Communications of the ACM*, Vol. 22, No. 11, November 1979.

[Mukherjee 1994] Mukherjee, B., L.T. Heberlein and K.N. Levitt, "Network Intrusion Detection," *IEEE Network*, pp. 26-41, May/June 1994.
[NCS 1987] National Computer Security Center, *Trusted Network Interpretation of the Trusted Systems Evaluation Criteria*, NCSC-TG-005, Version 1, July 1987.

[NRC 1989] National Research Council, *Growing Vulnerabilty of the Public Switched Networks: Implications for National Security Emergency Preparedness*, National Academy Press, Washington, DC, 1989.

[NRC 1991] National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, Washington, DC, 1991.

[NRC 1997] National Research Council, *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997.

[Neumann 1990] Neumann, P.G., "A Comparative Anatomy of Computer System/Network Anomaly Detection Systems," assembled by Peter G. Neumann, CSL, SRI BN-168, Menlo Park, CA, May 1990.

[Northcutt 2001] Northcutt, S., J. Novak, and D. McLachlan, *Network Intrusion Detection: an Analyst's Handbook*, New Riders, Indianapolis, IN, 2001.

[NSS 2000] NSS Group, "Intrusion Detection and Vulnerability Assessment," Group Test (Edition 1), an NSS Group Report, Oakwood House, Wennington, Cambridgeshire, PE28 2LX , UK, 2000.

[NSS 2001] NSS Group, Intrusion Detection Group Test (Edition 3), 2001. URL: http://www.nss.co.uk/

[Popek 1974] Popek, G.J., "Protection Structures," *Computer*, June 1974.

[Rivest 1992] Rivest R., The MD4 Message-Digest Algorithm, Network Working Group, Rivest 1992, April 1992.

[Rivest 1992a] Rivest R., The MD5 Message-Digest Algorithm, Network Working Group, Rivest 1992a, April 1992.

[Ross 2000] Ross, Seth. Unix System Security Tools. New York: McGraw-Hill. 2000.

[Saltzer 1975] Saltzer,J.H. and M.D. Schroeder,"The Protection of Information in Computer Systems," *Proceedings of the IEEE*, Vo l. 63,-No. 9, pp. 1278-1308, September 1975

[Schroeder 1977] Schroeder, M.D., D. Clark, J.H. Saltzer, "The MULTICS Kernel Design Project," *Proceedings of the 6th Symposium on Operating Systems Principles,"* 1977.
[Sekar 1999] Sekar, R. and P. Uppuluri, "Synthesizing Fast Intrusion Setection/Prevention Systems from High-Level Specifications," *Proceedings of the Usenix Security Symposium},* 1999

[Silverman 1983] Silverman, J.M., "Reflections on the Verification of the Security of an Operating System Kernel," *Communications of the ACM,* 1983.

[Smith 1993] Smith, D., "Enhancing Unix Security", 1993. URL: http://www.vtcif.telstra.com.au/pub/docs/security/sert-doc/unix-security.html

[Stevens 1990] Stevens W., Unix Network Programming, Prentice Hall, 1990.

[Sun 1991] Sun Microsystems, Inc., "Installing, Administering, and Using the Basic Security Module," 2550 Garcia Ave., Mountain View, CA 94043, December 1991.

[Tanenbaum 1989] Tanenbaum A., Computer Networks, Prentice-Hall International Inc.1989.

[Vaccaro 1989] Vaccaro, H.S. and G.E. Liepins, "Detection of Anomalous Computer Session Activity," *Proceeding of the IEEE Symposium on Research in Security and Privacy,* Oakland, CA, May 1989.

[Venema 1992] Venema W., BLURB file from TCP Wrapper system, anonymous ftp from cert.org, June 1992.

[Vigna 1999] Vigna, G. and R.A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection System," *Journal of Computer Security*, Vol. 7, No. 1, pp. 37-71, IOS Press, 1999

[Walker 1980] Walker, B.W., R.A. Kemmerer, and G.J. Popek, "Specification and Verification of the UCLA Unix Security Kernel," *Communications of the ACM,* Vol. 23, pp. 118-131, February 1980.

[Ware 1970] Ware, W.H., "Security Controls for Computer Systems," The Rand Corporation, classified document, February 1970, reissued as an unclassified document R-609-1, October 1979.