

Appendix A — References

1. 'ISO/IEC PDTR 15947, Information technology – Security techniques – IT intrusion detection framework', ISO/IEC JTC 1/SC 27 N2691.
2. The President's National Security telecommunications Advisory Committee, Network group Intrusion Detection, 'Subgroup Report on the NS/EP Implications of Intrusion Detection Research and Development', December 1997.
3. NATO AC/322 Infosec subcommittee (SC/4), AHWG/4 on the Interconnection of NATO networks documents and working papers, 2001.
4. 'Technical and Implementation Directive for the Interconnection of Communication and Information Systems (CIS)', INFOSEC.
5. Bellovin, Cheswick, 'Firewalls and Internet Security', Addison-Wesley, 1994.
6. Sasha, Beetle, 'A strict anomaly detection model for IDS', Phrack 56, source: www.phrack.com, 6-11-2000.
7. Rain Forest Puppy, 'A look at Whisker's anti-IDS techniques', 1999, source: www.wiretrip.net/rfp/, 6-11-2000.
8. Esmaili, M., R. Safavi-Naini and J. Pieprzyk, 'Intrusion detection: a survey'. In: S.J. Chung (ed.). Proceedings of the 12th International conference on Computer Communications 21-24 August 1995 in Seoul. Amsterdam, 1995, pp. 409-414.
9. Graf, 'The 1998 DARPA/AFRL Off-line Intrusion Detection Evaluation', 1998, source: http://www.raid-symposium.org/raid98/Prog_RAID98/Table_of_content.html, 6-11-2000.
10. McHugh, 'The 1998 DARPA Off-Line Intrusion Detection Evaluation', RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
11. Lippmann et al, 'Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation', RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
12. Source: www.gidos.org, 6-11-2000.
13. Paul Zavidniak, Logicon Inc.: 'Achieving Information Resiliency in the Defence Environment', Information and Security and Data Security Congress, February 2000.
14. Amoroso, 'Intrusion Detection: an introduction to Internet surveillance, correlation, traps, trace-back, and response', intrusion.net books, 1999.
15. Sommer, 'Intrusion Detection Systems as Evidence', 1998, source: http://www.raid-symposium.org/raid98/Prog_RAID98/Table_of_content.html, 6-11-2000.
16. Allen J. e.a., 'State of the Practice of Intrusion Detection Technologies', January 2000, Technical Rapport CMU/SEI-99-TR-028; ESC-99-028.
17. Paxson, Handley, 'Defending against NIDS evasion using traffic normalizers', RAID '99, Computer Networks, volume 34, number 4, 2000.
18. Source: <http://dev.whitehats.com/ids>, 6-11-2000.
19. Spafford, Zamboni, 'Intrusion Detection using Autonomous Agents', RAID '99, Computer Networks, volume 34, number 4, 2000.
20. Mell et al, 'A denial-of-service resistant intrusion detection architecture', RAID '99, Computer Networks, volume 34, number 4, 2000.
21. Source: <http://www.sdl.sri.com/emerald/project.html>, 6-11-2000.
22. Lippmann, Cunningham, 'Improving Intrusion Detection Performance using Keyword Selection and Neural Networks', RAID '99, Computer Networks, volume 34, number 4, 2000.
23. Michael, Ghosh, 'Using Finite Automata to Mine Execution Data for Intrusion Detection', RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
24. Ghosh, 'A Real-Time Intrusion Detection System Based on Learning Program Behaviour', RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
25. Farley, 'Visualisation of Intrusion Detection Data', source: <http://www.raid-symposium.org/raid2000/program.html>, 6-11-2000.
26. Toelle, Niggemann, 'Supporting Intrusion Detection by Graph Clustering and Graph Drawing', source: <http://www.raid-symposium.org/raid2000/program.html>, 6-11-2000.
27. Kim G.H., Spafford E.H., 'Experiences with Tripwire: Using Integrity Checkers for Intrusion Detection', source: www.cs.purdue.edu/coast/ids, 6-11-2000.
28. Crosbie, 'Applying genetic programming to intrusion detection', Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, November 1995.
29. Hochberg, J.; Jackson, K.; Stallings, C.; McClary, J.; DuBois, D.; Ford, J.: NADIR: An automated system for detecting network intrusions and misuse, in *Computers and Security* 12 (1993) 3, May, pp. 253-248.
30. Kantzavelou, I. and S.K. Katsikas, An attack detection system for secure computer systems - Outline for the solution. In L. Yngström and J. Carlsen (eds.), in *Information security in research and business: Proceedings of IFIP TC11 13th international conference on Information Security in Copenhagen, Denmark, 14-16 May 1997*. Chapman & Hall, London, etc., 1997, pp. 151-163.
31. Lee, W., and S.J. Stolfo, 'Data mining approaches for intrusion detection'. In: Proceedings of the 7th USENIX security symposium. San Antonio, 26-29 January 1998, pp. 79-93.

32. Bishop C.M., 'Neural networks for pattern recognition', Oxford University Press, 1995.
33. Bonifácio Jr., J.M., E.S. Moreira, A.M. Cansian and A.C.P.L.F. Carvalho, 'An adaptive intrusion detection system using neural networks', In: Proceedings of the IFIP SEC'98 conference Wien/Budapest. Chapman & Hall, August 1998.
34. Mounje, A. and B. Le Charlier, 'Continuous assessment of a UNIX configuration: integrating intrusion detection and configuration analysis'. In: Proceedings 1997 Symposium on Network and Distributed System Security San Diego, 10-11 February 1997, IEEE, Los Alamitos, pp. 27-35.
35. Kosoresow, A.P. and S.A. Hofmeyer, 'Intrusion detection via system call traces'. In: IEEE Software. IEEE, 1997, Vol. 14, no 5, pp. 35-42.
36. Sebring, M.M., E. Shellhouse, M.E. Hanna, R.E. Whitehurst, Expert Systems in Intrusion Detection, a Case Study, in Proceedings of the 11th National Computer Security Conference, Baltimore, 1990.
37. Kumar, S., 'Classification and detection of computer intrusions', PhD Thesis, Purdue University, 1995.
38. Porras, P.A., R.A. Kemmerer, Penetration State Transition Analysis - A Rule-based Intrusion Detection Approach, In 8th Annual Computer Security Applications Conference, 220-229, IEEE Computer Security Press, 1992.
39. Garvey, T.D, T.F. Lunt, Model based Intrusion Detection, in Proceedings of the 14th National Computer Security Conference, 372-185, 1991.
40. Ludovic M., 'GASSATA, a Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis', source: www.cs.purdue.edu/coast/ids, 6-11-2000.
41. Cannady J. , Mahaffey J. , 'The Application of Artificial Neural Networks to Misuse Detection: Initial Results', www.cs.purdue.edu/coast/ids.
42. Huang, X., Biondi, Ph., Linux Intrusion Detection system (LIDS), www.lids.org
43. IAP: Intrusion Alert Protocol, Gupta, Hewlett-Packard, IETF IDWG work-in-progress.
44. Hes, R. and Borking, J. (editors), 'Privacy Enhancing Technologies', 1998, A&V-11, NDPA, The Hague.