Intrusion detection: the art and the practice. Part I

Joseph S. Sherif
California Institute of Technology, Pasadena, California, USA
Rod Ayers
LAN International, Aliso Viejo, California, USA
Tommy G. Dearmond
California Institute of Technology, Pasadena, California, USA

Keywords
Computer crime,
Computer viruses,
Security products, Espionage,
System monitoring

Abstract
Organizations more often than not lack comprehensive security policies and are not adequately prepared to protect their systems against intrusions. This paper puts forward a review of state of the art and state of the applicability of intrusion detection systems and models. The paper also presents a classification of literature pertaining to intrusion detection.

Introduction

Too frequently today there are headlines about the latest hacker attack. They have broken into another system. They have stolen credit card lists. They have stolen military secrets. They have stolen trade secrets. The following books certainly make for interesting reading:

- *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (Stoll, 1990);
- *Takedown, The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It* (Shimomura, 1996);
- *The Hacker Crackdown* (Sterling, 1992); and
- *Masters of Deception: The Gang That Ruled Cyberspace* (Slatalla and Quittner, 1996);

They tell stories of extensive and sustained attacks against many computer systems. These were systems that in many circumstances were thought to be secure. And individuals who were determined and relentless in their pursuit carried out the attacks from "unsophisticated" computer installations like garages and apartments. Some did it just to prove it could be done, and because in some circles a successful attack was a recognized achievement of the first rank. Others carried out their attacks to create mischief, and to cause the greatest amount of havoc and damage.

Though one might think that with some 40 years (if, for the sake of discussion we posit 1960 as the "beginning" of the age") of modern computing, as we know it, surely the attacks must be isolated incidents. Surely, the technologies to defend computer systems should be commonplace. But such is simply not the case. In fact, it can be shown that the incidence of computer intrusion is growing, perhaps at an alarming rate.

Mahoney (2000) defines at least six types of computer attack:

1 *Worms* – self-replicating programs that spread across a network.
2 *Viruses* – programs that replicate when a user performs some action such as running a program.
3 *Server attacks* – a client exploits a bug in the server to cause it to perform some unintended action.
4 *Client attacks* – a server exploits a bug in a client to cause it to perform some unintended action.
5 *Network attacks (denial of service)* – a remote attacker exploits a bug in the network software or weakness in the protocol to cause a server, router or network to fail.
6 *Root attacks* – a user on a multi-user operating system obtains the privileges of another user (usually "root") by either obtaining the other user's password, or bypassing controls that restrict access.

Literature survey

Though the public awareness of the whole area of "intrusion detection" seems to have been more recent, it is certainly not a new area of inquiry. In fact, it has been an area of concern for most of what we know of "modern" computers. There have been a number of important milestones in the brief history of intrusion detection systems. The following list is consolidated from multiple sources:

Information Management & Computer Security
11/4 [2003] 175-186
© MCB UP Limited
[ISSN 0968-5227]
[DOI 10.1108/09685220310489544]

The Emerald Research Register for this journal is available at
http://www.emeraldinsight.com/researchregister
The current issue and full text archive of this journal is available at
http://www.emeraldinsight.com/0968-5227.htm

- *1960s*: The emergence of time-sharing systems demonstrated the need to control access to computer resources.
- *1970s*: The Department of Defense (DOD) Ware Report pointed out the need for computer security.
- *1970s* (mid to late): A number of systems were designed and implemented using security kernel architectures.
- *1980*: Anderson (1980) first proposed that audit trails should be used to monitor threats. The importance of such data had not been comprehended at that time and all the available system security procedures were focused on denying access to sensitive data from an unauthorized source.
- *1983*: The DoD trusted computer system evaluation criteria – the "orange book" – was published and provided a set of criteria for evaluating computer security control effectiveness
- *1987*: Denning (1987) presented an abstract model of an intrusion detection expert system (IDES). This paper was the first to propose the concept of intrusion detection as a solution to the problem of providing a sense of security in computer systems.
- *1988*: The Internet Worm program of 1988 – which infected thousands of machines and disrupted normal activities for several days – was detected primarily through manual means.

Lunt (1988) refined the intrusion detection model proposed by Denning (1987) and created the IDES prototype system. This system was designed to detect intrusion attempts with adaptation to gradual changes in behavior to minimize false alarms.

Smaha (1988) developed the Haystack system in order to assist Air Force security officers detect misuse of the mainframes used at Air Force bases.

Sebring *et al.* (1988) developed MIDAS (multics intrusion detection and alerting system) to monitor the National Computer Security Center Dockmaster system:

- *1989*: Wisdom and sense from the Los Alamos National Laboratory, and information security officer's assistant (ISOA) from Planning Research Corporation (Vaccaro and Liepins, 1989).
- *1990*: A new concept was introduced in 1990, with NSM (network security monitor, now called network intrusion detector or NID): instead of examining the audit trails of a host computer system, suspicious behavior was detected by passively monitoring the network traffic in a local area network (LAN) (Heberlein *et al.*, 1990).
- *1991*: A different idea was introduced with NADIR (network anomaly detection and intrusion reporter) and DIDS (distributed intrusion detection system): the audit data from multiple hosts were collected and aggregated in order to detect coordinated attacks against a set of hosts (Jackson *et al.*, 1991).
- *1994*: Crosbie and Spafford (1994-1995) suggested the use of autonomous agents in order to improve the scalability, maintainability, efficiency and fault tolerance of IDS. This idea fit well with the ongoing research on software agents in other areas of computer science.
- *1995*: An improved version of IDES was developed in 1995, called NIDES (next-generation intrusion detection expert system).
- *1996*: The design and implementation of GrIDS addressed the scalability deficiencies in most contemporary intrusion detection systems. This system facilitates the detection of large-scale automated or coordinated attacks, which may even span multiple administrative domains (Staniford-Chen *et al.*, 1996).
- *1998*: Anderson and Khattak (1998) offered an innovative approach to intrusion detection, by incorporating informational retrieval techniques into intrusion detection tools.
- *2002*: Wing (2002) advanced an automated technique for generating and analyzing attack graphs based on symbolic model checking algorithms. This technique is implemented in a tool suite.
- *2002*: Malladi *et al.* (2002) introduced new types of guessing attacks and developed procedures to analyze protocols subject to such attacks.

Table I gives bibliographic references on intrusion detection under various classifications for ease of use by the reader.

Conclusions

The threat and actuality of intrusion is real. More often than not, organizations are not prepared to protect themselves from intrusions. However, each organization should have a security policy and a strategy to combat intrusion efficiently and effectively. The strategy should include preparation, monitoring, detection, recovery and response. If this is implemented, organizations will be able to protect their systems, networks and their sensitive data.

Table I
Classification of intrusion detection (ID) literature under relevant areas

Intrusion detection relevant area	References
1. ***ID concepts, theory and methodology***	Axelsson (1999), Bace (2000), Dias *et al.* (1990), Dowell and Ramstedt (1990), Dunigan and Hinkel (1999), Enterasys (2001), Escamilla (1998), Eskin (2000), Forte (1999), Graham (1998), Gross (1997), Halme and Bauer (1995), Heady *et al.* (1990), Heberlein *et al.* (1990, 1991a,b), Helman *et al.* (1992), Hubbard *et al.* (1990), Ilgun (1992a, b) Ilgun *et al.* (1995), Jackson *et al.* (1991a, b), Kossakowski (1999), Kumar (1995), Lee (1999), Lee and Stolfo (1999), Lee *et al.* (1999a, b, c, 2000) Liepins and Vaccaro (1992), Lunt (1993a, b), Lunt *et al.* (1992, c), Mahoney (2000), Maiwald (1998), Mansfield *et al.* (1999), Marceau (2000), Mark (2000), McAuliffe *et al.* (1990), McConnell (1998), Mukherjee *et al.* (1994), Northcutt (1999a, b, 2000), Pichnarezyk *et al.* (1994), Puketza *et al.* (1996; 1997), Reavis (1999), Scambray *et al.* (1998), Snapp *et al.* (1991), Sundaram (1996), Ting *et al.* (1999), Wood (1999), Yip and Levitt (1998), Yuill *et al.* (1999), Zamboni and Spafford (1999), Zirkle (2000), Kim and Spafford (1997), Blain and Deswarte (1990), Debar *et al.* (2000), Puketza *et al.* (1996, 1997), Wing (2002)
2. ***Autonomous agents, expert systems***	
General	Crosbie (1995), Crosbie and Spafford (1995); Autonomous Agents (1995); Chan and Wei (2002)
AudES: audit expert systems	Tsudik and Summers (1990)
AID system	Sobirey *et al.* (1996)
Bro: real-time intrusion detection	Paxon (1998); Paxon and Handley (1999)
CIDF: common intrusion detection framework	Staniford-Chen *et al.* (1998)
COAST	Balasubramaniyan *et al.* (1998)
Clustering	Portnoy *et al.* (2001)
Data mining	Lee *et al.* (1997, 1998, 1999a, b, c, 2000, 2001)
Discovery	Tener (1986; 1988)
EMERALD: event monitoring enabling	Neumann and Parker (1989), Neumann and Porras (1999), Porras (1992), Porras and Kemmerer (1992), Porras and Neumann (1997)
ESSENSE	Valcarce *et al.* (1992)
GASSATA: genetic algorithm	Cedex (1993), Crosbie (1995), Me (1993, 1998)
GrIDS: graph-based intrusion detection system	Cheung and Levitt (1997), Cheung *et al.* (1999), Staniford-Chen *et al.* (1998)
Haystack	Smaha (1988), Smaha and Snapp (1996)
Hobids: host-based intrusion detection system	Hershkop *et al.* (2001), Lee *et al.* (1997), Lee and Xiang (2001), Mandanaris *et al.* (1999)
IDAMN: intrusion detection architecture for mobile networks	Samfat and Molva (1997), Didier and Molva (1997), Chan and Wei (2002)
IDES: intrusion detection expert system	Denning (1967), Denning and Neumann (1985), Denning *et al.* (1987)
MIDAS: Multics intrusion detection and alerting system	Sebring *et al.* (1988)
Machine learning	Frank (1994), Tener (1986, 1988), Weiss and Baur (1990), Lane and Brodley (1997a, b)
Markov chain	Ye (2000)
NIDX: network intrusion detection	Bauer and Koblentz (1998)
NADIR: network audit director and intrusion reporter	Hochberg *et al.* (1993)
NIDES: next generation	Anderson *et al.* (1995), Lunt (1988, 1989a, b, 1993a, b), Lunt and Jagannathan (1988), Lunt *et al.* (1992), Sebring *et al.* (1988)

(continued)

Table I

Intrusion detection relevant area	References
Neural networks	Debar et al. (2000), Ghosh and Schwartzbard (1999), Simonian (1990)
Nonparametric pattern recognition	Lankewics and Bernard (1991)
NSM: network security monitor	Heberlein *et al.* (1991a, b)
Petri nets	Frincke *et al.* (1998)
Phased approach expert system	Jackson *et al.* (1991a, b; 1994)
Pattern-based, peer-based, rank-based	Garvey and Lunt (1991), Ilgun (1992a, b), Mounji (1997), Porras (1992), Porras and Kemmerer (1992), Porras and Neumann (1997), Shieh and Gligor (1991), Sinclair *et al.* (1999), White *et al.* (1996)
RETISS: real-time security system using fuzzy logic	Carrettoni *et al.* (1991)
SAINT: Security analysis integration tool	Zamboni (1996), Zamboni and Spafford (1999)
SNORT	Roesch (1999)
SNMS: shadow network management system	Ong *et al.* (1999)
STAT: state transition analysis tool	Porras and Neumann (1997)
Statistical approach	Marchette (2001)
Visual model	Vert *et al.* (1998)
Wisdom and secure	Vaccaro and Liepins (1989)
3. *Audit, analysis, monitoring, surveillance*	Bishop (1989, 1995, 1999), Cedex (1993), Ko *et al.* (1994), Schneier (2000), Sibert (1988), Wee (1995), Wetmore (1993), Amoroso (1999), Anderson (1980), Apap *et al.* (2001), DeDios *et al.* (2001), Brentano (1991), Mell and McLarnon (1999), Habra *et al.* (1991, 1993), Helman *et al.* (1992), Lunt (1993a, b), Moitra (1992), Piccioto (1987), Teng (1990a, b), Wiler (2000)
4. *ID evaluation*	Lindquist and Jonsson (1997), Lippmann *et al.* (2000a, b), Lodin (1998), Lundin and Jonsson (1999), MIT (1999), Northcutt (1999a, b), Anderson *et al.* (1995), Anderson and Khattak (1998), Allen *et al.* (2000), Carnegie Mellon Software Engineering Institute (2000), Bace (1994, 2000)
5. *Anomaly detection*	Eskin (2000), Eskin *et al.* (2001a, b), Liepins and Vaccaro (1992), Seleznyov and Puuronen (1999), Teng *et al.* (1990a, b), Winkler (1990), Mahony (2000), Mahoney and Chan (2001), Vaccaro and Liepins (1989), Lee and Stolfo (1998, 1999), Lee *et al.* (1997, 1998, 1999a, b, c, 2000), Wiler (2002)
Misuse	Jackson *et al.* (1991a, b, 1994), Kumar (1995), Kumar and Spafford (1994, 1995), Neumann and Porras (1999), Smaha and Snapp (1996), Levitt (1992), Price (1997), Corbitt (1994)
System calls	Eskin *et al.* (2001a, b), Hofmeyer *et al.* (1998), Warrender *et al.* (1999)
Adaptive	Eskin *et al.* (2001a, b), Fan and Stolfo (2002), Fan *et al.* (2002), Feiertag *et al.* (1999), Halme and Bauer (1995), Halme and Kahn (1900)
Feature selection	Doak (1992)
Network-based	Denmac (1999), Wing (2002)
Host-based	Zirkle (2000)
Behavior-based	Herve (2000), Ye (2000)
Cooperative	Cheung and Levitt (1997), Cheung *et al.* (1999), SANS (2000)
Cost sensitive	Fan and Stolfo (2002), Fan *et al.* (2002), Lee (1999), Miller (1999), Panagiotis (1999), Stolfo *et al.* (2000)
6. *General references*	Amoroso (1999), Marchette (2001), Proctor (2000), Shimomura (1996), Sterling (1992), Stoll (1990), Toxen (2000), Bace (2000), Escamilla (1998), Northcutt (1999a, b), Schneier (2000), Spitzner (2001)

References

Allen, J., Christie, A., Fithin, W., McHugh, J., Pickel, J. and Stoner, E. (2000), "State of the practice of intrusion detection technologies", 99/TR-028, Carnegie Mellon University, Pittsburgh, PA.

Amoroso, E.G. (1999), "Intrusion detection: an introduction to Internet surveillance, correlation, trace back, traps and response", available at: Intrusion.net

Anderson, D., Frivold, T. and Valdes, A. (1995), "Next-generation intrusion setection expert system (NIDES)", technical report, SRI-CSL-95-07, International, Computer Science Lab., Menlo Park, CA.

Anderson, J.P. (1980), "Computer security threat monitoring and surveillance", technical report, Fort Washington, PA.

Anderson, R. and Khattak, A. (1998), "The use of information retrieval techniques for intrusion detection", *Proceedings of RAID*, Louvain-la-Neuve.

Apap, F., Honig, A., Hershkop, S., Eskin, E. and Stolfo, S. (2001), "Detecting malicious software by monitoring anomalous windows registry accesses", technical report, CUCS, Columbia University, New York, NY.

Autonomous Agents (1995), Technical report CSD-TR-95-022, Department of Computer Sciences, Purdue University, West Lafayette, IN.

Axelsson, S. (1999), "On a difficulty of intrusion detection", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Bace, R. (1994), "A new look at perpetrators of computer crime", *Proceedings of the 16th Department of Energy Computer Security Group Conference*, Denver, CO.

Bace, R. (2000), *Intrusion Detection*, Macmillan tecnical publication, Indianapolis, IN.

Balasubramaniyan, J.S., Garcia-Fernandez, J.O., Isacoff, D., Spafford, E.H. and Zamboni, D. (1998), "An architecture for intrusion detection using sutonomous sgents", COAST technical report 98/05, Purdue University, West Lafayette, IN.

Bauer, D. and Koblentz, M.E. (1998), "NIDX – an expert system for real-time network intrusion detection", *Proceedings of the IEEE Computer Networking Symposium*, New York, NY, pp. 98-106.

Bishop, M. (1989), "A model of security monitoring", *Proceedings of the 5th Annual Computer Security Applications Conference*, Tucson, AZ.

Bishop, M. (1995), "A standard audit log format", *Proceedings of the 1995 National Information Systems Security Conference*, Baltimore, MD.

Bishop, M. (1999), "Vulnerabilities analysis: extended abstract", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Blain, L. and Deswarte, Y. (1990), "An intrusion-tolerant security server for an open distributed system", *Proceedings of the European Symposium on Research in Computer Security*, Toulouse.

Brentano, J. (1991), "An expert system for detecting attacks on distributed computer systems", Master's thesis, Division of Computer Science, University of California, Davis, CA.

Carnegie Mellon Software Engineering Institute (2000), "State of the practice of intrusion detection technologies," technical report, CMU/SEI-99-TR-028, ECS-99-028.

Carrettoni, F., Castano, S., Martella, G. and Samarati, P. (1991), "RETISS: a real time security system for threat detection using fuzzy logic", *Proceedings of the 25th Annual IEEE International Carnahan Conference on Security Technology*, Taipei.

Cedex, C.S. (1993), *Genetic Algorithms, An Alternative Tool for Security Audit Trails Analysis*, Lodovic Me, SUPELEC.

Chan, P.C. and Wei, V.K. (2002), "Preemptive distributed intrusion detection using mobile agents," paper presented at the IEEE International Workshop on Enabling Technologies, Carnegie Mellon University, Pittsburgh, PA.

Cheung, S. and Levitt, K.N. (1997), "Protecting routing infrastructures from denial of service using cooperative intrusion detection", *Proceedings New Security Paradigms Workshop*, Langdale.

Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Rowe, J., Staniford-Chen, S., Yip, R. and Zerkle, D. (1999), "The Design of GrIDS: a graph-based intrusion detection system", Computer Science Department Technical report CSE-99-2, University of California, Davis, CA.

Corbitt, T. (1994), "The Computer Misuse Act," *Computer Fraud and Security Bulletin*, pp. 13-17.

Crosbie, M. (1995), "Applying genetic programming to intrusion detection", *Proceedings of AAAI Fall Symposium on Genetic Programming*, San Jose, CA.

Crosbie, M. and Spafford, E. (1995), "Defending a computer system using autonomous agents", *Proceedings of the 18th National Information Systems Security Conference*, Baltimore, MD.

Debar, H., Ludovic, M. and Wu, S.F. (Eds) (2000), "Recent advances in intrusion detection", *Third International Workshop, Raid 2000*, Springer Verlag, Toulouse.

DeDios, P., El-Khalil, R., Sarantakos, K., Miller, M., Eskin, E., Lee, W. and Stolfo, S. (2001), "Heuristic audit of network traffic: a data mining-based approach to network intrusion detection", technical report, CUCS, Columbia University, New York, NY.

Denmac Systems (1999), *Network Based Intrusion Detection*, Denmac Systems, Inc., Dearfield, IL

Denning, D. (1987), "An intrusion detection model", *IEEE Transactions on Software Engineering*, Vol. 13 No. 2, pp. 222-32.

Denning, D. and Neumann, P. (1985), *Requirements and Model for IDES – A Real-Time Intrusion Detection Expert System, Final Report*, Computer Science Laboratory, SRI International, Menlo Park, CA.

Denning, D., Edwards, D., Jagannathan, R., Lunt, T. and Neumann, P. (1987), "A prototype IDES: a real-time intrusion detection expert system", Computer Science Laboratory, SRI International, Menlo Park, CA.

Dias, G., Levitt, K.N. and Mukherjee, B. (1990), "Modeling attacks on computer systems: evaluating vulnerabilities and forming a basis for attack detection", paper presented at the SRI Intrusion Detection Workshop, Menlo Park, CA.

Didier, S. and Molva, R. (1997), " IDAMN: an intrusion detection architecture for mobile networks", *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 7.

Doak, J. (1992), "Intrusion detection: the application of feature selection, a comparison of algorithms, and the application of a network analyzer", Master's thesis, University of California, Davis, CA.

Dowell, C. and Ramstedt, P. (1990), "The computer watch data reduction tool", *Proceedings of the 13th National Computer Security Conference*, Washington, DC.

Dunigan, T. and Hinkel, G. (1999), "Intrusion detection and intrusion prevention on a large network: a case study", *Proceedings of the 1st Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, CA.

Enterasys Networks (2001), *Intrusion Detection System: Hackers are Getting Smarter, Enterasys Networks*, Andover, MA.

Escamilla, T. (1998), *Intrusion Detection: Network Security Beyond the Firewall*, John Wiley & Sons, New York, NY.

Eskin, E. (2000), "Anomaly detection over noisy data using learned probability distributions", *Proceedings of ICML 2000*, Menlo Park, CA.

Eskin, E., Lee, W. and Stolfo, S. (2001a), "Modeling system calls for intrusion detection with dynamic window sizes", *Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX II)*, Anaheim, CA.

Eskin, E., Arnold, A., Prerau, M., Portnoy, L. and Stolfo, S. (2002), "A geometric framework for unsupervised anomaly detection: detecting intrusions in unlabeled data", technical report, CUCS, Columbia University, New York, NY.

Eskin, E., Miller, M., Zhong, Z.D., Yi, G., Lee, W. and Stolfo, S. (2001b), "Adaptive model generation for intrusion detection systems", paper presented at the Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security.

Fan, W. and Stolfo, S. (2002), "Ensemble-based adaptive intrusion detection", *Proceedings SIAM International Conference on Data Mining*, Arlington, VA.

Fan, W., Lee, W., Stolfo, S. and Miller, M. (2002), "A multiple model cost-sensitive approach for intrusion detection", paper presented at the 11th European Conference on Machine Learning.

Feiertag, R., Benzinger, L., Rho, S. and Wu, S. (1999), "Intrusion detection intercomponent adaptive negotiation", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Forte, D. (1999), "Intrusion detection systems", *login*, Vol. 24 No. 1.

Frank, J. (1994), "Machine learning and intrusion detection: current and future directions", *Proceedings of the 17th National Computer Security Conference*, Baltimore, MD.

Frincke, D., Tobin, D. and Ho, Y. (1998), "Planning, Petri nets, and intrusion detection", *Proceedings of 21st National Information System Security Conference*, Crystal City, VA.

Garvey, T. and Lunt, T. (1991), "Model-based intrusion detection", *Proceedings of the 14th National Computer Security Conference*, Washington, DC.

Ghosh, A. and Schwartzbard, A. (1999), "A study in using neural networks for anomaly and misuse detection", *Proceedings of the 8th USENIX Security Symposium*.

Graham, R. (Ed.) (1998-2000), "FAQ: network intrusion detection systems", *InfoWorld*.

Gross, A. (1997), "Analyzing computer intrusions", PhD thesis, Department of Computer Sciences, University of California, San Diego, CA.

Habra, N., Le Charlier, B. and Mounji, A. (1991), "Preliminary report on advanced security audit trail analysis on UNIX", research report, Universitaires Notre Dame de la Paix, Namur.

Habra, N., Le Charlier, B. and Mounji, A. (1993), "Advanced security audit trail analysis on UNIX: implementation design of the NADF evaluator", research report, Universitaires Notre Dame de la Paix, Namur.

Halme, L. and Bauer, R.K. (1995), "AINT misbehaving – a taxonomy of anti-intrusion techniques", *Proceedings of the 18th National Information Systems Security Conference*, Baltimore, MD.

Halme, L. and Kahn, B. (1900), "Building a security monitor with adaptive user work profiles", *Proceedings of the 11th National Computer Security Conference*.

Heady, R., Luger, G., Maccabe, A.B. and Servilla, M. (1990), "The architecture of a network level intrusion detection system", Technical report CS90-20, Department of Computer Science, University of New Mexico, Albuquerque, NM.

Heberlein, T., Levitt, K. and Mukherjee, B. (1991a), "A method to detect intrusive activity in a networked environment", *Proceedings of the 14th National Computer Security Conference*.

Heberlien, T., Mukherjee, B., Levitt, K.N., Dias, G. and Mansur, D. (1991b), "Towards detecting intrusions in a networked environment", *Proceedings of the 14th Department of Energy Computer Security Group Conference*.

Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J. and Wolber, D. (1990), "A network security monitor", *Proceedings of the IEEE Symposium on Research in Security and Privacy*.

Helman, P., Liepins, G. and Richards, W. (1992), "Foundations of intrusion detection", *Proceedings of the 5th Computer Security Foundations Workshop*, Franconia, NH.

Hershkop, S., Apap, F., Glanz, E., D'alberti, T., Eskin, E., Stolfo, S. and Lee, J. (2001), "Hobids: a data mining approach to host based intrusion detection", technical report, CUCS, Columbia Univeristy, New York, NY.

Herve, D. (2000), "What is behavior-based intrusion detection?", Intrusion Detection FAQ, IBM Zurich Research Laboratory, SANS Institute Resources, Betheseda, MD.

Hochberg, J., Jackson, K., Stallings, K.C., McClary, J.F., DuBois, D. and Ford, J. (1993), "NADIR: an automated system for detecting network intrusion and misuse", *Computers and Security*, Vol. 12 No. 3, pp. 235-48.

Hofmeyer, S.A., Forrest, S. and Somayaji, A. (1998), "Intrusion detection using sequences of system calls", *Journal of Computer Security*, Vol. 6, pp. 151-80.

Hubbard, B., Haley, T., McAuliffe, N., Schaefer, L., Kelem, N., Wolcon, D., Feiertag, R. and Schaefer, M. (1990), *Computer System Intrusion Detection*, TIS Report No. 348, Trusted Information Systems, Inc. Bell State University, Muncie, IN.

Ilgun, K. (1992a), "USTAT – a real-time intrusion detection system for UNIX", Master's thesis, University of California, Santa Barbara, CA.

Ilgun, K. (1992b), "USTAT: a real-time intrusion detection system for UNIX", Master's thesis, University of California, Santa Barbara, CA.

Ilgun, K., Kemmerer, R.A. and Porras, P. (1995), "State transition analysis: a rule-based intrusion detection approach", *IEEE Transactions on Software Engineering*, Vol. 21 No. 3, pp. 181-99.

Jackson, K., DuBois, D. and Stallings, C. (1991a), "A phased approach to network intrusion detection", *Proceedings of the United States Department of Energy Computer Group Conference*.

Jackson, K., DuBois, D. and Stallings, C. (1991b), "An expert system application for network intrusion detection", *Proceedings of the 14th Department of Energy Computer Security Group Conference*, Washington, DC.

Jackson, K., Neumann, M.C., Simmonds, D., Stallings, C., Thompson, J. and Christoph, G. (1994), "An automated computer misuse detection system for UNICOS", *Proceedings of the Cray Users Group Conference*, Tours.

Kim, G. and Spafford, E.H. (1997), "Tripwire: a case study in integrity monitoring", in Denning, D. and Denning P. (Eds), *Internet Besieged: Countering Cyberspace Scofflaws*, Addison-Wesley, Englewood Cliffs, NJ.

Ko, C., Fink, G. and Levitt, K. (1994), "Automated detection of vulnerabilities in privileged programs by execution monitoring", *Proceedings of the 10th Annual Computer Security Applications Conference*, pp. 134-44.

Kossakowski, P. (1999), *Responding to Intrusions*, (CMU/SEI-SIM- 006), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Kumar, S. (1995), "Classification and detection of computer intrusions", PhD dissertation, Purdue University, West Lafayette, IN.

Kumar, S. and Spafford, E. (1994), "A pattern matching model for misuse intrusion detection", *Proceedings of the 17th National Computer Security Conference*, Baltimore, MD.

Kumar, S. and Spafford, E. (1995), "A software architecture to support misuse intrusion detection", *Proceedings of the 18th National Information Security Conference*, pp. 194-204.

Lane, T. and Brodley, C. (1997a), "An application of machine learning to anomaly detection", *Proceedings of the 20th National Information System Security Conference*, Baltimore, MD.

Lane, T. and Brodley, C.E. (1997b), "Sequence matching and learning in anomaly detection for computer security", *AAAI Workshop: Approaches to Fraud Detection and Risk Management*, AAAI Press, Menio Park, CA, pp. 43-9.

Lankewics, L. and Benard, M. (1991), "Real-time anomaly detection using a nonparametric pattern recognition approach", *Proceedings of the 7th Computer Security Applications Conference*, San Antonio, TX.

Lee, W. (1999), "A data mining framework for constructing features and models for intrusion detection systems", PhD thesis, Columbia University, New York, NY.

Lee, W. and Stolfo, S. (1998), "Data mining approaches for intrusion detection", *Proceedings, 7th USENIX Security Symposium*, San Antonio, TX.

Lee, W. and Stolfo, S.J. (1999), "Combining knowledge discovery and knowledge engineering to build IDSs", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Lee, W. and Xiang, D. (2001), "Information-theoretic measures for anomaly detection", *Proceedings of the 2001 IEEE Symposium on Security and Privacy*.

Lee, W., Park, C. and Stolfo, S. (1999a), "Towards automatic intrusion detection using NFR", *Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*.

Lee, W., Stolfo, S.J. and Chan, P.K. (1997), "Learning patterns from Unix processes execution traces for intrusion detection", *Proceedings of the AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management*, AAAI Press, Menlo Park, CA, pp. 50-6.

Lee, W., Stolfo, S. and Mok, K. (1998), "Mining audit data to build intrusion detection models", *Proceedings of the 4th International Conference on Knowledge Discovery and Data Mining*.

Lee, W., Stolfo, S.J. and Mok, K. (1999b), "Data mining in work flow environments: Experiences in intrusion detection", *Proceedings of the Conference in Knowledge Discovery and Data Mining*.

Lee, W., Stolfo, S.J. and Mok, K.W. (1999c), "A data mining framework for building intrusion detection models", *Proceedings of the Twentieth IEEE Symposium on Security and Privacy*, Oakland, CA.

Lee, W., Miller, M., Stolfo, S., Jallad, K., Park, C., Zadok, E. and Prabhakar, V. (2000), "Toward cost-sensitive modeling for intrusion detection", Technical report 002-00, CUCS, Columbia University, New York, NY.

Lee, W., Stolfo, S., Chan, P.K., Eskin, E., Fan, W., Miller, M., Hershkop, S. and Zhang, J. (2001), "Real time data mining-based intrusion detection", *Proceedings of DISCEX II*.

Levitt, K. (Ed.) (1992), *Proceedings of Workshop on Future Directions In Computer Misuse and Anomaly Detection*, University of California, Davis, CA.

Liepins, G. and Vaccaro, H.S. (1992), "Intrusion detection: its role and validation", *Computers and Security*, Vol. 11, Elsevier Science, Oxford, pp. 347-55.

Lindquist, U. and Jonsson, E. (1997), "How to systematically classify computer security intrusions", *Proceedings IEEE Symposium Research in Security and Privacy*, Oakland, CA.

Lippmann, R., Haines, J.W., Fried, D.J., Korba, J. and Das, K. (2000a), "The 1999 DARPA off-line intrusion detection evaluation", *Computer Networks*, Vol. 34, pp. 579-95.

Lippmann, R., Fried, D., Graf, I., Haines, J., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D., Cunninghan, R. and Zissman, M. (2000b), "Evaluating intrusion detection systems: the DARPA off-line intrusion detection evaluation", *Proceedings DARPA Information Survivability Conference*.

Lodin, S. (1998), *Intrusion Detection Product Evaluation Criteria*, Ernst & Young LLP, available at: docshow.net/ids.htm

Lundin, E. and Jonsson, E. (1999), "Privacy versus intrusion detection 'analysis'", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Lunt, T. (1988), "Automated audit trail analysis and intrusion detection: a survey", *Proceedings of the 11th National Computer Security Conference*, Washington, DC.

Lunt, T. (1989a), "Real-time intrusion detection", *Proceedings of COMPCON Spring '89*, San Francisco, CA.

Lunt, T. (1989b), "Knowledge-based intrusion detection", *Proceedings of the AI Systems in Government Conference*, Washington, DC.

Lunt, T. (1993a), "A survey of intrusion detection techniques", *Computers and Security*, Vol. 12, pp. 405-18.

Lunt, T. (1993b), "Detecting intruders in computer systems", *Proceedings of the Conference on Auditing and Computer Technology*.

Lunt, T. and Jagannathan, R. (1988), "A prototype real-time intrusion detection expert system", *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, Oakland, CA.

Lunt, T., Tamaru, Gilham, F., Jagannathan, R., Neumann, P., Javitz, H., Valdes, A. and Garvey, T. (1992), *A Real-time Intrusion Detection Expert System (IDES) – Final Technical Report*, Computer Science Laboratory, SRI International, Menlo Park, California.

McAuliffe, N., Wolcott, D., Schaefer, L., Kelem, N., Hubbard, B. and Haley, T. (1990), "Is your computer being misused? A survey of current intrusion detection technology", *Proceedings of the Sixth Annual Computer Security Applications Conference*, Tucson, AZ.

McConnell, J., Frincke, D.A., Tobin, D., Marconi, J. and Polla, D. (1998), "A framework for cooperative intrusion detection", *Proceedings of Twenty-First National Information System Security Conference*, Crystal City, VA.

Mahoney, M. (2000), "Computer security: a survey of attacks and defenses" available at: docshow.net/ids.htm

Mahoney, M. and Chan, P. (2001), "Detecting novel attacks by identifying anomalous network packet headers", Technical report CS-2001-2, Florida Institute of Technology, Melbourne, FL.

Maiwald, E. (1998), "Automating response to intrusions", paper presented at the 4th Annual UNIX and NT Network Security Conference, The SANS Institute, Orlando, FL.

Malladi, S., Alvis-Foss, J. and Malladi, S. (2002), "What are multi protocol guessing attacks and how to prevent them", *Proceedings of the 11th IEEE International Workshop on Enabling Technologies*, Carnegie Mellon University, Pittsburgh, PA.

Mandanaris, S., Christensen, M., Zerkle, D. and Hermis, K. (1999), "A data mining analysis of RTID alarms", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Marceau, C. (2000), "Characterizing the behavior of a program using multiple-length n-grams", *Proceedings of the New Security Paradigms Workshop*.

Mansfield, G., Ohta, K., Takei, Y., Kato, N. and Nemoto, Y. (1999), "Towards trapping wily intruders in the large", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Marchette, D. (2001), *Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint*, Springer Verlag, Berlin.

Mark, G. (2000), "Intrusion detection", *Software Technology Review*, Software Engineering Institute. Carnegie Mellon University, Pittsburgh, PA.

Me, L. (1993), "Security audit trail analysis using genetic algorithms", *Proceedings of the Twelfth International Conference on Computer Safety, Reliability, and Security*, Poznan.

Me, L. (1998), "GASSATA, a genetic algorithm as an alternative tool for security audit trails analysis", paper presented at the 1st International Workshop on the Recent Advances in Intrusion Detection, Louvain-la-Neuve.

Mell, P. and McLarnon, M. (1999), "Mobile agent attack resistant distributed hierarchical intrusion detection systems", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Miller, M. (1999), "Learning cost-sensitive classification rules for network intrusion detection using RIPPER", Technical report 035-99, CUCS, Columbia University, New York, NY.

MIT Lincoln Labs (1999), "DARPA intrusion detection evaluation", available at: www.ll.mit.edu

Moitra, A. (1992), "Real-time audit log viewer and analyzer", *Proceedings of the 4th Workshop on Computer Security Incident Handling*, Denver, CO.

Mounji, A. (1997), "Languages and tools for rule-based distributed intrusion detection", thesis, Faculte's Universitaires Notre-Dame de la Paix, Namur.

Mukherjee, B., Heberlein, L.T. and Levitt, K.N. (1994), "Network intrusion detection", *IEEE Network*, Vol. 8 No. 3, pp. 26-41.

Neumann, P.G. and Parker, D.B. (1989), "A summary of computer misuse techniques", *Proceedings of the 12th National Computer Security Conference*.

Neumann, P.G. and Porras, P.A. (1999), "Experience with Emerald to date", *SRI International, 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, CA, pp. 73-80.

Northcutt, S. (1999a), *Network Intrusion Detection: An Analyst's Handbook*, New Rider, Indianapolis, IN.

Northcutt, S. (1999b), "What the hackers know about you", Intrusion Detection FAQ, SANS Institute Resources, SANS Institute, Betheseda, MD.

Northcutt, S. (2000), "What is network based intrusion detection?", Intrusion Detection FAQ, SANS Institute Resources, SANS Institute, Betheseda, MD.

Ong, T.H., Tan, C.P., Tan, Y.T., Chew, C.K. and Ting, C. (1999), "SNMS – shadow network management system", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Panagiotis, A. (1999), "Intrusion detection Systems", *Daemon News*.

Paxon, V. (1998), "Bro: a system for detecting network intruders in real-time", *Proceedings of the 7th USENIX Security Symposium*, San Antonio, TX.

Paxon, V. and Handley, M. (1999), "Defending against network IDS evasion", *Proceedings of the 2nd International Workshop On Recent Advances in Intrusion Detection*, West Lafayette, IN

Piccioto, J. (1987), "The design of an effective auditing subsystem", *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, Oakland, CA.

Pichnarczyk, K., Weeber, S. and Feingold, R. (1994), "Unix incident guide: how to detect an intrusion", report CIAC-2305 R.1, Department of Energy Computer Incident Advisory Capability, Lawrence Livermore National Laboratory, Livermore, CA.

Porras, P. (1992), "STAT, a state transition analysis tool for intrusion detection", Master's thesis, Computer Science Department, University of California, Santa Barbara, CA.

Porras, P. and Kemmerer, R.A. (1992), "Penetration state transition analysis: a rule-based intrusion detection approach", *Proceedings of the 8th Annual Computer*

Security Applications Conference, San Antonio, TX.

Porras, P. and Neumann, P.G. (1997), "Emerald: event monitoring enabling responses to anomalous live disturbances", paper presented at the National Information Systems Security Conference, Baltimore, MD.

Portnoy, L., Eskin, E. and Stolfo, S.J. (2001), "Intrusion detection with unlabeled data using clustering", *Proceedings of ACM CSS Workshop on Data Mining Applied to Security*.

Price, K.E. (1997), "Host-based misuse detection and conventional operating systems' audit data collection", Master's thesis, Purdue University, West Lafayette, IN.

Proctor, P.E. (2000), *Practical Intrusion Detection Handbook*, Prentice-Hall, Englewood Cliffs, NJ.

Puketza, N., Chung, M., Olsson, R.A. and Mukherjee, B. (1997), "A software platform for testing intrusion detection systems", *IEEE Software*, Vol. 14 No. 5, pp. 43-51.

Puketza, N., Zhang, K., Chung, M., Mukherjee, B. and Olsson R.A. (1996), "A methodology for testing intrusion detection systems", *IEEE Transactions on Software Engineering*, Vol. 22 No. 10, pp. 719-29.

Reavis, J. (1999), "Do you have an intrusion detection response plan?", *Network World Fusion*, 13 September,.

Roesch, M. (1999), "Snort – lightweight intrusion detection for networks", *Proceedings of Lisa*.

Samfat, D. and Molva, R. (1997), "IDAMN: an intrusion detection architecture for mobile networks", *IEEE Journal on Selected Areas in Communications*, Vol. 15 No. 7.

SANS Institute Resources (2000), "What is the role of a file integrity checker like Tripwire in intrusion detection?", Intrusion Detection FAQ, SANS Institute Resources, Betheseda, MD.

Scambray, J., McClure, S. and Broderick, J. (1998), "Network intrusion-detection solutions", *InfoWorld*, 4 May.

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

Sebring, M., Shellhouse, E., Hanna, M. and Whitehurst, R. (1988), "Expert systems in intrusion detection: a case study", *Proceedings of the 11th National Computer Security Conference*.

Seleznyov, A. and Puuronen, S. (1999), "Anomaly intrusion detection systems: handling temporal relations between events", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Shieh, S. and Gligor, V.D. (1991), "A pattern-oriented intrusion detection model and its applications", *Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy*, Oakland, CA.

Shimomura, T. (1996), *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, Hyperion, New York, NY.

Simonian, R. (1990), "A neural network approach towards intrusion detection", *Proceedings of the 13th National Computer Security Conference*, Washington, DC.

Sinclair, C., Pierce, L. and Matzner, S.P. (1999), "An application of machine learning to network intrusion detection", paper presented at the 15th Annual Computer Security Applications Conference.

Slatalla, M. and Quittner, J. (1996), *Masters of Deception: The Gang That Ruled Cyberspac*, Harper, New York, NY.

Smaha, S.E. (1988), "Haystack: an intrusion detection system", *Proceedings of the 4th Aerospace*, Orlando, FL.

Smaha, S. and Snapp, S. (1996), "Method and system for detecting intrusion into and misuse of a data processing system", US555742, US Patent Office, Alexandria, VA.

Snapp, S., Brentano, J., Dias, G., Goan, T., Grance, T., Heberlein, T., Ho, C., Levitt, K., Mukherjee, B., Mansur, D., Pon, K. and Smaha, S. (1991), "A system for distributed intrusion detection", *Proceedings of COMPCON Spring '91*, San Francisco, CA.

Sobirey, M., Richter, B. and Konig, H. (1996), "The intrusion detection system AID: architecture, and experiences in automated audit analysis", *Proceedings of the IFIPTC6/TC11 International Conference on Communications and Multimedia Security*, Essen.

Spitzner, L. (2001), *Know Your Enemy: Revealing the Security Tools, Tactics and Motives of the Blackhat Community*, Addison-Wesley Publishing, Boston, MA.

Staniford-Chen, S., Tung, B. and Schnackenberg, D. (1998), "The common intrusion detection frame-work (CIDF)", *Proceedings of the Information Survivability Workshop*.

Staniford-Chen, S., Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Wee, C., Yip, R. and Zerkle, D. (1996), "GrIDS – a graph-based intrusion detection system for large networks", paper presented at the 19th National Information Systems Security Conference, Baltimore, MD.

Sterling, B. (1992), *The Hacker Crackdown*, Bantam, New York, NY.

Stolfo, S.J., Fan, W., Lee, W., Prodromidis, A. and Chan, P. (2000), "Cost-based modeling for fraud and intrusion detection: results from the JAM project", *Proceedings of the 2000 DARPA Information Survivability Conference and Exposition*.

Stoll, C. (1990), *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, New York, NY.

Sundaram, A. (1996), "An introduction to intrusion detection", *Crossroads: The ACM Student Magazine*, Vol. 2 No. 4, available at: acm.org/Crossroads.

Tener, W. (1986), "Discovery: an expert system in the commercial data security environment", *Proceedings of the IFIP Security Conference*, Monte Carlo.

Tener, W. (1988), "AI and 4GL: automated detection and investigation and detection tools", *Proceedings of the IFIP Security Conference*, Sydney.

Teng, H.S., Chen, K. and Lu, S.C. (1990a), "Security audit trail analysis using inductively generated predictive rules", *Proceedings of the 11th National Conference on Artificial Intelligence Applications*, IEEE Service Center, Piscataway, NJ, pp. 24-9.

Teng, H.S., Chen, K. and Lu, S.C. (1990b), "Adaptive real-time snomaly detection using inductively generated sequential patterns", *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy*, Oakland, CA.

Ting, C., Ong, T.H., Tan, Y.T. and Ng, P.Y. (1999), "Intrusion detection, Internet law enforcement, and insurance coverage to accelerate the proliferation of Internet business", *Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Toxen, B. (2000), *Real World Linux Security: Intrusion Prevention, Detection, and Recovery*, Prentice-Hall, Englewood Cliffs, NJ.

Tsudik, G. and Summers, R. (1990), "AudES – an expert system for security auditing", *Proceedings of the AAAI Conference on Innovative Applications in AI*, San Jose, CA, 1990, reprinted in *Computer Security Journal*, Vol. 6 No. 1, pp. 89-93.

Vaccaro, H.S. and Liepins, G.E. (1989), "Detection of anomalous computer session activity", *Proceedings Symposium on Research in Security and Privacy*, Oakland, CA.

Valcarce, E.M., Hoglund, G.W., Jansen, L. and Baillie, L. (1992), "ESSENSE: an experiment in knowledge-based security monitoring and control", *Proceedings of the 3rd USENIX Unix Security Symposium*, Baltimore, MD.

Vert, G., Frincke, D.A. and McConnell, J. (1998), "A visual mathematical model for intrusion detection", *Proceedings of the 21st National Information System Security Conference*, Crystal City, VA.

Warrender, C., Forrest, S. and Pearlmutter, B. (1999), "Detecting intrusions using system calls: alternative data models", *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE Computer Society, Los Alamitos, CA, pp. 133-45.

Wee, C. (1995), "LAFS: a logging and auditing file system", *Proceedings of the 11th Computer Security Applications Conference*, New Orleans, LA.

Weiss, W. and Baur, A. (1990), "Analysis of audit and protocol data using methods from artificial intelligence", *Proceedings of the Thirteenth National Computer Security Conference*, Washington, DC.

Wetmore, B. (1993), "Audit browsing", Master's thesis, University of California, Davis, CA.

White, G., Fisch, E.A. and Pooch, U.W. (1996), "Cooperating security managers: a peer-based intrusion detection system", *IEEE Network*, Vol. 10 No. 1, pp. 20-3.

Wiler, N. (2000), "Honeypots for distributed denial of service attacks", paper presented at the IEEE International Workshop on Enabling Technologies, Carnegie Mellon University, Pittsburgh, PA, June.

Wing, J. (2002), "Vulnerability analysis of networked systems", *Procceedings of the 11th IEEE International Workshop on Enabling Technologies*, June, Carnegie Mellon University, Pittsburgh, PA.

Winkler, J. (1990), "UNIX prototype for intrusion and anomaly detection in secure networks", *Proceedings of the 13th National Computer Security Conference*, October.

Wood, M. (1999), "Intrusion detection exchange format requirements", internet draft, Internet Engineering Task Force.

Ye, N. (2000), "A Markov chain model of temporal behavior for anomaly detection", *Proceedings of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*.

Yip, R. and Levitt, K. (1998), "Data level inference detection in database systems", *Proceedings of the Eleventh IEEE Computer Security Foundations Workshop*, Rockport, MA.

Yuill, K., Wu, S.F., Gong, F. and Huang, M.Y. (1999), "Intrusion detection for an ongoing attack", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Zamboni, D. (1996), "SAINT: a security analysis integration tool", paper presented at the Systems Administration, Networking and Security (SANS) Conference, Washington, DC.

Zamboni, D. and Spafford, E. (1999), "New directions for the AAFID architecture", *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection*, West Lafayette, IN.

Zirkle, L. (2000), "What is host-based intrusion detection?", Virginia Tech CNS. SANS Institute Resources, Intrusion Detection FAQ, Sans Institute, Betheseda, MD.

The authors would like to extend their sincere thanks to the referees and the editor Kevin Fitzgerald. The work described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration (NASA). Concerning the reference list we have tried to be reasonably complete; however, those articles that were not included were considered not to bear directly on the topics of this review or were inadvertently overlooked. We apologize to both the researchers and readers if we have omitted any relevant article.

Part II of this article will be published in Vol. 11 No. 5 of Information Management (Computer Security in October 2003.

Further reading

Anderson, R. (1994), "Liability and computer security: nine principles", paper presented at the 3rd European Symposium on Research in Computer Security, Brighton.

Debar, H., Becker, M. and Siboni, D. (1992), "A neural network component for an intrusion detection system", *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA.

Heberlein, T. (1995), *Network Security Monitor (NSM) – Final Report*, Lawrence Livermore National Laboratory, Livermore, CA.

Heberlein, L., Mukherjee, B. and Levitt, K. (1992), "Internetwork security monitor: an intrusion detection system for large-scale networks", *Proceedings of the 15th National Computer Security Conference*.

Helman, P. and Liepins, G. (1993), "Statistical foundations of audit trail analysis for the detection of computer misuse", *IEEE Transactions on Software Engineering*, Vol. 19 No. 9, pp. 886-901.

Jackson, K.A. (1999), *Intrusion Detection System (IDS) Product Survey*, Distributed Knowledge Systems Team; Computer Research and Applications Group; Computing, Information and Communications Division, Los Alamos National Laboratory, Los Alamos, NM.

Javitz, H. and Valdes, A. (1991), "The SRI IDES statistical anomaly detector", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA.

Lankewicz, L. and Bernard, M. (1990), "A nonparametric pattern recognition approach to intrusion detection", Technical report TUTR 90-106, Tulane University Department of Computer Science, New Orleans, LA.

Liepins, G. and Vaccaro, H.S. (1989), "Anomaly detection: purpose and framework", *Proceedings of the Twelfth National Computer Security Conference*, Washington, DC.

Sibert, W.O. (1988), "Auditing in a distributed system: SunOS MLS audit trails", *Proceedings of the Eleventh National Computer Security Conference*, Washington, DC.

TRW Defense Systems Group (1986), "Intrusion detection expert system feasibility study", Final report 46761.

Wee, C. (1996), "Policy-directed auditing and logging", PhD thesis, University of California, Davis, CA.

Winkler, J. (1992), "Intrusion and anomaly detection: ISOA", *Proceedings of the 15th National Computer Security Conference*.

Winkler, J. and Page, W.J. (1989), "Intrusion and anomaly detection in trusted systems", *Proceedings of the 5th Annual Computer Security Applications Conference*, Tucson, AZ.

Zerkle, D. and Levitt, K. (1996), "NetKuang – a multi-host configuration vulnerability checker", *Proceedings of the 6th USENIX Security Symposium*, San Jose, CA.