INTRUSION DETECTION:
A BIBLIOGRAPHY OF ONE DECADE (1993-2003)[1]

Enrique López González y Cristina Mendaña Cuervo

Departamento de Dirección y Economía de la Empresa, Universidad de León
Facultad de CC. EE. y Empresariales, Campus Vegazana E–24071 León (España)
Phone: +34 987 291742; E–mail: dde{elg,cmc}@unileon.es
URL: http://sicodinet.unileon.es

Contenido

1. INTRUSION DETECTION IN 1993

Anderson, D., Lunt, T., Javitz, H., Tumaru, A. and Valdes, A. (1993). **SAFEGUARD Final Report : Detecting Unusual Program Behavior Using the NIDES Statistical Component.** Technical Report, Computer Science Laboratory, SRI.

Braden, B. (1993). **NNStat**. Disponible en http://www.duth.gr/InfoBase/noc/nnstat.txt

[1] Este trabajo está soportado por el proyecto de investigación DPI 2001–0105 del MCT.

Debar, H. (1993). **Aplication des réseaux de neurones a la détection d'intrusions sur les systemes informatiques**. PhD thesis, Université de Paris 6.

Habra, N., Charlier, B. and Mounji, A. (1993). **Advanced Security Audit Trail Analysis on uniX. Implementation Design of the NADF Evaluator**. Technical Report, Computer Science Institute, University of Namur.

Javitz, H., Valdes, A., Lunt, T., Tamaru, A., Tyson, M. and Lowrance, J. (1993). **Next Generation Intrusion Detection Expert System (NIDES).** Technical Report AOI6-Rationales, SRI.

llgun, K. (1993). **USTAT : A Real-Time Intrusion Detection System for UNIX**. In Proceedings of the IEEE Symposium on Security and Privacy, p. 16-29.

Ko, C., Frincke, D., Heberlein, L., Levitt, K., Mukherjee, B. and Wee, C. (1993). **Analysis of an AIgorithm for Distributed Recognition and Accountability**. In Proceedings of First ACM Conference on Computer and Communications Security, p. 154-164.

Lunt, T. (1993). **Detecting Intruders in Computer Systems**. In Proceedings of the 1993 Conference on Auditing and Computer Technology. Disponible en http://www2.csl.sri.com/nides/index5.html

Lunt, T. (1993). **A Survey of Intrusion Detection techniques**. Computers and Security, 12(4), p. 405-418.

Mé, L. (1993). **Security Audit Trail Analysis Using Genetic Algorithms**. In Proceedings of the 12th International Conference on Computer Safety, Reliability and Security, p. 329-340.

Safford, D., Schales, D. and Hess, D. (1993). **The TAMU Security Package: an Ongoing response to the Internet Intruders in an Academic Environment**. In Proceedings of the Fourth USENIX Security Symposium.

Safford, D., Schales, D. and Hess, D. (1993).**Texas A&M Network Security Package Overview.** Disponible en ftp://coast.cs.purdue.edu/pub/tools/unix/netlog/TAMU/OVERVIEW

Wetmore, B. (1993). **Paradigms for the reduction of audit trails**. Master's thesis, Computer Science Department, University of California.

2. INTRUSION DETECTION IN 1994

Anderson, D., Lunt, T., Javitz, H., Tamaru, A. and Valdes, A. (1994). **NIDES: Software Users Manual . Beta-Update Release**, Disponible en http://www.sdl.sri.com/papers/7sri/.

Crosbie, M. and Spafford, G. (1994). **Defending a Computer System using Autonomous Agents**. Technical Report 95-022, Purdue University.

Denault, M., Gritzalis, D., Karagiannis, D. and Spirakis, P. (1994). **Intrusion detection: aproach and performance issues of the SECURENET system**. Computers & Security, 13, p. 495-508.

Frank, J. (1994). **Artificial Intelligence and Intrusion Detection: Current and Future Directions.** Technical Report NSA URP MDA904-93-C4085, University of California at Davis.

Frank, J. (1994). **Artificial Intelligence and Intrusion Detection: Current and Future Directions.** Disponible en http://seclab.cs.ucdavis.edu/papers/ncsc.94.ps

Jackson, K., Neuman, M., Simmonds, D., Stallings, C., Thompson, J. and Christoph, G. (1994). **An Automated Computer Misuse Detection System for UNICOS.** Technical Report LA-UR-94-3385, Los Alamos National Laboratory.

Javitz, H. and Valdes, A. (1994). **The NIDES Statistical Component Description and Justification**. Technical Report, SRI Computer Science Laboratory, Menlo Park, CA. Disponible en http://www.sdl.sri.com/nides/index5.html.

Ko, C., Fink, G. and Levitt, K. (1994). **Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring**. In Proceedings of the 10th Annual Computer Security Aplications Conference (ACSAC'94), p. 134-144. Disponible en http://seclab.cs.ucdavis.edu/papers/kfl94.ps

Krsul, I. (1994). **Authorship Analysis: Identifying The Author of a Program.** Technical Report CSDTR-94-030, Department of Computer Sciences, Purdue University.

Kumar, S. and Spafford, E. (1994). **A Pattern Matching Model for Misuse Intrusion Detection**. In Proceedings of the national computer security conference, p. 11-21. Disponible en http://www.cs.purdue.edu/coast/coast-library.html

Kumar, S. and Spafford, E. (1994). **An Aplication of Pattern Matching in Intrusion Detection**. Technical Report CSDTR-94-013, Purdue University. Disponible en http://www.cs.purdue.edu/coast/coast-library.html.

Landwehr, C., Bull, A., McDermott, J. and Choi, W. (1994). **A taxonomy of computer program security laws**. ACM Computing Surveys, 3(26), p. 211-254.

Lin, T. (1994). **Fuzzy Patterns in Data**. In 17th National Computer Security Conference.

Mé, L. (1994). **Audit de sécurité par algorithmes génétiques**. PhD thesis, Université de Rennes 1 Numéro d'ordre 1069.

Mukherjee, B., Heberlein, L. and Levitt, K. (1994). **Network Intrusion Detection**. IEEE Network, 8(3), p. 26-41. Disponible en http://seclab.cs.ucdavis.edu/papers.html.

Proctor, P. (1994). **Audit Reduction and Misuse Detection in Heterogeneous Environments: Framework and Aplication**. In Proceedings of the 10th Annual Computer Security Aplications.

Stutz, J. and Cheeseman, P. (1994). **A Short Exposition on Bayesian Inference and Probability.** Disponible en http://ic.arc.nasa.gov/ic/projects/bayes-group/html/bayes-theorem-long.html

Toure, M. (1994). **An Interdisciplinary Approach for Adding Knowledge to Computer Security Systems**. In Proceedings of the IEEE International Carnahan Conference on Security Technology. Albuquerque, Oct. 12-14, IEEE, p. 158-168.

3. INTRUSION DETECTION IN 1995

Anderson, D., Frivold, T. and Valdes, A. (1995). **Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES) (SRICSL-95-06).** Menlo Park, CA: Computer Science Laboratory, SRI International. Disponible en http://www.sdl.sri.com/nides/index5.html.

Anderson, D., Frivold, T. and Valdes, A. (1995). **Next-Generation Intrusion Detection Expert System (NIDES). A Summary (SRI-CSL-95-07).** Menlo Park, CA: Computer Science Laboratory, SRI International. Disponible en http://www.sdl.sri.com/nides.index5.html.

Anderson, D., Lunt, T., Javitz, H., Tamaru, A. and Valdes, A. (1995). **Safeguard Final Report: Detecting Unusual program Behavior Using the NIDES Statistical Component**. Disponible en http://www.sdl.sri.com/papers/safeguard/.

Aslam, T. (1995). **A taxonomy of Security Faults in the Unix Operating System.** Master's thesis, Purdue University.

Bishop, M. (1995). **A standard audit trail format.** In Proceedings of the Eighteenth National Information Systems Security Conference, p. 136-145.

Blomqvist, D. and Skantze, J. (1995). **Intrusion Detection: A Study**. Technical Report DoCS 95/62, Department of Computer Systems, Upsala University.

CERT/CC. (1995). **CERT Advisory CA-95.06.** Disponible en http://www.cert.org/advisories/CA-95.06.satan.html

Christoph, G., Jackson, K., Neuman, M., Siciliano, C., Simmonds, D., Stallings, C. and Thompson, J. (1995). **UNICORN : Misuse detection for UNICOS**. Technical Report LAUR-95-1108, Los Alamos National Laboratory.

Chung, M., Puketza, N., Olsson, R. and Mukherjee, B. (1995). **Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions**. In Proceedings of the 1995 National Information Systems Security Conference. Baltimore, Maryland, October 10-13, p. 173-183. Disponible en http://seclab.cs.ucdavis.edu/papers.html.

Cohen, F. (1995). **Re: Intrusion Detection**. Disponible en http://www.geek-girl.com/ids/0602.html

Cohen, W. (1995). **Fast Effective Rule Induction**. In Proceedings of the 12th International Conference on Machine Learning. Lake Tahoe. Disponible en http://www.research.att.com/~wcohen/.

Crosbie, M. and Spafford, G. (1995). **Active Defense of a Computer System using Autonomous Agents**. Technical Report 95-008, Purdue University. Disponible en http://www.cs.purdue.edu/coast/coast-library.html.

Crosbie, M. and Spafford, G. (1995). A**plying Genetic Programming to Intrusion Detectio**n. In Proceedings of the AAAI Fall Symposium on Genetic Programming. Cambridge, MA, Nov. 10-12, 1995. Menlo Park, CA: AAAI Press.

Digital Security InfoCenter (1995). **POLYCENTER Security Intrusion Detector for Digital UNIX, Version 1.2A.** Disponible en ftp://ftp.digital.com/pub/Digital/infofSPD/43-08-XX.txt

Eliot, L. (1995). **Typing your ID via AI**. AI Expert (January), p. 9-10.

Eschrich, S. (1995). **Real-time User Identification Employing Standard Unix Accounting**. Master's thesis, Department of Computer Science, College of Arts and Sciences, Florida State University.

Esmaili, M., Safavi-Naini, R. and Pieprzyk, J. (1995). **Intrusion detection: A survey**. In Proceedings of ICCC'95 (12th International Conference on Computer Communication), IOS Press, Amsterdam, p. 409-414.

Halme, L. and Bauer, R. (1995). **Ain't Misbehaving—a Taxonomy of Anti-Intrusion Techniques**. In Proceedings of 18th National Information Systems Security Conference. Baltimore, October 10-13, Gaithersburg, National Institute of Standards and Technology, p. 163-172.

Heberlein, L. and Staniford-Chen, S. (1995). **Holding intruders accountable on the Internet**. In Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, CA, p. 39-49.

Hinden, R. (1995). **IP Next Generation Overview.** Disponible en http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html

Hoagland, C. Wee, K. (1995). **Audit Log Analysis Using the Visual Audit Browser Toolkit**. Technical Report TR CSE-95-11, University C. Davis. Computer Science Department.

Jackson, K., Neuman, M., Simmonds, D., Stallings, C., Thompson, J. and Christoph, G. (1995). **Misuse and intrusion detection at Los Alamos National Laboratory.** Technical Report LA-UR-95-1039, Los Alamos National Laboratory.

Kumar, S. (1995). **Classification and Detection of Computer Intrusions**. PhD Thesis, Purdue University, West Lafayette, Indiana. Disponible en http://www.cs.purdue.edu/coast/coast-library.html.

Kumar, S. and Spafford, E. (1995). **A Software Architecture to suport Misuse Intrusion Detection**. Technical Report CSDTR-95-009, The COAST Project Department of Computer Sciences, Purdue University.

llgun, K., Kemmerer, R. and Porras, Ph. (1995). **State Transitian Analysis: A Rule-Based Intrusion Detection Aproach**. IEEE Transactions on Software Engineering, p. 181-199.

Maloof, M. and Michalski, R. (1995). **A Method for Partial-Memory Incremental Learning and its Aplication to Computer Intrusion Detection**. In Proceedings of the 7th IEEE International Conference on Tools with Artificial Intelligence.

Maloof, M. and Michalski, R. (1995). **A Partial Memory Incremental Learning Methodology and its Aplication to Computer Intrusion Detection**. Technical Report MLI 95-2, Machine Learning and Inference Laboratory, George Mason University.

Mé, L. (1995). **Un algorithme génétique pour détecter des intrusions dans un systeme informatique**. Valgo, 1(4), p. 68-78.

Soh, B. and Dillon, T. (1995). **Setting optimal intrusion detection thresholds**. Computers and Security, 14, p. 621-631.

Staniford-Chen, S. (1995). **Distributed Tracing of Intruders**. Master's thesis, University of California at Davis.

Thompson, J., Jackson, K., Stallings, C., Simmons, D., Siciliano, C. and Pedicini, G. (1995). **A Progress Report on UNICOS Misuse Detection at Los Alamos.** Technical Report LA-UR-953330, Los Alamos National Laboratory.

Wee, C. (1995). **LAFS: A Logging and Auditing File System**. In Proceedings of the 11th Computer Security Aplications Conference.

4. INTRUSION DETECTION IN 1996

Aslam, T., Krsul, I. and Spafford, E. (1996) **Use of a Taxonomy of Security Faults (Coast TR-96-051)**. West Lafayette, COAST Laboratory, Purdue University. Disponible en http://www.cs.purdue.edu/coast/coast-library.html.

Bace, B. (1996). **Session 6: Tools for Investigative Support**. In Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, November 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session6.html.

Bishop, M., Wee, C. and Frank, J. (1996). **Goal Oriented Auditing and Logging**. Disponible en http://seclab.cs.ucdavis.edu/papers/tocs-96.ps.

Cannady, J. and Harrell, J. (1996). **A Comparative Analysis of Current Intrusion Detection Technologies.** In Proceedings of the fourth Technology for Information Security Conference'96 (TISC'96).

Coffee, P. (1996).**Java, ActiveX Under a Microscope**. Disponible en http://www.zdnet.com/devhead/stories/articles/0,4413,1600418,00.html

Cohen, F. (1996). **A Mathematical Characterization of DCAs**. Disponible en http://all.net/books/dca/math.html

Cohen, F. (1996). **Characteristics of DCAs**. Disponible en http://all.net/books/dca/character.html

Cohen, F. (1996). **DCA's—A Class of Attacks**. Disponible en http://all.net/books/dca/class.html

Cohen, F. (1996). **Defenses Against DCAs**. Disponible en http://all.net/books/dca/defenses.html

Cohen, F. (1996). **Distributed Coordinated Attacks—Background.** Disponible en http://all.net/books/dca/background.html

Cohen, F. (1996). **Distributed Coordinated Attacks—Summary, Conclusions, and Further Work.** Disponible en http://all.net/books/dca/summary.html

Cohen, W. (1996). **Learning Trees and Rules with Set-Valued Features**. Disponible en http://www.research.att.com/~wcohen/

Computers and Law Class (1996). **Discovery of Computer Data**. Disponible en http://wings.buffalo.edu/Complaw/CompLawPapers/printup.html

Cramer, M., Cannady, J. and Harrell, J. (1996). **New Methods of Intrusion Detection using Control-Loop Measurement**. Disponible en http://www.infowar.comjsurvey/ids_newm.html.

Crosbie, M. and Spafford, E. (1996). **Evolving Event Driven Programs**. In Proceedings of the Genetic Programming 1996 Conference.

Dacier, M., Deswarte, Y. and KaAniche, M. (1996). **Quantitative Assessment of Operational Security: Models and Tools**. Technical Report 96493, LAAS.

Dasgupta, D. and Forrest, S. (1996). **Novelty Detection in Time Series Data Using Ideas from Immunology**. Disponible en http://cs.unm.edu/~forrest/publications/noveltydetection96.ps.

Denning, D. (1996). **Protection and Defense of Intrusion**. Disponible en http://www.cosc.georgetown.edu/denning/infosec/USAFA.html.

D'haeseleer, P., Forrest, S. and Helman, P. (1996). **An Immunological Aproach to Change Detection: Algorithms, Analysis and Implications**. In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society, IEEE Computer Society Press.

Digital Security InfoCenter (1996). **POLYCENTER Security Intrusion Detector**. Disponible en http://www.digital.com/infofsecurity/id.htm

Dockery, M. and Zajac, J. (1996). **Responding to Electronic Evidence Requests.** Electronic Evidence Journal 1, 1 (October), p. 1-4. Disponible en http://evidence.finder.com/dockery/FTP/eej10196.pdf.

Evans, J. and Frincke, D. (1996). **Trust Mechanisms for Hummingbird**. Disponible en www1.acm.org/crossroads/xrds2-4/humming.html

Fawcett, T. and Provost, F. (1996). **Combining data mining and machine learning for effective user proling**. In Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96), p. 8-13.

Fisch E. (1996). **Intrusion Damage Control and Assessment: A Taxonomy and Implementation of Automated Responses to Intrusive Behavior.** PhD thesis, A&M University, Texas, A&M University, College Station, Texas.

Forrest, S., Hofmeyr, S., Somayaji, A. and Longstaff, T. (1996). **A Sense of Self for Unix Processes**. In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, p. 120-128. Disponible en http://www.cs.unm.edu/~forrest/papers.html.

Gragg, S. (1996). **Session 7: New Ideas**. Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD-IV). Monterey, Nov. 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session7.html.

Heberlein, L. and Bishop, M. (1996). **Attack Class: Address Spoofing**. In Proceedings of The 19th National Information Security Conference. Disponible en http://seclab.cs.ucdavis.edu/papers.html

Koob, G. (1996). **Research Challenges to Operating System Security**. Proceedings of the DARPA/NSA Workshop on Operating System Security. May 22-23. Disponible en http://www.arpa.mil/itofProceedings/OS_Security/challenges/ challenges_long.html.

Kuykendall, D. (1996). **DIDS—Re: Intro; Question**. Disponible en http://www.geek-girl.com/ids/0790.html

Levitt, K. (1996). **Executive Summary**. Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, Nov. 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/exec_summ.html.

Levitt, K. (1996). **Session 2: Intrusion Detection Technology for Small-Scale Systems.** Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, CA, Nov. 12-14, 1996. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session2.html.

Lindqvist, U. (1996). **Observations on the Nature of Computer Security Intrusions**. Licentiate thesis 253L, School of Electrical and Computer Engineering, Chalmers University of Technology, Göteborg. Disponible en http://www.ce.chalmers.se/staff/jonsson/pubs/ul-lic.pdf

Lindqvist, U., Olovsson, T., and Jonsson, E. (1996). **An Analysis of a Secure System Based on Trusted Components.** In Proceedings of the Eleventh Annual Conference on Computer Assurance (COMPASS '96), Gaithersburg, June 17-21, p. 213-223. Disponible en http://www.ce.chalmers.se/staff/jonsson/pubs/comp96ul.pdf

Mé, L. (1996). **Genetic AIgorithms, a Biologically Inspired Aproach for Security Audit Trails Analysis**. Short paper, 1996 IEEE Symposium on Security and Privacy.

Mitchell, Ch. (1996). **Models for the Design of Human Interaction with Complex Dynamic Systems**. Disponible en http://www.isye.gatech.edu/~cm/papers/model_requirement.10.96.html

Moran, D. (1996). **Future Directions for Intrusion Detection**. Disponible en http://www.ai.sri.com/~debri/presentations/idwk9507/idwk9507.html

Porras, Ph. and Neumann, P. (1996). **EMERALD: Conceptual Overview Statement.** Disponible en http://www.sdl.sri.com/papers/emerald-position1/

Proctor, P. (1996). **Computer Misuse Detection System (CMDS) Concepts.** Disponible en http://cpits-web04.saic.com/satt.nsf/externalbycat

Pu, C., Black, A., Cowan, C. and Walpole, J. (1996). **A Specialization Toolkit to Increase the Diversity of Operating Systems.** In Proceedings of the 1996 ICMAS Workshop on Immunity-Based Systems.

Puketza, N., Zhang, K., Chung, M., Mukherjee, B. and Olsson, R. (1996). **A Methodology for Testing Intrusion Detection Systems**. Software Engineering, 22(10), p. 719-729. Disponible en http://seclab.cs.ucdavis.edu/papers.html.

Rasmusson, A. and Jansson, S. (1996). **Personal Security Assistance for Secure Internet Commerce**. Disponible en http://www.sics.se/

Samfat, D. (1996). **Architecture de sécurité pour réseaux mobiles**. PhD thesis, Ecole Nationale des Télécommunications de Paris.

Sawyer, J., Minsk, B. and Bisantz, A. (1996). **User Models and System Models: A Modeling Framework for Fault Diagnosis in Complex Systems**. Disponible en http://www.eng.buffalo.edu/~bisantz/pubs/um96pap.html

Schaefer, M. and Levitt, K. (1996). **Session 5: New Environments for Intrusion Detection.** In Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, Nov. 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session5.html.

Sharps, J. (1996). **Session 1: Policy-Driven Intrusion Detection and the Insider Threat.** Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, Nov. 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session1.html.

Sobirey, M. (1996). **The Intrusion Detection System Am**. Disponible en http://www-rnkslnformatik.tu-cottbus.de/~sobirey/aide.html.

Sobirey, M., Richter, B. and Koenig, H. (1996). **The Intrusion Detection System Am Architecture, and experiences in automated audit analysis**. In Proceedings of the IFIP TC6/ TC11 International Conference on Communications and Multimedia Security (CMS'96).

Spafford, G. (1996). **Session 4: Intrusion Detection in the Large**. In Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey, Nov. 12-14. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session4.html.

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**. In Proceedings of the 19th National Information Systems Security Conference. Disponible en http://seclab.cs.ucdavis.edu/papers.html

Sundaram, A. (1996). **An Introduction to Intrusion Detection**. Disponible en http://www1.acm.org/crossroads/xrds2-4/intrus.html

Touch Technologies (1996). **INTOUCH INSA—Network Security Agent**. Disponible en http://www.ttisms.com/tti/nsa_www.html

Varshney, P. (1996). **Distributed Detection and Data Fusion**. New York, Springer Verlag.

Wee, C. and Heberlein, T. (1996). **Session 3: New Attacks and New Twists on Existing Attacks.** Proceedings of the 4th Workshop on Future Direction in Computer Misuse and Anomaly Detection (CMAD IV). Monterey. Disponible en http://seclab.cs.ucdavis.edu/cmad/4-1996/session3.html.

White, G. and Pooch, V. (1996). **Cooperating Security Managers: distributed intrusion detection systems.** Computers & Security, 15 (5), p. 441-450.

White, G.; Fisch, E.; and Pooch, U. (1996). **Cooperating Security Managers: A Peer-Based Intrusion Detection System**. IEEE Network, 10 (1), p. 20-23.

5. INTRUSION DETECTION IN 1997

Ammann, P., Jajodia, S., McCollum, C. and Blaustein, B. (1997). **Surviving Information Warfare Attacks on Databases.** In Proceedings of the 1997 IEEE Symposium on Security and Privacy.

Bishop, M., Cheung, S. and Wee, Ch. (1997) **The Threat from the Net**. IEEE Spectrum 34, 8 (August), p. 56-63. Disponible en http://seclab.cs.ucdavis.edu/papers.html.

Cansian, A., Moreira, E., and Carvalho, A. (1997). **Network Intrusion Detection using Neural Networks**. In Proceedings of the International Conference on Computational Intelligence and Multimedia Aplications (ICCMA '97), p. 276-280.

Computer Science Laboratory (1997). **History of Intrusion Detection at SRI/CSL.** Disponible en http://www2.csl.sri.com/intrusion/intrusion-main.html

Cowan, C. and Pu, C. (1997). **Irnmunix: Survivability Through Specialization**. In Proceedings of the SEI Information Survivability Workshop.

Cresson-Wood, Ch. (1997). **Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies**. Sausalito, Baseline Software, 1997.

D'haeseleer, P., Forrest, S. and Helman, P. (1997). **A Distributed Approach to Anomaly Detection.** Disponible en http://www.cs.unm.edu/~forrest/papers.html (1997).

Dates, T., Jensen, D. and Caben, P. (1997). **Automatically Acquiring Rules for Event Correlation from Event Logs**. Technical Report 97-14, Dept. of Computer Science, University of Massachusetts.

Denning, D. (1997). **An Intrusion Detection Model**. IEEE Transactions on Software Engineering (SE-13), 2 (February), p. 222-232.

D'haeseleer, P., Forrest, S. and Helman, P. (1997). **A distributed aproach to anomaly detection**. Disponible en ftp://ftp.cs.unm.edu/pub/forrest/negselection97.ps.

Elgin, B. (1997). **Risky Business**. Disponible en http://www.zdnet.com/devhead/stories/articles/0,4413,1600421,00.html

Firth, R. (1997). **Detecting Signs of Intrusion**. (CMU/SEISIM-001). Pittsburgh, Software Engineering Institute, Carnegie Mellon University. Disponible en http://www.cert.org/security-improvement/modules/m01.html.

Forrest, S., Hofmeyr, S. and Somayaji, A. (1997). **Computer Immunology**. Communications of the ACM, 40(10), p. 88-96. Disponible en http://www.cs.unm.edu/~forrest/papers.html.

Fyodor. (1997). **The Art of Port Scanning**. Disponible en http://www.insecure.org/nmap/nmap_doc.html

Guttman, B. and Bagwill, R. (1997). **NIST Special Publication—Internet Security Policy: A Technical Guide**. Disponible en http://csrc.nist.gov/isptg/

Guttman, B. and Bagwill, R. (1997). **NIST Special Publication—Internet Security Policy: A Technical Guide—II.** Disponible en http://csrc.nist.gov/isptg/pdf/00CoverPage.pdf

Guttman, B. and Bagwill, R. (1997). **NIST Special Publication—Internet Security Policy: A Technical Guide—III.** Disponible en http://csrc.nist.gov/isptg/pdf/01Introduction.pdf

Guttman, B. and Bagwill, R. (1997). **NIST Special Publication—Internet Security Policy: A Technical Guide—IV.** Disponible en http://csrc.nist.gov/isptg/pdf/01TOC.pdf

Guttman, B. and Bagwill, R. (1997). **NIST Special Publication—Internet Security Policy: A Technical Guide—V**. Disponible en http://csrc.nist.gov/isptg/pdf/02GeneralPolicy.pdf

Hale, J. and Shenoi, S. (1997). **Catalytic Inference Analysis: Detecting Inference Threats due to Knowledge Discovery**. In Proceedings of the 1997 IEEE Symposium on Security and Privacy.

Hall, D. and Llinas, J. (1997). **An Introduction to Multisensor Data Fusion.** Proceedings of the IEEE 85, 1 (January), p. 6- 10.

Hashii, B. and Wee, C. (1997). **Audit Counter measures**. Disponible en http://seclab.cs.ucdavis.edu/misuse/Reports/ ACM-draft.pdf.

Hedbom, H., Lindskog, S. and Jonsson, E. (1997). **Preliminary Evaluation of the Security of a Non-Distributed Version of Windows NT**. In Proceedings of the Second Nordic Workshop on Secure Computing Systems, Helsinki, November 6-7. Disponible en http://www.ce.chalmers.se/staff/jonsson/nordsec-nt-final.fm55.pdf

Herringshaw, C. (1997). **Detecting Attacks on Networks**. IEEE Computer, 30(12), p. 16-17.

Howard, J. (1997). **A Taxonomy of Computer and Network Attacks. An analysis of security incidents on the Internet 1989-1995**. PhD thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania. Disponible en http://www.cert.org/research/JHThesis/Chapter6.html

Hunteman, W. (1997). **Automated Information System (AIS) Alarm System**. In Proceedings of the 20 th National Information Systems Security Conference, p. 394-405.

Ko, C., Ruschitzka, M. and Levitt, K. (1997). **Execution Monitoring of Security-Critical Programs in a Distributed System: A Specification-based Aproach.** In Proceedings of the 1997 IEEE Symposium on Security and Privacy.

Kosoresow, A. and Hofmeyr, S. (1997). **Intrusion Detection via System Call Traces**. IEEE Software, 14(5), p. 35-42.

Jonsson, E. and Olovsson, T. (1997). **A quantitative model of the security intrusion procese based on attacker behavior**. IEEE Transactions on Software Engineering, 23(4), p. 235-245. Disponible en http://www.ce.chalmers.se/staff/jonsson/a-quantitative-model-of-security-intrusions.ps.gz

Jou, Y., Gong, F., Sargor, C., Wu, S. and Cleaveland, R. (1997). **Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure**. Technical Report CDRL AO05, MCNC.

Lawrence Livermore National Laboratory, Sandia National Laboratories. (1997). **Intrusion Detection and Response**. Disponible en http://all.net/journal/btbs.ids.html

Lane, T. and Brodley, C. (1997). **An Aplication of Machine Learning to Anomaly Detection.** In Proceedings of the 20th National lnformation Systems Security Conference, p. 366-380.

Lane, T. and Brodley, C. (1997). **Detecting the Abnormal: Machine Learning in Computer Security**. Technical Report ECE97-1, Department of Electrical and Computer Engineering, Purdue University.

Lane, T. and Brodley, C. (1997). **Sequence Matching and Learning in Anomaly Detection for Computer Security**. In Proceedings of the AAAl-97 Workshop on Al Aproaches to Fraud Detection and Risk Management, p. 43-49.

Lebegue, P. (1997). **Extraction de connaissances pour la securité des systemes informatiques**. Raport de DEA d'fuformatique, Laboratoire de Recherche en fuformatique, Université Paris-Sud, France.

Lee, W., Stolfo, S. and Chan, P. (1997). **Learning Patterns from Unix Process Execution Traces for Intrusion Detection**. Working Notes AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management. Disponible en http://cs.fit.edu/~pkc/papers/aaai97.ps

Lemos, R. (1997). **ActiveX, Java Holes a Product of Internet Time**. Disponible en http:www.zdnet.com/zdnn.content/0910/zdnn0008.html (1997).

Lin, T. (1997). **Behavioral Clustering and Statistical lntrusion Detection**. Master's thesis, Department of Computer Science, College of Arts and Sciences, Florida State University.

Lindqvist, U. and Jonsson, E. (1997). **How to Systematically Classify Computer Security Intrusions**. In Proceedings of the 1997 IEEE Symposium on Security and Privacy. Oakland, May 4-7. Los Alamitos, CA: IEEE Computer Society Press. Disponible en http://www.ce.chalmers.se/staff/ulfl/sp97ul.pdf

Malkhi, D. and Reiter, M. (1997). **Unreliable intrusion detection in distributed computations**. In Proceedings of the 10th IEEE Computer Security Foundations Workshop.

McLain, F. (1997). **The Exploder Control Frequently Asked Questions.** Disponible en http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm

Mé, L., Alanou, V. and Abraham, J. (1997). **Utilisation de cartes de Kohonen pour détecter des intrusions dans un systeme informatique: une pré-étude**. Valgo, 1(5), p. 7-16.

Mimestar (1997). **SecureNet PRO Frequently Asked Questions**. Disponible en http://www.mimestar.com/html/product_faq.htm

Mimestar (1997). **SecureNet PRO: The Complete Network Security Solution.** Disponible en http://www.mimestar.com/html/products.htm

Mounji, A. (1997). **Languages and Tools for Rule-Based Distributed Intrusion Detection**. PhD thesis, Facultè Universitaire Notre de la Paix de Namur, Belgium. Disponible en ftp://ftp.info.fundp.ac.be/pub/users/amofthesis.ps.Z

Mounji, A. and Charlier, B. (1997). **Continuous Assessment of a Unix Configuration: Integrating Intrusion Detection and Configuration Analysis**. In Proceedings of the IEEE ISOC'97 Symposium on Network and Distributed Systems Security.

Network Flight Recorder (1997). **The Network Flight Recorder in Action!.** Disponible en http://www.nfr.net/products/technology.html

Network General Corporation (1997). **A Network Visibility Guide—Protecting Your Network: The Choice Between Active and Static Security Technologies**. Disponible en http://www.3dg.com/cybercop/ccvg/ccvg1.html

Network General Corporation (1997). **CyberCop Datasheet**. Disponible en http://www.3dg.com/cybercop/p_s/data1.html (1997).

NSTAC (1997). **Intrusion Detection Subgroup Report**. Disponible en http://jwww.ncs.gov/nstac/FIDSGREP.pdf.

Openheimer, D. and Martonosi, M. (1997). **Performance Signatures: A Mechanism for Intrusion Detection**. In Proceedings of the 1997 IEEE Information Survivability Workshop.

Peter, D. (1997). **Intrusion Detection Systems.** Disponible en http://www.pdaconsulting.com/ids.htm

Porras, Ph. and Neumann, P. (1997). **EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances**. In Proceedins of the 20th National Information Systems Security Conference. Disponible en http://www.sdl.sri.com/papers/emerald-niss97/ y también en http://www2.csl.sri.com/emerald/concepts.html

Powell, D., Schuster, S. and Amoroso, E. (1997). **Local Area Detection of Incoming War Dial Activity**. Disponible en http://www.att.com/isc/docs/war_dial_detection.pdf.

Price, K. (1997). **Host-based Misuse Detection and Conventional Operating Systems' Audit Data Collection**. Master's thesis, Purdue University.

Puketza, N., M.Chung, Olsson, R. and Mukherjee, B. (1997). **A Software Platform for Testing Intrusion Detection Systems.** IEEE Software, 14(5), p. 43-51. Disponible en http://seclab.cs.ucdavis.edu/papers.html

Ranum, M. (1997). **Security on Internet Time**. Disponible en http://www.clark.net/pub/mjr/pubs/index.shtml

Ranum, M., Landfield, K., Stolarchuk, M., Sienkiewicz, M., Lambeth, A. and Wall, E. (1997). **Implementing A Generalized Tool For Network Monitoring**. In Proceedings of the Eleventh Systems Administmtion Conference (LISA '97). Disponible en http://www.nfr.net/forum/publications/LISA-97.htm

Samfat, D. and Molva, R. (1997). **IDAMN : an Intrusion Detection Architecture for Mobile Networks**. IEEE Journal on Selected Areas in Communications.

Sandhu, R. and Samarati, P. (1997). **Authentication, Access Control, and Intrusion Detection**. In Tucker, A. *The Computer Science and Engineering Handbook*, p. 1929-1948. CRC Press.

Seminerio, M. (1997). **Hackers Claim ActiveX Can Be Used to Pilfer Money Online**. Disponible en http://www.zdnet.com/devhead/stories/articles/0,4413,1600422,00.html

Sobirey, M., Fischer-Hubner, S. and Rannenberg, K. (1997). **Pseudonymous Audit for Privacy Enhanced Intrusion Detection**. In Proceedings of the IFIP TC11 13th International Information Security Conference (SEC'97), Copenhagen, IFIP, Chapman & Hall, p. 151-163.

Somayaji, A., Hofmeyr, S. andForrest, S. (1997). **Principles of a Computer Immune System.** In Proceedings of the 1997 New Security Paradigms Workshop, p. 75-82. Disponible en http://www.cs.unm.edu/~forrest/papers.html

SonOffire. (1997). **Wardialling.** Disponible en http://newbie.darkridge.com/logs97/10.31.wardial.txt

Stolfo, S., Fan, W., Lee, W., Prodromidis, A. and Chan, P. (1997). **Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results**, Working Notes AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management. Disponible en http://cs.fit.edu/~pkc/papers/kdd97-fraud.ps

Stolfo, S., Prodromidis, A., Tselepis, S., Lee, W., Fan, W. and Chan, P. (1997). **JAM: Java Agents for Meta-Learning over Distributed Databases.** In Proceedings of the Third International Conference on Knowledge Discovery and Data Mining, p. 74-81. Disponible en http://cs.fit.edu/~pkc/papers/kdd97-jam.ps

Wingfield, N. (1997). **Java, ActiveX Security Elusive**. Disponible en http://news.cnet.com/news/0-1003-200-317102.html

Wu, S., Wang, F., Vetter, B., Cleaveland, R., Jou, Y., Gong, F. and Sargor, C. (1997). **Intrusion Detection for Link-State Routing Protocols**. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland.

6. INTRUSION DETECTION IN 1998

Adaptive Network Security Alliance (1998). **The Adaptive Network Security Alliance: Industry Leaders Teaming to Improve Enterprise Security**. Disponible en http://ansa.iss.net/

Amoroso, E. and Kwapniewski, R. (1998). **Selection Criteria for Intrusion Detection Systems**. In Proceedings of the 14th Annual Computer Security Aplications Conference (ACSAC'98). Pheonix, December 7-11,Los Alamitos, IEEE Computer Society Press.

Anderson, R. and Khattak, A. (1998). **The Use of Information Retrieval Techniques for Intrusion Detection**. In Proceedings of the First International Workshop on Recent Advances in fntrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Arndt, J. and Österdahl, T. (1998). **Network Security in Distributed Systems Using CORBA.** Disponible en http://www.etek.chalmers.se/~e3torb/CORBASecurity.pdf

Axelsson, S., Lindqvist, U., Gustafson, U. and Jonsson, E. (1998). **An Aproach to UNIX Security Logging**. In Proceedings of the 21st National Information Systems Security Conference (NISSC'98), Arlington, October 5-8. National Institute of Standards and Technology/National Computer Security Center, p. 62-75. Disponible en http://www.ce.chalmers.se/staff/jonsson/pubs/nissc98a.pdf

AXENT Technologies (1998). **Netprowler.** Disponible en http://www.axent.com/product/netprowler/default.htm

AXENT Technologies (1998). **Netprowler—II.** Disponible en http://www.axent.com/product/netprowler/npbrochure.htm

Balasubramaniyan, J., Garcia-Fernandez, J., Isacoff, D., Spafford, E. and Zamboni, D. (1998). **An Architecture for Intrusion Detection using Autonomous Agents (Coast TR 98-05).** West Lafayette, COAST Laboratory, Purdue University. Disponible en http://www.cs.purdue.edu/coast/projects/autonomous-agents.html.

Barrus, J. and Rowe, N. C. (1998). **A Distributed Autonomous-Agent Network-Intrusion Detection and Response System.** In Procedings of the 1998 Command and Control Research and Technology Symposium.

Bauer, D. and Koblentz, M. (1988). **NillX, a RealTime Intrusion Detection Expert System**. In Proceedings of the USENIX'88 Conference, p. 261-272.

Bonifácio, J. (1998). **An Adaptive Intrusion Detection System Using Neural Networks**. In Proceedings of the IFIP World Computer Congress—Security in Information Systems (IFIP-SEC '98). Viena, Austria, August/September. Disponible en http://www. icm-sc.sc.usp.br/~andre/papers.html.

Bonifácio, J. (1998). **Neural Networks Applied in Intrusion Detection Systems**. In Proceedings of the IEEE World Congress on Computational Intelligence (WCCI '98). Anchorage, May. Disponible en http://www.icmsc.sc.usp.br/~andre/papers.html.

Boulanger, A. (1998). **HAXOR A Passive Network Monitor /Intrusion Detection Sensor**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Brackney, R. (1998). **Cyber-Intrusion Response**. In Proceedings of the 17th IEEE Symposium on Reliable Distribution Systems. West Lafayette, October 20-23, 1990, Los Alamitos, IEEE Computer Society Press, p. 413-415

Bradley, K., Cheung, S., Puketza, N., Mukherjee, B. and Olsson, R. (1998). **Detecting Disruptive Routers: A Distributed Network Monitoring Aproach**. In Proceedings of the 1998 IEEE Symposium on Security and Privacy, p. 115-124. Disponible en http://seclab.cs.ucdavis.edu/papers/oakland98-paper.pdf

Brushi, D., Rosti, E. and Banfi, R. (1998). **A Tool for Pro-active Defense Against the Buffer Overrun Attack**. In Proceedings of the 1998 ESORICS Conference, in Lecture Notes in Computer Science, number 1485,Springer-Verlag, Berlin, p. 17-31.

Brutch, P., Brutch, T. and Pooch, U. (1998). **Electronic Quarantine: An Automated Intruder Response Tool.** In Proceedings of the 1998 Information Survivability Workshop (ISW'98).

Burgess, M. (1998). **Computer Immunology**. In Proceedings of the 12th Systems Administration Conference (LISA '98).

Büschkes, R. and Kesdogan, D. (1998)**. Intrusion Detection and User Privacy A Natural Contradiction?** In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Buschkes, R., Kesdogan, D. and Reichl, P. (1998). **How to Increase Security in Mobile Networks by Anomaly Detection**. In Proceedings of the 14th Annual Computer Security Aplications Conference (ACSAC'98).

Cannady, J. (1998). **Artificial Neural Networks for Misuse Detection**. In Proceedings of the 21st National Information Systems Security Conference. Arlington, Oct. 5-8. Disponible en http://csrc.nist.gov/nissc/1998/proceedings/paperF13.pdf.

Cannady, J. (1998). **The Aplication of Artificial Neural Networks to Misuse Detection: Initial Results.** In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://jwww.raid-symposium.org/raid98.

Cerias (1998). **Coast - audit trails format.** Project description. Disponible en http://www.cerias.purdue.edu/coast/projects/audit-trailsformat.html

CERT/CC. (1998). **CERT Advisory CA-98.01**. Disponible en http://www.cert.org/advisories/CA-98.01.smurf.html

CERT/CC. (1998). **Establish a Policy and Set of Procedures that Prepare Your Organization to Detect Signs of Intrusion**. Disponible en http://www.cert.org/security-improvement/practices/p040.html

CERT/CC. (1998). **Security for Information Technology Service Contracts. (CMU/SEI-SIM-003).** Disponible en http://www.cert.org/security-improvement/modules/m03.html

Chan, P. and Stolfo, S. (1998). **Toward Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection.** In Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining, p. 164-168. Disponible en http://cs.fit.edu/~pkc/papers/kdd98.pdf

Chan, P. and Stolfo, S. (1998). **Learning with Non-uniform Class and Cost Distributions: Effects and a Distributed Multi-classifier Approach,** In Working Notes KDD-98 Workshop on Distributed Data Mining, p. 1-9. Disponible en http://cs.fit.edu/~pkc/papers/ddm98.ps

Check Point Software Technologies (1998). **OPSEC Alliance Solutions Center.** Disponible en http://www.checkpoint.com/opsec/ (1998).

Chung, C., Gertz, M. and Levitt, K. (1998). **Aplication Level Misuse Detection in Relational DBMS**. In Proceedings of the 1998 UC Davis Student Workshop on Computing.

Cisco. (1998). **NetRanger Intrusion Detection System**. Disponible en http://www.cisco.com/warp/public/778/security/netranger/netra_ds.htm

Cisco. (1998). **NetRanger—General Concepts**. Disponible en http://www.cisco.com/warp/public/778/security/netranger/netra_qp.htm

Cisco. (1998). **The NetRanger Intrusion Detection System**. Disponible en http://www.cisco.com/warp/public/778/security/netranger/prodlit/netra_ov.htm

Clark, T. (1998).**Navy Fights New Hack**. (CNET News.com). Disponible en http://news.cnet.com/news/0-1003-200-333601.html?tag=st.cn.1

Cohen, F. (1998). **50 Ways to Defeat Your Intrusion Detection System**. Disponible en http://all.net/journal/netsec/9712.html.

Cohen, F. (1998).**A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model**. Disponible en http://all.net/journal/ntb/cause-and-effect.html

Colombo, A. (1998). **Better installations with photo beams.** SDM: Security Distributing & Marketing, 28 (13), p. 56-59.

Computer Security Institute (1998). **Tough Questions for IDS Vendors**. Disponible en http://www.gocsi.com/IDSques.htm

Cowan, C., Pu, C., Maier, D., Hinton, H., Bakke, P., Beattie, S., Grier, A., Wagle, P. and Zhang, Q. (1998). **StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks**. In Proceedings of the 7th USENIX Security Conference.

Daniels, T. and Spafford, E. (1998). **Problems with Network based Intrusion Detection for Enterprise Computing**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

DARPA and Air Intelligence Agency (1998). **CSAP21—Information Protection into the 21st Century.** Disponible en http://www.darpa.mil/isofia/ssd/FutureTech/sld001.htm

DARPA. (1998). **Darpa ITO Sponsored Research—Challenges**. Disponible en http://www.darpa.mil/itofresearch/lss/challenges.html

DARPA. (1998). **Intrusion Detection PI Meeting December 1998—Agenda.** Disponible en http://www.dyncorpis.com/darpa/meetings/id98dec/agenda.html

DARPA. (1998). **Intrusion Detection PI Meeting February 1998—Agenda and Presentations.** Disponible en http://www.dyncorpis.com/darpa/meetings/id98feb/agenda.html

Debar, H., Dacier, M. and Wespi, A. (1998). **Reference Audit Information Generation for Intrusion Detection Systems**. Internal RZ 2997, IBM Zurich Research Laboratory.

Debar, H., Dacier, M. and Wespi, A. (1998). **An Experimentation Workbench for Intrusion Detection Systems** RZ 2998. Zurich, Switzerland: IBM Research Division. Disponible en http://www.zurich.ibm.com/pub/sti/Security/extern/gsal/docs/.

Debar, H., Dacier, M., Nassehi, M.and Wespi, A. (1998). **Fixed vs. Variable-Length Patterns for Detecting Suspicious Process**. In Proceedings of the 1998 ESORICS Conference, in Lecture Notes in Computer Science, number 1485, Springer-Verlag, Berlin, p. 1-16.

Deswarte, Y. (1998). **Contribution of Quantitative Security Evaluation to Intrusion Detection**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

DuMouchel, W. and Schonlau, M. (1998). **A Comparison of Test Statistics for Computer Intrusion Detection Based on Principal Components Regression of Transition Probabilities**. In Proceedings of the 30th Symposium on the Interface: Computing Science and Statistics.

DuMouchel, W. and Schonlau, M. (1998). **A fast computer intrusion detection algorithm based on hypothesis testing of command transition probabilities**. In Proceedings of the Fourth International Conference of Knowledge Discovery and Data Mining (KDD'98), p. 189-193.

En Garde Systems (1998). **T-sight, the First Advanced Intrusion Investigation and Response Tool for Windows NT.** Disponible en http://engarde.com/software/t-sight/overview.html

Endler, D. (1998). **Intrusion Detection Aplying Machine Learning to Solaris Audit Data**. In Proceedings of the 14th Annual Computer Security Aplications Conference (ACSA C'98).

Erlinger, M. and Staniford-Chen, S. (1998). **IDWG Charter**. Disponible en http://www.zurich.ibm.com/Technology/Security/extern/idwg/charter.html

Escamilla, T. (1998). **Intrusion Detection (Network Security Beyond the Firewall)**. New York, Wiley Computer Publishing.

Ferraiolo, K. (1998). **Tutorial: The Systems Security Engineering Capability Maturity Model**. Disponible en http://csrc.nist.gov/nissc/1998/proceedings/tutorB5.pdf

Fish, E. and Richardson P. (1998). **The Emerging Law of Computer Networks—Finding Out What's There: Technical and Legal Aspects of Discovery.** Disponible en http://www.fr.com/publis/f_paper21.html

Floyd, S. (1998). **LBNL's Network Research Group**. Disponible en http://ftp.ee.lbl.gov/

Foote, S. (1998). **19 Infosecurity Predictions for '99.** Disponible en http://www.infosecuritymag.com/nov/cover.htm

Foote, S. (1998). **How Anti-hacker Software Could Have Kept Me Out of Your Company.** Disponible en http://www.netect.com/whitepaper.html

Franklin, L., Marzullo, K., Namprempre, C., Sussman, J., Krishnamurthy, R., Lin, M. and Ricciardi, A. (1998). **Combining Optimism and Intrusion Detection**. Technical Report **TR** CS98-605, Department of Computer Science and Engineering, University of California at San Diego.

Frincke, D. and Auernheimer, B. (1998). **Minitrack Introduction: Techniques for Secure System Development.** In Proceedings of the 31st Hawaii International Conference on System Science, p. 304-306.

Frincke, D., Tobin, D. and McConnell, J. (1998). **Research Issues in Cooperative Intrusion Detection Between Multiple Domains**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.csds.uidaho.edu/~hummer/html/papers.html.

Fyodor. (1998). **Remote OS Detection via TCP/IP Stack Fingerprinting**. Disponible en http://128.196.109.24/nmap/nmap-fingerprinting-article.txt

Gaudin, S. (1998). **Hack gain in malice, frequency.** Computerworld, 32 (41), p. 37-38.

Gérard, F. (1998). **Définition et implémentation d'un langage déclaratif pour l'analyse d'audit trails.** Master's thesis, Computer Science Institute, University of Namur.

Ghosh, A. and O'Connor, T. (1998). **Analyzing Programs for Vulnerability to Buffer Overrun Attacks**. In Proceedings of the 21st National Information Systems Security Conference (NISSC'9).

Ghosh, A., O'Connor, T. and McGraw, G. (1998). **An Automated Aproach for Identifying Potential Vulnerabilities in Software**. In Proceedings of the 1998 IEEE Symposium on Security and Privacy.

Ghosh, A., Wanken, J. and Charron, F. (1998). **Detecting Anomalous and Unknown Intrusions Against Programs**. In Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC'98). Phoenix, December 7-11. Los Alamitos, IEEE Computer Society Press, p. 259-267.

Girardin, L. and Brodbeck, D. (1998). **A Visual Aproach for Monitoring Logs**. In Proceedings of the 12th Systems Administration Conference (LISA '98).

Glave, J. (1998). **Back Orifice a Pain in the...?.** Disponible en http://www.wired.com/news/technology/0,1282,14092,00.html

Graf, I. (1998). **Results of DARPA 1998 Offline Intrusion Detection Evaluation.** Presentation at MIT Lincoln Laboratory PI Meeting, December 15. Disponible en http://ideval.ll.mit.edu/results-html-dir y en http://www.dyncorpis.com/darpa/meetings/id98dec/files/mit-ll.pdf.

Grundschober, S. and Dacier, M. (1998). **Design and Implementation of a Sniffer Detector**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Hancock, B. (1998). **Security Mailing Lists**. Computers & Security, 17 (6), p. 465-468.

Hedbom, H., Lindskog, S., Axelsson, S. and Jonsson, E. (1998). **A Comparison of the Security of Windows NT and UNIX.** In Proceedings of the Third Nordic Workshop on Secure IT Systems (NORD-SEC'98), Trondheim, November 5-6. Disponible en http://www.ce.chalmers.se/staff/sax/nt-vs-unix.pdf

Helmer, G., Wong, J., Honavar, V. and Miller, L. (1998). **Intelligent Agents for Intrusion Detection.** In Proceedings of the 1998 IEEE Information Technology Conference, Environment for the Future. Syracuse, Sept. 1-3. New York, IEEE, p. 121-124. Disponible en http://www.palisadesys.com/~ghelmer/Papers/ieee-98.ps

Ho, Y., Frinke, D. and Tobin, D. (1998). **Planning, Petri Nets, and Intrusion Detection.** In Proceedings of the 21st National Information Systems Security Conference, October, p. 346-361. Disponible en http://www.csds.uidaho.edu/director/petrinets.pdf y también en http://www.csds.uidaho.edu/~hummer/html/papers.html

Hofmeyr, S., Forrest, S. and D'haeseleer, P. (1998). **An Immunological Aproach to Distributed Network Intrusion Detection**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Hofmeyr, S., Forrest, S. and Somayaji, A. (1998). **Intrusion detection using sequences of system calls.** Journal of Computer Security, 6 (3), p. 151-180.

Hoglund, A., Hatonen, K. and Tuononen, T. (1998). **A UNIX Anomaly Detection System using Self-Organising Maps**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.zurich.ibm.com/pub/Other/RAID/Prog_RAID98/Full_Papers/hoglund_slides.html/index.htm

Horizon. (1998). **Defeating Sniffers and Intrusion Detection Systems**. Phrack Magazine 8, 54 (Dec. 25), p. 10-12. Disponible en http://pulhas.org/phrack/54/P54-10.html.

Hosmer, C. (1998). **Announcing the Formation of New High Technology Software Company.** Disponible en http://www.wetstonetech.com/pr9801.htm

Howard, J. and Longstaff, T. (1998). **A Common Language for Computer Security Incidents** (SAND98-8667). Albuquerque, Sandia National Laboratories, October. Disponible en http://www.cert.org/nav/Reports.html.

Huang, M. and Wicks, T. (1998). **A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Hurwitz Group (1998). **Information Security: Assessing Risks and Detecting Intrusions.** Disponible en http://www.summitonline.com/security/papers/hurwitz3.html

IBM Emergency Response Service and the Joint Research Centre of the EC. (1998). **First International Workshop on the Recent Advances in Intrusion Detection (RAID 98).** Disponible en http://www.zurich.ibm.com/pub/Other/RAID/RAID98(1998).

Ieong, R. and Pang, J. (1998). **Enhanced Network Intrusion Detection in a Smart Enterprise Environment**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Information Assurance Technology Analysis Center (1998). **Information Assurance Tools Database**. IATAC Information Assurance Technology Newsletter 1/3 (Spring), p. 4-5.

Internet Security Systems (1998). **Network- vs. Host-based Intrusion Detection**. Disponible en http://solutions.iss.net/products/whitepapers/nvh_ids.pdf

Intrusion detection & controls. (1998). **Security: For Buyers of Products,** Systems & Services, 35 (11), p. 106-114.

Irwin, V., Northcutt, S. and Ralph, B. (1998). **Building a Network Monitoring and Analysis Capability—Step by Step.** Disponible en http://www.nswc.navy.mil/ISSEC/CID/step.htm

Jonsson, E. (1998). **An Integrated Framework for Security and Dependability.** In Proceedings of the New Security Paradigms Workshop 1998, Charlottesville, September 22-25. Disponible en http://www.ce.chalmers.se/staff/jonsson/Paradigms-nspw98-print.rev0001.fm55.pdf

Jordan, S. (1998). **Discrete-Event Simulation for the Design and Evaluation of Physical Protection Systems**. In Proceedings of the 1998 Winter Simulation Conference. Disponible en http://www.acm.org/pubs/articles/proceedings/simulation/293172/p899-jordan/p899-jordan.pdf

Jou, Y., Wu, S., Gong, F., Sargor, C. and Cleaveland, R. (1998). **Design and Implementation of an Intrusion Detection System for OSPF Routing Networks**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAm'98). Disponible en http://jwww.raid-symposium.org/raid98.

Kahn, C., Porras, P., Staniford-Chen, S. and Thng, B. (1998). **A Common Intrusion Detection Framework.** Disponible en **http**://wwwisi.edujgostjcidfjpapersjcidf-jcs.ps y en http://www2.csl.sri.com/intrusion

Kemmerer, R. (1998). **NSTAT: A Model-based Real-time Network Intrusion Detection System.** Technical Report TRCS97-18, University of California, Santa Barbara. Disponible en http://www.cs.ucsb.edu/~kemm/netstat.html/documents.html .

Kemmerer, R. and Mayo, D. (1998). **NetSTAT: A Model-Based Real-Time Intrusion Detection System for Large Scale Heterogeneous Networks—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/E252-0.html

Kerr, D. (1998). **Hacker stoppers?** InformationWeek, n. 678, p. 140-143.

Kerstetter, J. (1998). **Low-Flying Hackers Pose Growing Threat**. Disponible en http://www.zdnet.com/pcweek/stories/news/0,4153,360254,00.html

Kleinwaechter, J. (1998). **The Limitations of Intrusion Detection Systems on High Speed Networks**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Kochmar, J. (1998). **Preparing to Detect Signs of Intrusion**. (CMU/SEI-SIM-005). Pittsburgh, Software Engineering Institute, Carnegie Mellon University. Disponible en http://www.cert.org/security-improvement/modules/m05.html.

Kossakowski, P. (1998). **Responding to Intrusions**. (CMU/SEISIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Disponible en http://www.cert.org/security-improvement/modules/m06.html.

Krsul, I., Spafford, E. and Tripunitata, M. (1998). **An Analysis of Some Software Vulnerabilities**. Proceedings of the 21st National Information Systems Security Conference. Arlington, Oct. 5-8. Disponible en http://csrc.nist.gov/nissc/1998/proceedings/paperD6.pdf.

Krsul, l. (1998). **Software vulnerability analysis**. PhD thesis, Purdue University, West Lafayette, Indiana.

Lane, T. (1998). **Filtering Techniques for Rapid User Classification**. In Proceedings of the AAAl-98/lCML-98 Joint Workshop on Al Aproaches to Time-Series Analysis.

Lane, T. (1998). **Machine Learning Techniques for the Domain of Anomaly Detection for Computer Security** (Coast TR 98-11). West Lafayette, IN: COAST Laboratory, Purdue University. Disponible en http://www.cs.purdue.edu/coast/coast-library.html.

Lane, T. and Brodley, C. (1998). **Aproaches to Online Learning and Concept Drift for User Identification in Computer Security**. In Proceedings of the Fourth lnternational Conference on Knowledge Discovery and Data Mining, p. 259-263.

Lane, T. and Brodley, C. (1998). **Temporal Sequence Learning and Data Reduction for Anomaly Detection.** In Proceedings of the Fifth ACM Conference on Computer and Communications Security, p. 150-158. Disponible en http://www.acm.org/pubs/articles/proceedings/commsec/288090/p150-lane/p150-lane.pdf

Lawrence Livermore National Laboratory Computer Security Technology Center. (1998). **NID Introduction**. Disponible en http://ciac.llnl.gov/cstc/nid/intro.html

Lee, W. and Stolfo, S. (1998). **Data Mining Aproaches for Intrusion Detection**. In Proceedings of the 7th Usenix Security Symposium (SECURITY '98), San Antonio, January. Disponible en http://www.cc.gatech.edu/~wenke/papers/usenix.ps y también en http://www.cs.columbia.edu/~sal/hpapers/USENIX/usenix.html

Lee, W., Stolfo, S. and Mok, K. (1998). **Mining Audit Data to Build Intrusion Detection Models.** In Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining (KDD '98), New York, August. Disponible en http://www.cc.gatech.edu/~wenke/papers/kdd98.ps

Levitt, K. (1998). **Global Guard**. In Proceedings of the DARPA Intrusion Detection PI Meeting. Lexington, Dec. 15-17. Disponible en http://www.dyncorp-is.com/darpa/meetings/id98dec/agenda.html.

Levitt, K. (1998). **GlobalGuard: A Protection Architecture for Survivability of Large Scale, High-Confidence Information Networks—1998 Project Summary.** Disponible en http://www.darpa.mil/itofpsum1998/F783-0.html

Lin, J., Wang, X. and Jajodia, S. (1998). **AbstractionBased Misuse Detection: High-Level Specifications and Adaptable Strategies**. In Proceedings of the Eleventh Computer Security Foundations Workshop.

Lin, M., Marzullo, K. and Ricciardi, A. (1998). **A New Model for Availability in the Face of Self-Propagating Attacks**. In New Sécurity Paradigms Workshop, p. 134-137.

Lin, M., Ricciardi, A. and Marzullo, K. (1998). **On the Resilience of Multicasting Strategies in a Failure-Propagating Environment**. Technical Report PDS-1998-003, UT Austin.

Lindqvist, U. and Jonsson, E. (1998). **A Map of Security Risks Associated with Using COTS.** Computer, 31(6), p. 60-66**.** Disponible en http://www.ce.chalmers.se/staff/jonsson/cots-security.pdf

Lindqvist, U., Kaijser, P. and Jonsson, E. (1998). **The Remedy Dimension of Vulnerability Analysis.** In Proceedings of the 21st National Information Systems Security Conference, Arlington, October 5-8, National Institute of Standards and Technology/National Computer Security Center, p. 91-98. Disponible en http://www.ce.chalmers.se/staff/ulfl/pubs/nissc98l.pdf

Lindqvist, U., Moran, D., Porras, Ph. and Tyson, M. (1998). **Designing IDLE: The Intrusion Data Library Enterprise**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Louvain-la-Neuve, September 14-16. Disponible en http://www.ce.chalmers.se/staff/jonsson/pubs/raid98-slides/index.htm

Lipmann, R., Cunningham, R., Fried, D., Carfinkel, S., Gorton, S., Graf, l., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D. and Zissman, M. (1998). **The 1998 DARPA/ AFRL Off-line Intrusion Detection Evaluation**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://ideval.ll.mit.edu/intro-html-dir.

Lipmann, R., Wyschogrod, D., Webster, S., Weber, D. and Gorton, S. (1998). **Using Bottleneck Verification to Find Novel New Attacks with a Low False Alarm Rate.** In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Lodin, S. (1998). **Intrusion Detection Product Evaluation Criteria**. Disponible en http://members.iquest.net/-swlodin/IDS_Prod_EvalCriteria.ps.

Loscocco, P. (1998). **The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments**. Disponible en http://www.jya.com/paperF1.htm

Loscocco, P. (1998). **The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments (Slides).** Disponible en http://www.cs.utah.edu/~sds/inevit-abs.html

Loyall, J. (1998). **Toolkit for Creating Adaptable Distributed Applications.** Proceedings of the DARPA Intrusion Detection Meeting. Dec. 15-17. Disponible en http://www.dist-systems.bbn.com/projects/OIT.

Lucent Technologies (1998). **Network Intrusion Detection in Action.** Disponible en http://www.lucent.com/dns/library/pdf/brochures/realsecure.pdf

Lunt, T. and Jagannathan, R. (1988). **A Prototype Real-Time Intrusion-Detection Expert System**. In Proceedings of the IEEE Symposium on Security and Privacy, p. 59-66.

Lutz, R., Helmer, G., Moseman, M., Statezni, D. and Tockey, S. (1998). **Safety Analysis of Requirements for a Product Family.** In Proceedings of the Third IEEE International Conference on Requirements Engineering, Colorado Springs. Disponible en http://www.palisadesys.com/~ghelmer/Papers/icree98.ps

Mansur, D. (1998). **Current Trends in the Threat to Computers: From Simple Hacking to Cyber Terrorism**. Disponible en http://doe-is.llnl.gov/SecRes/DOETools/99001latalk.pdf

Maxion, R. (1998). **Measuring Intrusion Detection Systems**. In Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.zurich.ibm.com/pub/Other/RAID/Prog_RAID98/Full_Papers/maxion.pdf.

Maxion, R., Banks, D. and Rocco, S. (1998). **Concerning Invictus: Detection of Unanticipated and Anomalous Events—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/E306-0.html

McClure, S. and Scambray, J. (1998). **Digitals entries**. InfoWorld, 20 (18), p. 1-4.

McConnell, J., Frincke, D., Tobin, D., Marconi, J. and Polla, D. (1998). **A Framework for Cooperative Intrusion Detection**. In Proceedings of the 21st National Inlormation Systems Security Conference (NISSC'98).

Mé, L. (1998). **GASSATA, A Genetic AIgorithm as an Alternative Tool for Security Audit Trails Analysis**. In Proceedings of the First international workshop on the Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/these/these-lm.html.

Medina, M. (1998). **A Layered Framework for Placement of Distributed Intrusion Detection Devices**. In Proceedings of the 21st National Information Systems Security Conference (NISSC'98).

Mell, P. (1998). **Automatic Policy Satisfaction and Verification for Intranet Wide Defense Systems Using Signature Based Intrusion Detection and Response Systems**. Master's thesis, Departement of Computer Science, University of California at Davis.

Moroni, P. (1998). **CERN Network Security Monitor**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Mounji, A. and Charlier, B. (1998). **Tools for Intrusion detection: Results and Lessons Learned from the ASAX Project**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Nassehi, M. (1998). **Anomaly Detection For Markov Models**. Technical Report rz3011, IBM Research Division, Zurich Research Laboratories.

Nassehi, M. (1998). **Characterizing Masqueraders For Intrusion Detection**. Technical Report RZ3003, IBM Research Division, Zurich Research Laboratories.

Naval Surface Warfare Center (1998). **SHADOW Indications Technical Analysis—Coordinated Attacks and Probes**. Disponible en http://www.nswc.navy.mil/ISSEC/CID/co-ordinated_analysis.txt

Net Nanny Software International (1998). **BioPassword: Undeniably Identified—An Overview of Our Patented Keystroke Dynamic Technology**. Disponible en http://www.biopassword.com/docs/BioPassword.PDF

Netect (1998). **HackerShield—Features and Benefits**. Disponible en http://www.netect.com/hs_features.html

Network Flight Recorder (1998). **Step-by-Step Network Monitoring Using NFR.** Disponible en http://www.nswc.navy.mil/ISSEC/CID/nfr.htm

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Intrusion Detection Systems: Suspicious Finds.** Disponible en http://www.data.com/lab_tests/intrusion.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Intrusion Detection Systems: Suspicious Finds-II.** Disponible en http://www.data.com/lab_tests/intrusion2.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Intrusion Detection Systems: Suspicious Finds-III.** Disponible en http://www.data.com/lab_tests/intrusion3.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Intrusion Detection Systems: Suspicious Finds-IV.** Disponible en http://www.data.com/lab_tests/intrusion4.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Intrusion Detection Systems: Suspicious Finds-V.** Disponible en http://www.data.com/lab_tests/intrusion5.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Lab Test Vendor Participants.** Disponible en http://www.data.com/lab_tests/intrusion_participants.html

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Suspicious finds**. Data Communications, 27 (11), p. 72-81.

Newman, D., Giorgis, T. and Yavari-Issalou, F. (1998). **Test Methodology.** Disponible en http://www.data.com/lab_tests/intrusion_method.html

Northcutt, S. (1998). **Intrusion Detection: Shadow Style—Step by Step Guide**. SANS Institute Report (November).

Overill, R. (1998). **How Re (Pro) active Should An IDS Be?** In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Overill, R. (1998). **Intrusion detection systems: threats, taxonomy, tuning**. Joumal of Financial Crime, 6(1), p. 49-51.

Paxson, V. (1998). **Bro: A System for Detecting Network Intruders in Real-time**. In Proceedings of the Seventh USENIX Security Symposium, San Antonio, Texas, January, Paper D, p. 31-51. Disponible en http://www.aciri.org/vern/papers.html.

Paxson, V. (1998). **Using Bro to detect network intruders: experiences and status**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raíd-symposium.org/raíd98.

Polla, D., McConnell, J., Johnson, T., Marconi, J., Tobin, D. and Frincke, D. (1998). **A Framework for Cooperative Intrusion Detection**. In Proceedings of the 21st National Information Systems Security Conference, p. 361-373, October. Disponible en http://www.csds.uidaho.edu/director/framework.pdf

Porras, Ph. and Valdes, A. (1998). **Live Traffic Analysis of TCP/IP Gateways**. In Internet Society Symposium on Networks and Distributed Systems Security. Disponible en http://www.sdl.sri.com/papers/gateway98/

Porras, Ph., Neumann, P. and Linne, D. (1998). **Analysis and Response for Intrusion Detection in Large Networks—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/E302-0.html

Power, R. and Farrow, R. (1998). **CSI Intrusion Detection System Resource**. Disponible en http://www.gocsi.com/ques.htm

Ptacek, T. and Newsham, T. (1998). **Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection**. Disponible en http://www.securityfocus.com/data/library/ids.ps y también en http://www.clark.net/pub/roesch/public_html/IDSpaper.pdf

Puldy, M. and Christensen, M. (1998). **Lessons Learned in the Implementation of a Multi-Location Network Based Real Time Intrusion Detection System**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Radcliff, D. (1998). **The Danger Within: Internal Employees—Not Outside Hackers—Can Be a Time Bomb Waiting to Blow**. Disponible en http://www.idg.net/crd_security_16529.html (1998).

Ranum, M. (1998). **Intrusion Detection: Challenges and Myths**. Disponible en http://www.nfr.net/forum/publications/id-myths.html

Ranum, M. (1998). **Is network intrusion detection software being used correctly?** Security Management, 42 (8), p. 126-128.

Ranum, M. and Mace, S. (1998). **Finding your firewall**. Byte.com, 23 (6), p. 96NA3-100NA3.

Reilly, M. and Stillman, M. (1998). **Open Infrastructure for Scalable Intrusion Detection**. In Proceedings of the 1998 IEEE Information Technology Conference: Information Environment for the Future.

Romberg, D. (1998). **Cyber sleuths keep tabs on network security**. Computing Canada, 24 (34), p. 27-28.

Rowe, N. and Schiavo, S. (1998). **An intelligent tutor for intrusion detection on computer systems**. Computers and Education, 31, p. 395-404. Disponible en http://www.cs.nps.navy.mil/people/faculty/rowe/idtutor.html

Ruighaver, T., Thorne, P. and Tan, K. (1998). **Evaluating a Real-time Anomaly-based Intrusion Detection System**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.orgjraid98.

Ryan, J., Lin, M. and Miikkulainen, R. (1998). **Intrusion Detection with Neural Networks**. In Advances in Neural Information Processing Systems Proceedings of NIPS'97, Denver. MIT Press.

Sanchez, L.; Kent, S. and DiBlasio, M. (1998). **External Routing Intrusion Detection Systems (ERIDS)—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/G403-0.html

Scambray, J., McClure, S. and Broderick, J. (1998). **Network Intrusion-Detection Solutions**. InfoWorld 20, 18 (May 4). Disponible en http://www.infoworld.com/cgi-bin/displayArchive.pl?/98/18/intrusa.dat.htm.

Schneier, B. and Kelsey, J. (1998). **Cryptographic Suport for Secure Logs on Untrusted Machines**. In Proceedings of the Seventh USENIX Security Symposium, p. 53-62.

Sekar, R., Caí, Y. and Segal, M. (1998). **A SpecificationBased Aproach for Building Survivable Systems**. In Proceedings of the 21st National Information Systems Security Conference (NISSC'98).

Shumway, R. (1998). **Common Sense—An Alternative Approach to Web Security.** Proceedings of the 21st National Information Systems Security Conference. Arlington, Oct. 5-8. Disponible en http://csrc.nist.gov/nissc/1998/proceedings/paperD8.pdf.

Sommer, P. (1998). **Intrusion Detection Systems as Evidence**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Spafford, E. and Winchester, A. (1998). **Enhanced Intrusion and Misuse Detection Technology—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/D848-0.html

Spafford, E. and Zamboni, D. (1998). **Release of the Alpha Version of the AAFID Prototype**. Disponible en http://www.cs.purdue.edu/coast/projects/aafid-announce.html

Spafford, E. and Zamboni, D. (1998). **AAFID: Autonomous Agents for Intrusion Detection**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Spafford, G. (1998). **Audit Trails Format**. Disponible en http://www.cs.purdue.edu/coast/projects/audit-trails-format.html

Staniford-Chen, S. (1998). **Common Intrusion Detection Framework (CIDF).** Disponible en http://seclab.cs.ucdavis.edu/cidf/

Stocksdale, G. (1998). **SANS/NSA Intrusion Detection Tools Inventory**. Disponible en http://www.sans.org/NSA/idtools.htm

Stolfo, S. (1998). **Fraud and Intrusion Detection for Financial Information Systems.** Disponible en http://www.cs.columbia.edu/~sal/JAM/PROJECT/EYR1997.html

Stolfo, S. (1998). **The JAM Project and Evaluation Update**. In Proceedings of the DARPA Intrusion Detection PI Meeting. Lexington, Dec. 15-17. Disponible en http://www.dyncorp-is.com/darpa/meetings/id98dec/agenda.html.

Surkan, Michael. (1998). **Entrax Lags Server Guards.** Disponible en http://www.zdnet.com/pcweek/reviews/0615/15entrax.html

Swartwood, D. and Heffernan, R. (1998). **Trends in Intellectual Property Loss, Survey Report.** Disponible en http://www.asisonline.org/stat12.html

Tai, T., Kiong, T., Hwee, O. and Ting, C. (1998**). NIDAR: The Design and Implementation of an Intrusion Detection System**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Theus, M. and Schonlau, M. (1998). **Intrusion Detection Based on Structural Zeroes**. Statistical Computing of Graphics Newsletter, 9(1), p. 12-17.

Tripwire Security Systems (1998). **Tripwire Academic Source Release 1.3.1.** Disponible en http://www.tripwiresecurity.com/products/ASR1_3.html

Tyson, W. and Linne, D. (1998). **Explaining and Recovering from Computer Break-ins—1998 Project Summary**. Disponible en http://www.darpa.mil/itofpsum1998/E293-0.html

Undy, M. and Antonelli, C. (1998). **Sifting the Network: Performing Packet Triage with NFR**. Technical Report 98--6, Center for Information Technology Integration, University of Michigan.

Van Ryan, J. (1998). **SAIC's Center for Information Security Technology Releases CMDS Verson 3.5.** Disponible en http://www.saic.com/news/may98/news05-15-98.html

Vaughn, R. (1998). **A Practical Approach to Sufficient INFOSEC**. In Proceedings of the 21st National Information Systems Security Conference.Arlington, Oct. 5-8. Disponible en http://csrc.nist.gov/nissc/1998/proceedings/paperA1.pdf.

Vert, G., Frincke, D. and McConnell, J. (1998). **A Visual Mathematical Model for Intrusion Detection**. In Proceedings of the 21st National Information Systems Security Gonference (NISSG'98), October , p. 329-337. Disponible en http://www.csds.uidaho.edu/director/vismath.pdf

Vigna, G. and Kemmerer, R. (1998). **NetSTAT: A Network-based Intrusion Detection Aproach**. In Proceedings of the 14th Annual Computer Security Aplication Conference. Scottsdale, December. Disponible en http://www.cs.ucsb.edu/~kemm/netstat.html/documents.html.

Warshaw, L., Matzner, S., Miranker, D., Obermeyer,L. and Spindler, D. (1998). **Monitoring Network Logs for Anomalous Activity**. Technical Report TP-99-1, Aplied Research Laboratories. Department of Computer Sciences, University of Texas, Austin.

Webster, S. (1998). **The Development and Analysis of Intrusion Detection AIgorithms.** Master's thesis, Department of Electrical Engineering and Computer Science, MIT.

Wespi, A., Dacier, M., Debar, H. and Nassehi, M. (1998). **Audit Trail Pattern Analysis for Detecting Suspicious Process Behavior**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Wilikens, M. (1998). **Dependability of Large-scale Infrastructures and Challenges for Intrusion Detection.** In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.orgjraid98.

Wilson, M. and Fitzloff, E. (1998). **Anti-intrusion group signs up 40 members.** InfoWorld, 20 (42), p. 1-2.

Wood, M. (1998). **Integrating Intrusion Detection into the NetworkjSecurity Infrastructure**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Ye, N., Giordano, J., Feldman, J. and Zhong, Q. (1998). **Information Fusion Techniques for Network Intrusion Detection**. In Proceedings of the 1998 Information Technology Conference, p. 117-120.

Ye, N., Hosmer, C., Giordano, J. and Feldman, J. (1998). **Critical Information Infrastructure Protection through Process Modeling and Model-based Information Fusion.** In Proceedings of the 1998 Information Sunlivability Workshop (ISW'98), p. 197-201.

Ziese, K. (1998). **The Rome Labs Experience**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.org/raid98.

Zissman, M. and Lippmann, R. (1998). **Intrusion Detection System Evaluation.** IA Newsletter 2,2 (Fall), p. 6-7.

7. INTRUSION DETECTION IN 1999

Abad-Peiro, J., Debar, H., Schweinberger, T. and Thommler, P. (1999). **FLAg Policy Language for Authorizations.** Technical Report RZ3126, Zurich Research Laboratory, IBM Research Division.

Ali, S. (1999). **Adventures in Anomaly Detection**. Disponible en http://www.cs.cmu.edu/~cheekofintrusion/final.ps.gz.

Almgren, M. (1999). **Design and Implementation of a Lightweight Tool for Detecting Web Server Attacks.** Technical Report RZ 3129, IBM Zurich Research Laboratory.

Amoroso, E. (1999). **Design and Integration Principles for Large Scale Infrastructure Protection.** ;login: The USENIX Association Magazine (September), p. 20-21.

Amoroso, E. (1999). **Intrusion Detection**. Sparta, Intrusion.Net Books.

Antonelli, C. J., Undy, M and Honeyman, P. (1999). **The Packet Vault: Secure Storage of Network Data**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Arona, A., Bruschi, D. and Rosti, E. (1999). **Adding availability to lag services of untrusted machines.** In Proceedings ofthe 15th Annual Computer Security Aplications Conference (ACSAC'99).

Asaka, M., Okazawa, S., Taguchi, A. and Goto, S. (1999). **A Method of Tracing Intruders by Use of Mobile Agents**. In Proceedings of the 9th Annual Conference of the Internet Society (INET'99).

Asaka, M., Onabuta, T. and Nakasuka, S. (1999). **Intrusion Detection and Intrusion Route Tracing by Use of Mobile Agents.** In Proceedings of the first Asia-Pacific Conference on Intelligent Agent Technology (IAT'99).

Asaka, M., Taguchi, A. and Goto, S. (1999). **The Implementation of IDA: An Intrusion Detection Agent System**. In Proceedings of the 11th Annual FIRST Conference on Computer Security Incident Handling and Response (FIRST'99).

Asaka, M., Tsuchiya, M., Onabuta, T., Okazawa, S. and Goto, S. (1999). **Local Attack Detection and Intrusion Route Tracing.** IEEE Transactions on Communications, E82-B(11), p. 1826-1833.

Astithas, P., Koutepas, G. and Maglaris, B. (1999). **Integrating Intrusion Detection and Network Management.** In Proceedings of the 6th HP Openview University Association Plenary Workshop (HPOVUA '99).

Avolio, F. (1999). **The Castle Defense**. Performance Computing, 17 (8), p. 42-46.

Axelsson, S. (1999). **On a Difficulty of Intrusion Detection.** In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99), Purdue University, West Lafayette, Indiana, September 7-9. Disponible en http://www.ce.chalmers.se/staff/sax/raid99.ps

Axelsson, S. (1999). **Research in Intrusion-Detection Systems : A Survey**. Technical Report 98-17, Department of Computer Engineering, Chalmers University of Technology, Göteborg. Disponible en http://www.ce.chalmers.se/staff/sax/survey.ps

Axelsson, S. (1999). **The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection.** In Proceedings of the 6th ACM Conference on Computer and Communications Security, Kent Ridge Digital Labs, Singapore, November 1-4, p. 1-7. Disponible en http://www.ce.chalmers.se/staff/sax/difficulty.pdf

AXENT (1999). **NetProwler—Advanced Network Intrusion Detection.** Disponible en http://www.axent.com/iti/netprowler/idtk_ds_word_1.html

Bace, R. (1999). **An Introduction to Intrusion Detection Assessment**. Disponible en http://solutions.iss.net/products/whitepapers/intrusion.pdf y también en http://ca.com/solutions/enterprise/etrust/intrusion_detection/product_infofintrusionassess.pdf

Baker, D., Cassandra, A. and Rashid, M. (1999). **CEDMOS: Complex Event Detection and Monitoring System**. Technical Report MCC-CEDMOS-002-99, Microelectronics and Computer Technology Corporation.

Baker, D., Christey, S., Hill, W. and Mann, D. E. (1999). **The Development of a Common Enumeration of Vulnerabilities and Exposures**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Barrufli, R., Milano, M. and Montanari, R. (1999). **Planning for Security Management**. In Proceedings of AAAI'99 Workshop on Al for Distributed lnformation Networking (AiDIN'99).

Bass, T. (1999). **Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness—Introduction**. Disponible en http://www.silkroad.com/paper/html/ids/node1.html

Bass, T. (1999). **Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems**. In Proceedings of the 1999 IRIS National Symposium on Sensor and Data Fusion. May 24-27, 1999. Disponible en http://www.silkroad.com/papers/html/iris.

Bass, T. and Gruber, D. (1999). **A Glimpse into the Future of ID.** ;login: The USENIX Association Magazine (July). Disponible en http://www.silkroad.com/papers/html/glimpse.

Bettati, R., Zhao, W. and Teodor, D. (1999). **Real-Time Intrusion Detection and Supression in ATM Networks**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Beyond Security. (1999). **NMap Port Scanner**. Disponible en http://www.securiteam.com/tools/NMap_Port_scanner.html

Bishop, M. (1999). **Vulnerabilities Analysis**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). West Lafayette, September 7-9. Disponible en http://www.cerias.purdue.edu/raidprog.html.

Boudaoud, K. and Labiod, H. (1999). **MA-NID: A Multi-Agent System for Network Intrusion Detection**. In Proceedings of the 8th International Conference on Intelligent Systems (ICIS-99).

Briney, A. (1999). **Budgets and Product Purchasing Trends**. Disponible en http://www.infosecuritymag.com/july99/chart2.htm

Briney, A. (1999). **Got Security?.** Disponible en http://www.infosecuritymag.com/july99/cover.htm.

Briney, A. (1999). **Security Overview & Executive Summary**. Disponible en http://www.infosecuritymag.com/july99/chart1.htm

Briney, A. (1999). **Under Attack & Underprepared**. Disponible en http://www.infosecuritymag.com/july99/under.htm.

Briney, A. and Rose, B. (1999). **Study Confirms Increased Security Risks of E-Commerce**. Disponible en http://www.icsa.net/news/press_room/1999/mag_survey.shtml

Brock, J. (1999). **NRC's Intrusion Detection and Response Capabilities (AIMD-99-273R)**. Washington, DC: United States General Accounting Office, August .

Brumley, D. (1999). **Invisible Intruders: Rootkits in Practice**. ;login: The USENIX Association Magazine (September), p. 27-29.

Brutch, P., Brutch, T. and Pooch, U. (1999). **Indicators of UNIX Host Compromise.** ;login: The USENIX Association Magazine (September), p. 30-35.

Bulatovic, D. and Velasevic, D. (1999). **A Distributed Intrusion Detection System Based on Bayesian Alarm Networks**. In Proceedings of CQRE'99, in Lecture Notes in Computer Science, number 1740, Springer-Verlag, Berlin, page 219.

Büschkes, R., Borning, M. and Kesdogan, D. (1999). **Transaction-based Anomaly Detection**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Buzzard, K. (1999). **Computer Security--What Should You Spend Your Money On?**. Computers & Security, 18 (4), p. 322-334.

Campbell, W. A. (1999). **Traditional Indications and Warnings for Host Based Intrusion Detection**. Disponible en http://www.bellevue.prc.com/recis/campbell.pdf.

CERT/CC. (1999). **CERT Incident Note IN-99-01 on scan**. Disponible en http://www.cert.org/incident_notes/IN-99-01.html

CERT/CC. (1999). **CERT Summary CS-99-02**. Disponible en http://www.cert.org/summaries/CS-99-02.html

Champion, T. and Durst, R. (1999). **Air Force Intrusion Detection System Evaluation Environment**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Chan, P., Fan, W., Prodromidis, A. and Stolfo, S. (1999). **Distributed data mining in credit card fraud detection,** IEEE Intelligent Systems, 14(6), p. 67-74. Disponible en http://cs.fit.edu/~pkc/papers/ieee-is99.pdf

Cheswick, B. (1999). **An Evening With Berford in Which a Cracker is Lured, Endured and Studied**. Disponible en http://jhunix.hcf.jhu.edu/pub/miscellaneous_security_papers/An_Evening_With_Berferd.ps.Z

Cheung, S. (1999). **An Intrusion Tolerance Aproach for Protecting Network Infrastructures**. PhD thesis, Computer Science Department, University of California at Davis.

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**. Technical Report CSE-99-2, Department of Computer Science, University of California at Davis. Disponible en http://seclab.cs.ucdavis.edu/papers.html.

Christey, S. (1999). **Re: IMPORTANT: CVE—Common Vulnerabilities and Exposures?.** Disponible en http://cve.mitre.org/archives/msg00430.html.

Christey, S., Mann, D. and Hill, W. (1999). **The Development of a Common Vulnerability Enumeration.** Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID '99). West Lafayette, September 7-9. Disponible en http://www.cerias.purdue.edu/raidprog.html.

Chung, C., Gertz, M. and Levitt, K. (1999). **DEMIDS: A Misuse Detection System for Database Systems.** In Proceedings of the 3rd International Working Conference on Integrity and Internal Control in Information Systems (IICIS'99).

Chung, C., Gertz, M. and Levitt, K. (1999). **Misuse Detection in Database Systems Through User Profiling**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Cohen, F. (1999). **Anatomy of a Successful Sophisticated Attack**. Disponible en http://www.all.net/journal/netsec/9901.html

Cohen, F. (1999). **Attack and Defense Strategies**. Disponible en http://all.net/journal/netsec/9907.html

Cohen, F. (1999). **Providing for Responsibility in a Global Information Infrastructure.** Disponible en http://www.all.net/journal/ntb/responsible.html

Cohen, F. (1999). **Returning Fire**. Disponible en http://all.net/journal/netsec/9902.html

Cohen, F. (1999). **Simulating Cyber Attacks, Defenses, and Consequences.** Disponible en http://all.net/journal/ntb/simulate/simulate.html

Cohen, F. (1999). **Simulating Network Security**. Disponible en http://www.all.net/journal/netsec/9904.html

Computer Associates (1999). **SessionWall-3.** Disponible en http://www.abirnet.com/products.html

Cosendai, Y., Dacier, M. and Scotton, P. (1999). **Intrusion Detection Mechanism to Detect Reachability Attacks in PNNI Networks**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Cowan, C., Beattie, S., Day, R., Pu, C., Wagle, P. and Walthinsen, E. (1999). **Protecting Systems from Stack Smashing Attacks with StackGuard**. Disponible en http://www.cse.ogi.edujDISCjprojectsjimmunixjlexpo.pdf.

Cunningham, R., Lipmann, R., Fried, D., Garfinkel, S., Graf, l., Kendall, K., Webster, S., Wyschogrod, D. and Zissman, M. A. (1999). **Evaluating Intrusion Detection Systems without Attacking your Friends: The 1998 DARPA Intrusion Detection Evaluation.** In Proceedings of the Third Conference and Workshop on Intrusion Detection and Response (SANS 1999).

CCyberSafe (1999). **Centrax Intrusion Detection Software Features and Benefits.** Disponible en http://www.centraxcorp.com/benefits.html

CyberSafe (1999). **Centrax Security Software**. Disponible en http://www.centraxcorp.com/zmedia/IRM%20Summer_Fall.pdf

Dacier, M. and Jackson, K. (1999). **Intrusion detection.** Computer Networks, 31 (23/24), p. 2433-2434.

Daniels, T. and Spafford, E. (1999). **Identification of host audit data to detect attacks on low-level IP vulnerabilities.** Journal of Computer Security, 7 (1), p. 3-35.

Dasgupta, D. (1999). **Immunity-Based Intrusion Detection Systems: A General Framework**. In Proceedings of the 22nd National Information Systems Security Conference (NISSC'99).

De Queiroz, J., da Costa Garfio, L. and Pirmez, L. (1999). **Micael: An Autonomous Mobile Agent System to Protect New Generation Networked Aplications**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

De Wolf, H. (1999). **The Jargon File**. Disponible en http://web.bilkent.edu.tr/Online/Jargon30/JARGON.HTML

Debar, H. and Dacier, M. (1999). **Towards a taxonomy of intrusion-detection systems.** Computer Networks, 31 (8), p. 805-822. Disponible en http://www.zurich.ibm.com/pub/sti/Security/extern/gsal/docs/

Deering, S. and Hinden, B. (1999). **Statement on IPv6 Address Privacy**. Disponible en http://playground.sun.com/pub/ipng/html/ipv6-address-privacy.html

Denning, D. (1999). **Who's Stealing Your Information?.** Disponible en http://www.infosecuritymag.com/apr99/cover.htm

Doyle, J. (1999). **Some Representational Limitations of the Common Intrusion Specification Language**. Disponible en http://www.medg.lcs.mit.edu/doyle/publications/cis199.pdf.

DuMouchel, W. (1999). **Computer Intrusion Detection Based on Bayes Foctors for Comparing Command Transition Probabilities**. Technical Report TR91, National Institute of Statistical Sciences (NlSS).

Dunigan, T. and Hinkel, G. (1999). **Intrusion Detection and Intrusion Prevention on a Large Network: A Case Stud**y. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Durst, R., Champion, T., Witten, B., Miller, E. and Spagnuolo, L. (1999). **Testing and Evaluating Computer Intrusion Detection Systems.** Communications of the ACM 42, 7 (July), p. 53-61.

Elbaum, S. and Munson, J. (1999). **Intrusion Detection Through Dynamic Software Measurement**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

En Garde Systems (1999). **T-sight RealTime—Main Window**. Disponible en http://engarde.com/software/tsight/tutorial/realtime/main.html

Enright, G. (1999). **IDS latest defence in war against network intruders.** Computing Canada, nº. (45), p. 27-28.

Erlinger, M. (1999). **Intrusion Detection Exchange Format (idwg).** Disponible en http://www.ietf.org/html.charters/idwg-charter.html

Farley, T. (1999). **Lessons Learned in Commercial IDS Development.** In Proceedings of the 2nd Intemational Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Farmer, D. and Venema, W. (1999). **Improving the Security of Your Site by Breaking Into It.** Disponible en http://www.clark.net/pub/roesch/public_html/improve_by_breakin.txt

Fawcett, T. and Provost, F. (1999). **Activity Monitoring: Noticing Interesting Changes in Behavior.** In Proceedings of the Fifth International Conference on Knowledge Discovery and Data Mining (KDD99), p. 28-35.

Fayad, A., Jajodia, S. and McCollum, C. (1999). **Aplication-Level Isolation Using Data Inconsistency Detection**. In Proceedings of the 15th Annual Computer Security Aplications Conference (ACSAC'99).

Feiertag, R., Benzinger, L., Rho, S., Wu, S., Levitt, K., Peticolas, D., Heckman, M., Staniford-Chen, S. and Zhang, C. (1999). **Intrusion Detection Inter-component Adaptive Negotiation**. In Proceedings of the 2nd Intemational Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Festa, P. (1999). **Defense Department Fights off Hackers**. (CNET News.com). Disponible en http://news.cnet.com/news/0-1005-200-339584.html?tag=st.ne.1005-200-343118

Frincke, D., Tobin, D. and Ho, Y. (1999). **A Framework for Cooperative Intrusion Detection**. Disponible en http://www.csds.uidaho.edu/~hummer/html/papers.html.

Fyodor. (1999). **Nmap Network Security Scanner Man Page**. Disponible en http://www.insecure.org/nmap/nmap_manpage.html

Fyodor. (1999). **Nmap—The Network Mapper**. Disponible en http://www.insecure.org/nmap/

Ghosh, A. and Schwartzbard, A. (1999). **A Study in Using Neural Networks for Anomaly and Misuse Detection**. In Proceedings of the 8th Usenix Security Symposium (SEC'99).

Ghosh, A. and Schwartzbard, A. (1999). **Analyzing the Performance of Program Behavior Profiling for Intrusion Detection**. In Proceedings of the 13th IFIP WG 11.3 Working Conference on Database Security.

Ghosh, A., Schwartzbard, A. and Schatz, M. (1999). **Learning Program Behavior Profiles for Intrusion Detection**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Ghosh, A., Schwartzbard, A. and Schatz, M. (1999). **Using Program Behavior Profiles for Intrusion Detection**. In Proceedings of the 2nd SANS Workshop On Intrusion Detection and Response (ID'99).

Girardin, L. (1999). **An Eye on Netwórk IntruderAdministrator Shootouts.** In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Goan, T. (1999). **A Cop on the Beat: Collecting and Appraising Intrusion Evidence.** Communications of the ACM 42, 7 (July), p. 46-52.

Goan, T. (1999). **A cop on the beat: Collecting and appraising intrusion evidence.** Communications of the ACM, 42 (7), p. 46-52.

Godwin, M. (1999). **Net to worry**. Communications of the ACM, 42 (12), p. 15-17.

Gorman, D. and Ruhl, M. (1999). **Intrusion Detection for Telephony Signalling**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Graham, R. (1999). **FAQ: Network Intrusion Detection Systems**. Disponible en http://www.robertgraham.com/pubs/network-intrusion-detection.html

Green, J., Marchette, D., Northcutt, S. and Ralph, B. (1999). **Analysis Techniques for Detecting Coordinated Attacks and Probes**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Gula, R. (1999). **Broadening the Scope of Penetration Testing Techniques**. Disponible en http://www.securityfocus.com/templates/forum_message.html?forum=2&head=7&id=7

Gunetti, D. and Ruffo, G. (1999). **Intrusion Detection through Behavioural Data**. In Proceedings of the Third Symposium on Intelligent Data Analysis (IDA'99).

Hancock, B. (1999). **US Plan for Government-Owned Infrastructure Intrusion Detection System Draws Fire.** Computers & Security, 18 (6), p. 467-468.

Harris Communications. (1999). **Stake Out I.D**. Disponible en http://www.commprod.harris.com/networksecurity/stakeout/

Harrison, A. (1999). **New Generation of Scanning Tools Mask Source of Attack.** Disponible en http://www.computerworld.com/home/print.nsf/all/99031596AA

Harrison, A. (1999). **Security Think Tank Releases Sniffer Tool**. Disponible en http://www.computerworld.com/home/print.nsf/all/990809BAA2/

Harrison, A. (1999). **When Good Scanners Go Bad**. Disponible en http://www.computerworld.com/home/print.nsf/all/9903229872

Hart, R., Morgan, D. and Tran, H. (1999). **An Introduction to Automated Intrusion Detection Approaches.** Information Management and Computer Security 7, 2, p. 76-82. Disponible en http://www.emerald-library.com/pdfs/04607bb2.pdf.

Heberlein, T. (1999). **Anomaly Detection of Misuse Reports**. Disponible en http://www.netsq.com/Information/RTID-Mining

Heidt, F. and Warren, R. (1999). **Covert Surveillance Channels: A Simple Method for Securing a Network Intrusion Detection Host**. In Proceedings of the ShadowCon'99.

Helmer, G., Wong, J., Honavar, V. and Miller, L. (1999). **Automated Discovery of Concise Predictive Rules for Intrusion Detection**. Technical Report TR99-01, Department of Computer Science, Iowa State University. Disponible en http://www.palisadesys.com/~ghelmer/Papers/tr9901.ps

Helmer, G., Wong, J., Honavar, V. and Miller, L. (1999). **Feature selection using a genetic algorithm for intrusion detection (GECCO'99)**. In Proceedings of the Genetic and Evolutionary Computation Conference. Disponible en http://www.palisadesys.com/~ghelmer/Papers/gecco99.ps

Hinden, R. (1999). **IP Next Generation (IPng).** Disponible en http://playground.sun.com/pub/ipng/html/ipng-main.html

Hinton, H., Cowan, C., Delcambre, L. and Bowers, S. (1999). **SAM: Security Adaptation Manager**. In Proceedings of the 15th Annual Computer Security Aplications Conference (ACSA C'99).

Hoffman, P. (1999). **A Novice's Guide to the IETF**. Disponible en http://www.imc.org/novice-ietf.html

Hofmeyr, S. (1999). **An Immunological Model ofDistributed Detection and its Aplication to Computer Security.** PhD thesis, University of New Mexico.

Hofmeyr, S. and Forrest, S. (1999). **Immunity by Design : An Artificial Immune System**. In Morgan-Kaufmann, editor, Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'99), p. 1289-1296.

Hosmer, C. Feldman, J. and Giordano, J. (1999). **Advancing Crime Scene Computer Forensic Techniques.** Disponible en http://www.wetstonetech.com/crime.htm

HP OpenView. (1999). **Features and Benefits of Node Sentry.** Disponible en http://www.openview.hp.com/products/node/features/.

HP OpenView. (1999). **HP OpenView Node Sentry Product Brief**. Disponible en http://www.openview.hp.com:80/pdfs/257.pdf

Huang, M. and Jasper, R. (1999). **A large scale distributed intrusion detection framework based on attack strategy analysis.** Computer Networks, 31 (23/24), p. 2465-2476.

IBM. (1999). **IBM Integrated Security Solutions: Comprehensive Security Solutions for Enabling e-business**. Disponible en http://www4.ibm.com/software/security/firstsecure/library/whitepapers/intsecsol.html

IBM. (1999). **SecureWay FirstSecure**. Disponible en http://www.software.ibm.com/security/firstsecure

ICSA.net (1999). **About ICSA**. Disponible en http://www.icsa.net/about_icsa/

ICSA.net (1999). **About the Intrusion Detection Systems Consortium.** Disponible en http://www.icsa.net/html/communities/ids/membership/index.shtml

Iguchi, M. and Goto, S. (1999). **Detecting Malicious Activities through Port Profiling**. IEEE Transactions on Information and Systems, E82-D(4), p. 784-792.

Information Assurance Technology Analysis Center. (1999). **Information Assurance Tools Report.** Disponible en http://www.iatac.dtic.mil/iatools.htm

Information Assurance Technology Analysis Center (1999). **About IATAC**. Disponible en http://www.iatac.dtic.mil/About.htm

InformationWeek (1999). **Extra Research from the Security Survey.** Disponible en http://informationweek.com/743/secure.htm

Ingram, D. (1999). **Autonomous Agents for Distributed Intrusion Detection in a Multi-host Environment**. Master's thesis, Naval Postgraduate School, United States Navy.

Internet Security Systems (1999). **Real-Time Attack Recognition and Response: A Solution for Tightening Network Security**. Disponible en http://solutions.iss.net/products/whitepapers/realtime.pdf

Internet Security Systems. (1999). **Real Secure.** Disponible en http://www.iss.net/prod/realsecure.pdf

Intrusion detection & controls (1999). **Security: For Buyers of Products**, Systems & Services, 36 (11), p. 109-121.

Irvine E. and Levin, T. (1999). **Toward a taxonomy and costing method for security services**. In Proceedings od the 15th Annual Computer Security Applications Conf. (ACSAC'99). Disponible en http://cisr.nps.navy.mil/downloads/QoSS_TaxCost_TR.pdf

Irwin, V. and Northcutt, S. (1999). **Shadow: Internet Threat Briefing—Stealth and Coordinated Attacks**. Disponible en http://www.nswc.navy.mil/ISSEC/CID/coordinated.ppt

Jackson, K. (1999). **Intrusion Detection System (IDS) Product Survey.** Technical Report LA-UR-99-3883, Los Alamos National Laboratory.

Jajodia, S., McCollum, C. and Ammann, P. (1999). **Trusted Recovery.** Communications of the ACM 42, 7 (July), p. 71-75.

Jansen, W., Mell, P. and Marks, D. (1999). **Aplying Mobile Agents to Intrusion Detection and Response**. Technical Report IR-6416, National Institute of Standards and Technology, Computer Security Division.

Ju, W. and Vardi, Y. (1999). **A Hybrid High-order Markov Chain Model for Computer Intrusion Detection**. Technical Report TR92, National Institute of Statistical Sciences (NISS).

Jonsson, E., Strömberg, L. and Lindskog, S. (1999). **On the functional relation between security and dependability impairments.** In Proceedings of the New Security Paradigms Workshop, Caledon Hills, September 23-25. Disponible en http://www.ce.chalmers.se/~larst/Publications/nspw99_A4.ps

Kato, N., Nitou, H., Ohta, K., Mansfield, G. and Nemoto, Y. (1999). **A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations.** IEICE Transactions on Communications, E82B(11), p. 1817-1825.

Kelsey, J. and Schneier, B. (1999). **Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs.** In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Kemmerer, R. (1999). **STAT Projects**. Disponible en http://www.cs.ucsb.edu/~kemm/netstat.html/projects.html

Kendall, K. (1999). **A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems.** Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Kerber, R. (1999). **A Handle on Hackers**. Disponible en http://www.boston.com/dailyglobe2/335/business/Handle_on_hackers%2b.shtml

Kim, G. and McHugh, J. (1999). **File Integrity Assessment**. Disponible en http://www.tripwiresecurity.com/company/press_releases/webcast.ppt

Kim, J. and Bentley, P. (1999). **Negative Selection and Niching by an Artificial Immune System for Network Intrusion Detection.** In Proceedings of the Genetic and Evolutionary Computation Conference (GECCO '99).

Kim, J. and Bentley, P. (1999). **The Artificial Immune Model for Network Intrusion Detection**. In Proceedings of the 7th European Congress on Intelligent Techniques and 80ft Computing (EUFIT'99).

Kim, J. and Bentley, P. (1999). **The Human Immune System and Network Intrusion Detection**. In Proceedings of the 7th European Congress on Intelligent Techniques and 80ft Computing (EUFIT'99).

Klein, D. (1999). **Defending against the Wily Buffer Webbased Attacks and Defenses**. In Proceedings of the 1st USENIX Workshop on Detection Symposium and Network Monitoring.

Kremer, H. (1999). **Real-Time Intrusion Detection for Windows NT Based on Navy IT-21 Audit Policy**. Master's thesis, Naval Postgraduate School, United States Navy.

Kuperman, B. and Spafford, E. (1999). **Generation of Aplication Level Audit Data via Library Interposition**. Technical Report TR-99-11, CERIAS.

Kvarnström, H., Hedbom, H., and Jonsson, E. (1999). **Security Implications of Distributed Intrusion Detection Architectures.** In Proceedings of 4th Nordic conference on secure IT-systems (NORDSEC '99), Nov. 1-2, Stockholm, p. 225-243.

LaMonaca, Mike. (1999). **Back Orifice Remote Administration Tool.** Disponible en http://www.rescomp.upenn.edu/docs/hype/old/bo.html

Lane, T. and Brodley, C. E. (1999). **Temporal Sequence Learning and Data Reduction for Anomaly Detection**. ACM Transactions on Information and System Security.

Larson, A. (1999). **Global Security Survey: Virus Attack**. Disponible en http://informationweek.com/743/security.htm.

Larson, A. (1999). **Global Security Survey: Virus Attack-II**. Disponible en http://informationweek.com/743/security2.htm .

Larson, A. (1999). **Global Security Survey: Virus Attack-III.** Disponible en http://informationweek.com/743/security3.htm

Larson, A. (1999). **Global Security Survey: Virus Attack-IV**. Disponible en http://informationweek.com/743/security4.htm

Larson, A. (1999). **Global Security Survey: Virus Attack-V**. Disponible en http://informationweek.com/743/security5.htm

Larson, A. (1999). **Global Security Survey: Virus Attack-VI**. Disponible en http://informationweek.com/743/security6.htm

Larson, A. (1999). **Worldwide Security Priorities**. Disponible en http://informationweek.com/743/securit3.htm

Lawrence Livermore National Laboratory Computer Security Technology Center. (1999). **NID Distribution Site**. Disponible en http://ciac.llnl.gov/cstc/nid/nid.html

Lee, W. (1999). **A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems**. PhD thesis, Computer Science Department, Columbia University.

Lee, W. and Stolfo, S. J. (1999). **Combining Knowledge Discovery and Knowledge Engineering to Build IDSs**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Lee, W., Park, C. and Stolfo, S. (1999). **Automated Intrusion Detection Using NFR : Methods and Experiences**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring. Disponible en http://www1.cs.columbia.edu/ids/publications/wenke-usenix99.ps

Lee, W., Stolfo, S. and Mok, K. (1999). **A Data Mining Framework for Building Intrusion Detection Models**. In Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, May. Disponible en http://www.cc.gatech.edu/~wenke/papers/ieee_sp99_lee.ps

Lee, W., Stolfo, S. and Mok, K. (1999). **AIgorithms for Mining System Audit Data**. In Lin, T. Y. and Cercone, N., Data Retrieval and Data Mining. Kluwer Academic Publishers.

Lee, W., Stolfo, S. and Mok, K. (1999). **Mining in a Data-flow Environment: Experience in Network Intrusion Detectio**n. In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD'99), San Diego, August. Disponible en http://www.cc.gatech.edu/~wenke/papers/kdd99.ps

Levitt, K. (1999). **GrIDS Requirements Document.** Disponible en http://olympus.cs.ucdavis.edu/arpa/grids/requirements.html

Lin, M., Marzullo, K. and Ricciardi, A. (1999). **On the Resilience of Broadcasting Strategies in a Failure-Propagating Environment**. Technical Report CS99-610, Department of Computer Science and Engineering, University of California at San Diego.

Lindqvist, U. (1999). **On the Fundamentals of Analysis and Detection of Computer Misuse**. PhD thesis, School of Electrical and Computer Engineering, Chalmers University of Technology, Göteborg.

Lindqvist, U. and Porras, Ph. (1999). **Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST).** In Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, May 9-12, p. 146-161. Disponible en http://www.sdl.sri.com/papers/pbest-sp99-cr/ y también en http://www.ce.chalmers.se/staff/jonsson/pubs/sp99lp.pdf

Lindskog, S., Lindqvist, U. and Jonsson, E. (1999). **lT Security Research and Education in Synergy.** In Proceedings of the 1st World Conference on Inlormation Security Education (WISE1), Kista, June 17-19. Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology, p. 147-162. Disponible en http://www.ce.chalmers.se/staff/jonsson/pubs/wise99l.pdf

Linger, R. (1999). **Systematic Generation of Stochastic Diversity as an Intrusion Barrier in Survivable Systems Software**. In Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences (HICSS'99).

Lipmann, R. and Cunningham, R. (1999). **Improving Intrusion Detection Performance using Keyword Selection and Neural Networks**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Lipmann, R., Cunningham, R., Fried, D., Graf, l., Kendall, K., Webster, S. and Zissman, M. (1999). **Results of the DARPA 1998 Of-Line Intrusion Detection Evaluation**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Liu, P., Jajodia, S. and McCollum, C. (1999). **Intrusion Confinement by Isolation in Iníormation Systems**. In Proceedings of the 13th IFIP Working Conference on Database Security.

Lopht Heavy Industries (1999). **Antisniff—Overview**. Disponible en http://www.lopht.com/antisniff/overview.html

Loshin, P. (1999). **Security on the new digital network.** Telecommunications - American Edition, 33 (1), p. 36-37.

Lundin, E. and Jonsson, E. (1999). **Privacy vs Intrusion Detection Analysis**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99), Lafayette, September 7-9. Disponible en http://www.ce.chalmers.se/staff/emilie/papers/Lundin_raid99.ps

Lundin, E. and Jonsson, E. (1999). **Some Practical and Fundamental Problems with Anomaly Detection**. In Proceedings of the fourth Nordic Workshop on Secure IT systems (NORDSEC'99), Kista, November 1-2. Disponible en http://www.ce.chalmers.se/staff/emilie/papers/Lundin_nordsec99.pdf

Luo, J. (1999). **Integrating Fuzzy Logic With Data Mining Methods for Intrusion Detection**. Master's thesis, Department of Computer Science, Mississipi State University. Disponible en ftp://ftp.cs.msstate.edu/publications/theses_dissertations/luo99thesis.ps.

Maloof, M. and Michalski, R. (1999). **AQPM: A System for Partial Memory Learning**. In Proceedings of the Eighth Workshop on Intelligent Information Systems, p. 70-79.

Manganaris, S., Christensen, M., Zerkle, D. and Hermiz, K. (1999). **A Data Mining Analysis of RTill Alarms**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Mann, D. and Christey, S. (1999). **Towards a Common Enumeration of Vulnerabilities**. Second Workshop on Research with Security Vulnerability Databases. West Lafayette, January 21-22. Disponible en http://cve.mitre.org/docs/cerias.html.

Mann, P. (1999). **Pentagon confronts mounting cyber risks.** Aviation Week & Space Technology, 150 (12), p. 82-83.

Mansfield, G. (1999). **Towards traping wily intruders in the large**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.cerias.purdue.edu/raidprog.html.

Marchette, D. (1999). **A Statistical Method for Profiling Network Traffic**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Maxion, R. (1999). **Cinnamon: Synthetic Data Generation**. Disponible en http://www.cs.cmu.edu/~maxion/invictus/cinnamon.html

Maxion, R. (1999). **Harbinger: Anomaly Detection Techniques.** Disponible en http://www.cs.cmu.edu/~maxion/invictus/harbinger.html

Maxion, R. (1999). **Invictus: Detection of Unanticipated Anomalies in Evolutionary Environments.** Disponible en http://www.cs.cmu.edu/~maxion/invictus

Maxion, R. (1999). **Invictus: Toward Dependable Systems**. Disponible en http://www.cs.cmu.edu/~maxion/invictus/InvQuad.jpg

Maynard, T. (1999). **Year 2000 Computer Remediation: Assessing Risk Levels in Foreign Outsourcing**. Disponible en http://www.SANS.ORG/newlook/resources/Y2K.htm

McGraw, G. (1999). **Java's 2's Verifier Becomes Confused by German Student's Security Attack**. Disponible en http://www.javaworld.com/javaworld/jw-04-1999/jw-04-flaw.html

McGraw, G. (1999). **Why Monitoring Mobile Code is Harder than It Sounds.** ;login: The USENIX Association Magazine (September), p. 18-20.

McKay, N. (1999). **Coming Soon: Back Orifice 2000**. Disponible en http://www.wired.com/news/technology/0,1282,20493,00.html

Mé, L. and Alanou, V. (1996). **Détection d'intrusions dans un systeme informatique: méthodes et outils**. TSI, 15(4), p. 429-450.

Mé, L. and Michel, C. (1999). **La détection d'intrusions : bref aper cu et derniers dévelopements**. In Actes du 10eme Forum sur la Sécurité des Systemes d'Information (EUROSEC'99).

Mell, P. (1999). **Acquiring and Deploying Intrusion Detection System.** National Institute of Standards and Technology's Information Technology Laboratory bulletin.

Mell, P. and McLarnon, M. (1999). **Mobile Agent Attack Resistant Distributed HierarchicalIntrusion Detection Systems**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Miller, M. (1999). **Learning Cost-Sensitive Classification Rules for Network Intrusion Detection using RIPPER**. Columbia University Computer Science Technical Report CUCS-035-1999. Disponible en http://www1.cs.columbia.edu/ids/publications/cucs-035-1999.pdf

MIT Lincoln Laboratory (1999). **DARPA Intrusion Detection Evaluation**. Disponible en http://www.ll.mit.edu/IST/ideval/index.html

Monrose, F., Wyckoff, P. and Rubin, A. (1999). **Distributed Execution with Remote Audit**. In Proceedings of the 1999 Network and Distributed System Security Symposium (NDSS'99).

Moritz, R. (1999). **CCIAPI: Common Content Inspection Application Programming Interface**. Disponible en www.stardust.com/cciapi/docs/010799/CCIAPIScopeDraft3011.doc

Mudge. (1999). **A Hacker's Approach to ID**. ;login: The USENIX Association Magazine (September), p. 36-39.

Mukkamala, R., Gagnon, J. and Jajodia, S. (1999). **Integrating data mining techniques with intrusion detection**. In Proceedings ofthe XIII AnnualIFIP WG 11.3 Working Conference on Database Security.

Mutaf, P. (1999). **Defending against a Denial-of-Service Attack on TCP**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Neikter, C. (1999). **Netbus Pro 2.01**. Disponible en http://netbus.org/features.html

Neil, S. (1999). **Arming the network the digital IDs**. PC Week, 16 (9), p. 123-124.

Network Associates (1999). **CyberCop CASL**. Disponible en http://www.nai.com/asp_set/products/tns/cccasl_intro.asp.

Network Associates (1999). **CyberCop Monitor**. Disponible en http://www.nai.com/asp_set/products/tns/ccmonitor_intro.asp

Network Associates (1999). **CyberCop Scanner**. Disponible en http://www.nai.com/asp_set/products/tns/ccscanner_intro.asp

Network Associates (1999). **Evading Intrusion Detection—Executive Summary**. Disponible en http://www.nai.com/products/security/advisory/papers/ids-simple.doc

Network Associates (1999). **Next Generation Intrusion Detection in High Speed Networks**. Disponible en http://www.nai.com/media/pdf/nai_labs/ids.pdf

Neumann, P. and Porras, Ph. (1999). **Experience with EMERALD to DATE**. In Proceedings olthe 1st USENIX Workshop on Intrusion Detection and Network Monitoring, p. 73-80. Disponible en http://www.sdl.sri.com/papers/det99/.

Northcutt, S. (1999). **Evaluating Intrusion Detection Systems Without Attacking Your Friends**, 86. Network Intrusion Detection. Indianapolis,New Riders.

Northcutt, S. (1999). **Network Intrusion Detection**. Indianapolis,New Riders.

Nuansri, N., Singh, S. and Dillon, T. S. (1999). **A Process StateTransition Analysis and its Aplication to Intrusion Detection.** In Proceedings of the 15th Annual Computer Security Aplications Conference (ACSAC'99).

Oakes, Ch. (1999). **Cracking Tools Get Smarter**. Disponible en http://www.wired.com/news/news/technology/story/18219.html

ODS Networks (1999). **CDMS: Computer Misuse Detection System**. Disponible en http://www.ods.com/security/products/cmds.shtml

Ong, T., Tan, Y. and Ting, C. (1999). **SNMS Shadow Network Management System**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Ott, J. (1999). **Preparing for the new millennium...** Information Systems Security, 8 (1), p. 3-5.

Overill, R. (1999). **Denial of Service Attacks: Threats and Methodologies**. Journal of Financial Crime, 6(4), p. 351-354.

Panda, B. and Giordano, J. (1999). **Defensive information warfare.** Communications of the ACM, 42 (7), p. 30-32.

Paxson, V. (1999). **Bro: A System for Detecting Network Intruders in Real-Time**. Computer Networks, 31:2435-2463.

Paxson, V. (1999). **Defending against network IDS evasion**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raíd-symposium.org/raíd99.

Paxton, V. (1999). **Experiences Learned from Bro**. ;login: The USENIX Association Magazine (September), p. 21-22.

PCWeek Online. (1999). **PC Week Labs Scoring Methodology**. Disponible en http://www.zdnet.com/pcweek/reviews/meth.html .

Perrochon, L., Kasriel, S. and Luckham, D. (1999). **Managing Event Processing Networks**. Technical Report CSLTR-99788, Computer Systems Laboratory, Stanford University.

Phillips, K. (1999). **NetProwler detects perimeter hack attacks**. PC Week, 16 (27), p. 73-74.

Phillips, K. (1999). **One if by Net, Two if by OS**. Disponible en http://www.zdnet.com/products/stories/ reviews/0,4161,389071,00.html

Porras, Ph., Neumann, P. and Linne, D. (1999). **The Common Intrusion Detection Framework Architecture.** Disponible en http://seclab.cs.ucdavis.edu/cidf/

Power, R. (1999). **CSI Round Table: Experts Discuss Present and Future Directions for ID Systems.** Computer Security Journal XIV, 1. Disponible en http://www.gocsi.com/roundtable.htm

Power, R. (1999). **Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey.** Computer Security Journal XV, 2. Disponible en http://www.gocsi.com/losses.htm.

Privacy.net (1999). **Privacy Analysis of Your Internet Connection—How It Works**. Disponible en http://privacy.net/analyze/analyzehow.asp

Prodromidis, A. and Stolfo, S. (1999). **Agent-Based Distributed Learning Aplied to Fraud Detection.** Technical Report CUCS-014-99, Department of Computer Science, Columbia University

Qianli, Z. and Xing, L. (1999). **Session State Transitian Based Large Network IDS**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Ranum, M. (1999). **A Taxonomy of Internet Attacks.** Disponible en http://www.clark.net/pub/mjr/pubs/index.shtml.

Ranum, M. (1999). **Some Tips on Network Forensics**. Computer Security Institute, 198 (September), p. 1-8.

Reuters (1999). **NATO Site, Email Suffers Hacks**. Disponible en http://news.cnet.com/news/0-1005-200-340625.html?tag=st.ne.1

Reuters (1999). **Some NASA Systems Easy Prey for Hackers**. Disponible en http://news.cnet.com/news/0-1005-200-342779.html?tag=st.ne.1005-200-343061

Reuters (1999). **White House Shuts down Web Site**. Disponible en http://news.cnet.com/news/0-1005-200-342364.html?tag=st.ne.1005-200-343118.

Ricciardi, S. (1999). **In pursuit of Internet intruders.** PC Magazine, 18 (21), p. 247-249.

Richards, K. (1999). **Network Based Intrusion Detection: A Review of Technologies.** Computers & Security, 18 (8), p. 671-682.

Riley, G. (1999). **CLIPS: A Tool for Building Expert Systems**. Disponible en http://www.ghg.net/clips/CLIPS.html

Robbins, J. (1999). **An Explanation of Computer Forensics**. Disponible en http://knock-knock.com/forens01.htm

Roesch, M. (1999). **Snort Lightweight Intrusion Detection for Networks**. In Proceedings of the USENIX LISA '99 conference.

Roesch, M. (1999). **The Snort Page**. Disponible en http://www.clark.net/~roesch/security.html.

Roger, M. (1999). **Analyse de Ficiliers de Logs**. Master's thesis, Université Paris 7 Denis Diderot, France.

Rowe, J. (1999). **Intrusion Detection and lsolation Protocol: Automated Response to Attacks**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Rubin, J. and O'Shea, T. (1999). **Axent NetProwler: Advanced Intrusion Detection On the Loose.** Network Computing, 10 (14), p. 17-18.

Ruiu, D. (1999). **Cautionary Tales: Stealth Coordinated Attack HOWTO.** Disponible en http://www.nswc.navy.mil/ISSEC/CID/Stealth_Coordinated_Attack.html

Sample, C. (1999). **A comparison of RealSecure and NetRanger.** Information Systems Security, 7 (4), p. 9-13.

Sandler, T. (1999). **Breaking into the bank. Institutional Investor**, 33 (9), p. 31-32.

SANS Institute Online. (1999). **SANS Institute Online—Home Page.** Disponible en http://www.sans.org/newlook/ home.htm

SANS Institute. (1999). **The 7 Top Management Errors that Lead to Computer Security Vulnerabilities**. Disponible en http://www.sans.org/newlook/resources/errors.htm

Schneier, B. and Kelsey, J. (1998). **Securing Network Audit Logs on Untrusted Machines**. In Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID'98). Disponible en http://www.raid-symposium.orgjraid98.

Schneier, B. and Kelsey, J. (1999). **Secure Audit Logs to Suport Computer Forensics**. ACM Transactions on Information and System Security, 1 (3), p. 23-36.

Schonlau, M., DuMouchel, W., Ju, W., Karr, A., Theus, M. and Vardi, Y. (1999). **Computer Intrusion: Detecting Masqueraders**. Technical Report TR95, National Institute of Statistical Sciences (NISS).

Schwartzbard, A. and Ghosh, A. (1999)**. A Study in the Feasibility of Performing Host-based Anomaly Detection on Windows NT**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/aid99.

Schwartzbard, A. and Ghosh, A. (1999). **Establishing Common Exploit Information for Intrusion Detection**. In Proceedings of the 2nd Workshop on Research with Security Vulnerability Databases.

Secure Computing (1999). **June 99 Intrusion Detection Market Survey**. Disponible en http://194.202.195.4/securecomputing/1999_06/survey/survey.html

Secure Computing (1999). **June 99 Intrusion Detection Market Survey— II.** Disponible en http://194.202.195.4/securecomputing/1999_06/survey/products_01.html

Secure Computing (1999). **June 99 Intrusion Detection Market Survey— III.** Disponible en http://194.202.195.4/securecomputing/1999_06/survey/products_02.html

Security Dynamics (1999). **Kane Security Monitor**. Disponible en http://www.securitydynamics.com/products/datasheets/kmds.html

Security Magazine (1999). **Security Suites**. Disponible en http://194.202.195.4/securecomputing/1999_02/testc/products.html

Security Magazine (1999). **Security Suites—II.** Disponible en http://194.202.195.4/securecomputing/1999_02/testc/products2.html

Security Research Alliance (1999). **Security Research Alliance—Overview**. Disponible en http://www.securityresearch.com/overviewmain.htm

Sekar, R. and Upuluri, P. (1999). **Synthesizing Fast Intrusion Prevention / Detection Systems from High-Level Specifications**. In Proceedings of the 8th USENIX Security Symposium.

Sekar, R., Bowen, T. and Segal, M. (1999). **On Preventing Intrusions by Process Behavior Monitoring**. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

Sekar, R., Guang, Y., Verma, S. and Shanbag, T. (1999). **A High-Performance Network Intrusion Detection System.** In Proceedings of the ACM Symposium on Computer and Communication Security (CCS'99).

Sellens, J. (1999). **On Reliability**. ;login: The USENIX Association Magazine (September), p. 46-52.

SEMPER. (1999). **IDWG Mail Archive**. Disponible en http://www.semper.org/idwg-public

Shankland, S. (1999). **U.S. Weapons Labs Shut Down Classified Networks**. (CNET News.com). Disponible en http://news.cnet.com/news/0-1003-200-340847.html?tag=st.ne.1002

Shipley, G. (1999). **ISS RealSecure Pushes Past Newer IDS Players**. Network Computing, 10 (10), p. 95-104.

Shipley, G. (1999). **Intrusion-Detection Systems.** Network Computing, 10 (20), p. 72-73.

Shipley, G. (1999). **Intrusion Detection, Take Two.** Network Computing, 10 (23), p. 44-57.

Siegel, C. (1999). **Intrusion detection: Making the business case**. Information Systems Security, 8 (2), p. 58-68.

Sielken, R. (1999). **Aplication Intrusion Detection**. Technical Report CS-99-17, Dept. of Computer Science, University of Virginia.

Sielken, R. and Jones, A. (1999). **Aplication Intrusion Detection Systems: The Next Step**. Disponible en http://www.cs.virginia.edu/~jones/IDSresearch/Documents/AplicationIDS_Jones-Sielken.pdf.

Sinclair, C., Pierce, L. and Matzner, S. P. (1999). **An Aplication of Machine Learning to Network Intrusion Detection**. In Proceedings ofthe 15th Annual Computer Security Aplications Conference (ACSAC'99).

Sitaker, K. (1999). **How to Find Security Holes**. Disponible en http://www.dnaco.net/~kragen/securityholes.html

Sobirey, M. (1999). **Michael Sobirey's ID Systems Page**. Disponible en http://www-rnks.informatik.tucottbus.de/~sobirey/ids.html

Sommer, P. (1999). **Intrusion detection systems as evidence.** Computer Networks, 31 (23/24), p. 2477-2487.

Song, D., Shaffer, G. and Undy, M. (1999). **Nidsbench a Network Intrusion Detection Test Suite.** In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99) . Disponible en http://www.raid-symposium.org/raid99.

Spafford, G. (1999). **Audit Trail Reduction**. Disponible en http://www.cs.purdue.edu/coast/projects/audit-trails-reduce.html.

Spafford, G. (1999). **Autonomous Agents for Intrusion Detection**. Disponible en http://www.cs.purdue.edu/coast/projects/autonomous-agents.html

Spafford, E. and Zamboni, D. (1999). **New directions for the AAFID architecture**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Spitzner, L. (1999). **How to Build a Honeypot**. Disponible en http://www.enteract.com/~lspitz/honeypot.html

Spitzner, L. (1999). **Know Your Enemy**. Disponible en http://www.enteract.com/~lspitz/enemy.html

Spitzner, L. (1999). **Know Your Enemy: II**. Disponible en http://www.enteract.com/~lspitz/enemy2.html

Spitzner, L. (1999). **Know Your Enemy: III**. Disponible en http://www.enteract.com/~lspitz/enemy3.html

Stallings, W. (1999). **IPv6: The New Internet Protocol**. Disponible en http://www.comsoc.org/pubs/surveys/stallings/stallings-orig.html

Staniford-Chen, S. (1999). **IDS Standards: Lessons Learned to Date**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Stillerman, M. and Marceau, C. (1999). **Intrusion detection for distributed applications.** Communications of the ACM, 42 (7), p. 62-69.

Stillerman, M., Marceau, C. and Stillman, M. (1999). **Intrusion Detection for Distributed Applications**. Communications of the ACM 42, 7 (July), p. 62-69.

Stocksdale, G. (1999). **CIDER Documents**. Disponible en http://www.nswc.navy.mil/ISSEC/CID/

Stocksdale, G. (1999). **NSA Glossary of Terms in Security and Intrusion Detection.** Disponible en http://www.sans.org/NSA/glossary.htm

Stolfo, S., Backenroth, A. and Chan, Ph. (1999). **The JAM Project**. Disponible en http://www.cs.columbia.edu/~sal/JAM/PROJECT/

Taber, M. (1999). **The Sams Crack Level Index, Ch. 26 Levels of Attack. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network.** Disponible en http://www.damocles.com/~kronvold/Hacker/docs/v0000027.htm

Takada, T. and Koike, H. (1999). **NIGELOG : Protecting Logging Information by Hiding Multiple Backups in Directories**. In Proceedings of the 10th International Workshop on Database and Expert Systema Aplications (DEXA '99).

Talpade, R., Kim, G. and Khurana, S. (1999). **NOMAD : Traffic-Based Network Monitoring Framework for Anomaly Detection.** In Proceedings of the Fourth IEEE Symposium on Computers and Communications.

The Internet Engineering Task Force (1999). **Overview of the IETF**. Disponible en http://www.ietf.org/overview.html

Ting, C., Ong, T., Tan, Y. and Ng, P. (1999). **Intrusion Detection, Internet Law Enforcement and Insurance Coverage to Accelerate the Proliferation of Internet Business**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Tobin, D. (1998). **Detecting Intrusions Cooperatively Across Multiple Domains**. IA Newsletter 2, 2 (Fall), p. 10.

Tripunitara, M. and Dutta, P. (1999). **A middleware aproach to asynchronous and backward compatible detection and prevention**. In Proceedings of the 15th Annual Computer Security Aplications Conference (ACSAC'99).

University of Idaho (1999). **Hummer Project Intrusion Detection System**. Disponible en http://www.csds.uidaho.edu/~hummer/home.html

Upadhyaya, S. J. and Kwiat, K. (1999). **A distributed concurrent intrusion detection scheme based on assertions**. In Proceedings of the SGS Intemational Symposium on Performance Evaluation of Gomputer and Telecommunication Systems, p. 369-376.

Van Doorn, L. (1999). **Computer Break-ins: A Case Study**. Disponible en http://www.alw.nih.gov/Security/FIRST/papers/general/holland.ps

Vandenwauver, M., Claessens, J., Moreau, W., Vaduva, C. and Maier, R. (1999). **Why Enterprises Need More than Firewalls and Intrusion Detection Systems**. In Proceedings of the Eighth IEEE Intemational Workshops on Enabling Technologies: Infrastructure for Gollaborative Enterprises (WETIGE'99), p. 152-157.

Velissarios, J. and Santarossa, R. (1999). **Practical security issues with high-speed networks.** Journal of High Speed Networks, 8 (4), p. 311-323.

Verton, D. (1999). **Cyberattacks Against DOD up 300 Percent this Year.** Disponible en http://www.fcw.com/fcw/articles/fcw_11031999_attack.asp

Vigna, G. and Kemmerer, R. (1999). **NetSTAT: A network-based intrusion detection system.** Journal of Computer Security, 7 (1), p. 37-71.

Vranesevich, J. (1999). **How to Become a Hacker Profiler**. Disponible en http://www.antionline.com/SpecialReports/profiling-index.html

Warrender, C., Forrest, S. and Pearlmutter, B. (1999). **Detecting Intrusions Using System Calls : Alternative Data Models**. In Proceedings of the 1999 IEEE Symposium on Security and Privacy.

Warshaw, L., Obermeyer, L., Miranker, D. and Matzner, S. (1999). **VenusIDS: An Active Database Component íor Intrusion Detection**. Technical Report LR-ISL--99-04, Aplied Research Laboratories, University of Texas, Austin.

Wee, C. (1999). **Audit logs: to keep or not to keep?**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/raid99.

Wespi, A. and Debar, H. (1999). **Building an Intrusion-Detection System to Detect Suspicious Process Behavior.** In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.raid-symposium.org/aid99.

Wespi, A., Dacier, M. and Debar, H. (1999). **An Intrusion-Detection System Based on the Teiresias Pattern-Discovery Algorithm**. Technical Report RZ3103, Zurich Research Laboratory, IBM Research Division.

Wespi, A., Dacier, M. and Debar, H. (1999). **Intrusion Detection Using Variable-Length Audit Trail Patterns**. Technical Report RZ 3164, IBM Zurich Research Laboratory. Disponible en http://domino.watson.ibm.com/library/CYBERDIG.NSF/95f0a8c5802d9417852566a90057461f/02a4ec9d5b79ae14852567da0034838f/$FILE/rz3164.ps.

Weston, R. (1999). **Security Survey Methodology**. Disponible en http://informationweek.com/743/securit2.htm

Wood, M. (1999). **Selecting a Site for the Software Sentry.** Security Management, 43 (12), p. 47-49.

Wu, T., Malkin, M. and Boneh, B. (1999). **Building intrusion tolerant aplications**. In Proceedings of the 8th USENIX Security Symposium.

Yasin, R. (1999). **Intrusion detectors get more precise, adaptable.** InternetWeek, n. 768, p. 1-2.

Yasin, R. (1999). **Users weed out bad applets.** InternetWeek, n. 763, p. 1-2.

Yasin, R. (1999). **Rise in Instrusions Sparks Concern**. Disponible en http://www.internetwk.com/story/INW19991130S0007

Yuill, J., Wu, S., Gong, F. and Huang, M. (1999). **Intrusion Detection for an On-Going Attack**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99). Disponible en http://www.cerias.purdue.edu/raidprog.html.

Zagar, M. (1999). **Data Compression Reference Center**. Disponible en http://www.rasip.fer.hr/research/ compress/index.html

8. INTRUSION DETECTION IN 2000

Abily, V. and Ducassé, M. (2000). **Benchmarking a distributed intrusion detection system based on ASAX: Preliminary results**. Extended abstract presented at RAID'2000.

Agarwal, R. and Joshi, M. (2000). **PNrule: A New Framework for Learning Classifier Models in Data Mining (A Case-Study in Network Intrusion Detection).** Technical Report RC 21719, IBM Watson Research Center.

Alessandri, D. (2000). **Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems**. Technical Report RZ3225, IBM Research, Zurich Research Laboratory.

Alessandri, D. (2000). **Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 183-196. Disponible en http://www.raid-symposium.org/raid2000/Materials/Papers/24/Alessandri_foils_RAID2000.pdf

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J. and Stoner, E. (2000). **State of the Practice of Intrusion Detection Technologies**. Technical Report CMU /SEI-99TR-028, Software Engineering Institute, Carnegie Mellon University. Disponible en http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf

Almgren, M., Debar, H. and Dacier, M. (2000). **A Lightweight Tool for Detecting Web Server Attacks**. In Proceedings of the Year 2000 Network and Distributed Systems Security Symposium (NDSS 2000).

Axelsson, S. (2000). **A Preliminary Attempt to Aply Detection and Estimation Theory to Intrusion Detection.** Technical Report 00-4, Dept. of Computer Engineering, Chalmers University of Technology. Disponible en http://www.ce.chalmers.se/staff/sax/detection-model.ps

Axelsson, S. (2000). **Aspects of the Modelling and Performance of Intrusion Detection**. Technical Report 319L, Department of Computer Engineering, Chalmers University of Technology. Disponible en http://www.ce.chalmers.se/staff/sax/ids-lic.pdf

Axelsson, S. (2000). **Intrusion Detection Systems: A Taxonomy and Survey**. Technical Report 99-15, Dept. of Computer Engineering, Chalmers University of Technology. Disponible en http://www.ce.chalmers.se/staff/sax/taxonomy.ps

Bass, T. (2000). **Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness**. Communications of the ACM, 43(4), p. 99-105.

Bass, T. (2000). **Intrusion Detection Systems And Multisensor Data Fusion.** Communications of the ACM, 43 (4), p. 99-107.

Bejtlich, R. (2000). **Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events**. Disponible en http://home.satx.rr.com/bejtlich/intv2-8.pdf.

Bejtlich, R. (2000). **Network Intrusion Detection and Third Party Effects**. Disponible en http://home.satx.rr.com/bejtlich/nid_3pev101.pdf.

Bellare, M. and Yee, B. (1997). **Forward Integtity For Secure Audit Logs**. Disponible en http://www.cs.ucsd.edu/~bsy/pub/fi.ps.

Bellovin, S. (2000). **The ICMP Traceback Message. Work in progress**. Disponible en http://www.research.att.com/~smb/papers/draft/bellovinitrace-OO.txt.

Bernaschi, M., Gabrielli, E. and Mancini, L. (2000). **Linux Kernel Enhancements for Immediate Intrusion Detection**. Disponible en ftp://ftp.iac.rm.cnr.it/pub/BufOverP/BufOverA.ps.gz.

Biskup, J. and Flegel, U. (2000). **On Pseudonymization of Audit Data for Intrusion Detection**. In Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, in Lecture Notes in Computer Science, number 2009, Springer-Verlag, Berlin, p. 161-180.

Biskup, J. and Flegel, U. (2000). **TransactionBased Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 28-48.

Bowen, T. and Segal, M. E. (2000). **Remediation of Aplication-Specific Security Vulnerabilities at Runtime**. IEEE Software, 17(5), p. 59--67.

Bowen, T., Chee, D., Segal, M., Sekar, R., Shanbhag, T. and Upuluri, P. (2000). **Building Survivable Systems: An Integrated Aproach Based on Intrusion Detection and Confinement**. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX'OO).

Bridges, S. and Vaughn, R. (2000). **Fuzzy Data Mining and Genetic AIgorithms Aplied to Intrusion Detection**. In Proceedings of the 23rd National Information Systems Security Conference (NISSC 2000). Baltimore, October. Disponible en http://www.cs.msstate.edu/~bridges/papers/nissc2000.pdf

Bridges, S. and Vaughn, R. (2000). **lntrusion Detection via fuzzy Data Mining**. In Proceedings of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, June 19-23, p.109-122. Disponible en http://www.cs.msstate.edu/~bridges/papers/Canada-00.pdf

Bruschi, D., Cavallaro, L. and Rosti, E. (2000). **Less harm, less worry or how to improve network security by bounding system offensiveness**. In Proceedings of the 16th Annual Computer Security Aplications Conference (ACSAC 2000).

Burch, H. and Cheswick, B. (2000). **Tracing Anonymous Packets to Their Aproximate Source.** In Proceedings of the 14th USENIX Systems Administration Conference (LISA 2000), p. 313-322.

Burgess, M., Haugerud, H. and Straumsnes, S. (2000). **Measuring system normality. Work in progress**. Disponible en http://www.iu.hioslo.nof-mark/research/MeasureSystem/.

Cannady, J. (2000). **Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks**. In Proceedings of the 23rd National Information Systems Security Conference (NISSC 2000).

Carver, C. and Pooch, U. (2000). **An Intrusion Response Taxonomy and its Role in Automatic Intrusion Response**. In Proceedings of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop, West Point, June 6-7, p. 129-135.

Carver, C., Hill, J., Surdu, J. and Pooch, U. (2000). **A Methodology for Using Intelligent Agents to provide Automated Intrusion Response**. In Proceedings of the IEEE Systems, Man and Cybernetics Information Assurance and Security Workshop, West Point, June 6-7, p. 110-116.

Cheung, S. and Levitt, K. N. (2000). **A FormalSpecification Based Aproach for Protecting the Domain Name System**. In International Conference on Dependable Systems and Networks (DSN'OO), p. 641-651.

Cooper, M. (2000). **An Intrusion Detection Systems (IDS) Overview**. Disponible en http://www.xinetica.com/tech_explained/general/ids/wp_ids.pdf.

Criscuolo, P. (2000). **Distributed Denial of Service**. Technical Report CIAC-2319, ClAC, Lawrence Livermore National Laboratory, US Department of Energy.

Cunningham, R. and Rieser, A. (2000). **Detecting Source Code of Attacks that Increase Privilege**. Extended abstract presented at RAID'2000.

Cupens, F. and Ortalo, R. (2000). **LAMBDA: A Language to Model a Database for Detection of Attacks**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 197-216.

Dailianas, A., Yemini, Y., Florissi, D. and Huang, H. (2000). **MarketNet: Market-Based Protection of Network Systems and Services An Aplication to SNMP Protection**. In Proceedings of the IEEE Infocom 2000.

Daniels, T. and Spafford, E. (2000). **Subliminal Traceroute in TCP/IP**. In Proceedings of the 23rd National Information Systems Security Conference (NISSC 2000).

Daniels, T. and Spafford, E. (2000). **A Network Audit System íor Host-based Intrusion Detection (NASHill) in Linux**. In Proceedings of the 16th Annual Computer Security Aplications Conference (ACSAC 2000) New Orleand.

Darling, T. and Shayman, M. (2000). **A Markov Decision Model for Intruder Location in IP Networks**. In Proceedings of the IEEE Conference on Decision and Control.

Darling, T. and Shayman, M. (2000). **Network Intrusion Location Using Markov Decision Processes**. Extended abstract presented at RAID'2000.

Debar, H., Dacier, M. and Wespi, A. (2000). **A Revised Taxonomy for Intrusion-Detection Systems**. Annales des Télécommunications, 55, p.7-8.

Deri, L. and Suin, S. (2000). **Improving Network Security Using Ntop**. Extended abstract presented at RAID'2000.

Dowland, P. and Fumen, S. (2000). **A conceptual intrusion monitoring architecture and thoughts on practical implementation**. In Proceedings of the World Computer Congress 2000.

Dowland, P. and Furnen, S. (2000). **Enhancing Operating System Authentication Techniques**. In Proceedings of the Second International Network Gonference (ING 2000), p. 253-261.

Dunigan, T. (2000). **Backtracking spoofed packets**. Disponible en http://www.epm.ornl.gov/~dunigan/oci/back.ps.

Dunigan, T. and Ostrouchov, G. (2000). **Flow Characterization for Intrusion Detection**. Disponible en http://www.epm.ornl.gov/~ost/id/tm.pdf.

Eckmann, S., Vigila, G. and Kemmerer, R. (2000). **STATL: An Attack Language for State-based Intrusion Detection**. In Proceedings of the ACM Workshop on Intr'Usion Detection.

Erbacher, R. and Frincke, D. (2000). **Visualization in detection of intrusions and misuse in large scale networks**. In Proceedings of the International Conference on Information Visualisation (IV2000), London, May 2000, p. 294-299. Disponible en http://www.csds.uidaho.edu/director/VisLarge.pdf

Eskin, E. (2000). **Anomaly Detection layer Noisy Data using Learned Probability Distributions**. In Proceedings of the Seventeenth International Conference on Machine Learning (ICML'OO). Palo Alto, July. Disponible en http://www1.cs.columbia.edu/ids/publications/anomaly-icml00.ps

Eskin, E., Miller, M., Zhong, Z., Yi, G., Lee, W. and Stolfo, S. (2000). **Adaptive Model Generation for Intrusion Detection Systems**. In Proceedings of the ACMCCS Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security, Athens, November. Disponible en http://www1.cs.columbia.edu/ids/publications/adaptive-ccsids00.pdf

Fan, W., Lee, W., Stolfo, S. and Miller, M. (2000). **A Multiple Model Cost-Sensitive Aproach for Intrusion Detection.** In Proceedings of the Eleventh European Conference on Machine Learning (ECML 2000), LNAI 1810, Barcelona, May. Disponible en http://www.cc.gatech.edu/~wenke/papers/ecml00.ps y también en http://www1.cs.columbia.edu/ids/publications/cost-ecml00.ps

Farley, T. (2000). **Visualization of lntrusion Detection Data**. Extended abstract presented at RAID'2000.

Feiertag, R. and Rho, S. (2000). **Intrusion detection inter-component adaptive negotiation.** Computer Networks, 34 (4), p. 605-621.

Feiertag, R., Kahn, C., Porras, P., Schnackenberg, D., Staniford-Chen, S. and Tung, B. (2000). **A Common Intrusion Specification Language (CISL)**. Specification draft. Disponible en http://www.gidos.org/drafts/language.txt.

Feiertag, R., Rho, S., Benzinger, L., Wu, S., Redmond, T., Zhang, C., Levitt, K., Peticolas, D., Heckman, M., Staniford-Chen, S. and McAlemey, J. (2000). **Intrusion Detection Inter-component Adaptive Negotiation**. Computer Networks, 34(4), p. 605--621.

Flack, C. and Atallah, M. (2000)**. Better Logging through Formality**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 1-16.

Forrest, S. and Hofmeyr, S. (2000). **Inmunology as Information Processing**. In Segel, L. A. and Cohen, l., *Design PrincipIes for the Immune System and Other Distributed Autonomous Systems*, Santa Fe Institute Studies in the Sciences of Complexity. Oxford University Press, p. 361-387.

Fratto, M. (2000). **Integrated Security Suites**. Network Computing, 11 (24), p. 85-87.

Fratto, M. (2000). **Security.** Network Computing, 11 (25), p. 29-33.

Frincke, D. (2000). **Balancing Cooperation and Risk in Intrusion Detection**. TISSEC, 3(1), p. 1-29. Disponible en http://www.csds.uidaho.edu/director/balcooprisk.pdf

Frincke, D. and Ming-Yuh, H. (2000). **Recent advances in intrusion detection systems.** Computer Networks, 34 (4), p. 541-545.

Furnell, S. and Dowland, P. (2000). **A conceptual architecture for real-time intrusion monitoring**. Information Management & Computer Security, 8(2), p. 65-75.

Ghosh, A., Michael, C. and Schatz, M. (2000). **A RealTime Intrusion Detection System Based on Learning Program Behavior**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 93-109.

Gigandet, C. (2000). **Integration of Host-based Intrusion Détection Systems into the Tivoli Enterprise Console**. Technical Report RZ3253, IBM Research, Zurich Research Laboratory.

Gil, T. (2000). **MULTOPS: a data-structure for denial-of-service attack detection**. Master's thesis, Division of Mathematics and Computer Science, Vrije Universiteit.

Gorodetski, V., Kotenko, l. and O.Karsaev (2000). **Framework for Ontology-based Representation of Distributed Knowledge in Multiagent Network Security System**. In Proceedings of the 4th World Multiconference on Systems, Cybernetics and Informatics (SCI-2000).

Han, J. (2000). **Near Real-Time Detection of Abnormal Network Behavior Using NetFlow**. Disponible en http://www.eecs.umich.edu/~jungheeh/prelim.pdf.

Higgins, K. (2000). **A Welcome Intrusion**. InternetWeek, nº. 815, p. 39-41.

Hoagland, J. (2000). **Specifying and Implementing Security Policies Using LaSCO, the Language for Security Constraints on Objects.** PhD thesis, Department of Computer Science, University of California,Davis.

Hofmeyr, S. and Forrest, S. (2000). **Architecture for an Artificial Immune System.** Evolutionary Computation, 8(4), p. 443473.

Hughes, J. (2000). **Conservation of Flow as a Security Mechanism in Network Protocols**. Master's thesis, Computer Science Department, University of California at Davis.

Hughes, J., Aura, T. and Bishop, M. (2000). **Using Conservation of Flow as a Security Mechanism in Network Protocols**. In Proceedings of the 2000 IEEE Symposium on Security and Privacy.

Hutchison, A. and Welz, M. (2000). **IDS/A: An Interface between Intrusion Detection System and Aplication**. Extended abstract presented at RAID'2000.

Ingram, D., Kremer, H. and Rowe, N. (2000). **Distributed Intrusion Detection for Computer Systems Using Communicating Agents**. In Proceedings of the 2000 Command and Control Research and Technology Symposium (CCRTS).

Jain, K. and Sekar, R. (2000). **User-Level Infrastructure for System Call Interposition : A Platform for Intrusion Detection and Confinement.** In Proceedings of the Year 2000 Network and Distributed Systems Security Symposium (NDSS 2000).

Jang, H. and Kim, S. (2000). **A Self-Extension Monitoring for Security Management**. In Proceedings of the 16th Annual Computer Security Aplications Conference (ACSA C 2000).

Jansen, W., Mell, P., Karygiannis, T. and Marks, D. (2000). M**obile Agents in Intrusion Detection and Response**. In Proceedings of the 12th Annual Canadian Information Technology Security Symposium.

Jon Doyle, H. and Szolovits, P. (2000). **On widening the scope of attack recognition languages**. Disponible en http://www.medg.lcs.mit.edu/projects/maita/documents/cc2/trends/examples.pdf

Julisch, K. (2000). **Dealing with False Positives in Intrusion Detection**. Extended abstract presented at RAID'2000. Disponible en http://www.raid-symposium.org/raid2000/Materials/Abstracts/50/50.pdf

Kent, S. (2000). **On the trail of intrusions into information systems**. IEEE Spectrum, 37 (12), p. 52-55.

Kerschbaum, F., Spafford, E. and Zamboni, D. (2000). **Using embedded sensors for detecting network attacks.** CERIAS TR 2000-25. Disponible en https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2000-25.pdf

Ko, C. (2000). **Logic Induction of Valid Behavior Specifications for Intrusion Detection**. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, p. 142-153.

Ko, C., Fraser, T., Badger, L. and Kilpatrick, D. (2000). **Detecting and Countering System Intrusions Using Software Wrapers**. In Proceedings of 9th USENIX Security Symposium (SEC 2000).

Krügel, C. and Toth, T. (2000). **A Survey on Intrusion Detection Systems**. Technical Report TUV-1841-00-11, Distributed Systems Group, Technical University of Vienna.

Kuri, J., Navarro, G., Mé, L. and Heye, L. (2000). **A Pattern Matching Based Filter for Audit Reduction and Fast Detection of Potential Intrusions.** In Proceedings of the Third lnternational Workshop on the Recent Advances in lntrusion Detection (RAlD'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 17-27. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/KNMH00.pdf

Kvarnstrom, H., Lundin, E. and Jonsson, E. (2000). **Combining fraud and intrusion detection meeting new requirements**. In Proceedings of the fifth Nordic Workshop on Secure lT Systems (NordSec2000).

Lee, W. and Stolfo, S. (2000). **A Framework for Constructing Features and Models for Intrusion Detection Systems**. ACM Transactions on Information and System Security (TISSE), 3(4), November. Disponible en http://www.cc.gatech.edu/~wenke/papers/ids_framework.ps

Lee, W., Fan, Stolfo, S. and Mok, K. (2000). **Adaptive Intrusion Detection: A Data Mining Approach**. Artificial Intelligence Review, Kluwer Academic Publishers, 14(6), p. 533-567, December. Disponible en http://www.cc.gatech.edu/~wenke/papers/ai_review.ps

Lee, W., Fan, W., Miller, M., Stolfo, S. and Zadok, E. (2000). **Toward Cost-Sensitive Modeling for futrusion Detection and Response**. In Proceedings of the Workshop on Intrusion Detection Systems, 7th ACM Conference on Computer and Communication Security. Athens, November. Disponible en http://www.cc.gatech.edu/~wenke/papers/cost_modeling.ps y también en http://www1.cs.columbia.edu/ids/publications/wenke-acmccsk2-cost.ps

Lee, W., Miller, M., Stolfo, S., Jalladand, K., Park, C., Zadok, E. and Prabhakar, V. (2000). **Toward Cost-Sensitive Modeling for Intrusion Detection**. Technical Report CUCS-002-00, Computer Science Department, Columbia University.

Lee, W., Nimbalkar, R., Yee, K., Patil, S., Desai, P., Tran, T. and Stolfo, S. (2000). **A Data Mining and CillF Based Aproach for Detecting Novel and Distributed futrusions**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), Toulouse, October, in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 49-65. Disponible en http://www.cc.gatech.edu/~wenke/papers/lee_raid.ps

Li, Y., Wu, N., Jajodia, S. and Wang, X. (2000). **Enhancing Profiles for Anomaly Detection Using Time Granularitie**s. In Proceedings of the first ACM Workshop on Intrusion Detection Systems.

Lindskog, S. (2000). **Observations on Operating System Security Vulnerabilities.** Licentiate thesis 332L, School of Electrical and Computer Engineering, Chalmers University of Technology, Göteborg.

Lippmann, R. and Haines, J. (2000). **Improving intrusion detection performance using keyword selection and neural networks.** Computer Networks**,** 34 (4), p. 597-613.

Lipmann, R., Haines, J., Fried, D., Korba, J. and Das, K. (2000). **Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 162-182. Disponible en http://www.raid-symposium.org/raid2000/Materials/Papers/27/RLippmann-RAID2000.pdf

Lipmann, R., Haines, J., Fried, D., Korba, J. and Das, K. (2000). **The 1999 DARPA off-line intrusion detection evaluation.** Computer Networks, 34 (4), p. 579-596.

Lipmann, R., Fried, D., Graf, l., Haines, J., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D., Cunningham, R. and Zissman, M. (2000). **Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation**. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition. Disponible en http://www.darpa.mil/itofpsum1998/F791-0.html

Liu, P., Jajodia, S. and McCollum, C. (2000). **Intrusion confinement by isolation in information systems.** Journal of Computer Security, 8 (4), p. 243-279.

Loyall, J., Pal, P., Schantz, R. and Webber, F. (2000). **Building Adaptive and Agile Aplications Using Intrusion Detection and Response**. In Proceedings of the Year 2000 Network and Distributed Systems Security Symposium (NDSS 2000).

Lundin, E. and Jonsson, E. (2000). **Anomaly-based intrusion detection: privacy concerns and other problems.** Computer Networks, 34 (4), p. 623-640.

Luo, J. and. Bridges, S. (2000). **Mining Fuzzy Association Rules and Fuzzy Frequency Episodes for Intrusion Detection**, *International Journal of Intelligent Systems*, 15(8), p.687-704.

Malan, G., Watson, D., Jahanian, F. and Howell, P. (2000). **Transport and Aplication Protocol Scrubbing**. In Proceedings of the IEEE INFOCOM 2000 Conference.

Maloof, M. and Michalski, R. (2000). **Selecting Examples for Partial Memory Learning**. Machine Learning, 41(1), p. 27-52.

Manganaris, S. and Christensen, M. (2000). **A data mining analysis of RTID alarms.** Computer Networks, 34 (4, p. 571-577.

Mansfield, G. and Ohta, K. (2000). **Towards trapping wily intruders in the large.** Computer Networks, 34 (4), p. 659-670.

Mantha, K., Chinchani, R., Upadhyaya, S. and Kwiat, K. (2000). **A Comprehensive Simulation Platform for Intrusion Detection in Distributed Systems**. In Proceedings of the 2000 Summer Computer Simulation Conference (SCSC 2000).

Manzano, Y. (2000). **Policies to Enhance Computer and Network Forensics**. Technical Report TR-000902, Computer Science Department, Florida State University.

Marceau, C. (2000). **Characterizing the Behavior of a Program Using Multiple-Length N-grams**. In Proceedings of the New Security Paradigms Workshop 2000.

Marrakchi, Z., Mé, L., Vivinis, B. and Morin, B. (2000). **Flexible Intrusion Detection Using Variable-Length Behavior Modeling in Distributed Environment: Aplication to CORBA Objects**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID '2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 130-144. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/MMVM00.pdf

Maxion, R. and Tan, K. (2000). **Benchmarking Anomaly-Based Detection Systems**. In International Conference on Dependable Systems and Networks, New York, IEEE Computer Society Press, p. 623-630.

McHugh, J. (2000). **The 1998 Lincoln Laboratory IDS Evaluation**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 145-161.

Mell, P.and Marks, D. (2000). **A denial-of-service resistant intrusion detection architecture**. Computer Networks, 34 (4), p. 641-658.

Morris, J. (2000). **Second looks**. PC Magazine, 19 (5), p. 74-75.

Mukkamala, R., Gagnon, J. and Jajodia, S. (2000). **Integrating data mining techniques with intrusion detection**. In Atluri, V. and Hale, J. *Research Advances in Database and Inlormation Systems Security*, p. 33-46. Kluwer Publishers.

Nauta, K. and Lieble, F. (2000). **Offtine Network Intrusion Detection: Looking for Footprints.** Disponible en http://www.sas.com/solutions/public_sector/white_papers/30626_0200.pdf.

Neely, D. (2000). **Pioneering Security**. Security Management, 44 (7), p. 24-25.

Ning, P., Wang, X. and Jajodia, S. (2000). **A Query Facility for Common Intrusion Detection Framework**. In Proceedings of the 2Srd National Information Systems Security Conference (NISSC 2000).

Ning, P., Wang, X. and Jajodia, S. (2000). **Modeling Requests among Cooperating Intrusion Detection Systems**. Computer Communications, 23(17), p. 1702-1715.

Oman, P., Schweitzer, E. and Frincke, D. (2000). **Concerns about Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems**. In Proceedings of the 27th Annual Western Protective Relay Conferences, October. Disponible en http://www.csds.uidaho.edu/director/SCADA.pdf

Pal, P., Webber, F., Schantz, R. and Loyall, J. (2000). **Intrusion Tolerant Systems**. In Proceedings of the Third Information Survivability Workshop (ISW-2000).

Park, K. and Lee, H. (2000). **A proactive aproach to distributed DoS attack prevention using route-based packet filtering**. Technical Report CSD-TR-00-017, Dept. of Computer Sciences,Purdue University.

Perrochon, L., Jang, E., Kasriel, S. and Luckham, D. (2000). **Enlisting Event Patterns for Cyber Battlefield Awareness**. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX'OO).

Petkac, M. and Badger, L. (2000). **Security Agility in Response to Intrusion Detection**. In Proceedings of the 16th Annual Computer Security Aplications Conference (ACSAC 2000).

Portnoy, L. (2000). **Intrusion Detection with Unlabeled Data using Clustering.** Undergraduate Thesis. Columbia University: December. Disponible en http://www1.cs.columbia.edu/ids/publications/cluster-thesis00.pdf

Pouzol, J. (2000). **Détection d'Intrusions dans les Systemes Informatiques**. Master's thesis, Institut de Formation Supérieure en Informatique, Université de Rennes 1.

Pouzol, J. and Ducassé, M. (2000). **Handling Generic Intrusion Signatures is not Trivial**. Extended abstract presented at RAID'2000.

Ragsdale, D., Carver, C., Humphries, J. and Poocil, U. (2000). **Adaptation Techniques for Intrusion Detection and Intrusion Response.** In Proceedings of the 2000 IEEE International Conference on Systems, Man, and Cybernetics (SMC 2000), p. 2344-2349.

Rapoza, J. (2000). **Icepac puts hack attempts in deep freeze**. PC Week, 17 (14), p. 79-80.

Rathmell, A., Dorscilner, J., Knights, M. and Watkins, L. (2000). **Early Warning & Threat Assessment for Information Assurance**. Extended abstract presented at RAID'2000.

Reshef, E. (2000). **Closing those e-business application loopholes.** Communications News, 37 (4), p. 30-31.

Rhodes, B., Mahaffey, J. and Cannady, J. (2000). **Multiple Self-Organizing Maps for Intrusion Detection**. In Proceedings of the 29rd National Information Systems Security Conference (NISSC 2000).

Riordan, J. and Alessandri, D. (2000). **Target Naming and Service Apoptosis**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 217-226.

Savage, S., Wetherall, D., Karlin, A. and Anderson, T. (2000). **Practical Network Suport for IP Thaceback**. In Proceedings of the 2000 ACM SIGCOMM Conference, p. 295-306.

Schick, S. (2000). **Hackers will get in at some point: Author.** Computer Dealer News, 16 (22), p. 1-2.

Schnackenberg, D., Djahandari, K. and Sterne, D. (2000). **Infrastructure for Intrusion Detection and Response**. In Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'OO).

Schonlau, M. and Theus, M. (2000). **Detecting masquerades in intrusion detection based on unpopular commands.** Information Processing Letters, 76 (1/2), p. 33-38.

Seleznyov, A. (2000). **Using Temporal-Probabilistic Network Aproach for Automatic Pattern Generation in Misuse Intrusion Detection**. In Proceedings of the 15th International Symposium on Computer and Information Sciences (ICSIC 2000).

Shipley, G. (2000). **Watching the Watchers: Intrusion Detection**. Network Computing, 11 (22), p. 135-141.

Sieglein, W. (2000). **Be Very E-fraid: Protecting Your Network from the Dangers of E-Commerce**. Business Credit, 102 (9), p. 42-44.

Somayaji, A. and Forrest, S. (2000). **Automated Response Using System-Call Delays**. In Proceedings of 9th USENIX Security Symposium (SEG 2000).

Song, D. and Perrig, A. (2000). **Advanced and Authenticatd Marking Schemes for IP Traceback**. Technical Report UCB/CSD00-1107, Computer Science Division, University of California, Berkeley.

Spafford, E. and Zamboni, D. (2000). **Data Collection Mechanisms for Intrusion Detection Systems**. Techreport CERIAS TR 2000-08. Disponible en https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2000-08.pdf

Spafford, E. and Zamboni, D. (2000). **Intrusion detection using autonomous agents.** Computer Networks, 34 (4), p. 547-571.

Spafford, E. and Zamboni, D. (2000). **Design and implementation issues for embedded sensors in intrusion detection**. Extended abstract presented at RAID'2000.

Staniford, S., Hoagland, J. and McAlerney, J. M. (2000). **Practical Automated Detection of Stealthy Portscans**. In Proceedings of the 7th AGM Gonlerence on Gomputer and Gommunication Security (GGS 2000).

Staniford-Chen, S. (2000). **IDWG: Progress towards an open IDS alert standard**. Extended abstract presented at RAID'2000.

Stephenson, P. (2000). **Where Is the IDS?** Information Systems Security, 8 (4), p. 6-11.

Stephenson, P. (2000). **The Aplication of Intrusion Detection Systems in a Forensic Environment**. Extended abstract presented at Third International Workshop on the Recent Advances in Intrusion Detection (RAID 2000), Toulouse. Disponible en http://www.raidsymposium.org/raid2000/program.html

Stocksdale, G. (2000). **NSA Glossary of Terms Used in Security and Intrusion Detection**. Disponible en http://www.sans.org/newlook/resources/glossary.htm.

Stolfo, S., Fan, W., Lee, W., Prodromidis, A. and Chan, P. (2000). **Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAMProject**. In Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'2000). IEEE Computer Press, p. II 130-144. Disponible en http://cs.fit.edu/~pkc/papers/discex00.pdf y también en http://www1.cs.columbia.edu/ids/publications/cucs-002-00.ps

Stone, R. (2000). **CenterTrack: An IP averIar Network for Tracking DoS Floods**. Disponible en http://www.us.uu.net/gfx/projects/security/centertract_new.pdf

Swimmer, M. (2000). **Review and Outlook ofthe Detection of Viruses using Intrusion Detection Systems**. Extended abstract presented at RAID'2000.

Takada, T. and Koike, H. (2000). **Tudumi: Log Jnformation Visualization System for Intrusion Detection**. Technical Report UEC-IS-TR-2000-08, Graduate school of Information Systems, University Of Electro-Communications, Tokyo.

Tarman, T. and Witzke, E. (2000). **Intrusion Detection Considerations for Switched Networks.** Technical Report SAND2000-1570C, Sandia National Laboratories.

Toelle, J. and Niggemann, O. (2000). **Suporting Intrusion Detection by Graph Clustering and Graph Drawing**. Extended abstract presented at RAID'2000.

Valdes, A. and Skinner, K. (2000). **Adaptive, Model-Based Monitoring for Cyber Attack Detection.** In Proceedings of the Third Intemational Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907, Springer-Verlag, Berlin, p. 80-92. Disponible en http://www.sdl.sri.com/papers/adaptbn/.

Valdes, A. and Skinner, K. (2000). **Adaptive, Model-Based Monitoring And Threat Detection.** SRI International. Disponible en http://www.raid-symposium.org/raid2000/Materials/Papers/Valdes/avaldes_raidA.pdf

Vigna, G., Eckmann, S. and Kemmerer, R. (2000). **Attack Languages**. In Proceedings of the IEEE Information Survivability Workshop.

Vigna, G., Eckmann, S. and Kemmerer, R. (2000). **The STAT Tool Suite**. In Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX'OO).

Wagner, D., Foster, J., Brewer, E. and Aiken, A. (2000). **A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities**. In Proceedings of the Year 2000 Network and Distributed Systems Security Symposium (NDSS 2000).

Watkins, A. (2000). **An immunological Aproach to Intrusion Detection**. In Proceedings of the 12th Annual Canadian Information Technology Security Symposium.

Wespi, A., Dacier, M. and Debar, H. (2000). **Intrusion Detection Using Variable-Length Audit Trail Patterns**. In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID'2000), in Lecture Notes in Computer Science, number 1907,Springer-Verlag, Berlin, p. 110-129.

Wespi, A., Debar, H., Dacier, M. and Nassehi, M. (2000). **Fixed- vs. variable-length patterns for detecting suspicious process behavior.** Journal of Computer Security, 8 (2/3), p. 159-181.

Yaghmour, K. and Dagenais, M. R. (2000). **Measuring and Characterizing System Behavior Using Kernel-Level Event Logging.** In Proceedings of 2000 USENIX Annual Technical Conference.

Yang, J., Ning, P., Wang, X. S. and Jajodia, S. (2000). **CARDS: A Distributed System for Detecting Coordinated Attacks**. In Proceedings of the 15th International Conference on Information Security (IFIP/SEC 2000), p. 171-180.

Yasinsac, A. (2000). **Detecting Intrusions in Security Protocols**. In Proceedings of the 7th ACM Conference on Computer and Communication Security.

Yuill, J. and Wu, F. (2000). **Intrusion-detection for incident-response, using a military battlefield-intelligence process.** Computer Networks, 34 (4), p. 671-697.

Zamboni, D. (2000). **Doing Intrusion Detection Using Embedded Sensors**. Techreport CERIAS TR 2000-21. Disponible en https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2000-21.pdf

Zhang, Y. and Lee, W. (2000). **Intrusion Detection in Wireless Ad-Hoc Networks.** In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000). Boston, August. Disponible en http://www.cc.gatech.edu/~wenke/papers/mobicom00.ps

Zhang, Y. and Paxson, V. (2000). **Detecting Backdoors**. In Proceedings of the 9th USENIX Security Symposium.

Zhang, Y. and Paxson, V. (2000). **Detecting Steping Stones**. In Proceedings of the 9th USENIX Security Symposium.

9. INTRUSION DETECTION IN 2001

Alberts Ch. and Dorofee A. (2001). **OCTAVESM Criteria, Version 2.0** TECHNICAL REPORT (CMU/SEI-2001-TR-016). Disponible en http://www.cert.org/archive/pdf/01tr016.pdf

Agarwal, R. and Joshi, M. (2001). **PNrule: A New Framework for Learning Classifier Models in Data Mining (A Case Study in Network Intrusion Detection)**. In Proceedings of the first SIAM International Conference on Data Mining.

Alessandri, D., Cachin, Ch., Dacier, M., Deak, O., Julisch, K., Randell, B., Riordan, J., Tscharner, A., Wespi, A. and Wuest, C (2001) **Towards a taxonomy of intrusion detection systems and attacks.** Technical Report Research Report RZ-3366, IBM Research, Zurich Research Laboratory.

Allaire (2001). **Detecting Intrusions: Methods of detecting intrusion attempts and security breaches**. Disponible en http://www.allaire.com/DocumentCenter/Partners/ASZ_ASWPS_Detecting_Intrusions. pdf.

Allen, Julia (2001). **The CERT® Guide To System and Network Security Practices.** Addison-Wesley. Disponible en http://www.cert.org/security-improvement/#modules

Almgren, M. and Lindqvist, U. (2001). **Aplication-Integrated Data Collection for Security Monitoring**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 22-36. Disponible en http://www.sdl.sri.com/papers/raid2001/.

Asaka, M., Onabuta, T., Inoue, T., Okazawa, S. and Goto, S. (2001). **A New Intrusion Detection Method Based on Discriminant Analysis**. IEICE Transactions on Information and Systems, E84-D(5), p. 570-577.

Aslam, J., Cremonini, M., Kotz, D. and Rus, D. (2001). **Using Mobile Agents íor Analyzing Intrusion in Computer Networks**. In Proceedings of the Workshop on Mobile Object Systems at ECOOP 2001.

Baccala, B. (2001). **TCPdump. Connected: An Internet Encyclopedia**, 3rd ed. Disponible en http://www.freesoft.org/CIE/Topics/55.htm.

Barbara, D., Wu, N. and Jajodia, S. (2001). **Detecting Novel Network Intrusions Using Bayes Estimators**. In Proceedings of the first SIAM lntemational Conference on Data Mining (SDM 2001).

Barber, R. (2001). **The Evolution of Intrusion Detection Systems--The Next Step.** Computers & Security, 20 (2), p. 132-145.

Biermann, E., Cloete, E. and Venter, L. (2001). **A comparison of Intrusion Detection systems.** Computers & Security, 20 (8), p. 676-683.

Cabrera, J., Lewis, L., Qin, X., Lee, W., Prasanth, R., Ravichandran, B. and Mehra, R. (2001). **Proactive Detection of Distributed Denial of Service Attacks U sing MIB Thaffic Variables A Feasibility Study**. In Proceedings of the seventh IFIP/IEEE International Symposium on Integrated Network Management (IM 2001), Seattle, May. Disponible en http://www.cc.gatech.edu/~wenke/papers/im01.ps

Cédric, M. and Mé, L. (2001). **ADeLe: an Attack Description Language for Knowledge-based Intrusion Detection**. In Proceedings of the 16th International Conference on Information Security. Kluwer. June. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/MM01.pdf

Coit, C., Staniford, S. and McAlerney, J. (2001). **Towards Faster Patern Matching for Intrusion Detection or Exceeding the Speed of Snort.** In DARPA Information Survivability Conference and Exposition (DISCEX II).

Crosbie, M. and Kuperman, B. (2001). **A Building Block Aproach to Intrusion Detection**. Short paper presented at RAID'2001.

Cruickshank, D. (2001). **Who's Hacking Into Your System Now?** Canadian Manager, 26 (2), p. 12-13.

Cunningham, R. and Stevenson, C. S. (2001). **Accurately Detecting Source Code of Attacks That Increase Privilege**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 104-116.

Curry D. and Debar, H. (2001). **Intrusion detection message exchange format data model and extensible markup language (XML) document type definition**. Internet draft. Disponible en http://www.ietf.org/internetdrafts/draft-ietf-idwg-idmef-xml-05.txt

Dan Z., Premkumar, G., Xiaoning Z. and Chao-Hsien C. (2001). **Data Mining for Network Intrusion Detection: A Comparison of Alternative Methods.** Decision Sciences, 32 (4), p. 635-660.

DARPA (2001). **DARPA intrusion detection evaluation**. Disponible en http://www.ll.mit.edu/IST/ideval/

Debar, H. and Wespi, A. (2001). **Aggregation and Correlation of Intrusion-Detection Alerts**. Technical Report RZ3360, IBM Research, Zurich Research Laboratory.

Debar, H. and Wespi, A. (2001). **Aggregation and Correlation of Intrusion-Detection Alerts**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), number 2212, p. 85-103.

Deri, L., Suin, S. and Maselli, G. (2001). **Design and Implementation of an Anomaly Detection System: an Empirical Aproach**. Submitted to NOMS'2002. Disponible en http://luca.ntop.org/ADS.pdf.

Dickerson, J. A., Dickerson, J. E., Juslin, J. and Koukousoula, N. (2001). **Charocterizing Intrusions with Visual Data Mining**. Disponible en http://www.cs.hut.fi/~juslin/fire_specs.pdf.

Douglas, M. and Chan, P. (2001). **A Protocol Language Approach to Generating Client-Server Software.** In Proceedings of Thirteenth International Conference Parallel and Distributed Computing and Systems, p. 649-654. Disponible en http://cs.fit.edu/~pkc/papers/pdcs01.pdf

Doyle, J., Kohane, l., Long, W., Shrobe, H. and Szolovits, P. (2001). **Agile Monitoring for Cyber Defense**. In Proceedings of the Second DARPA Information Suroivability Gonference and Exposition (DISGEX-II).

Doyle, J., Kohane, l., Long, W., Shrobe, H. and Szolovits, P. (2001). **Event Recognition Beyond Signature and Anomaly**. In Proceedings of the 2001 IEEE Workshop on Information Assumnce and Security, p. 17-23.

Eckmann, S. (2001). **Translating Snort rules to STATL scenarios**. Short paper presented at RAID'2001.

Eckmann, S., Vigila, G. and Kemmerer, R. (2001). **STATL Definition**. Technical Report 2000-19, Department of Computer Science, University of California, Santa Barbara.

Erbacher, R. and Frincke, D. (2001). **Visual Behavior Characterization for Intrusion and Misuse Detection**. In Proceedings of the SPIE 2001 Conference on Visual Data Exploration and Analysis VIII, San Jose, p. 210-218. Disponible en http://www.csds.uidaho.edu/director/VisBehavior.pdf

Eskin, E., Lee W. and Stolfo, S. (2001). **Modeling System Calls for Intrusion Detection with Dynamic Window Sizes**. In Proceedings of DISCEX II. June. Disponible en http://www1.cs.columbia.edu/ids/publications/smt-syscall-discex01.pdf

Fan, W., Miller, M., Stolfo, S., Lee, W. and Chan, P. (2001). **Using Artificial Anomalies to Detect Unknown and Known Network Intrusions.** In Proceedings of the First IEEE International Conference on Data Mining, San Jose, November. Disponible en http://www.cc.gatech.edu/~wenke/papers/artificial_anomalies.ps y también en http://cs.fit.edu/~pkc/papers/icdm01.pdf

Feinstein, B., Matthews, G. and White, J. (2001). **The intrusión detection exchange protocol (idxp)**. Internet draft. Disponible en http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-03.txt

Flajolet, P., Guivarch, Y., Szpankowski, W. and Vallee, B. (2001). **Hidden Pattern Statistics**. In Proceedings of the Twenty-Eighth International Colloquium on Automata, Languages and Programming (ICALP 2001).

Forrest, S. and Hofmeyr, S. (2001). **Engineering an immune system.***Graft*. 4(5), p. 5-9. Disponible en http://www.cs.unm.edu/~forrest/publications/EIS.pdf

Forrest, S. and Hofmeyr, S. (2001). **Immunology as information processing.** In L.A. Segel and I. Cohen, *Design Principles for the Immune System and Other Distributed Autonomous Systems*. Santa Fe Institute Studies in the Sciences of Complexity. New York, Oxford University Press. Disponible en http://www.cs.unm.edu/~forrest/publications/iaipEIS.pdf

Frincke, D. and Wilhite, E. (2001). **Distributed Network Defense**. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, West Point, June, p. 236-238. Disponible en http://www.csds.uidaho.edu/director/Dis.NetworkDef.pdf

Fumell, S., Magklaras, G., Papadaki, M. and Dowland, P. (2001). **A Generic Taxonomy for Intrusion Specification and Response**. In Proceedings of Euromedia 2001.

Gaffney, J. and Ulvila, J. (2001). **Evaluation of Intrusion Detectors: A Decision Theory Aproach**. In Proceedings of the 2001 IEEE Symposium on Security and Privacy.

Gil, T. and Poletto, M. (2001). **MULTOPS: a datastructure for bandwidth attack detection**. In Proceedings of the 10th USENIX Security Symposium.

Gopalakrishna, R. (2001). **A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents**. Technical Report 2001-44, CERlAS, Department of Computer Science, Purdue University.

Goregaoker, S. (2001). **A Method for Detecting Intrusions on Encrypted Traffic**. Master's thesis, Department of Computer Science, Florida State University.

Graham, R. (2001). **NIDS-Pattern Search vs. Protocol Decode**. Computers & Security, 20 (1), p. 37-41

Greenberg, E. and McLaughlin, C. (2001). **Eliminate Security Risks**. PC Magazine, 20 (18), p. 78-81.

Hartje, R. (2001). **NFR appliance nips, analyzes attacks.** eWeek, 18 (7), p. 68-69.

Hedbom, H., Lindskog, S. and Jonsson, E. (2001). **Risks and dangers of security extensions**. In Proceedings of Security and Control of IT in Society-II (IFIP SCITS-II), Bratislava, June 15-16, p. 231-248.

Helmer, G., Wong, J., and Madaka,S. (2001). **Anomalous intrusion detection system for hostile Java applets.** Journal of Systems & Software, 55 (3), p. 273-286. Disponible en http://www.palisadesys.com/~ghelmer/Papers/JSS-HostileApplets.ps

Helmer, G., Wong, J., Slagell, M., Honavar, V., Miller, L. and Lutz, R. (2001). **A Software Fault Tree Aproach to Requirements Analysis of an Intrusion Detection System.** In Proceedings of the 1st Symposium on Requirements Engineering for Information Security. Disponible en http://www.palisadesys.com/~ghelmer/Papers/SFTA-ID.ps

Helmer, G., Wong, J., Slagell, M., Honavar, V., Miller, L. and Lutz, R. (2001). **Software Fault Tree and Colored Petri Net Based Specification, Design and Implementation of Agent-Based Intrusion Detection Systems**. Disponible en http://www.palisadesys.com/~ghelmer/Papers/CPN-IDS.ps

Hossain, M. and Bridges, S. (2001). **A framework for an adaptive intrusion detection system with data mining**. In Proceedings of the 13th Annual Canadian Information Technology Security Symposium, Ottawa, June. Disponible en http://www.cs.msstate.edu/~bridges/papers/citss-2001.pdf

Hu V., Frincke, D. and Ferraiolo, D. (2001).T**he Policy Machine for Security Policy Management.** International Conference on Computational Science. Vol.2, p 494-506. Disponible en http://www.csds.uidaho.edu/director/policymachine.pdf

Huin, M. (2001). **Pattern Matching et détection d'intrusion**. Disponible en http://eleves.mines.u-nancy.fr/~huin/fake/filtres.html.

Ingram, D., Kremer, H. and Rowe, N. (2001). **Distributed Intrusion Detection for Computer Systems Using Communicating Agents**. In Proceedings of the 6th International Command and Control Research and Technology Symposium (CCRTS 2001).

Inoue, H. and Forrest, S. (2001). **Anomaly Intrusion Detection at the Aplication Layer**. Short paper presented at RAID'2001.

ISSOFNSA (2001). **Intrusion Detection Tools**. Disponible en http://www.nswc.navy.mil/ISSEC/CID /id_secure.mdb.

Johnston, S. (2001). **The Impact of Privacy and Data Protection Legislation on the Sharing of Intrusion Detection Information**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 150-171.

Ju, W. and Vardi, Y. (2001). **Profiling UNIX Users And Processes Based on Rarity of Occurrence Statistics with Aplications to Computer Intrusion Detection**. Short paper presented at RAID'2001.

Kilpatrick, I. (2001). **Set a Honey Pot Trap to Improve Your Security**. British Journal of Administrative Management, Nov/Dec, 28, p. 16.

Ko, C., Brutch, P., Rowe, J., Tsafnat, G. and Levitt, K. (2001). **System Health and Intrusion Monitoring Using a Hierarchy of Constraints**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 190-204.

Krügel, C. and Toth, T. (2001). **Aplying mobile agent technology to intrusion detection**. In Proceedings of the ICSE Workshop on Software Engineering and Mobility.

Krügel, C. and Toth, T. (2001). **Sparta A mobile agent based intrusion detection system.** In Proceedings of the First International IFIP TC-11 Working Conference on Network Security.

Lee, W. and Xiang, D. (2001). **Information-Theoretic Measures for Anomaly Detection**. In Proceedings of the 2001 IEEE Symposium on Security and Privacy. Oakland, May 2001. Disponible en http://www.cc.gatech.edu/~wenke/papers/entropy_modeling.ps

Lee, W., Stolfo, S., Chan, P., Eskin, E., Fan, W., Miller, M., Hershkop, S. and Zhang, J. (2001). **Real Time Data Mining-based Intrusion Detection.** In Proceedings of the Second DARPA Information Survivability Conference and Exposition (DISCEX II), p. 85-100. Disponible en http://cs.fit.edu/~pkc/papers/discex01.pdf y también en http://www.cc.gatech.edu/~wenke/papers/dids_discex01.ps

Lindqvist, U. and Porras, Ph. (2001). **eXpert-BSM: A Host-based Intrusion Detection Solutions for Sun Solaris**. Disponible en http://www.sdl.sri.com/papers/expertbsm-acsac01/.

Liu, Q., Bridges, S. and Banicescu, I. (2001). **Parallel genetic algorithms for tuning a fuzzy data mining system**. In Proceedings of the Artificial Neural Networks in Engineering Conference (ANNIE 2001), St. Louis, November 4-7. Disponible en http://www.cs.msstate.edu/~bridges/papers/annie2001.pdf

Luo, J., Bridges, S. and Vaughn, R. (2001). **Fuzzy Frequent Episodes for Real-time Intrusion Detection.** FUZZIEEE 2001, Melbourne, December 2-5. Disponible en http://www.cs.msstate.edu/~bridges/papers/fuzzieee-2001.pdf

Mahoney, M. and Chan, P. (2001). **Detecting Novel Attacks by Identifying Anomalous Network Packet Headers**. Technical Report CS-2001-2, Department of Computer Sciences, Florida Institute of Technology.

Marchette, D. (2001). **Computer Intrusion Detection and Network Monitoring.**Springer-Verlag, New York.

McNichols, S. (2001). **What's New with Outdoor Security**. SDM: Security Distributing & Marketing, 31 (10), p. 63-66.

Mé, L. and Cédric, M. (2001). **Intrusion Detection: A Bibliography**. Supélec. Technical report SSIR-2001-01. September. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/bibid_raid2001.ps

Mé, L., Cédric, M. and Heye, L. (2001). **A language for a comprehensive description of attacks**. Short paper presented at the 2001 IEEE Symposium on Security and Privacy, Oakland, May. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/oaklan01.pdf

Mé, L., Marrakchi,Z., Cédric, M., Debar, H. and Cuppens, F. (2001). **La détection d'intrusions : les outils doivent coopérer.** Revue de l'Electricité et de l'Electronique. No 5, mai, p. 50-55. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/Mal.01.pdf

Meier, M. and Holz, T. (2001). **Intrusion Detection Systems List and Bibliography**. Disponible en http://www-rnks.informatik.tucottbus.dejenjsecurity jids.html.

Mueller, P.and Shipley, G. (2001). **To Catch A Thief**. Network Computing, 12 (17), p. 36-39.

Mueller, P.and Shipley, G. (2001). **Dragon Claws Its Way To The Top.** Network Computing, 12 (17), p. 45-57.

Park, K. and Lee, H. (2001). **On the Effectiveness of Probabilistic Packet Marking for IP Thaceback under Denial of Service Attack**. In Proceedings of the IEEE Infocom 2001.

Park, K. and Lee, H. (2001). **On the effectiveness of route-based packet filtering for distributed DoS attack prevention in powerlaw internets**. In Proceedings of ACM SIGCOMM 01.

Patton, S., Yurcik, W. and Doss, D. (2001). **An Achilles Heel in Signature-Based IDS: Squealing False Positives in SNORT.** Short paper presented at RAID'2001.

Paul, B. (2001). **DoS: Internet Weapons of Mass Destruction**. Network Computing, 12 (1), p. 67-70.

Pepe, M. (2001). **Protecting Your Client.** Computer Reseller News, 9/10/2001, n. 962, p. 52-58.

Ploskina, B. (2001). **A Net Unprotected**. Interactive Week, 8 (30), p. 13-14.

Ploskina, B. (2001). **Seek and Destroy.** Interactive Week, 8 (33), p. 45-47.

Portnoy, L., Eskin, E. and Stolfo, S. (2001). **Intrusion detection with unlabeled data using clustering.** In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001). Philadelphia, November 5-8. Disponible en http://www1.cs.columbia.edu/ids/publications/cluster-ccsdmsa01.pdf

Pouzol, J. and Ducassé, M. (2001). **From Declarative Signatures to Misuse IDS**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 1-21.

Roger, M. and Goubault-Larrecq, J. (2001). **Log auditing through model cilecking**. In Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW'01), p. 220-236.

Rossey, L., Cunningham, R., Fried, D., Rabek, J., Lipmann, R. and Haines, J. (2001). **LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed.** Short paper presented at RAID'2001.

Samarah, M. and Chan, P. (2001). **Distributed Communication for Highly Mobile Agents**, Fourth Pacific Rim International Workshop on Multi-agents. Disponible en http://cs.fit.edu/~pkc/papers/prima01.pdf

Sanchez, L., Milliken, W., Snoeren, A., Tchakountio, F., Jones, C., Kent, S., Partridge, C. and Strayer, W. (2001). **Hardware Suport for a Hash-Based IP Thaceback**. In Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEX 11), p. 146-152.

SANS Institute (2001). **Intrusion Detection FAQ**. Disponible en http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

Savage, S., Wetherall, D., Karlin, A. and Anderson, T. (2001). **Network Suport for IP Thaceback.** IEEE/A CM Transactions on Networking, 9(3), p. 226-237.

Schultz, M., Eskin, E. and Stolfo, S. (2001). **Malicious Email Filter A UNIX Mail Filter that Detects Malicious Windows Executables**. In Proceedings of USEN IX Annual Technical Conference FREENIX Track. Boston, June. Disponible en http://www1.cs.columbia.edu/ids/publications/mef-frenix01.pdf

Schultz, M., Eskin, E., Zadok, E. and Stolfo, S. (2001). **Data Mining Methods for Detection of New Malicious Executables**. In Proceedings of the 2001 IEEE Symposium on Security and Privacy. Oakland, May. Disponible en http://www1.cs.columbia.edu/ids/publications/binaryeval-ieeesp01.pdf

Sekar, R., Bendre, M., Dhurjati, D. and Bollineni, P. (2001). **A Fast Automaton-Based Method for Detecting Anomalous Program Behaviors**. In Proceedings of the 2001 IEEE Symposium on Security and Privacy.

Seleznyov, A. (2001). **A Methodology to Detect Anomalies in User Behavior Basing on its Temporal Regularities**. In Proceedings of the 16th International Conference on Information Security (IFIPjSEC 2001).

Seleznyov, A. and Puuronen, S. (1999). **Anomaly Intrusion Detection Systems: Handling Temporal Relations between Events**. In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID '99). West Lafayette, September. 7-9. Disponible en http://www.cerias.purdue.edu/raidprog.html.

Shavlik, J., Shavlik, M. and Fahland, M. (2001). **Evaluating Software Sensors for Actively Profiling Windows 2000 Computer Usérs**. Short paper presented at RAID'2001.

Singh, H., Furnell, S., Lines, B. and Dowland, P. (2001). **Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining**. In Proceedings of the International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM) 2001.

Siraj, A., Bridges, S. and Vaughn, R. (2001). **Fuzzy cognitive maps for decision support in intrusion detection systems.** In Proceedings of ISFA- NAFIPS-2001, July 25 - 28. Disponible en http://www.cs.msstate.edu/~bridges/papers/nafips2001.pdf

Slagell, M. (2001). **The Design and Implementation of MAms (Mobile Agent Intrusion Detection System).** Master's thesis, Computer Science Department, lowa State University.

Snoeren, A., Partridge, C., Sanchez, L., Jones, C., Tchakountio, F., Kent, S. and Strayer, W. (2001). **Hash-Based IP Traceback**. In Proceedings of the ACM SIGCOMM 2001 Conference on Aplications, Technologies, Architectures, and Protocols for Computer Communication, p. 3-14.

Snyder, D. (2001). **On-line Intrusion Detection Using Sequences of System Calls**. Master's thesis, Department of Computer Science, Florida State University.

Song, D. and Perrig, A. (2001). **Advanced and Authenticated Marking Schemes for IP Traceback**. In Proceedings of the IEEE Infocom 2001.

Stephenson, P. (2001). **France and the Art of Intrusion Detection**. Information Systems Security, 9 (6), p. 5-8.

Sterne, D., Djahandari, K., Wilson, B., Babson, B., Schnackenberg, D., Holliday, H. and Reid, T. (2001). **Autonomic Response to Distributed Denial of Service Attacks**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 134-149.

Upuluri, P. and Sekar, R. (2001). **Experiences with Specification-Based Intrusion Detection**. In Proceedings of the Fourth Intemational Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 172-189.

Valdes, A. and Skinner, K. (2001). **Probabilistic Alert Correlation.** In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 54-68. Disponible en http://www.sdl.sri.com/papers/raid2001-pac/.

Valdes, A., Deswarte, Y., Dutertre, B., Saidi, H. and Staidou, V. (2001). **An Architecture for the Flexible Deployment of IntrusionTolerant Services Across Enterprise Systems**. Short paper presented at RAID'2001.

Vergetis L. and Barbara, L. (2001). **Secure Enough?.** Buildings, 95 (2), p. 34-39.

Vigna, G., Kemmerer, R. and Blix, P. (2001). **Designing a Web Highly-Configurable Intrusion Detection Sensors.** In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212Springer-Verlag, Berlin, p. 69-84.

Wagner, D. and Dean, D. (2001). **Intrusion Detection via Static Analysis**. In Proceedings of the 2001 IEEE Symposium on Security and Privacy.

Wang, X., Reeves, D., Wu, S. and Yuil, J. (2001). **Sleepy Watermark Tracing: an Active Network-Based Intrusion Response Framework**. In Proceedings of the 16th International Conference on Information Security (IFIP/SEC 2001).

Wei, H., Frincke, D. and Carter O. (2001). **Cost-Benefit Analysis for Network Intrusion Systems**. In Proceedings of the 28th Annual Computer Security Conference & Exhibition, Washington. Disponible en http://www.csds.uidaho.edu/director/costbenefic.pdf

Welz, M. and Hutchison, A. (2001**). Interfacing Trred Aplications with Intrusion Detection Systems**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 37-53.

Wen-Hua J. and Vardi, Y. (2001). **A Hybrid High-Order Markov Chain Model for Computer Intrusion Detection.** Journal of Computational & Graphical Statistics, 10 (2), p. 277-295.

Williams, P., Anchor, K., Bebo, J., Gunsch, G. and Lamont, G. (2001). **CDIS: Towards a Computer Immúne System for Detecting Network Intrusions**. In Proceedings of the Fourth International Symposium on the Recent Advances in Intrusion Detection (RAID'2001), in Lecture Notes in Computer Science, number 2212, Springer-Verlag, Berlin, p. 117-133.

Wong, J., Helmer, G., Naganathan, V., Polavarapu, S., Honavar, V. and Miller, L. (2001). **SMART Mobile Agent Facility**. Journal of Systems and Software, Vol. 56, p. 9-22.

Wood, M. and Erlinger, M. (2001).**Intrusion detection message exchange requirements**. Disponible en http://www.ietf.org/proceedings/01mar/I-D/idwg-requirements-05.txt

Yasinsac, A. (2001). **An Environment for Security Protocol Intrusion Detection**. Special edition of the Journal of Computer Security. Disponible en http://www.cs.fsu.edu/~asinsac/Papers/asOl.pdf.

Yasinsac, A. and Manzano, Y. (2001). **Policies to Enhance Computer and Network Forensics**. In Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, p 92-95.

Zamboni, D. (2001). **Using Internal Sensors for Computer Intrusion Detection.** CERIAS TR 2001-42. Disponible en https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2001-42.pdf

Zhu, D., Premkumar, G., Zhang, X. and Chu, C. (2001). **Data Mining for Network Intrusion Detection: Acomparison of Alternative Methods**. Decision Sciences, 32 (4), p. 635-659.

10. INTRUSION DETECTION IN 2002

Albers, P., Camp, O., Percher, J., Jouga, B., Mé, L. and Puttini, R. (2002). **Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches**. In Proceeding of the 1st International Workshop on Wireless Information Systems" (WIS-2002), ICEIS 2002 and the 4th International Conference on Enterprise Information Systems, Ciudad Real, 3-6 April. Disponible en http://www.supelec-rennes.fr/ren/perso/bjouga/documents/wis-short2002.pdf

Anthes, G. (2002). **Autoimmune Computer Systems**. Computerworld, 36 (50), p. 38.

Apap, F., Honig, A., Hershkop, S., Eskin, E.and Stolfo, S. (2002). **Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses**. In Proceedings of the Fifth International Symposium on Recent Advances in Intrusion Detection (RAID-2002). Zurich, October 16-18. Disponible en http://www1.cs.columbia.edu/ids/publications/rad-raid02.pdf

Bhattacharyya, M., Hershkop, S., Eskin, E.and Stolfo, S. (2002). **MET: An Experimental System for Malicious Email Tracking.** In Proceedings of the 2002 New Security Paradigms Workshop (NSPW-2002). Virginia Beach, VA: September 23rd - 26th, 2002. Disponible en http://www1.cs.columbia.edu/ids/publications/met-nspw02.pdf

Bischoff, G. (2002). **Hacking Off The Hackers**. Telephony, 243 (13), p. 24-27.

Bishop, M. (2002). **Trends in academic research: vulnerabilities analysis and intrusion detection.** Computers & Security, 21 (7), p. 609-612.

Cabrera, J., Lewis, L., Qin, X., Lee, W., Mehra, R. (2002). **Proactive Intrusion Detection - A Study on Temporal Data Mining**. In D. Barbara and S. Jajodia, Applications of Data Mining in Computer Security. Kluwer Academic Publishers.

Dyck, T. (2002). **Integrity Stops Security Leaks**. eWeek, 19 (11), p. 51-52.

Eckmann, S., Vigna, G. and Kemmerer, R. (2002). **STATL: An attack language for state-based intrusion detection.** Journal of Computer Security, 10 (1/2), p. 71-104.

Erbacher, R., Walker, K. and Frincke, D. (2002). **Intrusion and Misuse Detection in Large-Scale Systems.** *IEEE Computer Graphics and Applications*, 22(1). Disponible en http://www.csds.uidaho.edu/director/visualization.pdf

Eskin, E., Arnold, A., Prerau, M., Portnoy, L. and Stolfo S. (2002). **A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data.** In Data Mining for Security Applications. Kluwer. Disponible en http://www1.cs.columbia.edu/ids/publications/uad-dmsa02.pdf

Fisher, D. (2002). **Living With Worms, Viruses and Daily Security Alerts**. eWeek, 19 (6), p. 20-21.

Florez, G., Bridges, S. and Vaughn, R. (2002). **An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection.** In Proceedings of the North American Fuzzy Information Processing Society Conference (NAFIPS 2002), New Orleans, June 27-29. Disponible en http://www.cs.msstate.edu/~bridges/papers/nafips2002a.pdf

Frincke, D. (2002). **Guest editor's preface.** Journal of Computer Security, 10 (1/2), p. 1-3.

Helmer, G., Wong, J., Honavar, V. and Miller, L. (2002). **Automated discovery of concise predictive rules for intrusion detection.** Journal of Systems & Software, 60 (2), p. 165-175. Disponible en http://www.palisadesys.com/~ghelmer/Papers/software-practice.ps

Helmer, G., Wong, J., Slagell, M., Honavar, V., Miller, L. and Lutz, R. (2002). **A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System**. Requirements Engineering Journal, 7 (4), p. 207-220. Disponible en http://www.palisadesys.com/~ghelmer/Papers/SFTA-ID-journal.ps

Honig, A., Howard, A., Eskin, E. and Stolfo, S. (2002). **Adaptive Model Generation: An Architecture for the Deployment of Data Minig-based Intrusion Detection Systems**. Data Mining for Security Applications. Kluwer. Disponible en http://www1.cs.columbia.edu/ids/publications/amg-dmsa02.pdf

Iheagwara, Ch. and Blyth, A. (2002). **Evaluation of the performance of ID systems in a switched and distributed environment: the RealSecure case study.** Computer Networks, 39 (2), p. 93-112.

Karagiannis, K. (2002). **Artificially Intelligent Security.** PC Magazine, 21 (15), p. 136-137.

Kerschbaum, F., Spafford, E. and Zamboni, D. (2002). **Using internal sensors and embedded detectors for intrusion detection.** Journal of Computer Security, 10 (1/2), p. 23-70.

Kvarnström, H. (2002). **Securing and Evaluating Fraud and Intrusion Detection Systems.** Licentiate thesis 3L, School of Computer Science and Engineering, Department of Computer Engineering, Chalmers University of Technology, Göteborg.

Lee, W., Fan, W., Miller, M., Stolfo, S. and Zadok, E. (2002). **Toward cost-sensitive modeling for intrusion detection and response.** Journal of Computer Security, 10 (1/2), p. 5-22. Disponible en http://www.cc.gatech.edu/~wenke/papers/jcs_lee.ps

Lee, W., Stolfo, S. and Mok, K. (2002). **Algorithms for Mining System Audit Data.**. In T. Lin, Y. Yao, and L. Zadeh (eds), Data Mining, Rough Sets, and Granular Computing. Physica-Verlag. Disponible en http://www.cc.gatech.edu/~wenke/papers/alg_chapter.ps

Liao, Y. and Vemuri, V. (2002). **Use of K-Nearest Neighbor classifier for intrusion detection**. Computers & Security, 21 (5), p. 439-448.

Liu, Z., Flórez, G. and Bridges, S. (2002). **A Comparison of Input Representation in Neural Networks: A Case Study in Intrusion Detection**. In Proceedings of the International Joint Conference on Neural Networks, May 12-17, Honolulu. Disponible en http://www.cs.msstate.edu/~bridges/papers/IJCNN2002.pdf

Lundin, E. (2002). **Aspects of employing fraud and intrusion detection systems.** Licentiate thesis 2L, School of Computer Science and Engineering, Department of Computer Engineering, Chalmers University of Technology, Göteborg.

Mahoney, M. and Chan, P. (2002). **Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks**. In Proceedings of the Eighth International Conference on Knowledge Discovery and Data Mining, p. 376-385. Disponible en http://cs.fit.edu/~pkc/papers/kdd02.pdf

Middlemiss, J. (2002). **Financial Institutions Get Serious About Security**. Wall Street & Technology, 20 (10), p. 26-27.

Mohiuddin, S., Hershkop, S., Bhan, R. and Stolfo S. (2002). **Defending against a large Scale Denail of Service Attack** In Proceedings of the 3rd Annual IEEE Information Assurance Workshop. United States Military Academy West Point, New York: June 17-19. Disponible en http://www1.cs.columbia.edu/ids/publications/dude_ias_2002.pdf

Morin, B., Mé, L., Debar,H. and Ducassé M. (2002). **M2D2: A Formal Data Model for IDS Alert Correlation**. In Proceedings of the 5th International Symposium on the Recent Advances in Intrusion Detection, October, in Lecture Notes in Computer Science, number 2516, Springer-Verlag. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/Mal.02.pdf

Mueller, P. and Shipley, G. (2002). **Cisco's NIDS Solution Grows Up.** Network Computing, 13 (22), p. 32-33.

Mychalczuk, M. (2002). **Drowning in Data**. Security Management, 46 (11), p. 70-73.

Piazza, P. (2002). **A Honeypot of Your Own**. Security Management, 46 (11), p. 76.

Piscitello, D. (2002). **Intrusion Detection...Or Prevention?** Business Communications Review, 32 (5), p. 42-45.

Product Solutions Outdoor Protection (2002). **Security: For Buyers of Products**, Systems & Services, 39 (7), p. 8-17.

Puttini, R., Marrakchi, Z. and Mé, L. (2002). **Bayesian Classification Model for Real-Time Intrusion Detection.** In Proceedings of the 22th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering (MAXENT'2002). August. Disponible en Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/PMM02.pdf

Radcliff, D. (2002). **Wanted: A Clear View of Vulnerability**. Computerworld, 36 (37), p. 34-35.

Rosenthal, D. (2002). **Intrusion Detection Technology: Leveraging The Organization's Security Posture**. Information Systems Management, 19 (1), p. 35-44.

Savage, M. (2002). **Startup 'Ignites' Security Strategy For Channel**. Computer Reseller News, nº1017, p. 41-42.

Spinellis, D. and Gritzalis, D. (2002). **Panoptis: Intrusion detection using a domain-specific language.** Journal of Computer Security, 10 (1/2), p. 159-176.

Staniford, S., Hoagland, J. and McAlerney, J. (2002). **Practical automated detection of stealthy portscans.** Journal of Computer Security, 10 (1/2), p. 105-135.

Thurman, M. (2002). **Merger Blows Out Security Walls**. Computerworld, 36 (44), p. 30.

Thurman, M. (2002). **Rogue Nodes Routed as Security Recruits Hired.** Computerworld, 36 (35), p. 36.

Triantafyllopoulos, K. and Pikoulas, J. (2002). **Multivariate Bayesian Regression Applied to the Problem of Network Security.** Journal of Forecasting, 21 (8), p. 579-594.

Venter, H.and Eloff, J. (2002). **Vulnerabilities categories for intrusion detection systems.** Computers & Security, 21 (7), p. 617-619.

Verton, D. (2002). **Web Apps Become New Weakest Security Link.** Computerworld, 36 (49), p. 1.

Yasinsac, A. (2002). **An environment for security protocol intrusion detection.** Journal of Computer Security, 10 (1/2), p. 177-188.

Zimmermann, J. and Mé, L. (2002). **Les systèmes de détection d'intrusions : principes algorithmiques**. MISC, juin, numéro 3, p. 24-30. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/ZM02.pdf

Zimmermann, J., Mé, L. and Bidan, Ch. (2002). **Introducing reference flow control for intrusion detection at the OS level.** In Proceedings of the 5th International Symposium on the Recent Advances in Intrusion Detection, October, in Lecture Notes in Computer Science, number 2516, Springer-Verlag. Disponible en http://www.supelec-rennes.fr/rennes/si/equipe/lme/PUBLI/ZMB02.pdf

11. INTRUSION DETECTION IN 2003

Álvarez, G. and Petrovíc, S. (2003). **A new taxonomy of Web attacks suitable for efficient encoding**. Computers & Security, 22 (5), p. 435-449.

Botha, M. and Von Solms, R. (2003). **Utilising fuzzy logic and trend analysis for effective intrusion detection.** Computers & Security, 22 (5), p. 423-434.

Bruno, L. (2003). **Digital defenses.** Red Herring, (121), p. 52-53.

CERT Coordination Center (2003). **CERT/CC Overview Incident and Vulnerability Trends.** Carnegie Mellon University. May. Disponible en http://www.cert.org/present/cert-overview-trends/

Chan, P. Mahoney, M. and Arshad, M. (2003). **Learning Rules and Clusters for Anomaly Detection in Network Traffic,** In V. Kumar, J. Srivastava & A. Lazarevic, *Managing Cyber Threats: Issues, Approaches and Challenges*, Kluwer. Disponible en http://cs.fit.edu/~pkc/papers/cyber.pdf

Cho, S. and Park, H. (2003). **Efficient anomaly detection by modeling privilege flows using hidden Markov model**. Computers & Security, 22 (1), p. 45-55.

Harris, R. (2003). **What Price Security?** CFO, 19 (9), p. 54-58.

Heller, K., Svore, K., Keromytis, A. and Stolfo S. (2003). **One Class Support Vector Machines for Detecting Anomalous Window Registry Accesses**. CU Tech Report April 2003. Disponible en http://www1.cs.columbia.edu/ids/publications/OCSVM.pdf

Helmer, G., Wong, J., Honavar, V., Miller, L. and Wang, Y. (2003). **Lightweight agents for intrusion detection.** Journal of Systems & Software, 67(2), p. 109-122.

Hershkop, S., Ferster, R., Bui, L., Wang, K. and Stolfo S. (2003). **Host-based Anomaly Detection by Wrapping File System Accesses.** CU Tech Report April. Disponible en http://www1.cs.columbia.edu/ids/publications/wraps-final.pdf

Iheagwara, Ch., Blyth, A. and Singhal, M. (2003). **A comparative experimental evaluation study of intrusion detection system performance in a gigabit environment.** Journal of Computer Security, 11 (1), p. 1-33.

Keanini, T. (2003). **Vulnerability Management Technology**. Computer Technology Review, 23 (5), p.18-19.

Kim, H. and Chan, P. (2003). **Learning Implicit User Interest Hierarchy for Context in Personalization,** In Proceedings International Conference on Intelligent User Interfaces, p. 101-108. Disponible en http://cs.fit.edu/~pkc/papers/iui03.pdf

Mahoney, M. and Chan, P. (2003). **An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection**, In Proceedings 6th Symposium Recent Advances on Intrusion Detection. Disponible en http://cs.fit.edu/~pkc/papers/raid03.pdf

Middlemiss, J. (2003). **Intruder Alert.** Wall Street & Technology, 21 (1), p. 42-43.

Moulton, R. and Coles, R. (2003). **A contest to evaluate IT security services management**. Computers & Security, 22 (3), p. 204-206.

Piazza, P. (2003). **Who's Afraid of Computer Bugs?** Security Management, 47 (3), p. 40-41.

Robertson, S., Siegel, E., Miller, M. and Salvatore J. Stolfo. (2003). **Surveillance Detection in High Bandwidth Environments.** In Proceedings of the 2003 DARPA DISCEX III Conference. April, 2003. Disponible en http://www1.cs.columbia.edu/ids/publications/SD-DiscexIII.pdf

Schultz, E. (2003). **Internet security: what's in the future?** Computers & Security, 22 (2), p. 78-79.

Sequeira, D. (2003). **Intrusion Prevention Systems.** Business Communications Review, 33 (3), p. 36- 41

Stolfo, S., Hershkop, S., Wang, K., Nimeskern, O. and Hu C. (2003). **Behavior Profiling of Email.** In Proceedings of the 1st NSF/NIJ Symposium on Intelligence & Security Informatics (ISI 2003). Tucson, June 2-3. Disponible en http://www1.cs.columbia.edu/ids/publications/nsf-nij-emt.pdf

Stolfo, S., Hershkop, S., Wang, K., Nimeskern, O. and Hu C. (2003). **A Behavior-based Approach to Securing Email Systems. Mathematical Methods, Models and Architectures for Computer Networks Security**. In Proceedings published by Springer Verlag, Sept. 2003. Disponible en http://www1.cs.columbia.edu/ids/publications/EMT-ACNS03.pdf

Stolfo, S., Hu, C., Li, W., Hershkop, S., Wang, K. and Nimeskern O. (2003). **Combining Behavior Models to Secure Email Systems.** CU Tech Report. Disponible en http://www1.cs.columbia.edu/ids/publications/EMT_weijen.pdf

Venezia, P. (2003). **NetDetector Captures Intrusions**. InfoWorld, 25 (27), p. 32-33.

Venter, H. and Eloff, J. (2003). **A taxonomy for information security technologies.** Computers & Security, 22 (4), p. 299-307.

Wang, K. and Stolfo, S. (2003). **One Class Training for Masquerade Detection**. CU Tech Report April 2003. Disponible en http://www1.cs.columbia.edu/ids/publications/masquerade.pdf