

## **Bibliography of Network-based Anomaly Detection Systems**

- [1] A. Lakhina, M. Crovella, and C. Diot, "Characterization of network-wide traffic anomalies in traffic flows," *ACM Internet Measurement Conference (IMC)*, 2004.
- [2] A. Soule, K. Salamatian and N. Taft, "Combining Filtering and Statistical methods for anomaly detection," *ACM/Usenix IMC*, 2005.
- [3] Anzen Computing Inc., Washington, <http://www.anzen.com/products/afj/> .
- [4] AXENT Technologies, Inc. <http://www.axent.com/product/ita/ita.htm>.
- [5] C. Taylor and F. Jim, "NATE- Network Analysis of Anomalous Traffic Events, A Low-Cost Approach," *New Security Paradigms Workshop*, 2001.
- [6] D. Barbara, N. Wu and S. Jajodia, "Detecting novel network intrusion using bayes estimators," *SIAM Conference on Data Mining*, 2001.
- [7] D. Holdon, "A rule-based intrusion detection system," *IFIP TC11 8th International Conference*, 1992.
- [8] D. J. Ragsdale, C. A. Carver, J. W. Humphries and U. W. Pooch, "Adaptation Techniques for Intrusion Detection and Intrusion Response Systems," *IEEE International Conference on Systems, Man, and Cybernetics*, 2000.
- [9] D. Samfat and R. Molva, "IDAMN: An Intrusion Detection Architecture for Mobile Networks", *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 7, 1997.
- [10] D. S. Bauer and M. E. Koblenz, "NIDX - An expert system for real-time network intrusion detection," *IEEE Computer Networking Symposium*, 1988.
- [11] G. B. White and U. W. Pooch, "Cooperating Security Managers: distributed intrusion detection systems," *Computers & Security* vol. 15, no. 5, pp. 441-450, 1996.
- [12] G. H. Kim and E. H. Spafford, "Experiences with Tripwire: Using integrity checkers for intrusion detection", *Systems Administration, Networking and Security Conference III, USENIX*, 1994.

- [13] G. Tsudik and R. Summers, "AudES - an expert system for security auditing," *AAAI Conference on Innovative Applications in AI*, 1990.
- [14] H. Debar and B. Dorizzi, "An application of a recurrent network to an intrusion detection system," *International Joint Conference on Neural Networks*, 1992.
- [15] H. S. Javitz and A. Valdes "The NIDES Statistical Component: Description and Justification", *SRI International*, 1993.
- [16] H. S. Javitz and A. Valdes, "The SRI IDES Statistical Anomaly Detector," *IEEE Symposium on Security and Privacy*, 1991.
- [17] H. S. Javitz, D. E. Denning and P. G. Neumann, "Analytical techniques development for a Statistical Intrusion Detection System (SIDS) based on accounting records," *SRI International*, 1986.
- [18] H. Wang, D. Zhang and K. G. Shin, "Detecting SYN Flooding Attacks," *IEEE INFOCOM*, 2002.
- [19] J. Hochberg, K. Jackson, C. Stallings, J. F. McClary, D. DuBois and J. Ford, "NADIR: An automated system for detecting network intrusions and misuse", *Computers & Security*, vol. 12, no. 3, pp. 235-248, 1993.
- [20] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," *IEEE Symp Sec and Priv*, 2004.
- [21] K. Wang, S. Stolfo, "Anomalous Payload-Based Network Intrusion Detection," *Recent Advances in Intrusion Detection (RAID)*, 2004.
- [22] L. Ertoz, E. Eilertson, A. Lazarevic, P.-N. Tan, V. Kumar, J. Srivastava and P. Dokas, "The MINDS: Minnesota Intrusion Detection System," *Next Generation Data Mining*, MIT Press, 2004.
- [23] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood and D. Wolber, "A network security monitor," *IEEE Symposium on Research in Security and Privacy*, 1990.
- [24] L. T. Heberlein *et al.*, "A Network Security Monitor," *Symposium on Research in Security and Privacy*, 1990.

- [25] M. M. Sebring, E. Sellhouse, M. E. Hanna and R. A. Whitehurst, "Expert system in intrusion detection: A case study," *National Computer Security Conference*, 1988.
- [26] M. M. Williamson, "Throttling viruses: Restricting propagation to defeat malicious mobile code," *ACSAC Security Conference*, 2002.
- [27] M. Mahoney, "Network Traffic Anomaly Detection Based on Packet Bytes," *ACM Symposium on Applied Computing (SAC)*, 2003.
- [28] M. V. Mahoney and P. K. Chan, "Learning Rules for Anomaly Detection of Hostile Network Traffic," *IEEE International Conference on Data Mining*, 2003.
- [29] M. V. Mahoney and P. K. Chan, "Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks." *ACM SIGKDD international conference on Knowledge discovery and data mining*, 2002.
- [30] M. V. Mahoney and P. K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile network Traffic," *Technical Report, Florida Tech.*, 2001.
- [31] P. G. Neumann and F. Ostapik, "Audit Trail Analysis and Usage Data Collection and Processing, Part 2," *Computer Science Laboratory, SRI International*, 1987.
- [32] P. G. Neumann and P. A. Porras, "Experience with EMERALD To Date," *USENIX Workshop on Intrusion Detection and Network Monitoring*, 1999.
- [33] P. Proctor, "Audit reduction and misuse detection in heterogeneous environments: Framework and applications," *Computer Security Applications Conference*, 1994.
- [34] R. Heady, G. Luger, A. Macabe, M. Servilla and J. Sturtevant, "A prototype implementation of a network-level intrusion detection system," *Technical Report CS91-11, Department of Computer Science, University of New Mexico*, 1991.
- [35] R. Janakiraman, M. Waldvogel and Q. Zhang, "Indra: A peer-to-peer approach to network detection and prevention", *IEEE WETICE 2003 Workshop on Enterprise Security*, 2003.
- [36] R. Winkler, "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," *National Computer Security Conference*, 1990.

- [37] S. Chenug, "The Design of GrIDS: A Graph-Based Intrusion Detection System," *U.C. Davis Computer Science Department Technical Report CSE-99-2*, 1999.
- [38] S. E. Schechter, J. Jung, and A. W. Berger, "Fast detection of scanning worm infections," In E. Jonsson, A. Valdes, and M. Almgren, editors, *Recent Advances in Intrusion Detection (RAID)*, vol. 3224 of *Lecture Notes in Computer Science*, pages 59-81. Springer, 2004. ISBN 3-540-23123-4.
- [39] S. E. Smaha, "Haystack: An Intrusion Detection System," *IEEE Fourth Aerospace Computer Security Applications Conference*, 1988.
- [40] S. R. Snapp, "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype," *National Computer Security Conference*, 1991.
- [41] S. Staniford, A. J. Hoagland and J. M. McAlerney, "Practical Automated Detection of Stealthy Portscans," *Computer and Communications Security*, 2000.
- [42] W. R. E. Weiss and A. Baur, "Analysis of audit and protocol data using methods from artificial intelligence," *National Computer Security Conference*, 1990.
- [43] W. T. Tener, "Discovery: An expert system in the commercial data security environment," *IFIP TC11 International Conference on Security*, 1989.
- [44] Y. Gu, A. McCullum and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," *ACM/Usenix IMC*, 2005.