Sebastian Roschke, Feng Cheng, Christoph Meinel: "Using Vulnerability Information and Attack Graphs for Intrusion Detection"
in Proceedings of the 6th International Conference on Information Assurance and Security (IAS 2010), IEEE Press, Atlanta, USA, pp. 104-109, 8, 2010. ISBN: 978-1-4244-7408-0.

that the system and its algorithms improve their workflow. The extraction of information from exploit databases is also considered as interesting research topic and valuable source of information for the IDS and correlation process.

In this paper, we propose the integration of the AG workflow with an IDS management system to improve alert and correlation quality. The approach uses the information sources of the AG workflow: automatically extracted vulnerability information, system information, and the calculated graph. The vulnerability and system information is used to prioritize and tag the incoming IDS alerts. The AG is used during the correlation process to filter incorrect correlation results. An architecture is described consisting of an *Event Gatherer*, a *Correlation Module*, an *Attack Graph Creation* module, and a *Frontend* for the user. The *Correlation Engine* works based on pluggable *Correlation Modules* and uses the *Alert Storage*, the *Vulnerability Information* and *System Information* as input. The *Frontend* works on alert information which is tagged and filtered based on the *Vulnerability Information* and *System Information*. A prototype is implemented using unified data models for system information and vulnerability information. Automatic extraction of vulnerabilities is applied to utilize most recent vulnerability descriptions.

REFERENCES

[1] Laureano, M., Maziero, C., Jamhour, E.: Protecting host-based intrusion detectors through virtual machines. Computer Networks **51**(5), pp. 1275-1283 (2007).

[2] F-Secure Linux Security: *http://www.f-secure.com/linux-weblog/* (accessed Mar 2010), F-Secure Corporation (2006-2009).

[3] Samhain IDS: WEBSITE: *http://www.la-samhna.de/samhain/* (accessed Mar 2010).

[4] Snort IDS: WEBSITE: *http://www.snort.org/* (accessed Mar 2010).

[5] Prelude IDS: WEBSITE: *http://www.prelude-ids.com/* (accessed Mar 2010), PreludeIDS Technologies (2005-2009).

[6] Debar, H., Curry, D., Feinstein, B.: *The Intrusion Detection Message Exchange Format, Internet Draft*, Technical Report, IETF Intrusion Detection Exchange Format Working Group (July 2004).

[7] Roschke, S., Cheng, F., Schuppenies, R., and Meinel, Ch.: "Towards Unifying Vulnerability Information for Attack Graph Construction", In: Proceedings of *12th Information Security Conference (ISC'09)*, Springer LNCS, vol. 5735, pp. 218-233, Pisa, Italy (Sep 2009).

[8] Cheng, F., Roschke, S., Schuppenies, R., and Meinel, Ch.: "Remodeling Vulnerability Information", In: Proceedings of *5th Inscrypt Conference (Inscrypt'09)*, Springer LNCS, Beijing, China, December 2009 (to appear).

[9] R. Sadoddin, A. Ghorbani: *Alert Correlation Survey: Framework and Techniques*, In: Proceedings of the International Conference on Privacy, Security and Trust (PST'06), ACM Press, Markham, Ontario, Canada, pp. 1-10 (2006).

[10] Mitre Corporation: *Common vulnerabilities and exposures*, CVE Website: *http://cve.mitre.org/* (accessed Mar 2010).

[11] K. Julisch: *Clustering intrusion detection alarms to support root cause analysis*, In: ACM Transactions on Information and System Security, vol. 6, Issue 4, pp. 443-471 (2003).

[12] F. Cuppens: *Managing alerts in a multi-intrusion detection environment*, In: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), IEEE Press, New-Orleans, USA, pp. 0-22 (Dec 2001).

[13] A. Valdes and K. Skinner: *Probabilistic alert correlation*, In: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID'00), London, UK, Springer LNCS 2212, pp.54-68 (2001).

[14] H. Debar and A. Wespi: *Aggregation and correlation of intrusion-detection alerts*, In: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID'01), London, UK, Springer LNCS 2212, pp. 85-103 (2001).

[15] P. Ning, Y. Cui, and D. Reeves: *Constructing attack scenarios through correlation of intrusion alerts*, In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02) ACM Press, Washington, DC, USA, pp. 245-254 (2002).

[16] X. Qin: *A Probabilistic-Based Framework for INFOSEC Alert Correlation*, PhD thesis, Georgia Institute of Technology (2005).

[17] W. L. Xinzhou Qin: *Statistical causality analysis of infosec alert data*, In: Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID'03), London, UK, Springer LNCS 2820, pp. 73-93 (2003).

[18] S. Manganaris, M. Christensen, D. Zerkle, and K. Hermiz: *A data mining analysis of rtid alarms*, In: Computer Networks, vol. 34, Issue 4, pp. 571-577 (2000).

[19] A. Siraj and R. B. Vaughn: *A cognitive model for alert correlation in a distributed environment*, In: Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI'05), IEEE Press, Atlanta, GA, USA, pp. 218-230 (2005).

[20] P. Ning, D. Xu, C. G. Healey, and R. S. Amant: *Building attack scenarios through integration of complementary alert correlation method*, In: Proceedings of the Network and Distributed System Security Symposium (NDSS'04), The Internet Society, San Diego, California, USA (2004).

[21] P. A. Porras, M. W. Fong, and A. Valdes: *A mission-impact-based approach to infosec alarm correlation*, In: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID'02), London, UK, Springer LNCS, pp. 95-114 (2002).

[22] Tedesco, G. and Aickelin, U.: *Real-Time Alert Correlation with Type Graphs*, In: Proceedings of the 4th international Conference on Information Systems Security (ISS'09), Springer LNCS 5352, Hyderabad, India, pp. 173-187 (2008).

[23] Ning, P. and Xu, D.: *Adapting Query Optimization Techniques for Efficient Intrusion Alert Correlation*, Technical Report, North Carolina State University at Raleigh (2002).

[24] Roschke, S., Cheng, F., and Meinel, Ch.: "An Advanced IDS Management Architecture", In: *Journal of Information Assurance and Security*, Dynamic Publishers Inc., vol. 51, Atlanta, GA 30362, USA, ISSN 1554-1010, pp. 246-255 (Jan 2010).

[25] Schneier, B.: Attack Trees: Modeling Security Threats. In Journal *Dr. Dobb's Journal*, online available from *http://www.ddj.com/architect/184411129* (Dec 1999)

[26] Sheyner, O., Haines, J., Jha, S., Lippmann, R., and Wing, J. M.: Automated Generation and Analysis of Attack Graphs. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P'2002)*, IEEE Press, Washington DC, USA, pp. 273-284 (May 2002)

[27] Steven Noel and Sushil Jajodia Managing attack graph complexity through visual hierarchical aggregation In *Proceedings of Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC 2004)*, ACM, Washington DC, USA, pp. 109-118 (Oct 2004)

[28] X. Ou, S. Govindavajhala, and A. Appel MulVAL: A Logic-based Network Security Analyzer, In: *Proceedings of 14th USENIX Security Symposium*, USENIX Association, Baltimore, MD, pp. 8-8 (Aug 2005).

[29] OSV Database: "Open source vulnerability database", Website: http://osvdb.org/ (accessed Mar 2010).

[30] Mitre Corporation: "Common vulnerabilities and exposures", Website: http://cve.mitre.org/ (accessed Mar 2010).

[31] Mitre Corporation, "Open Vulnerability and Assessment Language", OVAL Website: http://oval.mitre.org/ (accessed Mar 2010).

[32] Secunia Advisories, Website: http://secunia.com/advisories/ (accessed Mar 2010).

[33] SecurityFocus, "Security Focus Bugtraq", Website: http://www.securityfocus.com/ (accessed Mar 2010).

[34] NIST, "National Vulnerability Database", NVD Website: http://nvd.nist.gov/ (accessed Mar 2010).

[35] P. Mell, K. Scarfone, and S. Romanosky: "A complete guide to the common vulnerability scoring system version 2.0", Website: http://www.first.org/cvss/ (accessed Mar 2010).

[36] V. N. L. Franqueira and M. van Keulen: "Analysis of the NIST database towards the composition of vulnerabilities in attack scenarios", Technical Report, TR-CTIT-08-08, University of Twente, Enschede, February 2008.

[37] T. Hughes, O. Sheyner: "Attack scenario graphs for computer network threat analysis and prediction", In: *Journal of Complexity*, Wiley Periodicals, Inc., vol. 9(2), pp. 15-18 (2004).