IntAleGen: **Int**egrated **Ale**rt **Gen**eration in Multi Pronged attacks on Networked Systems

Vandana P. Janeja [*], Nabil Adam[†‡], Josephine Namayanja[*]
[*]{janeja, jona1}@umbc.edu, [‡]Nabil.Adam@dhs.gov
[*]*University of Maryland, Baltimore County*
[†]*Rutgers University*
[‡]*Science & Technology Directorate, Department of Homeland Security*

Networked systems such as computer networks, sensor networks, and industrial control systems are increasingly facing the threat of unauthorized access. Intrusion detection systems [1] identify threats using signatures of unauthorized access or attacks. There are few systems discovering ‘zero day’ attacks [2, 3, 4] where the attack signature is unknown.

Example 1 – two pronged computer network attack: First, attack on the organization’s computer network. Intruders take advantage of vulnerabilities in the public-facing web servers. Hackers secretively scout the network from compromised workstations, targeted beforehand as part of a coordinated prolonged attack [7]. Second, spear-phishing [8] attack on a partner’s network, which shares key resources. Hackers obtain a privileged account and compromise a root domain controller shared by the organization and its partner. Intruders try to recreate and assign privileges triggering an alarm. Indeed such an attack occurred at the Pacific Northwest National Laboratory [7]. Despite the lab’s well-protected security perimeter, the attacks made it through in a coordinated and prolonged process.

Cyber security systems may generate a series of alarms [5, 6]. The alarms received in such a complex domain comprise of raw messages received from multiple sources where an alert has to be generated as an aggregated output. However, the attack maybe distributed across locations or spread out over time making it difficult to integrate these alarms and identify if this is a single malicious attack. Here alarm may have attributes such as the source, destination, port, length of packet, time-stamp and source may have attributes such as type, port, frequency of use. We address the discovery of an integrated alert in a networked system from alarms generated by (a) disparate sources, and (b) across prolonged period of time. Our approach comprises of (1) Alarm source characterization, (2) temporal lag determination, (3) alarm clustering using (1) and (2).

References:

[1] Zurutuza U, Uribeetxeberria R, Zamboni D. 2008. A data mining approach for analysis of worm activity through automatic signature generation. In: Dirk Balfanz & Jessica Staddon, ed., 'AISec', ACM. pp. 61-70.

[2] Mohammed M. M. Z. E, Chan H. A, Ventura N, Hashim M, Amin I, Bashier E. 2010. Detection of Zero-day Polymorphic Worms using Principal Component Analysis. In: Sixth International Conference on Networking and Services (2010). IEEE, pp: 277-281. DOI: 10.1109/ICNS.2010.45

[3] Wang K, Stolfo S. J. 2004. Anomalous Payload-based Network Intrusion Detection. In: Symposium on Recent Advances in Intrusion Detection, Sophia Antipolis, France.

[4] Wang L, Li Z, Chen Y, Fu Z J, Li X. 2010. Thwarting Zero-Day Polymorphic Worms With Network-Level Length-Based Signature Generation. In: IEEE/ACM Transactions on Networking. Volume: 18, Issue: 1, Pp: 53-66. DOI: 10.1109/TNET.2009.2020431

[5] Costa M , Crowcroft J , Castro M , Rowstron A, Zhou L, Zhang L, Barham P. 2005. Vigilante: End-to-End Containment of Internet Worms. In: Proceedings of the Symposium on Systems and Operating Systems Principles (SOSP)

[6] Cheetancheri S G, Agosta J M, Dash D H, Levitt K N, Rowe J, Schooler E M. 2006. A Distributed Host-based Worm Detection System. In: Proceedings of the 2006 SIGCOMM workshop on Largescale attack defense LSAD 06. ACM Press, pp: 107-113. DOI: 10.1145/1162666.1162668

[7] 7 Lessons: Surviving A Zero-Day Attack, Pacific Northwest National Laboratory CIO Jerry Johnson takes you inside the cyber attack that he faced down--and shares his security lessons learned. September 19, 2011, John FoleyInformationWeek

http://www.informationweek.com/news/security/attacks/231601692, Last accessed 2011

[8] FBI: Spear-Phishing ,

http://www.fbi.gov/news/stories/2009/april/spearphishing_040109,Last accessed 2011