Poster: A Logic Based Network Forensics Model for Evidence Analysis

Anoop Singhal
National Institute of Standards and Technology
anoop.singhal@nist.gov

Changwei Liu
George Mason University
cliu6@gmu.edu

Duminda Wijesekera
George Mason University
National Institute of Standards and Technology
dwijesek@gmu.edu

ABSTRACT

Network forensics is an extension of the network security model, which traditionally emphasizes prevention and detection of network attacks. It addresses the need for dedicated investigative capabilities for investigation of malicious behavior in networks. Modern-day attackers tend to use sophisticated multi-stage, multi-host attack techniques and anti-forensics tools to cover their attack traces. Due to the current limitations of intrusion detection and forensic analysis tools, reconstructing attack scenarios from evidence left behind by the attackers of an enterprise system is challenging. In particular, reconstructing attack scenarios by using the information from IDS alerts and system logs that have a large number of false positives is a big challenge.

Many researchers have proposed to aggregate redundant alerts and correlate them to determine multi-step attacks [1]. This method is non-automated and rather ad-hoc. As an improvement, Wang at el. [7] proposed automating the process by using a fuzzy-rule based hierarchical reasoning framework to correlate alerts using so-called local rules and group them using so-called global rules. However, this approach falls apart when evidence is destroyed, and it does not assess the potential of the evidences admissibility so that the constructed attack scenario presented to a judge or jury has legal standing. In this talk, we will present a model [4] that systematically addresses how to resolve the above problems to reconstruct the attack scenario. These problems include a large amount of data including non-relevant data, missing evidence or evidence destroyed by anti-forensic techniques. Our system is based on a Prolog reasoning system MulVAL [6] using known vulnerability databases and an anti-forensics database that we plan to extend to a standardized database like the NIST National Vulnerability Database (NVD).

In this model, we use different methods, including mapping the evidence to system vulnerabilities, inductive reasoning and abductive reasoning to reconstruct attack scenarios. Besides, for the legal purpose, we codified the federal rules to this tool, aiming to help judge whether the evidence that is used to reconstruct the attack scenarios could be admissible in the court [5]. In addition, in order to help the investigators to quantify the probability of an attack path we use Bayesian Network to calculate the cumulative likelihood of the evidences.

The goal of this research is to provide a tool that can reduce the investigators' time and effort in reaching definite conclusion about how an attack occurred. Also, this tool can be used to assist judge/jury or law students to better understand a multi-step, multi-host attack towards an enterprise network by using a visual graph and probabilities. Our experimental results indicate that such a reasoning system can be useful for network forensics analysis.

Keywords

Network forensics; cybercrime; digital evidence; Prolog reasoning; network attack scenario; evidence graph; admissibility

Disclaimer

This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

REFERENCES

[1] H. Debar ,A. Wespi, Aggregation and correlation of intrusion-detection alerts, In Recent Advances in Intrusion Detection, LNCS 2212, pages 85 – 103, 2001.

[2] C. Liu, A. Singhal, D. Wijesekera, *Mapping Evidence Graphs to Attack Graphs*, IEEE International Workshop on Information Forensics and Security, December, 2012.

[3] C. Liu, A. Singhal, D. Wijesekera. *Using Attack Graphs* in *Forensic Examinations*. ARES, page 596-603. IEEE Computer Society, (2012).

[4] C. Liu, A. Singhal, D. Wijesekara, "A Logic Based Network Forensics Model for Evidence Analysis", IFIP International Conference on Digital Forensics, Orlando, Florida, January 24-26 2015.

[5] C.Liu, A.Singhal, and D.Wijesekera. Relating Admissibility Standards for Digital Evidence to Attack Scenario Reconstruction, JDFSL 9(2):181-196 (2014).

[6] MulVALV1.1, Jan30, 2012. http://people.cis.ksu.edu/xou/mulval/.

[7] W. Wang, T.E. Daniels, A graph based approach towards network forensics analysis, ACM Transactions on Information and System Security (TISSEC), 12 (1), Oct 2008.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.
ACM 978-1-4503-3832-5/15/10.
DOI: http://dx.doi.org/10.1145/2810103.2810106