Expected results of conceptual learning

Štefan Balogh, [1] Peter Švec [1] and Alexander Šimko [2]

[1] Faculty of Electrical Engineering, Slovak Technical University, Bratislava
[2] Comenius University in Bratislava, Mlynská dolina, 84248 Bratislava

Abstract. In this paper we discuss the result of conceptual learning suitable for use in specific detection systems.

Keywords: conceptual learning, attack detection.

1 Expected results of conceptual learning

1.1 Future direction

The great efforts of the scientific community are currently focused on increasing the security of information systems, as their dissemination to every area of our lives is an unstoppable process. The attackers and criminals thus exploited their weaknesses in information systems, they get into different areas of our lives and can abuse it for their own benefit.

Currently, it is necessary to look for solutions that can work automatically as much as possible and are able to respond in a short time to current changes or new attacks.

For fast response and learning, it is necessary to have the information available as soon as possible, which will be included in automated detection systems. This involves depending on the algorithm that provides the automation, either updating the rules or teach the system for new knowledge.

For the necessary acceleration, it would be helpful if a system that shares knowledge could provide data directly to learning systems, or to the systems that generate new rules. It is also possible to consider or test to share not only attack information, but also given detection rules, if they are written in a similar format as shared data about the attack.

More and more work is there, where ontological rules are used for detection [1][2].

If the functionality of such systems will be proven, it would be possible to use conceptual learning to generate the rules.

To be able to use the results of conceptual learning, the resulting rules should be like the rules that the proposed detection systems use. Therefore, it is necessary to analyze in detail the rules of existing detection tools, such as ZEEK OWASP, Snort, Suricata, or mod security [3][4][5][6]. Detection systems that directly use ontological rules in detection can be a valuable resource, also [2][7].

However, the great variability and increase in the number of rules for detection gradually reduces real time detection and the whole prices become time-consuming or hardware intensive. It would be useful here to test the merging of rules into a common decision tree [8][9].
Creating a comprehensive solution for sharing knowledge about attacks and detection rules for these attacks can be a significant step forward in the field of security compared to the current situation.

.

References

1. Munir, R. F., Ahmed, N., Razzaq, A., Hur, A., & Ahmad, F. (2011, December). Detect HTTP Specification Attacks Using Ontology. In *2011 Frontiers of Information Technology* (pp. 75-78). IEEE.
2. Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks. *Information Sciences*, *254*, 19-38. night, Michelle (2017).
3. Tidjon, L. N., Frappier, M., & Mammar, A. (2020, April). Intrusion detection using astds. In *International Conference on Advanced Information Networking and Applications* (pp. 1397-1411). Springer, Cham.
4. Online https://github.com/schubergphilis/mod_security/tree/master/files/default/owasp-modsecurity-crs-2.2.8
5. Online https://github.com/SpiderLabs/owasp-modsecurity-crs/tree/v3.3/dev/rules
6. Online https://github.com/coreruleset/coreruleset/tree/v4.0/dev/rules
7. Ulicny, B. E., Moskal, J. J., Kokar, M. M., Abe, K., & Smith, J. K. (2014). Inference and ontologies. In *Cyber Defense and Situational Awareness* (pp. 167-199). Springer, Cham.
8. Abdelhalim, A., Traore, I., & Nakkabi, Y. (2016). Creating Decision Trees from Rules using RBDT-1. *Computational Intelligence*, *32*(2), 216-239.
9. Khan, Z. M. A., Saeidlou, S., & Saadat, M. (2019). Ontology-based decision tree model for prediction in a manufacturing network. *Production & Manufacturing Research*, *7*(1), 335-349.