Abstract for poster in: Proceedings of the National Symposium on Moving Target Research, June 2012.

A Semantic Approach to Situational Awareness for Intrusion Detection

Sumit More, Mary Matthews, Anupam Joshi and Tim Finin
University of Maryland, Baltimore County
{sumitm1,math1,joshi,finin}@umbc.edu

We describe a situation-aware intrusion detection system that integrates heterogeneous sources of information to build and maintain a semantically rich knowledge base (KB) with information about cyber threats and vulnerabilities. Most current intrusion detection and prevention systems rely on signature-based approaches to detect attacks. When an attack signature is not available, such as for a new or significantly modified exploit, such systems are much less effective. Moreover, these intrusion detection systems are point-based solutions that do not make effective use of heterogeneous data sources, which can provide important information related to intrusions which are not yet available as signature patterns. This information can also help detect *low and slow* attacks in which small intrusions that are spatially and temporally apart combine to build a more elaborate attack.

We have prototyped a system that uses the apptoach to recognize potential attacks. The knowledge base is constructed and kept current by integrating information from several sources, represented as ontologies, rules and facts using the Semantic Web languages OWL and RDF. The ontologies and facts are kept current by integrating information from data from vulnerability databases such as NVD, concepts and facts extracted from text from various Web sources, including news, blog posts and chat rooms, and facts about the state of a system being protected produced by an IDS system such as Snort or Wireshark.

The foundation of our knowledge base rests on an OWL ontology developed by Undercoffer [4] that provides a vocabulary for concepts, properties and relations to describe attacks in terms of their the means (e.g., BufferOverFlow, synFlood), consequences (e.g., DenialOfService, PrivilegeEscalation) and targets (e.g., systems, processes, and software versions). We use natural language processing techniques including text classification, named entity recognition, entity linking and concept spotting to extract information from Web text and represent it using extensions to these ontologies [3]. The output of existing IDS systems at the network and host level [1] are also represented as RDF data using these ontologies. The results are integrated and reasoned over using the ontology axioms and custom rules to identify potential attacks. We evaluated our initial prototype system in a series of experiments on stack-based buffer overflow exploits in Adobe Reader and Acrobat [2] with promising results, demonstrating the feasibility of a situational awareness approach to detecting new attacks.

[1] S. More, M. Mathews, A. Joshi and T. Finin, A Knowledge-Based Approach To Intrusion Detection Modeling, IEEE Workshop on Semantic Computing and Security, May 2012.

[2] S. More, Situation Aware Intrusion Detection Model, MS Thesis, University of Maryland, Baltimore County, May 2012.

[3] V. Mulwad, W. Li, A. Joshi, T. Finin and K. Viswanathan, Extracting Information about Security Vulnerabilities from Web Text, IEEE Workshop on Intelligence for Information Security, August 2011.

[4] J. Undercoffer, A. Joshi, T. Finin and J. Pinkston. Using DAML+OIL to Classify Intrusive Behaviors, Knowledge Engineering Review, 18:3, pp 221-241, 2004.

This work was partially supported by grant FA9550-08-1-0265 from the Air Force Office of Scientific Research and a gift from Northrop Grumman Corporation. For more information, see http://ebiq.org/j/98.