Adaptive Observation-Centric Anomaly-Based Intrusion Detection: Modeling, Analysis and Evaluation *

Zonghua Zhang
School of Information Science, JAIST
zonghua@jaist.ac.jp

RESEARCH OBJECTIVE

Anomaly-based intrusion detection is about discrimination of malicious and legitimate patterns of activities (system or user-driven) in variables characterizing system normality. Due to the nonstationarity and increasingly complexity of today's computer systems, perfect normality characterization is always deemed to be an unreachable goal for any anomaly detection model. Because of the same reason, most of existing anomaly detection techniques are based solely on expert knowledge or intuition in a given operating environment, and the cost have to pay is allow the limits to exist in terms of expected false alarms. Our research objective is to develop and design effective and efficient models, methods and techniques for anomaly-based intrusion detection in hosts and networks with provision of adaptability, dependability, and scalability.

ACHIEVEMENTS (Aims & Solutions)

- Motivated by the observation that the fundamental understanding of the computing environments is an initial but essential step in the process of developing an effective anomaly detection model, and based on the similarity between anomaly detection and induction reference problem, we present a statistical framework for analyzing the general behavior of anomaly detection models from the perspective of their observable subjects/operating environments. The objective is to lay a theoretical foundation for the modeling and developing of our specific anomaly detectors in the subsequent stage of our work. To enrich the framework, we examine some challenging issues currently exist and present potential solutions, including host-based and network-based normality characterization, evaluation of anomaly detectors, etc.; The framework also involves some case studies and comparative analysis on several typical anomaly detectors, for the sake of presenting a formal way for the understanding and development of anomaly detectors' operational characteristics, and therefore bring them to broader applications. (Ref. (4))

*GRP Report, Mar., 2006

- Taking the constructed framework as starting point, and with the objective to capture the normality drifts of computer systems behavior driven by users or system itself, we develop three versions of SVM-based anomaly detectors, which employ three modified Support Vector Machines as the kernel detection scheme. Our modification aims to break the traditional assumption that anomaly detectors are always fed with training data that are readily available with desired quality in batch, and thus enable them to be trained online periodically for the sake of adapting to the new computing environments without triggering excessive false alerts. To validate those anomaly detector's performance, we implement the experiments by reforming 1998 DARPA BSM data set collected at MIT's Lincoln Labs, and conduct the comparative studies with the original algorithms. The experimental results verify that our new designed anomaly detectors outperform the original ones with fewer support vectors (SVs) and less training time without sacrificing detection accuracy. (Ref. (3)(6))

- Based on the observations that anomaly detectors differ in detection coverage and blind spots, and different observable subjects provide different information for disclosing malicious intentions, we present another framework for the correlation of several parameteriable observation-specific anomaly detectors. Our hope is that a collection of simple surrogates based on specific operating environments can cooperate well and evolve into generic models with broader anomaly detection coverage and less false alerts. The cooperation between four host-based anomaly detectors is formulated as a multi-agent partially observable markov decision process (POMDP). A policy-gradient reinforcement learning algorithm is then employed to search in an optimal cooperation manner, with a set of parameters controlling individual anomaly detector's behavior. As the specific implementation of the framework, we develop an integrated anomaly detection model with a core component Autonomic Detection Coordinator (ADC) to defend against host-based intrusive anomalies, and a host-based experimental scenario is developed for its implementation showing satisfactory performance. The model is also extended as the basic analytical tool for the modeling and analysis of multi-stage coordinated attacks in computer networks. The definitions and properties derived from the models (both defender-centric and attacker-centric) present us a formal way for the development of countermeasures to thwart or mitigate such attacks. Taking into account the specific concerns of attackers and defenders, two algorithms called Attackers Nondeterministic Trail Searching algorithm (ANTS) and Attacker's Pivots Discovery by Backward Searching algorithm (APD-BS) are developed respectively. The former one aims to search for the most efficient concurrent actions for attackers, and the latter one intends to discover the attacker's significant observations for defenders.(May. 2004 $\sim$ present, Ref. (1)(2)(5))

FUTURE WORK

- To enrich the observation-centric analysis that we have carried out. We will extend our SVM-based anomaly detectors, which originally worked in the environments constructed by system calls (mainly frequency property), to some other operating environments such as shell command lines. Our main objective is to explore the relationship between the anomaly detector's performance and their computing environments.

- To extend the anomaly detection models that we have developed. We attempt to extend our integrated anomaly detection model to countermine those distributed attacks (e.g. worms, Dos, etc.). Although ADC's extended version, which is called *Janus*, has been applied to the modeling and analysis of multi-stage coordinated attacks in computer networks, its implementation (especially two algorithms ANTS and ADP-BS) worth further consideration with the specific computing environments. The model is also expected to dynamically preserve the desirable capability of information systems in the face of malicious intrusive attacks, i.e., survivability, and detect those attacks in their early stage so that cost-sensitive anti-attack strategies can be taken to mitigate threats in both scope and severity, mainly thwart attack's spread and prevent the further penetration.

SELECTED PUBLICATIONS

1. Z. Zhang, H. Shen, "Towards a Framework for the Correlation of Observation-Centric Anomaly Detectors: Modeling, Analysis, and Evaluation", *Submitted to IEEE Trans. on Reliability.*

2. Z. Zhang, H. Shen, "Modeling and Analysis of Multi-Stage Coordinated Attacks in Computer Networks," *Submitted to DSN2006.*

3. Z. Zhang, H. Shen, "Application of Online-training SVMs for Real-time Intrusion Detection with Different Considerations," Journal of *Computer Communications*, Vol.28, No. 12, July 2005, pp.1428-1442, Elsevier Science.

4. Z. Zhang, H. Shen, "A Brief Observation-Centric Analysis on Anomaly-based Intrusion Detection", to appear in the *International Journal of Network Security.*

5. Z. Zhang, H. Shen, "Constructing Multi-Layer Boundary to Defend Against Intrusive Anomalies: An Autonomic Detection Coordinator," *Proceedings of the International Conference on Dependable Systems and Networks (DSN2005)*, pp.118-127, Jun., 2005, Yokohama, Japan.

6. Z. Zhang, H. Shen, "Online Training of SVMs for Real-time Intrusion Detection," *Proceedings of the 18th IEEE International Conference on Advanced Information Networking and Applications (AINA2004)*, Vol 1, pp.568-p573, Mar., 2004, Fukuoka, Japan.