Analysis and Design of Effective Methods for Anomaly-based Intrusion Detection *

Zonghua Zhang, Student No. 320017
zonghua@jaist.ac.jp, School of Information Science, JAIST

RESEARCH OBJECTIVE

Anomaly-based intrusion detection is about discerning intrusive and normal patterns of activities based on the normality characterization of information systems. The common goal of anomaly-based intrusion detection is to detect intrusive attacks as many as possible with fewer false alerts. Generally, our work is to study effective models, methods and techniques for anomaly-based intrusion detection in hosts and networks with provision of adaptability, dependability, and scalability.

ACHIEVEMENTS (Aims & Solutions)

- Based on the characterization of the frequencies of system calls executed by the privileged programs in UNIX system, and breaking the strong traditional assumption that training data for anomaly detectors are readily available with high quality in batch, meanwhile to solve the "concept drift" problem of normal behavior traces, we modified conventional SVM, Robust SVM and One-class SVM respectively based on the idea from Online SVM, and compared their performance with that of the original ones. Both the theoretical analyse and experiments indicate that our modified SVMs can be trained online, and outperform the original ones with fewer SVs and less training time withoug decreasing detection accuracy. (Apr. 2003 $\sim$ May. 2004, Ref. (1)(5)(6)(7))

- To insight into the operational capabilities and limits of anomaly detectors, and evaluate them in a convictive way, both anomaly detection models themselves and their operating environment worth insightful analyse. Based on the similarity with induction problem, we cast anomaly detection in a statistical framework, which facilitates the analyse of their anticipated behavior from a high level. Existing problems and possible solutions about the characterization of normality for the observable subjects that from hosts and network have been discussed respectively, together with the case studies about the detection capabilities of several typical anomaly detection models. Our studies shows that the fundamental understanding of the observable subjects is the elementary stage in the process of establishing and effective anomaly detection model, especially when we face

*The Report for GRP Mid-evaluation, Mar.2005

the dilemma between anomaly detection performance and the computational cost. (Mar. 2004 $\sim$ Oct. 2004, Ref. (3))

- We have developed an integrated anomaly detection model, called Autonomic Detection Coordinator, which constructs a multi-layer boundary to defend against host-based intrusive anomalies by correlating several observation-specific anomaly detectors. The cooperation between independent meta-detectors were formulated as a partially observable Markov decision process (POMDP), and a policy-gradient reinforcement learning algorithm is applied to search in an optimal cooperation manner, with the objective to achieve broader detection coverage with fewer false alerts. The distributed architecture enables its scalability to a more complex situation and the dependability to tolerate the faults of elemental detectors. Moreover, the behavior of the coordinator can be adjusted easily by setting a reward signal, to meet the diverse demands of changing system situations. A preliminary experiment is implemented, together with some comparative studies, to demonstrate the coordinator's performance in terms of admitted criteria. (May. 2004 $\sim$ present, Ref. (2)(4))

FUTURE WORK

- Both theoretical analysis and experiments are still needed to verify our proposed autonomic detection coordinator. Specifically, besides the mathematical modeling of the coordinator, the probabilistic behaviors of individual anomaly detectors and their complementary operation worth more insightful analysis. In meantime, reducing the computational cost by abstracting effective observations for the individual anomaly detectors of the coordinator is also of our concern.

- Give further analyse on the anticipated behavior of the coordinator. Some other consensus strategies, or combination methods from the data fusion domain are also worth exploration.

- We will extend our model to the various computer networks, with the objective to countermine the distributed attacks such as worms, DoSs. Anomalies in MANETs, wireless networks or sensor networks are also expected to be detected through the optimal cooperation of location-centric anomaly detectors, with their respective special characteristics.

PUBLICATION LIST

1. Z. Zhang, H. Shen, "Online Training of SVMs for Real-time Intrusion Detection Based on Improved Text Categorization Model ", to appear in *Computer Communications*, Elsevier Science, 2005.

2. Z. Zhang, H. Shen, "Constructing Multi-Layer Boundary to Defend Against Intrusive Anomalies: An Autonomic Detection Coordinator", *The International Conference on Dependable Systems and Networks (DSN2005)*, Yokohama, Japan, June 28-July 1, 2005.

3. Z. Zhang, H. Shen, "A Brief Observation-Centric Analysis on Anomaly-based Intrusion Detection ", *The First Information Security Practice and Experience Conference, (ISPEC2005)*, April 11-14, 2005, Singapore.

4. Z. Zhang, H. Shen, "Dynamic Combination of Multiple Host-based Anomaly Detectors with Broader Detection Coverage and Less False Alerts", *4th International Conference on Networking (ICN'05)*, April 17-21, 2005, Reunion Island, France.

5. Z. Zhang, H. Shen, "Online Training of SVMs for Real-time Intrusion Detection," *18th IEEE Int. Conf. on Advanced Information Networking and Applications (18thAINA)*, Vol 1, p568-p573, Fukuoka, Japan, March, 2004.

6. Z. Zhang, H. Shen, "Capture the Drifting of Normal Behavior Traces for Adaptive Intrusion Detection Using Modified SVMs," *3rd Int. Conf. on Machine Learning and Cybernetics (ICMLC2004)*, P3045-3051, ShangHai, August, 2004.

7. Z. Zhang, H. Shen, "Suppressing False Alarms of Intrusion Detection Using Improved Text Categorization Methods," *IEEE Int. Conf. on e-Technology, e-Commerce and e-Service (EEE2004)*, p163-p166, TaiWan, March, 2004.