Proceedings of the

FTRA AIM 2012

The 2012 FTRA International Conference on
Advanced IT, engineering Management
for Industrial Technology

February 6~8, 2012, Hana Square, Korea University, Korea
Computing Semantic Distance Using Ontologies
WEIJIE LIU, YONGJUN ZHU, WOOJU KIM, HAKJIN KIM

T-Grid: A Domain based Trusted Grid Model with Purging of Untrustworthy Transactions
P. SURESH KUMAR, P. SATEESH KUMAR, S. RAMACHANDRAM

User-privacy and modern smartphones: A Siri(ous) dilemma
Dimitrios Damopoulos, Georgios Kambourakis, Marios Anagnostopoulos, Stefanos Gritzalis, Jong Hyuk Park

Location Privacy Pre-protection through Markov Chain for Wireless Sensor Networks
Yuan Tian, Biao Song, Eui-nam Huh

An Adaptive and Efficient Remote Screen Transmission Protocol for Mobile Thin Client
Biao Song, Wei Tang, Eui-nam Huh

Attack Strategies Construction and Exchange Model in a Collaborative Cloud Computing environment
Doan Man Nguyen, Jun Young Park, Sang Ho Na, Tian Yuan, Eui-Nam Huh

User Model with Life in Cyber-Individual
Bofeng Zhang, Jianxing Zheng, Jianhua Ma, Yinshe Li, Guobing Zou

Efficient Error-tolerant String Search Techniques for Supporting Mobile Applications
Jongik Kim, Eunseok Lee

Computation Offloading for Energy Conservation of Multi-Interface Smartphone in Mobile Cloud Computing
Yun Won Chung

Resource Provision Technique with Mobility Grouping in Mobile Cloud Computing
JiSu Park, Byoungwook Kim, HeonChang Yu, EunYoung Lee

A Collaborative Processing Scheme for Continuous Nearest Neighbor Monitoring in Mobile Navigation
Hyung-Ju Cho, Rize Jin, Tae-Sun Chung

Hybrid Remote Display Protocol for mobile Thin Client Computing
Wei Tang, Biao Song, Tien Dung Nguyen, Eui Nam Huh
Attack Strategies Construction and Exchange Model in a Collaborative Cloud Computing environment

NGUYEN DOAN MAN, JUN-YOUNG PARK, SANG-HO NA, TIAN YUAN and EUI-NAM HUH
Department of Computer Engineering
KyungHee University
REPUBLIC OF KOREA
{parkhans, shna, tianyuan, huh}@icns.khu.ac.kr, doanman1985@gmail.com

Abstract
Intrusion Detection Systems (IDSs), nowadays, critically becomes an important security component in the novel commercial computing models to detect malicious behaviors timely and protect either network infrastructure or individual hosts from the serious damage of attacks. For Cloud Computing, various application scenarios and complexity at a higher level make the traditional IDS approaches difficult to find out the actual threats from the novel multi-step attacks, which stem from the new vulnerabilities of Cloud environments. Therefore, information about novel attack scenarios is an urgent requirement to operate IDSs built in Cloud Computing more efficiently and accurately. This paper focuses on developing a data mining-based approach to construct new attack scenarios from the sequences of low-level alerts gathered from multiple traditional IDSs. In addition, an Attack Signature Exchange (ASE) model between Interconnect Clouds in a Collaborative Cloud Computing environment which is considered as a prior knowledge exchange is also presented.

Key-words: Intrusion Detection System, Cloud Computing, Attack scenario, Attack Signature, Collaborative Cloud

1. Introduction
One of the drawbacks of current IDSs is generating the number of alerts each day and a considerable proportion is false alerts, which makes managing meaningful and important security events a cumbersome duty for an administrator [2]. This issue is exaggerated as IDSs are involved in Cloud Computing. Through the use of virtualization and resource sharing, Clouds serve with a single set of physical resources a large user base with different needs. Therefore, virtualization contributes to build a complex computing model where numerous hosts of different Cloud customers (CCs) can exist on the same physical machine. This not only creates a considerable amount of new security vulnerabilities but also makes IDSs distributed to monitor virtual machines (VMs) on Clouds produce much more alerts per day than ever. Alert correlation is one of the proposed methods to address this issue when it is efficient to manage the large volume of raw alerts that are raised by heterogeneous IDSs [3]. In addition, the output of alert correlation processes is a set of high-level alerts to represent multi-step attacks accurately, while most alerts raised by current IDSs only include information about each single attack step, which cannot reflect the damage of novel attacks fully.

However, to develop an efficient alert correlation model, the key requirement is prior knowledge for attack scenarios, or attack signatures. Therefore, in this paper we propose a data mining-based algorithm to discover new multi-step attack scenarios from raw alerts raised by multiple IDS sensors located in Cloud’s infrastructure. We also present an ASE model for IDSs located in Interconnected Clouds to share new knowledge about attack strategies which have already been discovered in a Collaborative Cloud Computing system.

2. Attack Scenario Construction

2.1 IDS Framework
Figure 1 shows our proposed IDS framework which can be applied into Cloud infrastructure to protect CCs’ VMs from being compromised by either external or internal attacks. Besides the IDS sensors, which are traditional IDSs and integrated to each VM to monitor and produce raw alerts for corresponding intrusions, two other main components are Attack Scenario Builder (ASB) and Alert Correlation (AC), which is considered as an alert correlation engine to detect multi-step attacks from the dataset of alerts with the support of attack signatures stored in Scenario Database.

Figure 1: The Attack Scenario Construction and Detection framework
2.2 Attack Scenario Builder

ASB is responsible for receiving raw alerts from IDS sensors, aggregating them into hyper alerts and then analyzing these hyper alerts to detect novel attack strategies with a data mining-based approach. The idea of mining attack sequential patterns comes out from the fact that different multi-stage attack strategies taken by the attacker usually have their own attack behavior sequence patterns. Series of attacker’s behaviors launched with certain intent have time consecutive association and appeared in ordered sequence [1].

2.2.1 Mining Phase

The process of mining frequent attack patterns starts after the set of raw alerts is converted into hyper alerts and divided into time-ordered alert sequences through Attack Scenario Time Windows (ASTW). We construct an Attack Occurrence matrix to describe the temporal relation between alert types. In this $N \times N$ matrix where $N$ is the number of known attack types, $d_{ij}$ represents the number of attack sequences where alert $j$ occurs consequent after the initial alert $i$. With this matrix, we can find out the most possible attack behaviors after a successful attack behavior in the same ASTW. The greater $d_{ij}$ is, the more possible of the occurrence of attack behavior $j$ after attack $i$.

Next a corresponding Attack Occurrence Probability (AOP) matrix $P$ is built, each cell of which keeps a value $p_{ij}$, the probability that attack $j$ occurs after the occurrence of attack $i$ in an ASTW. If $p_{ij} \geq \delta$, a predefined probability threshold, we can infer that attack type $i$ and attack type $j$ have a causal relation. Therefore, these attack sequences where alert $j$ occurs consequent after the initial alert $i$ are collected as candidate attack sequences for further analysis.

2.2.2 Correlation Phase

Beside attack occurrence probabilities that we got from the statistical approach, for improving the accuracy of attack scenario model, we also consider the correlation-ship of the real alerts in a training database via the measure Correlation Rate $Cor(A, B)$. The larger correlation rate is, the more possibility they belong to the same attack scenarios.

We consider that there are $n$ pairs of alerts $a_i, b_i$ whose attack types are A and B, respectively, in the training database of real alerts.

$$Cor(A, B) = \frac{\sum_{i=1}^{n} Cor(a_i, b_i)}{n} \quad (1)$$

2.2.3 Attack Scenario Graph

From the results of matrix $P$ and Correlation Rate, we construct the final novel attack scenarios and illustrate them into Attack Scenario Graphs (ASG). These ASGs are considered as attack signatures which are used at AC module to analyze the future dataset of alerts and then detect new intrusions.

3. Signature Exchange Model in Collaborative Cloud Model

The ASE model is a solution to exchange knowledge about novel attacks between Interconnect Clouds of a Collaborative Cloud environment. In this framework, a centralized XML-based signature base called Security Management Domain can download new signatures from Interconnect Clouds in the same Collaborative environment or public sources on Internet and publish them to all Interconnect Clouds on the same Cloud environment.

![Figure 2: Attack Signature Exchange model](image)

4. Conclusion

In this paper, we applied a pattern mining approach to extract novel attack scenarios from the sequences of raw alerts that are collected from distributed IDSs in a Cloud Computing environment. By statistics about frequency of occurrences of the alert sequences, we could find out the frequent attack sequences which are considered as the candidate multi-step attacks and use them as materials to build ASGs. Therefore, the final ASGs are provided to AC module, the main component of our IDS framework, to detect the novel multi-step attacks in Clouds accurately from a huge amount of raw alerts collected. Finally, the ASE model for Collaborative Cloud Computing environments, which helps to improve the efficiency of alert correlation processes in each Cloud with attack knowledge from other members, are also introduced.

REFERENCES

