http://dx.doi.org/10.7236/JIIBC.2013.13.3.9
JIIBC 2013-3-2

네트워크 보안에서 모니터링 기반 실시간 침입 탐지

A Real-Time Intrusion Detection based on Monitoring in Network Security

임승철*

Seung-Cheol Lim

요 약 최근 침입 탐지 시스템은 공격의 수가 극적으로 증가하고 있기 때문에 컴퓨터 네트워크 시스템에서 아주 중요한 기술이다. 어려운 침입에 대한 감시데이터를 분석하기 때문에 침입 탐지 방법의 대부분은 실시간적으로 침입을 탐지하지 않는다. 네트워크 침입 탐지 시스템은 개별 사용자, 그룹, 원격 호스트와 전체 시스템의 활동을 모니터링하고 그들이 발생할 때, 내부와 외부 모두에서 의심 보안 위반을 탐지하는 데 사용한다. 그것은 시간이 지남에 따라 사용자의 행동 패턴을 학습하고 이러한 패턴에서 벗어나는 행동을 감지한다. 본 논문에서 알려진 시스템의 취약점 및 침입 시나리오에 대한 정보를 인코딩하는 데 사용할 수 있는 규칙 기반 구성 요소를 사용한다. 두 가지 방법을 통합하는 것은 침입 탐지 시스템 권한이 있는 사용자 또는 센서 침입 탐지 시스템 (IDS)에서 데이터를 수집 RFM 분석 방법론 및 모니터링을 사용하여 비정상적인 사용자 (권한이 없는 사용자)에 의해 침입뿐만 아니라 오용을 탐지하기위한 포괄적인 시스템을 만든다.

Abstract Recently, Intrusion detection system is an important technology in computer network system because of has seen a dramatic increase in the number of attacks. The most of intrusion detection methods do not detect intrusion on real-time because difficult to analyze an auditing data for intrusions. A network intrusion detection system is used to monitors the activities of individual users, groups, remote hosts and entire systems, and detects suspected security violations, by both insider and outsiders, as they occur. It is learns user's behavior patterns over time and detects behavior that deviates from these patterns. In this paper has rule-based component that can be used to encode information about known system vulnerabilities and intrusion scenarios. Integrating the two approaches makes Intrusion Detection System a comprehensive system for detecting intrusions as well as misuse by authorized users or Anomaly users (unauthorized users) using RFM analysis methodology and monitoring collect data from sensor Intrusion Detection System(IDS)

Key Words : Intrusion Dection, Sensor IDS, Network Security, System Monitoring,

Ⅰ. Introduction

Through Internet access from outside of using illegal and illegal intrusion are deployed in many cases in recently. As many companies and organizations are received and got a lot of damages from attacking

*정회원, 우송대학교 컴퓨터정보학과
접수일자 : 2013년 4월 12일, 수정완료 : 2013년 5월 17일
게재확정일자 : 2013년 6월 14일

Received: 12 April 2013 / Revised: 17 May 2013 /
Accepted: 14 June 2013
*Corresponding Author: sclim@wsu.ac.kr
Dept. of Computer Information Science, Woosong University, Korea

inside and outside. In addition, network environments and intrusion system are with curiosity and heroism. But nowadays, flowing of illegal information ranging from the purpose of cyber terrorism attacks are growing performing, and growing of Internet links to be accelerated with the increasing of the network, diversity attack paths and intelligent analysis of attack and tracing techniques are becoming difficult to detection. So this network intrusion attempts and diversification has been more increasing and has new effective designs making hardening, by the attacking users and the development of new attack methods, systems of the network security area was to expand in this area. Intrusion detection is the process of monitoring the activities of a computer or network system and analyzing them for signs of intrusion or attacks [1]. The intrusion detection system (IDS) is the software or hardware that automates this monitoring and analysis. The intrusion detection depends on two basic processes to work: monitoring the underlying system activity and analyzing the resulting event data. The analysis process can be conducted by means of two main techniques: the first is misuse detection, in which data is analyzed to find intrusions matching predefined attack signatures kept by the IDS, and the second is anomaly detection, in which data is analyzed to spot anomalies different from a predefined normal profile of the protected system that using Sensor to collection data. And other way it is for detects wide variety of intrusions to attacks previously known and unknown and suggests need to learn or adapt to attacks or changes in behavior. Design system for detect intrusion in timely fashion because system may need to be real-time, especially when system responds to intrusion and system may suffice to report intrusion occurred a few minutes or hours ago. Today, there are generally two types of intrusion detection systems: anomaly detection and misuse detection.

Anomaly detection approaches attempt to detect intrusion by noting significant departures from normal behavior [2]. Misuse detection techniques attempt to model attacks on a system as specific patterns, and then systematically scan the system for the occurrences of these patterns [3]. This process involves a specific encoding of previous behaviors and actions that were deemed intrusive or malicious.

Real-Time intrusion detection is controlling activity of users to detection of unusual and abnormal activity or events in real-time and detects break-ins or attacks through various data sources from logs, audits, surveillance and network traffic. In addition, this paper using monitor system continuously and report suspicious all users activities [4].

Anomaly detection approaches attempt to detect intrusion by noting significant departures from normal behavior [2]. Misuse detection techniques attempt to model attacks on a system as specific patterns, and then systematically scan the system for the occurrences of these patterns [3]. This process involves a specific encoding of previous behaviors and actions that were deemed intrusive or malicious.

Real-Time intrusion detection is controlling activity of users to detection of unusual and abnormal activity or events in real-time and detects break-ins or attacks through various data sources from logs, audits, surveillance and network traffic. In addition, this paper using monitor system continuously and report suspicious all users activities [4].

II. A Real-Time Intrusion Detection System

We use this techniques for detecting abnormal users of monitor and through the network of illegal intrusion detection in order to continue to occur for each case record and able to track and prevent intrusion or intrusion resulting from a loss in order to minimize the system raising from all activities of the closer data for research and analysis is needed. Real-Time system events related to the audit data

huge amount to the data analysis and storage overhead and effectively to achieve real-time intrusion detection because of the difficulty and take long time security audit data, filtering, through clustering then real-time multi-agent network of unnecessary system load and reduce the load applied to the rapidly changing internet. And other attack is misuse users and anomaly users system got a lot of damage from inside and outside threat. So In this framework will focus on audit data training we use a monitoring to show activities all of users and record it in real-time.

Intrusion detection techniques are generally classified into two categories: anomaly detection misuse detection. Anomaly detection assumes that misuse or intrusions are highly correlated to abnormal behavior exhibited by either a user or the system. Anomaly detection approaches must first baseline the normal behavior of the object being monitored, and then use deviations from this baseline to detect possible intrusions. Anomaly detection approaches have been implemented in expert systems that use rules for normal behavior to identify possible intrusions [5], in establishing statistical models for user or program profiles [6], and in using machine learning to recognize anomalous user [7]. Misuse detection techniques attempt to model attacks on a system as specific patterns, and then systematically scan the system for occurrences of these patterns. This process involves a specific encoding of previous behaviors and actions that were deemed intrusive or malicious. in this framework misuse detection methods involved off-line analysis of audit trails normally recorded by host machines. For instance, a security officer would manually inspect audit trail log entries to determine if failed root login attempts were recorded. Manual inspection was quickly replaced by automated analysis tools that would scan these logs based on specific patterns of intrusion. Misuse detection approaches include expert systems [8], model-based reasoning [9], state transition analysis [10], and keystroke dynamics monitoring [11]. Nowadays, the vast majority of commercial and research intrusion detection tools are misuse detection tools that identify attacks based on attack signatures.

Ⅲ. Proposed Real-Time Intrusion Detection and Simulations

1. Real-Time Intrusion detection based on state transition

Using a real-time intrusion detection expert system is an intrusion of the state of the system as representing a transition road to the State Transition Analysis Technique (STAT) in Fig 1, (state transition of the technique in real-time detection of mismatch detection system): distributed intrusion detection to intrusion of an individual host is determined by set of vulnerabilities each o handled separately from host because the host normal level but when you look at the level of network security vulnerabilities have big sides are exposed. In addition, monitoring is the action of all users appreciate the vast amount of data needed to analyze because of the burden is big.

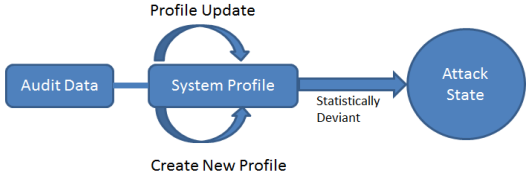

Fig. 1. Misuse of state transition using detection algorithm
그림 1. 탐지 알고리즘을 사용하여 상태 전이의 오용

STAT of the state transition Petri-Net and transition monitoring [12], transition have not attacked by them every time, they thought to even times, transition monitoring intrusion detection research with the transition to this state even for a single act of abuse fragmented mainly because of the diagnosis negative decision error state transition to technology is a short diagnostic we will miss, so many

aggression. As an example, the user's action are not described set of state transition but that is create a new profile of update accompanied by a non-aggression is a matter of time that occurs frequently fail to detect. Especially we focus on detection techniques on the command name, command change because depends on you if leave the system interpreted as a normal command is used within the system call is harmful even difficult to find. Real-Time detection system in the state transition diagram technique has pre side effects. Real-Time intrusion detection capability to perform the first multi-host targeting network-based intrusion detection for analysis need to fence a host of different environments due each host structure presence and the operating system audit sub-system characteristics different limitations because of the limitation on operating security system represents. Nowadays, intrusion detection encompasses event log analysis for insider threat detection; network traffic analysis for threat detection; security configuration management; and file integrity checking. Clearly, current intrusion detection requires properties of both network and host-based intrusion detection systems. Intrusion detection is network-based when the system is used to analyze network packets. This is in contrast to host-based intrusion detection, which relates to processing data that originates on computers themselves, such as event and kernel logs. Network packets are usually "sniffed" off the network, although they can derive from the output of switches and routers. The most common protocol targeted is TCP/IP. Network sources are unique because of their proximity to unauthenticated, or outside, users. They are positioned to detect attempts originating outside the network.

There are many attack scenarios that would not be detected by host-based technology, thereby highlighting the differences between the two. Unauthorized access occurs when an outsider comes in over the network and logs into the system uninvited. This can be detected by host-based systems once the attacker is inside, but the ultimate goal is to detect them before they get access [13], or during the process of getting access as follow in Fig 2.

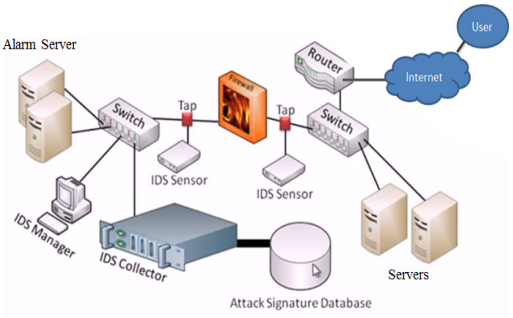

Fig. 2. Multiple host-based systems according to the diversity of the operating system vulnerabilities

그림 2. 운영체제 취약점의 다양성에 따른 호스트기반 다중 시스템

We using RFM to improve and analysis user's profile, analysis access log such as (who, host, recently, interval, total number of attempt, risk abomination), connection failed, some users attempt to access users or based on the contents of the log abnormal behavior to diagnose and predict the risk weights. The risk propagation of an intrusion alert level to determine the levels of RFM to reflect the weighting formula (1) is as follow:

$$\text{Alert Level (warning)} = \text{Risk} * \text{Event Spread of Invasive} * \text{Weight of RFM} \quad (1)$$

The agent is specific host on the network packets or system calls generated through the receiver module accepts. Receiving module is a random pattern and the input of the agent compared with the internal pattern of intrusion risk and spread of invasive and calculated according to the classification of the level of alert is sent to the transmitter module. According to the calculation of the alert level for transmitting module to the analyzer we can assign multi-level role, delegating the task assignments and alert because the

higher-level security warning message when we are dangerous too quickly to inform the security manager. If we find a new attack pattern we should be documented immediately and the processing of a new intrusion patterns as possible, causing minimal damage should be occurred. The ideal pattern scenarios without additional model is only relevant portion of any damage should be updated or added. These requirements agent model consists of several components, modules, object-oriented design, which can be making when the quality is possible[14]. Between modules interfaces the implementation of the methods that need to be changed. In particular, the processing of intrusion patterns change over a certain number of times when the attack pattern in a specific attack pattern processing module that processes the algorithm of the model without affecting the rest needs to be modified. Agent model in the attack pattern calculated by comparing the alert level for the process and the process of adding new attack pattern graphs follow Fig 3.

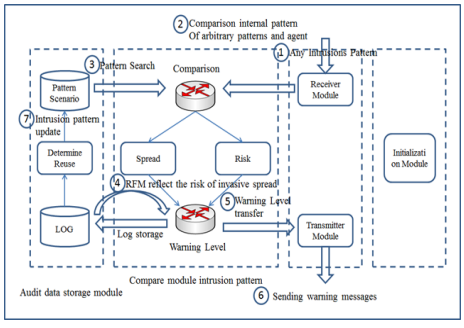

Fig. 3. Intrusion of the agent and the alert level for the comparison of the pattern calculated
그림 3. 에이전트의 침입 계산된 패턴비교에 대한 경고수준

2. Real-Time Intrusion Detection Algorithm

We using an agent model whether a random pattern, the pattern of intrusion detection and warning bell to calculate the algorithm is as follow in Fig 4. The alert level to calculate the input pattern is detected, the level of risk based and propagation level after first identifying a weight of RFM warning level can be calculated.

3. Simulations

The anomaly and misuse detection systems were tested on the same test data. The test data consisted of 139 non-intrusive sessions, and 22 intrusive sessions. Although would have been preferable to use a larger number of intrusive sessions for testing, there were so few intrusive sessions in the DARPA data that all other intrusion data were used to train the misuse detection system. The performance of any intrusion detection

```
Procedure DetectionCalLevel
Input
Int PatternEntry;
Output
Int DangerLevel;
Int TransLevel;
Int DetectionLevel;
{
Reset
Loop
        Get PatternEntry
        if(PatternEntry==Internal)
                Calculation DangerLevel
                if(Patternentry==‘Minimum Status’) DangerLevel=0
                elseif(PatternEntry==‘Warning Status’) DangerLevel=1
                elseif(PatternEntry==‘Caution Status’) DangerLevel=2
                elseif(PatternEntry==‘Serious Status’) DangerLevel=3
                elseif(PatternEntry==‘Maximum Status’) DangerLevel=4
                TransLevel Calculation
                if(PatternEntry==‘No Trans Status’) TransLevel=0;
                elseif(PatternEntry==‘Partially Trans Status’) TransLevel=1
                elseif(PatternEntry==‘Full Trans Status’) TransLevel=2
                Weight Calculation
                DetectionLevelCalculation
                DetectionLevel: = DangerLevel*TransLevel*Weight
                Display Message
        else go to Loop
}
```

Fig. 4. Real-Time Intrusion Detection Agent Warning Level
그림 4. 실시간 침입 탐지 에이전트 경고수준

system must account for both the detection ability and the false positive rate. We observed both of these factors while varying the leak rate used by the leaky bucket algorithm. The performance of the IDS should by judged in terms of both the ability to detect intrusions, and by false positives, incorrect classification of secure behavior as insecure. We used receiver operating characteristic (ROC) curves to compare intrusion detection ability to false positives. A ROC curve is a parametric plot, where the parameter is the sensitivity of the system to what it perceives to be insecure behavior. The curve is a plot of the likelihood that an intrusion is detected, against the likelihood that a non-intrusion is misclassified for

a particular parameter, such as a threshold. In Fig 5 display two ROC curves, one for a low leak rate, and one for a high leak rate.

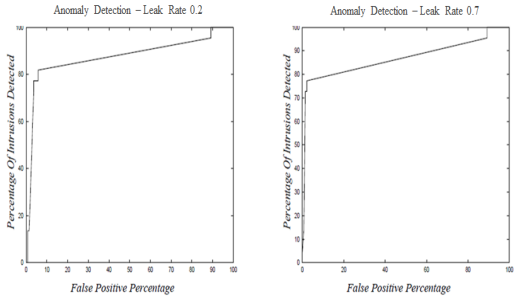

Fig. 5. Anomaly detection results for two different leak rates
그림 5. 두 개의 서로 다른 누설률에 대한 이상 탐지결과

For the leak rate of 0.2, to achieve detection better than 77.3%, one must be willing to accept a dramatic increase in false positives. At 77.3% can be achieved with a false positive rate is only 3.6%. When the leak rate is 0.7, a detection rate of 77.3% can be achieved with a false positive rate of only 2.2%. And also produced for the performance of our misuse detection system. While the performance was not nearly as good as the anomaly detection system in terms of false positive (which was a high as 5% for even low sensitivity rate), the misuse detection system displayed very high detection abilities, especially surprising due to the small number of sessions used to train the system.

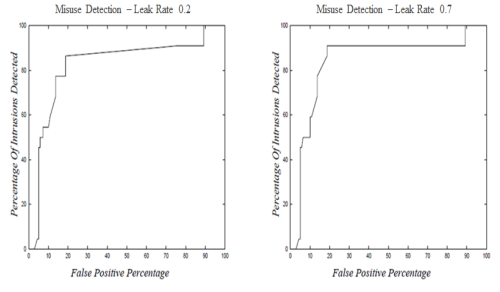

Fig. 6. Misuse detection results for two different leak rates
그림 6. 두 개의 서로 다른 누설률에 대한 오용 탐지결과

As illustrated in Fig 6, with a leak rate of 0.7, the system was able to detect as much as 90.9% of all intrusions with a false positive rate of 18.7%. Other host-based misuse detection systems can currently provide similar detection capabilities with lower false positive rates.

IV. Conclusion

In this paper, we have rule-based component that can be used to encode information about known system vulnerabilities and intrusion scenarios. We use RFM technique to improve and analysis and update user's profile so we can know all activities of users, we can detect because we using system monitoring to show and record it. And we believe that combined network-based and host-based intrusion detection systems effectively prevent attacks from insider and outsider as well. We prevent before hacker attack, detection if it has anomaly deriving from our system and after detect it we responding.

For the future, research for Real-Time Multi-agent IDS Security will more stable vulnerabilities system, detection misuse and anomaly users from inside and outside network, stable implementation of the system, it can get help from intrusion items, classified, record warning, system monitoring, provide step analysis and this using all of these techniques can control and record activities all of users (authorized and unauthorized), can detect negative decision error and attack from the audit data in real-time.

Reference

[1] M.F. Buckley, "Computer Event Monitoring and Analysis," PhD thesis, Dept of Electrical and Computer Eng, Carnegie mellon Univ, Pittsburgh, PA, May 1992.

[2] A.K. Ghosh, J. Wanken, and F. Charron. Detecting

anomalous and unknown intrusions against programs. In Proceedings of the 1998 Annual Computer Security Applications Conference (ACSA'98), December 1998.

[3] W. Lee, S. Stolfo, and P.K. Chan. Learning patterns from Unix process execution traces for intrusion detection. In Proceedings of AAA197 Workshop on Al Methods in Fraud and Risk Management, 1997.

[4] T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannthan, C. Jalili, H.S. Javitz, A. Valdos, P.G. Neumann, and T.D. Garvey. A real-time intrusion-detection expert system (ides). Technical Report, Computer Science Laboratory, SRI International, February 1992.

[5] W. Lee, S. Stolfo, and P.K. Chan. Learning patterns from unix process execution traces for intrusion detection. In Proceedings of AAA197 Workshop on AI Methods in Fraud and Risk Management, 1997.

[6] P.A. Porras and P.G. Neumann. Emerald: Event monitoring enabling responses to anomalous live disturbances. In Proceedings of the 20th National Information System Security Conference, pages 353-365, October 1997.

[7] A.K, Ghosh, J. Wanken, and F. Charron. Detecting anomalous and unknown intrusions against programs. In Proceedings of the 1998 Annual Computer Security Applications Conference (ACSA 98), December 1998.

[8] W.W. Cohen. Fast effective rule induction. In Machine Learning: Proceedings of the Twelfth International Conference. Morgan Kaufmann, 1995.

[9] S. Kumar and E.H. Spafford. A pattern matching model for misuse intrusion detection. The COAST Project, Purdue University, 1996.

[10] P.A. Porras and R.A. Kemmerer. Penetration state transition analysis - a rule-based intrusion detection approach. In Eighth Annual Computer Security Applications Conference, pages 220-229. IEEE Computer Society Press, November 1992.

[11] S. Kumar and E.H. Spafford. A pattern matching model for misuse intrusion detection. The COAST Project, Purdue University, 1996.

[12] K. Ilgun, R.A. Kemmerer, and P.A. Porras. State transition analysis: A ruls-based intrusion detection system. IEEE Transactions on Software Engineering, 21(3), March 1995.

[13] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", September 11, 2003.

[14] JJ Park, GS Choi, IK Park, JJ Kang, "Digital Modeling of a Time delayed Continuous-Time System", Journal of The institute of Internet, Broadcasting and Comm., vol. 12, issue 1, pp. 211-216, Feb. 2012.

저자 소개

임 승 철(정회원)

- 1985년 : 한양대학교 전자공학과 학사
- 1994년 : 전북대학교 정보통신과 석사
- 2003년 : 전북대학교 영상공학과 박사
- 2006년 ~ 현재 : 우송대학교 컴퓨터정보학과 교수

<주관심분야 : 이동통신, 컴퓨터네트워크, 임베디드시스템소프트웨어>