한국시뮬레이션학회 '00추계학술대회 논문집 2000.11.11 아주대학교

침입 탐지 시스템 평가를 위한 Experimental Frame의 디자인

김형종, 조대호
성균관대학교 전기전자 및 컴퓨터공학부

Abstract

침입 탐지 시스템은 네트워크나 호스트에 대한 오용, 남용, 또는 허가되지 않은 접근을 탐지하는 기능을 갖는 시스템이다. 최근 침입들은 그 종류가 매우 다양화되고, 탐지하기가 매우 어려운 형태로 나타나고 있다. 이러한 침입으로 대표적인 것이 분산 공격과 스텔시 공격(Stealthy Attack)이 있다. 분산 공격은 침입자가 공간적으로 분산되어 이를 탐지하기 어렵게 하는 공격을 말하며, 스텔시 공격은 시간적으로 분산되어 이를 탐지하기 어려운 경우를 말한다. 침입 탐지 시스템의 모델링 및 시뮬레이션을 위해서는 침입 탐지 시스템 모델에 필요한 침입을 제공하고, 침입에 대한 탐지 능력을 평가 하기 위한 experimental frame을 디지인 해야 한다. 본 연구에서는 분산 공격과 스텔시 공격 기능을 갖는 침입 생성 모델링 방법을 소개하며, 침입 생성을 위해 요구되는 침입 정보 베이스의 역할 및 저장 정보를 소개한다. 또한, 침입에 대한 탐지 능력 평가를 위한 Transducer 모델의 디자인을 소개한다.

Key word : Intrusion Detection System(IDS), Distributed Attack, Stealthy Attack, Experimental Frame, Intrusion Generator, Transducer

I. 서론

침입 탐지(Intrusion Detection)는 네트워크나 호스트에 대한 오용, 남용, 또는 허가되지 않은 접근에 대한 문제를 다룬다[1]. 침입 탐지 시스템은 이러한 침입 탐지 기능을 컴퓨터 시스템으로 하여금 수행하도록 하는 소프트웨어를 말한다. 침입 탐지 시스템은 시스템과 네트워크의 다양한 데이터 원천을 통해서 얻은 정보를 수집, 분석함으로써 침입의 징후를 찾아내고, 내부에 침입의 탐지를 위한 지식을 소유한다. 최근 크래커들의 침입이 매우 지능적이고 다양화되면서 이를 탐지하기 위한 침입 탐지 시스템도 효과적인 시스템 구조와 침입 탐지 지식을 소유한 형태로 발전하고 있다. 복잡한 시스템 구조와 다양한 침입 탐지 지식을 가지고 있는 경우, 각 시스템 내부의 구성 요소들의 상호 작용과 상호 작용에 의한 결과를 예측하는 것은 매우 어렵다. 이러한 시스템의 구조와 동적인 특성을 파악하는데 가장 많이 활용되는 것이 시뮬레이션 모델을 만드는 것이다. 특정 침입 탐지 시스템의 구조적 특성과 동적 특성이 일치하는 모델을 만들고 이 모델을 실행 할 때 실제 시스템의 특성을 파악하는 것이 매우 용이해 진다. 본 연구에서는 이러한 시뮬레이션 모델의 평가를 위한 기반 환경이 되는 EF(Experimental Frame)의 디자인을 살펴보고자 한다[2]. EF는 모델에 입력을 제공해 주기 위한 Generator모델과 모델의 출력을 분석하기 위한 Transducer로 구성된다. 본 연구의 Generator 모델은 침입을 생성하는 모델이 된다. 보안 시스템 모델에 침입의 일부가 되는 네트워크 입력과 침입이 아닌 네트워크 입력을 동시에 제공한다. 또한, Transducer는 평가 대상 모델의 출력을 Generator 모델이 발생시킨 침입과 비교, 분석하여 침입의 탐지 여부를 결정한다. 특히, 본 연구에서는 False Positive 비율과 False Negative 비율을 성능 지수로 할 경우의 Transducer 디자인을 보여 주고자 한다.

II. 배경 이론

1. 침입 탐지 시스템

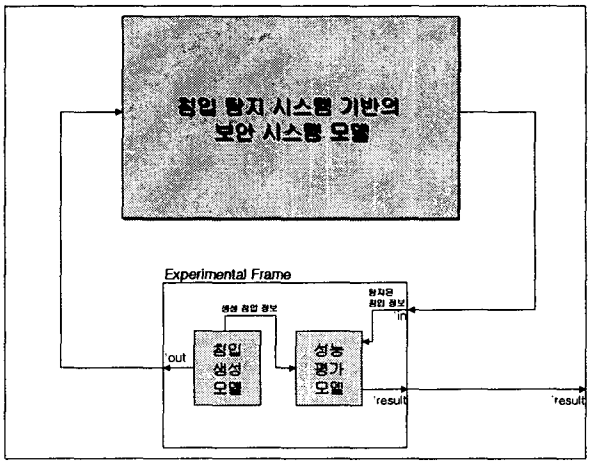
침입 탐지 시스템은 허가되지 않은 외부 사용자의 침입 시도와 내부 사용자의 권한 남용을 탐지하는 시스템이다[1]. 침입 탐지 시스템의 침입 탐지 접근 방법에는 오용 탐지(misuse detection)와 비정상 행위 탐지(anomaly detection) 방법이 있다[3][4][5]. 오용 탐지 방법은 침입이라고 생각되는 패턴을 저장해 놓고, 이에 일치 또는 유사한 사용자의 행위가 나타났을 때 이를 탐지하는 것이다. 오용 탐지에는 주로 전문가 시스템이 사용되며, 전문가 시스템은 사용자의 작업 절차와 저장되어 있는 침입 특성을 가지고 추론을 하게된다. 비정상 행위 탐지 방법은 시스템이나 네트워크에서 일어나는 행위들 중 일반적이지 않고, 발생 빈도가 매우 적은 행위의 발생을 탐지하는 방법이다. 이러한 탐지 방법은 침입자(attacker)의 행위가 일반 사용자의 행위와 주목할 만큼 다르다는 가정을 기반으로 한다. 이를 위해서 정상적인 행위의 특성 정보가 필요하며, 침입 탐지 시스템은 사용자의 행동의 특성을 분석하는데 이 정보를 사용하게 된다. 일반적으로, 비정상 행위 탐지 기법은 통계적 기법이나 뉴럴 네트워크 등을 사용한다. 최근 개발되고 있는 침입 탐지 시스템은 이 두 가지 탐지 기법을 모두 사용하여 좀 더 효과적인 침입 탐지를 하고자 한다.

침입 탐지 시스템은 침입의 탐지에 사용되는 데이터의 원천에 따라 시스템 데이터 기반 침입 탐지 시스템과 네트워크 데이터 기반의 침입 탐지 시스템으로 나누는 것이다[3][4][5]. 시스템 데이터 기반 침입 탐지 시스템은 단일 호스트 내에서 발생하는 침입을 탐지하는 시스템으로 주로 시스템 내부의 로그 파일이나 감사 파일을 사용한다. 네트워크 데이터 기반의 침입 탐지 시스템은 네트워크 트레픽에서 침입의 패턴을 찾아내는 방법으로 침입을 탐지한다. 시스템 데이터 기반 침입 탐지 시스템은 단일 시스템 대상 공격은 탐지 할 수 있지만, 다중 시스템 대상 공격은 탐지가 어렵다. 반면, 네트워크 기반 침입 탐지 시스템은 다중 시스템 대상 공격의 탐지에는 적당하지만, 시스템 내부의 오용이나 남용에 대한 탐지가 어렵다. 최근의 침입 탐지 시스템은 이 두 가지 침입 탐지 시스템의 조합한 형태로 구성되어, 다양한 침입을 탐지 할 수 있는 능력을 소유하도록 구성된다.

2. 침입의 유형

침입의 유형에 대한 분류는 수년간 여러 학자들에 의해서 진행되어 왔다. 침입 유형의 분석은 침입의 탐지 시스템의 침입 탐지 지식을 결정하는 중요한 연구 분야이다. [6]에서는 3,000대의 컴퓨터에서 20년 동안의 남용 예를 통해서 9가지의 오용 계층을 나누었다. 각 계층은 NP1부터 NP9까지로 명명되며, NP1 클래스는 물리적인 단계의 오용을, NP2 클래스는 하드웨어 레벨의 오용을 정의하며, NP3 클래스부터 NP9 클래스까지는 소프트웨어 레벨의 오용을 명시한다. [7]에서는 [6]의 9계층 중에서 NP5, NP6, NP7 클래스의 계층을 더욱 세분화하여 정의하였다. [7]에서 세분화한 3개의 계층은 소프트웨어 레벨의 침입 중 그 빈도 수와 방법이 점점 증가하고 있는 분야로써 이 연구를 통해서 좀더 실제적인 침입의 분류가 이루어 졌다. [8]은 침입에 대한 통계적인 분석과 패턴 합성을 통해서 침입의 경향을 제시하였다. [9]에서는 정보 시스템에 문제가 발생하는데 원인이 될 수 있는 94가지의 메커니즘을 소개하였다.

III. Experimental Frame 디자인



<Figure 1> Experimental Frame을 사용한 보안 시스템 평가 방법

<Figure 1>은 EF를 사용하여 보안 시스템을 평가할 경

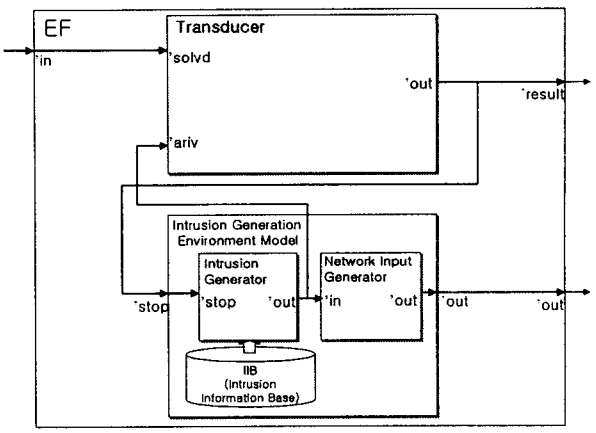
우의 모델의 전체 구조를 보여 주고 있다. 보안 시스템의 평가를 위해서 EF는 크게 침입 생성 모델과 성능 평가 모델을 하위 모델로 갖는다. 침입 생성 모델은 보안 시스템 모델에게 침입을 생성해 주기 위한 모델이고, 여기서 생성된 침입 정보는 성능 평가 모델에게도 제공된다. 성능 평가 모델은 보안 시스템 모델을 통해서 받은 "탐지된 침입정보"와 침입 생성 모델을 통해서 입력받은 "생성 침입 정보"를 비교하여 보안 시스템 모델의 성능을 평가하게 된다.

1. EF의 전체 구조

<Figure 2>은 본 연구에서 제안하는 침입 탐지 시스템 평가를 위한 EF를 보여 주고 있다.

EF는 <Figure 1>의 침입 생성 모델에 해당하는 IGEM(Intrusion Generation Environment Model)과 성능 평가 모델에 해당하는 Transducer로 구성된다. 그리고, IGEM은 IGM(Intrusion Generator Model), NIGM(Network Input Generator Model)과 IIB(Intrusion Information Base)로 구성된다.

IGM은 침입을 생성하기 위한 모델이고, NIGM은 IGM



<Figure 2> Experimental Frame의 전체 구조

으로부터 받은 침입 정보 기반으로 네트워크의 입력을 발생시키기 위한 모델이다. NIGM은 정상적인 데이터 통신에 해당하는 네트워크 입력을 발생시킨다. 정상적인 네트워크 입력의 경우, 침입 탐지 시스템 모델의 false positive alarm의 원인이 된다.

IIB는 침입 생성을 위한 정보를 저장해 놓은 저장 공간

<Table 1> IIB(Intrusion Information Base)의 스키마

Field Name	Data Type	설 명
Intrusion Type	Integer	침입의 타입
Intrusion Name	String	침입의 이름
Is_Spoofed	Boolean	Source Address가 스푸핑이 되었는가?
Is_Slow	Boolean	Stealthy 공격인가?
Is_Source Distributed	Boolean	공격자가 분산되어 있느가?
Is_Target Distributed	Boolean	공격 대상이 분산되어 있는가?
Attack Count	Integer	공격을 구성하는 네트워크 입력의 개수
Interarrival Time	Time Type	공격을 구성하는 네트워크 입력의 도착 간격
Slow Interarrival Time	Time Type	Stealthy 공격일 때의 네트워크 입력의 도착 간격
Destination Type	Integer	공격 대상 호스트의 타입
Protocol	Integer	공격이 사용하는 프로토콜
Port	Integer	공격이 사용하는 포트

으로써, 침입 생성을 위한 필수적인 정보를 저장한다. IGM을 통해서 발생된 침입은 Transducer의 입력으로 제공되고, 평가 대상이 되는 모델의 출력은 다시 Transducer의 입력으로 제공된다.

2. IGEM(Intrusion Generation Environment Model)의 디자인

IGEM은 침입 탐지 시스템의 평가를 위해 입력을 제공하는 모델이다. IGEM은 IGM, NIGM과 IIB로 구성된다. IGEM은 IIB를 기반으로 침입을 생성해 준다. IIB는 침입 생성을 위한 기본 정보를 저장해 놓고 있다. IIB는 침입 정보를 추상화하여 저장하고 있으며, IGM은 IIB의 하나의 레코드를 선택하여 해당 레코드의 정보에 기초하여 침입을 생성하게 된다. IIB는 침입 정보를 저장하기 위해<Table 1>과 같은 스키마를 갖는다. IIB의 스키마의 Intrusion Type 필드는 침입의 종류를 분류하기 위한 속성이다. Intrusion Type은 생성되는 침입의 성격에 따라 다음 4가지의 속성을 갖는다.

Intrusion Type 1. One Network 입력 침입 : 하나의 네트워크 입력으로 시스템의 오동작이나 자원의 고갈을 일으킬 수 있는 공격을 말한다. 예를 들면, Land Attack의 경우, 같은 송신 IP 주소와 수신 IP 주소, 같은 송신 포트와 수신 포트를 갖는 네트워크 입력을 전송하여 해당 네트워크를 마비 시키는 공격이다. 이외에도, "Ping of Death", "X-max Tree", Winnuke", "Address Probe", "Port Probe", "Mail Bomb"등이 있다. 침입 탐지의 관점에서 볼 때 이러한 공격은 하나의 네트워크 입력을 점검함으로써 탐지 할 수 있다.

Intrusion Type 2. Scanning and Exploiting 침입 : 목적지 호스트나 네트워크의 정보를 얻어내기 위한 공격이다. 그리고, 네트워크 입력의 도착 간격이 길어 질 수 있는 가능성을 갖는 공격이다. 이러한 타입의 공격에는 "Address Scanning", "Port Scanning", "Mscan", "Cgi-query Exploiting"등이 있다. 침입 탐지 시스템의 입장에서 이러한 공격을 탐지하기 위해서는 침입 탐지를 위한 버퍼를 유지시키는 시간이 다른 공격보다 길어야 한다.

Intrusion Type 3. DoS(Denial of Service) 침입 : DoS 공격은 네트워크, 시스템 또는 응용 프로그램의 자원들을 마비시키는 공격이다. 특히, 본 연구에서 Intrusion Type 3은 다수개의 네트워크 입력으로 공격이 구성된 DoS를 말한다. 여기에는 "SYN Flood", "Ping Flood", " 다중 ICMP echo 요청", "Web page의 잦은 요청"등이 있다.

Intrusion Type 4. Unix 명령어 기반 침입 : Unix 명령어 기반 침입은 수많은 경우의 수를 갖는다. 그러나, 대부분의 Unix기반 침입은 특정 사용자의 권한을 얻어내는 것이다. 권한을 얻어내는 방법에는 특정 권한으로 쉘을 만드는 방법과 특정 사용자의 패스워드를 얻어 내는 방법이 있다. 특정 권한의 쉘을 얻기 위한 방법에는 버퍼 오버플로우 공격이나, SETUID 프로그램을 이용하는 방법 이 있다. 슈퍼유저의 비밀 번호를 얻는 방법에는 "Password Cracking"과 "Password Guessing" 방법이 있다. 이러한 침입들은 매우 많은 경우의 수를 갖기 때문에 추상화가 요구된다. "Password Guessing"의 경우 공격 패턴의 단순성 때문에, 모델링이 용이하다. 그러나, "Password Cracking"과 슈퍼유저의 쉘을 얻어내는 공격은 그 패턴을 찾아내는 것이 어렵기 때문에, 모델링이 쉽지 않다. 본 연구에서는 이러한 침입을 생성하기 위해 유닉스 명령어의 pool을 만들고, Unix 명령어 기반 침입의 한 침입을 생성할 때 해당 침입을 구성하는 특정 명령어들의 집합을 특정 순서에 따라 생성하도록 하였다. 또한, 침입을 구성하는 명령어와 명령어의 사이에는 침입에 해당하지 않은 입력이 존재할 수 있다.

본 연구에서의 4개의 Type의 침입 분류는 침입을 모델링하여 이를 침입 탐지 시스템 모델의 평가를 위해 재생성 하기 위한 것이다. 특히, Intrusion Type 2, 3, 4의 경우는 공격자와 공격대상이 분산될 수 있다. 또한, Intrusion Type 2, 4번의 경우 스텔시 공격이 가능하다. Intrusion Type 1, 2, 3, 4에서 스푸핑 공격이 가능하다. <Table 1>의 스키마의 각 필드는 스푸핑 공격, 분산 공격, 스텔시 공격들이 갖는 속성들을 표현할 수 있도록 구성되었다.

3. Transducer의 디자인

Transducer는 침입 탐지 시스템의 평가를 위한 목적에 맞도록 디자인된다. <Figure 2>에서와 같이 Transducer 모델은 IGEM내부의 IGM으로부터 발생한 침입을 'ariv

포트를 통해서, EF의 외부로부터의 입력을 'solvd 포트를 통해서 받아들인다. 'ariv 포트를 통해서 들어온 입력은 Transducer의 GenIntrusion_List에 삽입되고, 'solvd 포트를 통해서 들어온 입력은 Transducer의 DetIntrusion_List에 삽입된다. Transducer는 Observation Interval이라는 내부 스케줄링 시간을 가지고, 시뮬레이션 모델의 관측 시간을 결정한다. Observation Interval이 끝나는 시점에 Transducer는 GenIntrusion_List와 DetIntrusion_List를 사용해서 평가 대상이 되었던 침입 탐지 시스템 모델의 성능을 평가한다. 평가 방법은 Transducer내의 두 리스트를 비교 조사하는 것이다. 침입이 발생한 시간을 기준으로 일정 시간 안에 탐지된 침입이 있는지를 검색한다. 만일, 발생시킨 침입이 DetIntrusion_List에 존재하지 않는 경우 이를 False Negative로 인식한다. 또한, 발생되지 않은 침입을 탐지한 경우 이를 False Positive로 인식한다.

IV. 결론 및 향후과제

본 연구에서는 복잡 다변화되고 있는 침입을 탐지하기 위한 침입 탐지 시스템의 평가를 위한 침입 탐지 시스템 모델의 Experimental Frame의 디자인을 제시하였다. 본 연구의 EF는 IGEM과 Transducer로 구성된다. IGEM은 침입 탐지 시스템에 침입을 생성해 주며, Transducer는 생성된 침입에 대한 시스템의 탐지 능력을 점검하기 위한 모델이다. IGEM은 침입은 재현하기 위해 IIB를 가지고 있으며, IIB는 침입에 대한 핵심 적인 정보를 가지고, 침입을 생성하도록 도와준다. IIB의 침입 정보는 각 침입이 갖는 성격에 따라 4개의 Type으로 구분하였다. IIB 기반 침입 생성은 차후 새로운 침입이 추가 될 때 이를 쉽게 반영할 수 있도록 하는 기반을 제공하며, 스탤시 공격, 분산 공격과 스푸핑공격을 생성 할 수 있도록 디자인되었다. IGEM을 IGM과 NIGM으로 구분하여 생성할 침입을 선택하는 모델과 선택된 침입을 사용 네트워크 입력을 제공하는 모델을 구분하였다. 본 연구를 통해 디자인 및 구현된 EF는 이미 분산 침입 탐지 모델의 평가에 적용되었다[10].

향후, 본 연구에서 디자인된 침입 탐지 시스템 평가를 위한 EF모델은 각종 보안 시스템 모델의 평가를 위한 일반성을 갖는 모델로 디자인 및 구현 될 것이다.

V. 참고 문헌

[1] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, Network Intrusion Detection, IEEE Network, Vol. 8, No. 3, pp26-41, May/June 1994.

[2] B. P. Zeigler, Object-Oriented Simulation with Hierarchical, Modular Models. San Diego, CA, USA: Academic Press, 1990.

[3] E. Amoroso, "Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response," Intrusion.Net Books, 1999.

[4] R. Bace, Intrusion Detection, Macmillan Technical Publishing, 2000.

[5] S. Northcutt, Network Intrusion Detection An Analysts Handbook, New Riders Publishing, 1999.

[6] P. Neumann and D. Parker, A Summary of computer misuse techniques, In Proceedings of the 12th National Computer Security Conference, October 1989, pp. 396-407.

[7] U. Lundqvist and E. Jonsson, How to Systematically Classify Intrusions, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, 1997.

[8] J. Howard, An Analysis of Security Incidents on the Internet 1989-1995, Ph.D. thesis, Carnegie-Mellon University, Pittsburgh, Pa ,1997.

[9] F. Cohen, C Phillips et al., A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model, Sandia National Laboratories, September, 1998.

[10] Hyungjong Kim, Taeho Cho "Hierarchical Modeling and Simulation of Intrusion Detection System," JSST International Conference, October, 2000.