컴퓨터 면역 시스템을 기반으로 한 지능형 침입탐지시스템

이 종 성† · 채 수 환††

요 약

컴퓨터망의 확대 및 컴퓨터 이용의 급격한 증가에 따른 부작용으로 컴퓨터 보안 문제가 중요하게 대두되고 있다. 이에 따라 침입자들로부터 침입을 줄이기 위한 침입탐지시스템에 관한 연구가 활발하다. 본 논문은 비정상적인 행위를 탐지하는 침입탐지시스템에 관해 고찰하고, 컴퓨터 면역시스템을 바탕으로 한 지능형 IDS 모델을 제안한다. 제안한 모델에서 지능형 IDS들은 여러 컴퓨터에 분산되고, 분산된 IDS들 중 어느 하나가 특권 프로세스(privilege process)에 의해 발생된 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지한 경우 이를 다른 IDS들과 서로 동적으로 공유하여 새로운 침입에 대한 면역력을 향상시킨다.

Intelligent Intrusion Detection System based on Computer Immune System

Jong-Sung Lee† · Soo-Hoan Chae††

ABSTRACT

Computer security is considered important due to the side effect generated from the expansion of computer network and rapid increase of the use of computers. Intrusion Detection System(IDS) has been an active research area to reduce the risk from intruders. This paper discusses IDS of detecting anomaly behaviors and proposes a new intelligent IDS model, which consists of several computers with intelligent IDS, based on computer immune system. The intelligent IDSs are distributed and if any of distributed IDSs detect anomaly system call among system call sequences generated by a privilege process, the anomaly system call can be dynamically shared with other IDSs. This makes the intelligent IDSs improve the ability of immunity for new intruders.

1. 서 론

컴퓨터 및 네트워크 기술의 발전에 따른 컴퓨터간의 상호 연결성의 증가로 인해 컴퓨터 보안 문제가 중요하게 대두되고 이로 인해 침입 탐지 시스템(Intrusion Detection System : IDS)에 관한 연구가 활발히 진행되고 있다[1, 2, 3].

침입 탐지 시스템은 불법적인 침입으로부터 컴퓨터를 보호하기 위해 침입을 탐지하고 이에 대한 적절한 조치를 취하는 역할을 수행한다. 침입 탐지 시스템은 크게 데이터의 소스(source)를 기반으로 하는 분류 방법과 침입의 모델을 기반으로 하는 분류 방법으로 나눌 수 있으며, 데이터 소스를 기반으로 하는 분류 방법은 호스트로부터 생성되고 모아진 감사(audit) 데이터를 침입 탐지에 사용하는 호스트 기반(host based)

※ 본 연구는 재단법인 한국항공대학교 창천문화재단 '99 학술연구비에 의해 수행되었음.
† 준 회 원 : 한국항공대학교 대학원 컴퓨터공학과
†† 정 회 원 : 한국항공대학교 컴퓨터공학과 교수
논문접수 : 1999년 5월 31일, 심사완료 : 1999년 11월 19일

과, 네트워크의 패킷 데이터를 모아 침입을 탐지하는데 사용하는 네트워크 기반(network based)으로 구분할 수 있다. 또한 침입 모델을 기반으로 하는 침입탐지시스템의 일반적인 분류 방법은 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있는 동안 이 프로파일에서 벗어나는 행위들을 탐지하는 비정상적인 행위 탐지(anomaly detection) 방법과, 시스템의 알려진 취약점들을 이용한 공격 행위들에 대한 공격 특징 정보를 통해 침입을 탐지하는 오용 침입탐지(misuse detection) 방법으로 분류할 수 있다[4].

일반적인 침입탐지시스템의 중요 요구사항은 시스템 관리자 없이도 지속적으로 수행되어야 하며, 컴퓨터 시스템에 최소한의 오버헤드를 부과해야 하고, 새로운 침입 유형의 변화에 대한 자체 학습 기능과, 어떤 침입탐지모듈에 결함이 발생되어도 전체 침입탐지시스템에 큰 영향을 주지 않는 결함 허용 관리 기능, 그리고 시스템의 정상상태를 침입이라고 탐지하는 긍정적 결함(false positive) 및 시스템의 침입상태를 정상상태로 판단하는 부정적 결함(false negative)과 같은 잘못된 침입 탐지를 방지해야 한다[3, 5, 6].

이와 같은 침입 탐지 서비스의 요구에 따라 최근에 비정상적인 행위 탐지(anomaly detection) 방법을 중심으로 다양한 기법과 모델들이 개발되어 왔으나 컴퓨터 통신망의 복잡성, 대상 시스템의 원초적 취약성, 정보 보호에 대한 이해 부족 및 새로운 불법 침입 기법의 개발 등으로 기존의 어떤 기법 또는 모델도 완전하지 못한 실정이다.

본 논문은 비정상적인 행위를 탐지하는 침입탐지시스템에 관해 고찰하고, 특권 프로세스(privilege process)가 수행할 때 발생하는 시스템 호출 순서 중 비정상적인 시스템 호출을 탐지하여 이를 분산된 각각의 침입탐지 시스템들이 서로 동적으로 공유하여 침입자로부터 시스템의 침입에 대한 면역력을 향상시키는 새로운 개념의 지능형 침입탐지시스템을 제안한다.

2. 비정상적인 행위 탐지 방법에 대한 관련 연구

비정상적인 행위 탐지 방법은 시스템 또는 사용자의 행위가 정상 행위로부터 벗어나는 것을 탐지하는 것으로 이를 위해 시스템 또는 사용자의 정상 행위를 기록한 감사 데이터로부터 여러 가지 방법을 통해 정상 행위를 추출한 후, 수행되는 시스템의 행위가 정상 행위에 벗어나면 경고를 발생한다. 즉, 비정상적인 행위 탐지 방법은 전에 학습되지 않은 행위가 시스템에서 발생하면 침입으로 간주한다. 비정상적인 행위 탐지 방법은 예측하지 못한 시스템 취약점을 이용하려는 시도를 탐지할 수 있어 새로운 침입을 자동으로 탐지할 수 있으며, 어떤 보안 취약점을 직접적으로 이용하지는 않지만 특권을 오용하는 공격도 탐지할 수 있다. 그러나, 구성된 정상 행위 정보가 시스템의 모든 정상 행위를 포함하지 않기 때문에 긍정적 결함(false positive) 오류가 발생할 확률이 높으므로 이를 낮추는 방안이 모색되고 있다.

이하 대표적인 비정상적인 행위 탐지 방법을 간단하게 살펴보고 이를 통해 컴퓨터 면역 시스템을 기반으로 한 지능형 침입탐지 시스템의 제안 배경을 설명한다.

통계적 접근 방법은 침입탐지시스템에 가장 많이 사용되는 방법으로, 탐지과정은 먼저 사용자나 사용자가 실행시킨 프로세스의 행위를 관찰하고, 각각의 행위에 대한 프로파일을 생성한 후, 사용자 및 시스템의 행위가 기설정된 정상 행위로부터 벗어나는지 감시한다. 이 접근 방법은 어떤 행위의 발생 순서를 고려하지 않고 단지 발생 빈도 수만으로 정상 행위를 모델링하므로 동적으로 수행되는 시스템을 모델링하는데 제한적이라는 단점을 갖고 있으나, 현재 많은 침입탐지 시스템들과 프로토타입에 사용되고 있다[7, 8].

전문가 시스템은 if-then-action의 규칙 표현 방식에 따라 전문가의 지식을 표현하는 인공지능 기법으로 사용자의 정상 행위를 표현하는데 규칙 표현을 사용하였으며 대표적인 침입탐지시스템은 Wisdom&Sense[9]와 AT&T의 ComputerWatch[10]가 있다. 이 방법은 새로운 사용 패턴을 추가하기 위해 규칙 집합을 생성하는 전문가가 필요하여 정확한 정상 행위를 지속적으로 구축하기가 어렵다는 문제점이 있다.

신경망을 이용한 접근은 두 개 정보 집합간의 관계성을 학습하기 위해 사용하는 알고리즘적 기술로서, 이 방법은 명령어의 순서를 신경망으로 학습시켜서 다음에 수행될 명령어를 미리 예측할 수 있게 한다. 이 방법은 많은 연산량을 요구하는 기술이므로 침입탐지 시스템에 폭넓게 사용되고 있지 않다.

사용자 중심 접근 방법은 SECURENET 프로젝트[11]을 수행하는 동안 개발된 방법으로 시스템에서 사용자들이 수행할 태스크들의 집합에 의해 사용자들의 정상 행위를 모델링한 후, 각각의 사용자가 수행할 수

〈표 1〉 비정상행위 탐지를 위한 침입탐지 시스템 비교

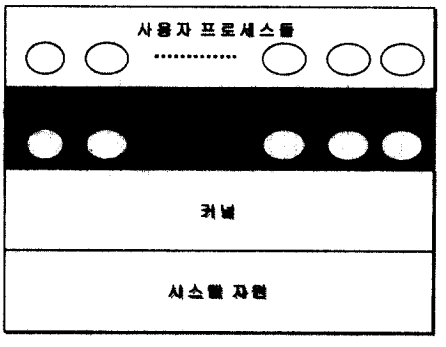
침입 탐지 시스템 종류	데이터 소스		탐지 방법					학습능력		오용탐지 지원
	호스트 기반	네트워크 기반	통계적	전문가 시스템	신경망	사용자 중심	컴퓨터 면역시스템	초기 학습	자치적 학습	
ComputerWatch	●			●				●		
Haystack	●		●					●		●
IDES	●		●					●		●
NIDES	●		●					●		●
NSM(NID)		●	●					●		●
MIDAS	●		●	●				●		
W&S	●		●	●				●		
NADIR	●			●				●		●
SECURENET	●		●		●	●		●		
New Maxico 연구	●						●	●		

있는 태스크 집합을 관리하고, 발생된 어떤 행위가 태스크 패턴과 일치하지 않으면 경보를 발생한다. 이 방법의 단점은 새로운 사용자가 추가되면 이 사용자가 수행할 수 있는 정상 행위를 다시 모델링해야 하므로 침입탐지 시스템의 확장성에 원초적인 문제를 안고 있다.

컴퓨터 면역시스템은 자연 면역시스템(natural immune system)을 모델링한 것으로서 1994년도에 S.Forrest 교수에 의해 면역 시스템과 컴퓨터 보안의 결합에 대해 소개된 후 지속적으로 연구되고 있으나, 실질적으로 어떻게 자연 면역시스템 아이디어를 컴퓨터 보안에 적용시킬 것인가에 대한 연구는 부족한 상태이다[11, 12, 13].

이상에서 살펴본 현재까지 알려져 있는 대표적인 비정상 행위 탐지 방법을 사용하는 침입탐지 시스템들을 데이터 소스와 전술한 침입탐지 방법에 따라 분류하고, 자치적 학습능력 존재 유무에 따라 다시 분류하면 <표 1>과 같다[4, 8, 15, 16].

그러나, 이와 같은 시스템들은 초기 학습 기능만 존재하는 정적인 시스템이고 각 시스템들마다 시스템에 대한 동일한 정상행위 지식을 가지고 있으므로 어떤 하나의 시스템이 침입 받으면 동일한 방법으로 다른 시스템이 침입을 받을 확률이 증가하므로 전체 침입탐지 시스템의 결함 허용 수준이 낮아진다. 따라서, 침입탐지시스템의 중요 요구사항인 새로운 침입 유형의 변화에 대한 자체 학습 기능과 결함 허용 관리에 적합하지 못하다.



(그림 1) 탐지 대상 시스템의 특징

3. 제안한 컴퓨터 면역시스템을 기반으로 한 지능형 침입탐지시스템

3.1 탐지 대상

본 논문에서 탐지 대상 객체는 특권 프로그램을 수행하는 특권 프로세스[1]와 시스템 서버[2]로 한다. 그 이유를 일반적인 운영체제 구성 특징에 의해 살펴보면 다음과 같다.

일반적인 운영체제는 (그림 1)에 도시된 바와 같이, OS 커널이 모든 시스템 자원(메모리, 디스크, 파일, CPU)을 관리하고, 모든 시스템 자원은 단지 시스템 호출을 통해 접근될 수 있다. 일반적으로 커널은 시스템 자원을 보호하기 위해 접근제어를 통한 보호 메커니즘을 제공한다. 따라서, 커널은 사용자 프로세스의 행위를 제한하여 사용자 프로세스에 의한 보안 위반을 방지할 수 있다. 그러나, 특권 프로세스들과 시스템 서버

1) setuid 프로그램(예를 들어, ping, ufsrestore, rdist 등)을 수행시키는 프로세스와 같이 시스템 관리자 권한으로 수행하는 프로세스를 칭하며, 이후 본 논문에서는 프로세스와 혼용하여 사용한다. solaris 2.6(SunOS 5.6)에 75개의 setuid 프로그램 존재.

2) ftpd 프로그램 등을 수행시키는 프로세스를 칭하며 이 또한 시스템 관리자 권한으로 수행하는 프로세스이므로 특권 프로세스와 동일한 것으로 간주한다.

들은 고유의 작업을 수행하기 위해 커널의 보호 메커니즘을 우회하여 시스템자원을 접근할 수 있다. 예를 들어, 사용자가 패스워드를 변경하기 위해서는 시스템 자원인 /etc/passwd 파일 변경을 요구하는데 이때 사용자에게 루트 권한이 부여되어야 한다. 특권 프로세스들과 시스템 서버들은 커널의 일부분으로 구성할 수 있으나, 일반적으로 커널이 비대해지는 것을 방지하기 위해 (그림 1)과 같이 커널밖에 구성한다.

이에 따라 사용자 프로세스의 경우 OS 커널의 보호 메커니즘에 의해 자원접근에 제한을 받으나 특권 프로세스와 시스템 서버의 경우 관리자 권한을 획득하므로 인해 OS 커널에 의한 접근 제어에 제한을 받지 않고 시스템자원을 사용할 수 있으므로 악의적으로 시스템 자원을 사용할 수 있다. 따라서, 이와 같은 이유로 본 논문에서 특권 프로세스를 탐지대상으로 사용한다.

3.2 탐지대상 모델 및 패턴DB 정의

[정의 1] 시스템 감사 궤적(System Audit Tail : SAT)

시스템 S가 수행하는 동안 감사 서브시스템에 정의된 이벤트의 발생 순서를 의미한다.

$$SAT = Ae_1, Ae_2, Ae_3, \cdots, Ae_n, Ae_{n+1}, \cdots$$

각각의 이벤트들은 발생된 시간 정보를 가지며

$$T(Ae_1), T(Ae_2), T(Ae_3), \cdots, T(Ae_n), T(Ae_{n+1}), \cdots$$

으로 나타내고,

감사 이벤트들 간의 시간 순서는

$$T(Ae_n) < T(Ae_{n+1}) \text{ 단 } n \geq 1$$

로 표현한다.

[정의 2] 프로세스 행위 궤적(Process Behavior Trace : PBT)

프로세스 i에 대한 프로세스 행위 궤적은

$$PBT_i = SC_{i1}, SC_{i2}, SC_{i3}, \cdots, SC_{in}, SC_{in+1}, \cdots, \text{ 단 } 1 \leq i \leq M^{3)}$$

으로 나타내며, 프로세스가 수행하는 동안 발생하는 시스템 호출 순서(system call sequence)를 의미한다.

각각의 시스템 호출은 호출된 시간 정보를 가지며

$$T(SC_{i1}), T(SC_{i2}), T(SC_{i3}), \cdots, T(SC_{in}), T(SC_{in+1}), \cdots$$

으로 나타내고,

시스템 행위들 간의 시간 순서는

$$T(SC_{in}) < T(SC_{in+1})$$

로 표현한다.

[정의 3] 시스템 감사 행위 궤적과 프로세스 행위 궤적과의 관계

시스템 S에서 수행되는 모든 프로세스에 의해 생성되는 프로세스 행위 궤적(PBT)은 시스템 감사 행위(SAT)의 부분집합이다.

$$SAT \supset PBT_i \text{ 단 } 1 \leq i \leq M$$

[정의 4] 실존 정상 행위 패턴DB(Live Normal behavior Pattern : NP)

일정시간 정상적으로 수행되는 프로세스에 의해 생성되는 프로세스 행위 궤적(PBT)을 일정한 크기 단위로 나누어 구성한 궤적들의 집합을 의미한다.

프로세스 P에 대한 정상 행위 패턴은

$$P_{NP} = \{P_{NP1}, P_{NP2}, P_{NP3}, P_{NP4}, \cdots, P_{NPn}\},$$

이때 n은 프로세스 P에 대한 정상 행위 패턴 수를 의미한다.

[정의 5] 합성정상행위패턴DB(Composition Normal behavior Pattern : CNP)

동질형 시스템들에서 침입탐지대상 프로세스들(P_1, P_2, P_3,… P_N)이 정상적으로 수행하면서 가질 수 있는 거의 모든 프로세스 행위 궤적(PBT)들의 집합을 의미한다.

$$CNP = \{P_{1PBT}, P_{2PBT}, P_{3PBT}, \cdots, P_{NPBT}\}$$

[정의 6] 탐지자 패턴DB(Detector Pattern : DP)

비정상적으로 수행되는 프로세스에 의해 생성되는 프로세스 행위 궤적(PBT)을 일정한 크기 단위로 나누어 구성한 궤적들의 집합(ASP) 중 합성정상 행위 패턴(CNP)에 존재하지 않는 비정상 행위 패턴(AP)들 중 Hamming Distance(HD)가 일정 수(α) 이상인 패턴들의 집합을 의미한다.

즉, 프로세스 P에 대한 비정상 행위 패턴(AP)은 $P_{AP} = P_{ASP} - P_{CNP}$이고,

3) M은 시스템 S가 제공하는 최대 한도로 생성할 수 있는 프로세스 수로서 최대 프로세서 수는 커널에 존재하는 프로세서 테이블의 총 엔트리 수를 의미한다.

탐지자 패턴DB는 $P_{DP} = \{P_{AP}(x) \mid HD(x) > \alpha\}$ 이다.

[정의 7] 어떤 행위패턴 i의 Hamming Distance(HD(i))

행위패턴 DB의 모든 패턴들 중 행위패턴 i와 가장 유사도가 가까운 패턴과의 차이 값을 의미한다.

즉, $HD(i) = \min\{$행위패턴 DB의 모든 행위 패턴들과 행위패턴 i와의 차$\}$

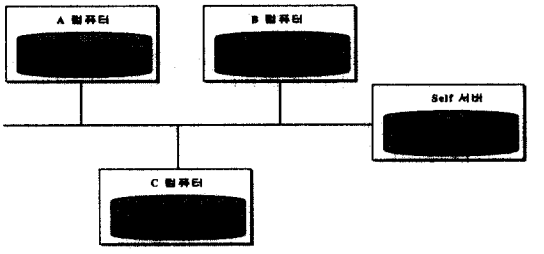
3.3 제안한 침입탐지시스템의 특징

기존의 침입탐지 시스템이 사용자의 행위 중심으로 침입을 탐지하는 것에 반해 제안한 침입탐지시스템은 전술한 바와 같이 운영체제의 특권 프로세스(privileged process)가 정상적으로 수행하면서 발생하는 시스템 호출을 일정한 크기 단위로 분리하여 구성한 정상 행위 시스템 호출 DB를 이용하여 상기 특권 프로세스가 동작하는 동안 수행 경로가 정상 행위 시스템 호출 DB에서 벗어나 수행할 경우 이를 침입으로 탐지한다. 따라서, 제안한 침입탐지시스템의 탐지범위는 탐지대상 프로세스의 비정상 행위를 이용하여 침입하는 모든 공격방법으로, 공지된 공격 방법으로는 버퍼오버플로우 공격을 탐지할 수 있다.

제안한 지능형 침입탐지시스템은 다음과 같은 본질적인 프로세스 성격에 바탕을 두고 수행된다. 즉, 프로세스는 그것이 생성하는 시스템 호출에 의해 특징지어지고, 동일한 프로세스의 다른 사용은 부분적으로 서로 다른 시스템 호출 순서를 갖으며, 동일한 환경에서 수행되는 프로세스는 시스템 호출의 공통된 부분열이 존재하고, 정상 패턴들은 프로세스의 정상 행위를 모델링하는 데 사용될 수 있으며, 침입은 프로세스의 실행 코드 상에서 비정상 경로로 수행한다[13, 17, 18, 19].

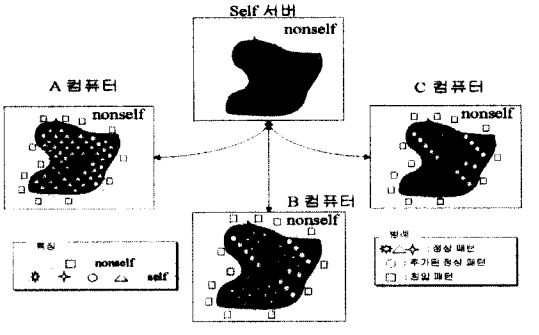
한편, 특권 프로세스의 정상 행위를 수집하는 방법은 [13]에서 소개한 정상 상태에서 일정기간동안 특권 프로세스의 행위 정보를 수집하여 구성하는 실존 정상 행위 수집 방법과 특권 프로세스의 모든 정상 행위를 얻기 위해 인위적인 경우를 만들어 특권 프로세스의 행위 정보를 수집하는 합성 정상 행위 수집 방법, 그리고 [18]에서 소개한 소프트웨어 개발자에 의해 제공되는 기능 검증 테스트(FVT)를 사용하여 특권 프로세스의 행위 정보를 수집하는 방법으로 나누어진다.

제안한 침입탐지시스템에서 각각의 컴퓨터는 실존 정상 행위 수집 방법으로 특권 프로세스의 정상 행위를 수집하여 정상 행위 시스템 호출 DB를 구성하고, self[4] 서버는 합성 정상 행위 수집 방법으로 특권 프로세스에 대한 정상 행위 시스템 호출 DB를 구성한다 ((그림 2) 참조).



(그림 2) 제안한 지능형 침입탐지 시스템 구조

제안한 침입탐지시스템은 (그림 3)에 도시된 바와 같이 각 컴퓨터의 정상 행위 시스템 호출 DB를 서로 다르게 구성하므로 A 컴퓨터가 침입되었다고 해서 동일하게 다른 컴퓨터가 침입되지 않는 면역 시스템의 다양성 성질을 제공하며, 각 컴퓨터의 침입탐지시스템이 이웃한 컴퓨터의 침입탐지시스템으로부터 침입 패턴 정보와 정상패턴 정보를 전달받으므로 전체 시스템이 수행하는 동안 침입에 대한 면역력이 증가된다.



(그림 3) 제안한 지능형 침입탐지 시스템에서 정상 행위 패턴 및 침입 패턴 공유하는 개념

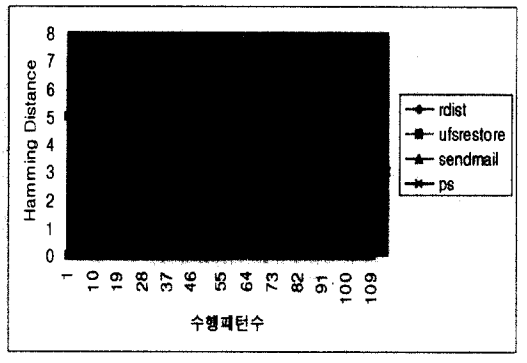
3.4 패턴DB 구성

제안한 침입탐지시스템은 특권 프로세스에 대한 정상 및 침입 시스템 호출 패턴정보를 관리하기 위해 self 서버에 존재하는 합성 정상행위DB, 그리고 각 컴

4) self와 noself는 면역시스템에서 유래된 용어로서 본 논문에서 self는 합법적인 사용자, 허가된 행동 등을 의미하고, nonself는 침입자, 컴퓨터 바이러스, 트로이목마, 스프핑 등을 의미한다.

퓨터에 존재하는 실존 정상행위DB와 침입패턴을 저장하는 탐지자DB로 구성된다

각 DB의 크기는 탐지 대상프로세스에 의존하는데 (그림 4)를 통해 시스템 호출 패턴 길이를 7로 한 경우 ufsrestore 프로세스를 이용한 공격[22], ps 프로세스를 이용한 공격[24], rdist 프로세스를 이용한 공격[25], 그리고 sendmail 프로세스를 이용한 공격[26]에 따라 발생되는 시스템 호출 패턴들과 합성 정상 행위 패턴들과의 hamming distance 차이를 이용하여 탐지자 DB를 구성하는 것을 설명한다. 이때, 테스트를 통해 구한 각 프로세스에 대한 합성 정상 행위 패턴 개수는 50, 71, 450, 512이고, 실존 정상 행위 패턴은 상기 정상행위패턴보다 적은 13, 16, 130, 125이다.



(그림 4) 공격에 사용된 특권 프로세스의 시스템 호출과 정상패턴과의 비교(패턴길이가 7인 경우)

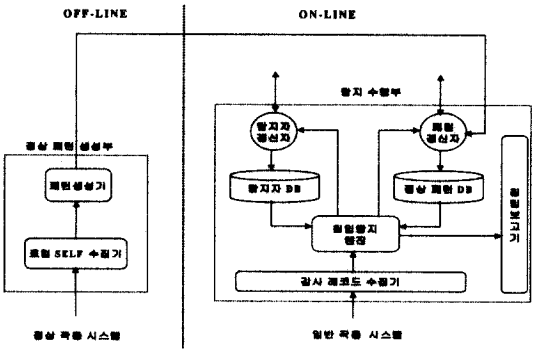
도시된 바와 같이 ufsrestore의 경우 hamming distance가 7이상인 패턴들만으로 탐지자DB를 구성할 경우 7개의 패턴으로 구성되고, rdist의 경우 hamming distance가 6이상인 패턴들만으로 탐지자DB를 구성할 경우 10개의 패턴으로 구성되며, sendmail의 경우 hamming distance가 2이상인 패턴들만으로 탐지자DB를 구성할 경우 5개의 패턴으로 구성되고, ps의 경우 hamming distance가 1이상인 패턴들만으로 탐지자DB를 구성할 경우 3개의 패턴으로 구성된다. 이때, 각 프로세스에 적용되는 hamming distance 값은 보안 강도에 의해 결정된다.

따라서, 제안한 침입탐지시스템에서는 합성 정상행위 DB, 실존 정상행위 DB와 탐지자DB의 크기 구성을 (1)과 같이하여 신속한 탐지를 통해 실시간으로 침입을 탐지할 수 있게 한다.

$$\text{탐지자 DB 크기} < \text{실존 정상행위 DB 크기} <<< \text{합성정상행위 DB 크기} \quad (1)$$

3.5 시스템 구성

제안한 시스템을 구성하는 하나의 컴퓨터의 구성 요소를 (그림 5)를 참조하여 살펴보면 다음과 같다. 각각의 컴퓨터에 설치되는 제안한 침입탐지 시스템은 크게 오프라인으로 수행되는 정상패턴생성부와 온라인으로 수행되는 탐지수행부로 대별된다.



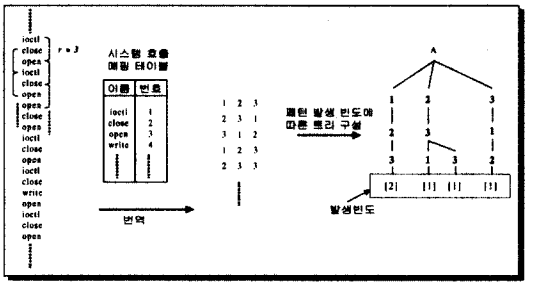
(그림 5) 각각의 컴퓨터에 대한 제안한 침입탐지 시스템

3.5.1 정상패턴생성부

정상패턴생성부는 각 컴퓨터가 정상 상태, 즉 정상 사용자가 정상적인 수행을 할 때 발생하는 프로세스의 시스템 호출 순서를 로컬 self수집기를 통해 수집한 후, 패턴생성기를 통해 구성한다. 프로세스에 대한 시스템 호출 순서는 Solaris 2.6 BSM(Basic Security Module)의 감사서브시스템(audit subsystem)을 통해 구한다[21].

한편, 패턴생성기는 입력된 프로세스의 시스템 호출 순서를 r-contiguous-bits 방식[12]에 따라 r 크기단위로 분리하여 시스템 호출 순서를 트리로 표현한다. 프로세서 A에 의해서 생성되는 시스템 호출에 대해 r을 3으로 하여 정상 트리를 구성하는 것을 (그림 6)을 참조하여 살펴보면 다음과 같다.

먼저, 프로세스 A가 수행하면서 연속해서 시스템 호출을 생성하면, 생성되는 순서에 따라 시스템 호출 매핑 테이블에 시스템 호출 이름을 등록하고 번호를 부여하여 추후 해당하는 시스템 호출 이름을 정수 값으로 번역한 후 자주 발생하는 패턴에 대해 추후 검색을 빠르게 하기 위해 패턴 발생 빈도에 따라 트리를 구성한다.

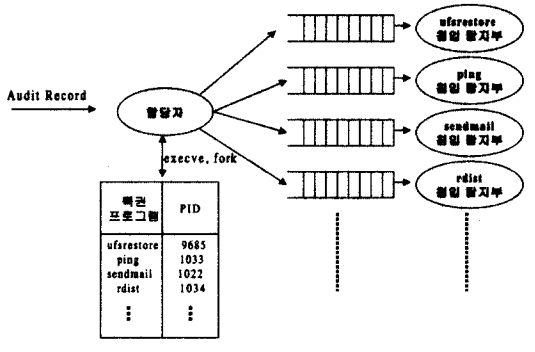


(그림 6) 프로세스 A에 대한 시스템 호출 패턴 생성 과정 예

3.5.2 탐지수행부

탐지수행부는 공지된 침입 패턴 정보를 저장한 탐지자 DB와 이를 관리하는 탐지자갱신자와, 정상패턴생성부로부터 전달된 특권 프로세스의 정상행위 패턴을 저장한 정상 패턴 DB와 이를 관리하는 패턴 갱신자와, 감사서브시스템에서 제공하는 감사 레코드를 수집하는 감사레코드수집기와, 수집된 감사레코드로부터 시스템 호출을 분리하여 해당되는 침입 탐지부를 기동시켜 침입을 탐지하는 침입탐지엔진과, 그리고 침입 발생을 알리는 침입보고기로 구성된다. 한편, 탐지자 DB와 정상 패턴 DB에 저장된 시스템 호출 패턴은 (그림 6)과 같은 트리구조로 각각 저장된다

침입탐지엔진을 보다 상세히 살펴보면, (그림 7)과 같이 감사레코드수집기를 통해 감사서브시스템에서 제공하는 감사 레코드를 입력받은 후, 할당자가 수집된 감사 레코드에 특권 프로그램을 수행시키기 위한 execve 시스템 호출이 있는지 조사하여, 존재하는 경우 프로그램 프로세스 매핑 테이블에 등록시키고 해당되는 침입탐지부를 기동시킨다. 한편, 수집된 감사레코드 중

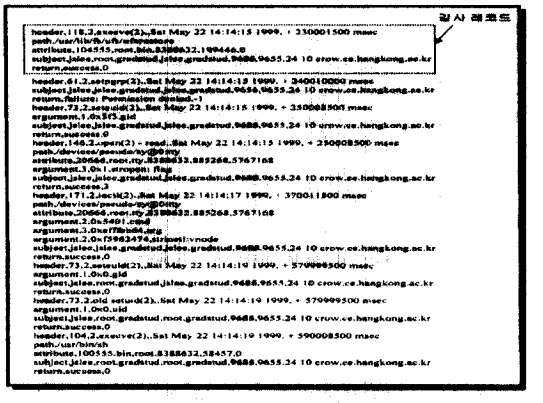


(그림 7) 침입탐지 엔진

fork 시스템 호출이 있는 경우, 부모 프로세스의 프로그램과 생성된 프로세스의 PID를 매핑시켜 해당 프로그램의 침입탐지부를 기동시킨다.

프로그램 프로세스 매핑 테이블을 사용하는 이유는 BSM에서 제공하는 감사 레코드에는 현재 수행하는 프로그램에 대한 정보가 존재하지 않고, 프로그램을 수행하는 프로세스 번호만 존재하기 때문에 프로그램과 프로세스를 매핑시키는 수단이 필요하다.

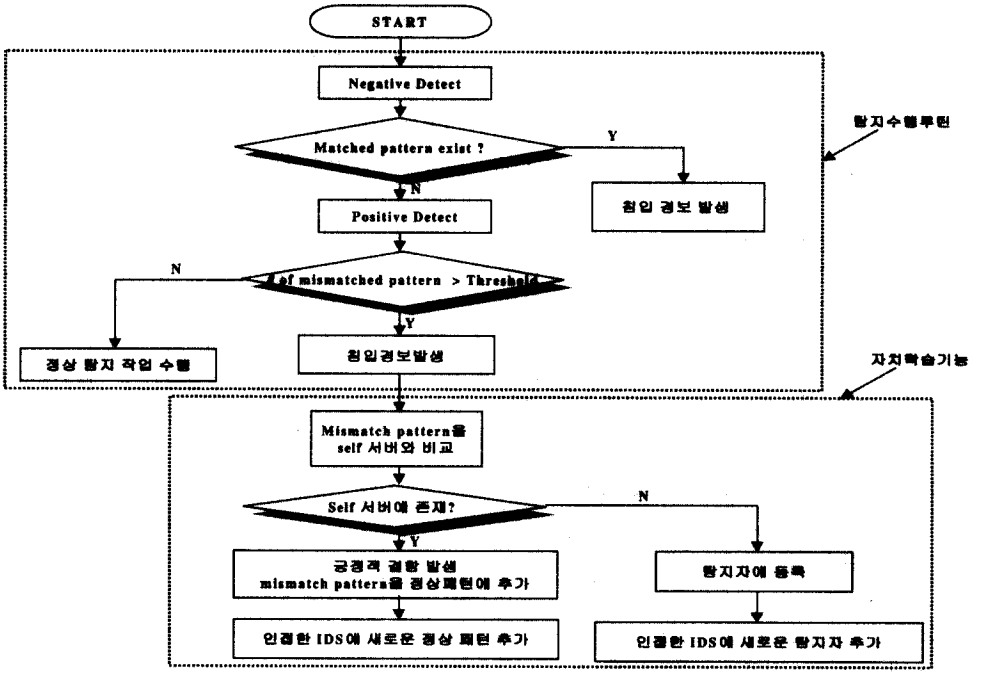
이후, 할당자는 (그림 8)과 같이 입력되는 감사 레코드 중 프로그램 프로세스 매핑 테이블에 등록된 PID ((그림 8)에서는 9685)에 해당하는 감사 레코드의 시스템 호출부분을 분리하여 침입탐지부(즉, ufsrestore 침입탐지부)에 전달하여 탐지를 수행한다.



(그림 8) ufsrestore 프로그램을 수행할 때 발생하는 감사 레코드 예

이때, ufsrestore 침입탐지부는 할당자로부터 전달되는 시스템 호출 seteuid, open, ioctl, seteuid, setuid, execve을 통해 후술할 탐지 방법에 따라 루트 쉘을 획득하는 것을 탐지한다. 한편 침입탐지부는 패턴DB와 빠른 패턴 매칭을 위해 상기 시스템 호출들을 정상패턴생성부의 시스템 호출 매핑 테이블을 참조하여 시스템 호출 번호로 변경하여 탐지를 수행한다.

전술한 각각의 침입탐지부는 (그림 9)의 탐지자루틴에 도시된 바와 같이 탐지자DB를 이용한 반대측 탐지(negative detect)와 정상패턴DB를 이용한 긍정적 탐지(positive detect)를 수행하며, 임계치에 의해 경보를 발생하는 경우 탐지자갱신자와 패턴갱신자를 통해 self 서버와 통신하여 탐지자DB와 정상패턴DB를 갱신시켜 침입으로부터 침입탐지 시스템의 면역력을 증가시킨다.



(그림 9) 제안한 지능형 침입탐지 시스템의 동작 알고리즘

이를 상세히 살펴보면, 외부로부터 전달된 침입 패턴 정보 즉 탐지자를 이용하여 반대측 선택 방식(negative selection)에 따라 현재 프로세스가 발생하는 시스템 호출들을 감시하여 탐지자DB에 존재하는 시스템호출 순서(즉, 탐지자)와 일치하는 시스템호출이 존재하면 이를 침입으로 간주하여 침입보고기를 통해 시스템관리자에게 알린다.

침입탐지엔진은 반대측 탐지를 통해 프로세스가 발생하는 시스템 호출을 감시한 후, 상기 프로세스에 의해 발생된 시스템 호출과 정상패턴DB의 내용과 비교하여 상기 프로세스에 의해 발생된 시스템 호출 중 정상패턴DB에 존재하지 않는 패턴이 임계치보다 많이 존재하면 이를 침입으로 간주하여 침입보고기를 통해 시스템관리자에게 알린다. 임계치는 보안정책에 따라 조절할 수 있어, 임계치를 낮추면 보안강도가 높아지는 반면 긍정적 결함 발생 확률이 증가하며, 임계치를 높이면 부정적 결함 발생확률이 증가한다.

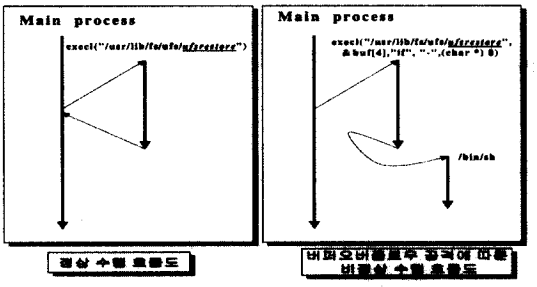
한편, 침입탐지엔진은 침입 경보가 발생하면 탐지자 갱신자와 패턴갱신자를 통해 self 서버와 통신하면서 (그림 9)의 자치학습기능을 수행한다. 이를 상세히 살펴보면, 침입탐지엔진은 존재하지 않는 패턴(들)들을 self 서버에 전송하여 합성정상행위 DB에 일치하는 패턴(들)의 존재 유무를 판단하여 패턴(들)이 존재하는 경우(즉, hamming distance가 0인 경우) 현재 프로세스에 대한 침입 탐지는 긍정적 결함이므로 상기 패턴(들)을 모든 컴퓨터의 정상패턴 DB에 추가하여, 추후에 이와 동일한 패턴에 의해 긍정적 결함이 발생하는 것을 방지한다. 만일 합성정상행위 DB에 일치하는 패턴(들)이 존재하지 않는 경우, hamming distance가 일정치 이상인 패턴(들)을 모든 컴퓨터의 탐지자 DB에 추가하여 추후 이와 같은 시스템 호출 패턴을 발생하는 프로세스의 수행을 반대측 탐지 단계에서 빠르게 탐지할 수 있게 한다.

4. 실 험

본 장에서는 여러 시스템 공격 방법 중 최근에 가장 많이 사용되고 있는 버퍼오버플로우 공격을 수행할 때 제안한 침입탐지시스템의 탐지 과정을 설명한다.

버퍼오버플로우 공격 방법은 프로세스의 메모리 구조를 이용해서 지정된 메모리의 양보다 더 많은 양의 데이터(공격자의 기계코드 포함)를 프로그램 메모리

영역에 적으므로 (그림 10)에 도시된 바와 같이 정상 흐름을 비정상 흐름으로 바꾸어 공격자의 기계코드(예를 들어, 쉘 프로그램)를 수행하게 한다. 이때, 공격 대상 프로그램이 setuid 프로그램이므로 루트 권한으로 기계코드를 수행한다(예를 들어, 루트 쉘 생성).



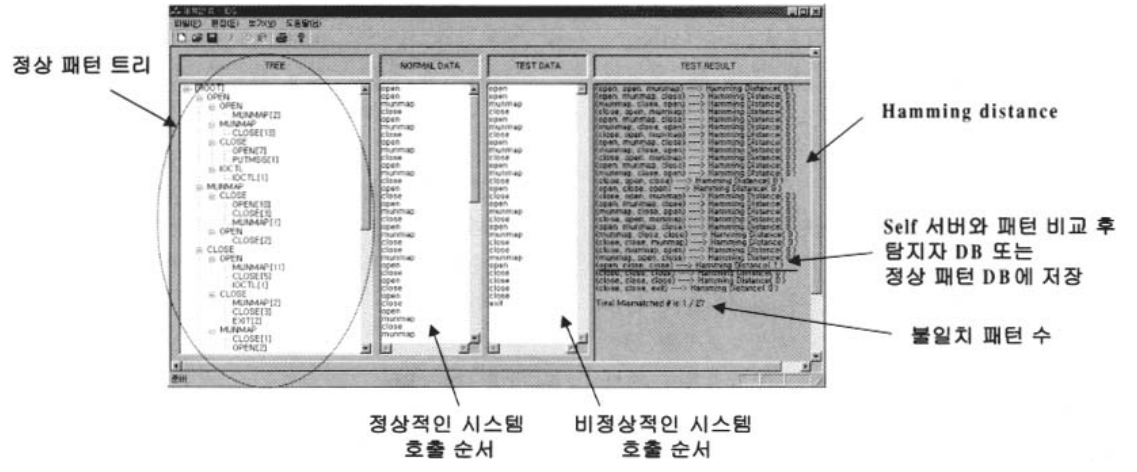
(그림 10) 프로세스의 정상 수행과정과 버퍼오버플로우 공격을 통해 루트 권한을 획득하는 과정

실험에서 공격에 사용한 특권 프로그램은 ufsrestore 프로그램[22]과 ping 프로그램[23], 그리고 rdist 프로그램[25]로 이중 ufsrestore와 ping프로그램을 통해 버퍼오버플로우공격을 받았을 때 발생하는 시스템호출 순서와 각각의 정상 패턴[5]을 비교하여 hamming distance와 패턴 불일치 개수를 카운트한 결과를 (그림 11)과 (그림 12)를 통해 살펴보며 다음과 같다. 이때, r의 값은 3으로 한다.

먼저, (그림 11)은 ping 버퍼오버플로우 공격을 시도한 경우에 발생한 결과로서 이 경우에 정상 패턴과 다른 open, close, close가 존재하며, 이 패턴이 self 서버에 존재하면, 정상 패턴 DB에 저장하고, self 서버에 존재하지 않은 경우 인접한 모든 컴퓨터의 탐지자 DB에 저장하여 추후에 ping 프로그램을 수행할 때 open, close, close 순서로 시스템 호출이 발생하면 침입 시도를 한다고 판단한다.

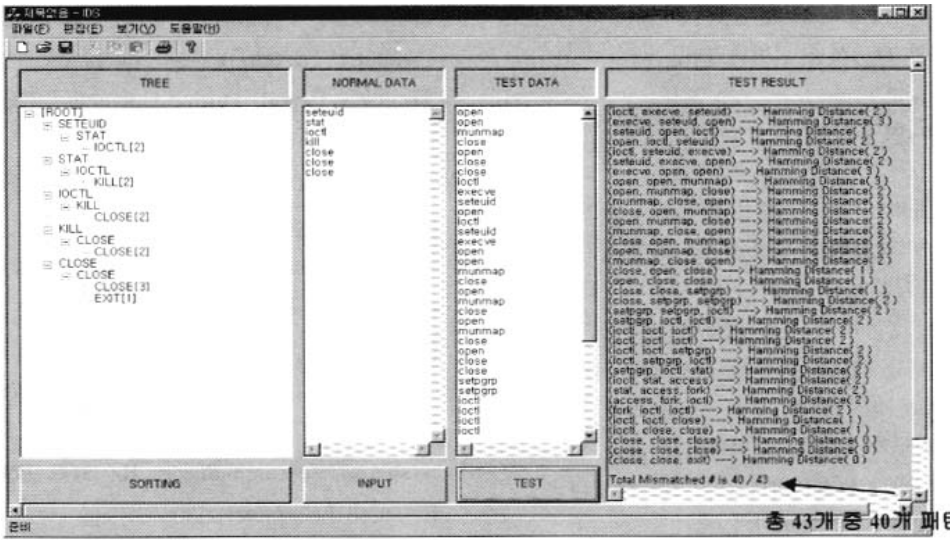
한편, (그림 12)는 ufsrestore 프로그램 공격이 성공한 경우에 발생한 결과로서 이 경우에 정상패턴DB에 저장된 패턴 수가 적음을 통해 현재 시스템에서 ufsrestore에 대한 사용을 거의 하지 않고 있음을 알 수 있다. 따라서, 현재 발생한 시스템 호출 중에 총 40 개의 패턴이 정상 패턴과 불일치하므로 경보를 발생하고, 불일치하는 패턴이 self 서버에 존재하는지 판단하여, 그 결과에 따라 모든 컴퓨터의 탐지자DB와 정상 패턴 DB를 갱신시켜, 전체 침입탐지시스템의 면역력을 향상시킨다.

끝으로, (그림 13)을 통해 SunOS 5.6 Ultra-5_10에 설치된 제안된 모델에 대한 일부분의 프로토타입에 의해 rdist 프로그램을 이용하여 버퍼오버플로우 공격[25]이 발생한 경우 이를 탐지하는 것을 살펴보면 다음과 같다.

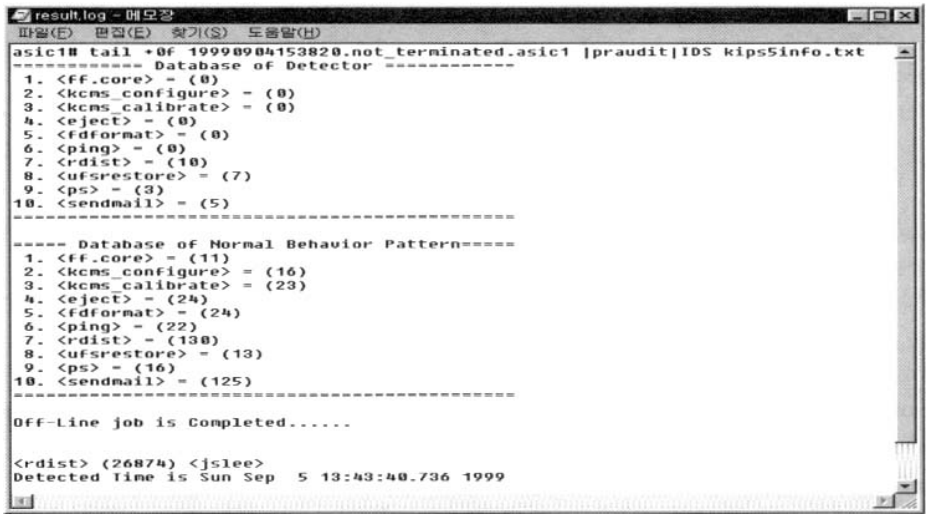


(그림 11) 제안한 침입탐지시스템에 ping 프로그램의 공격 실패를 적용한 예

5) ufsrestore의 경우에는 ufsrestore가 지원하는 옵션을 가지고 정상적인 사람이 정상적으로 백업 장치를 독취하는 동안에 발생하는 시스템 호출을 저장한다. 여기에서는 단지 ufsrestore를 실행한 경우를 정상 패턴으로 설정하였다. 한편, ping의 경우에는 일부의 옵션을 적용하여 정상 패턴을 생성한다.



(그림 12) 제안한 침입탐지시스템에 ufsrestore 프로그램 공격을 적용한 예



(그림 13) 프로토타입에서 rdist 프로그램을 이용한 공격 탐지 예

도시된 바와 같이, 제안한 모델의 프로토타입은 탐지 대상 프로그램에 대한 탐지자DB와 실존정상행위DB를 구성한 후, 탐지를 수행하던 중 rdist 프로그램을 수행시키는 프로세스의 행위가 비정상인 경우, 이를 침입이라 판정하고 침입에 사용된 프로그램 이름과 이 프로그램을 기동시킨 프로세스 번호 및 프로세스 소유자 ID, 그리고 탐지 시간에 관한 정보를 출력한다. (그림 13)을 통해 프로토타입은 10개의 탐지대상 프로그램을 감시하고, self 서버로부터 rdist, ufsrestore, ps, sendmail에 대한 새로운 침입 탐지자패턴을 전달받았음을 알 수 있다.

일반적으로 비정상 침입탐지 시스템을 실험하는데 있어 이미 알려진 침입 시나리오를 사용한다. 이때, 실험할 대상 시스템이 이미 패치된 경우 원하는 침입 결과를 얻을 수 없는 문제점이 있다. 특히, 버퍼오버플로우의 경우는 OS 버전, 프로세서 종류에 따라 시스템 침입 성공 여부가 다르므로 실험할 침입 시나리오를 찾기가 힘들다. 따라서, 본 논문에서는 전술한 바와 같

이 다섯 개의 침입 시나리오[22-26]를 이용하여 제안한 침입탐지 시스템의 타당성을 설명하였다.

5. 결론 및 향후 연구과제

본 논문에서는 컴퓨터 면역 시스템을 기반으로 한 새로운 지능형 침입탐지 시스템의 모델을 제시하였다. 제안한 모델은 분산된 각각의 침입탐지 시스템들이 서로 침입정보를 동적으로 공유하여 침입자들로부터의 침입에 대한 면역력을 향상시킨다. 이렇게 함으로써 새로운 침입을 효과적으로 방지할 수 있다. 한편, 이와 같은 접근은 최근에 연구가 활발하게 진행되고 있는 인공생명(A-life)의 접근방향과 동일하며 이는 인공생명의 새로운 적용 연구분야를 제시한 셈이다.

향후 연구과제는 특권 프로세스의 모든 정상 행위에 대한 시스템 호출 패턴들을 관리하는 self 서버의 효율적인 구축과, ftp와 같이 많은 사용자들이 사용하는 프로그램들을 대상으로 제안한 시스템을 적용하고, 제안한 침입탐지시스템의 구체적인 성능 평가에 대한 연구가 필요하다.

참 고 문 헌

[1] James Cannady, Jay Harrell, "A Comparative Analysis of Current Intrusion Detection Technologies," http://iw.gtri.gatech.edu/Papers/ids_rev.html 1998. 2.

[2] Mansour Esmaili, Rei Safavi-Naini, "Case-Based Reasoning for Intrusion Detection," Computer Security Applications Conference pp.214-222, 1996.

[3] Jai Sundar B. Spafford E, "Software Agents for Intrusion Detection," Technical Report, Purdue University, Department of Computer Science, 1997.

[4] 은유진, 박정호, "침입탐지 기술 분류 및 기술적 구성요소", 정보보호센터 정보보호 뉴스 1998. 7. 통권 13호.

[5] Crosbie M, Spafford E, "Applying Genetic Programming to Intrusion Detection," Technical Report, Purdue University, Department of Computer Science, 1996.

[6] Crosbie M, Spafford E, "Active Defense of a Computer System using Autonomous Agents," Technical Report, Purdue University, Department of Computer Science, 1995.

[7] Paul Helman and Gunar Liepins, "Statistical foundations of audit trail analysis for the detection of computer misuse," IEEE Transactions on Software Engineering, 19(9):886-901, September, 1993.

[8] Herve Debar, Marc Dacier and Andreas Wespi, "Towards a Taxonomy of Intrusion Detection Systems," Research Report, RZ 3030 IBM Zurich Research Laboratory, 1998.

[9] H. S. Vaccaro and G. E. Liepins, "Detection of anomalous computer session activity," In Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy, pp.280-289, 1989.

[10] Cheri Dowell and Paul Ramstedt, "The ComputerWatch data reduction tool," In Proceedings of the 13th National Computer Security Conference, pp.99-108, Washington, DC, October 1990.

[11]Paul Spirakis et al, "SECURENET : A network-riented intelligent intrusion prevention and detection system," Network Security Journal, 1(1), November 1994.

[12] S. Forrest, S. Hofmeyr, and A. Somayaji, "Computer immunology," Communications of the ACM, Vol.40, No.10 pp.88-96, 1997.

[13] S. A. Hofmeyr, A. Somayaji, and S. Forrest. "Lightweight Intrusion Detection for Networked Operating Systems" Journal of Computer Security, Vol.6 pp.151-180, 1998.

[14] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a Computer Immune System," New Security Paradigms Workshop, september, 1997

[15] 전문석, "침입탐지 모델분석 및 설계," 정보보호센터 최종보고서, 1996. 12.

[16] 이종성, 채수환, "분산 침입 탐지 에이전트를 기반으로 한 지능형 침입탐지시스템 설계," 한국정보처리학회 논문지 제6권 제5호, 1999. 5.

[17] Ko C, Fink G, Levitt K. "Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring," In Proceedings of the 1994 Computer Security Applications Conference, 1994.

[18] Kosoresow AP, S. Hofmeyr, "Intrusion Detection via System Call Traces," IEEE Software, Vol.14 No.5, pp.35-42, 1997. 9.

[19] H. Debar, M. Dacier M. Nassehi and A. Wespi, "Fixed vs. Variable-Length Patterns for Detecting Suspicious Process Behavior," Research Report, RZ 3012 IBM Zurich Research Laboratory, 1998.

[20] S. Forrest, A. Proceedings of the Sixth Workshop on Hot Topics in Operating Systems, Computer Society Press, Los Alamitos, CA, pp.67-72, 1997.

[21] SunSoft, Mountain View, Californina, SunSHIELD Basic Security Module Guide, 1995.

[22] Sun Security Bulletin #00169, 1998/4/28 http://www.certcc.or.kr/advisory/ka98/ka98-65.txt

[23] Sun Security Bulletin #00174 1998/11/13/ http://sunsolve.Sun.COM/pub-cgi/us/sec2text?secbull/174

[24] http://www.rootshell.com/archive-j457nxiqi3gq59dv/199707/psrace.c.html

[25] http://161.53.42.3/~crv/security/bugs/SunOS/rdist6.html

[26] http://www.rootshell.com/archive-j457nxiqi3gq59dv/199807/solaris-sendmail-8.8.4.sh.html

이 종 성

e-mail : jslee@hanul.hangkong.ac.kr

1994년 2월 한국 항공대학교 전자계산학과 졸업(이학사)

1996년 2월 한국 항공대학교 전자계산학과 대학원 졸업(이학 석사)

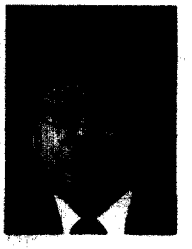
1999년 한국 항공대학교 컴퓨터공학과 대학원 박사과정수료

1996년~1998년 한국 항공대학교 컴퓨터공학과 시간강사

1998년~현재 순천대학교 정보통신공학과 시간 강사

1999년~현재 현대전자연수원 강사

관심분야 : Computer Security, Intrusion Detection System, 인공생명, 병렬/분산처리, High Performance Computing, 등임



채 수 환

e-mail : chae@mail.hangkong.ac.kr

1973년 한국 항공대학교 항공전자공학과 졸업(공학사)

1985년 미국 Univ. of Alabama 전산공학과 졸업(공학석사)

1988년 미국 Univ. of Alabama 전기공학과 졸업(공학박사)

1973년~1977년 공군교육사령부 통신학교 교관

1977년~1983년 금성통신 근무(연구원)

1996년~1997년 영국 Newcastle upon tyne 대학교 교환교수

1989년~현재 한국항공대학교 컴퓨터공학과 교수

관심분야 : 컴퓨터 구조, 병렬처리시스템, 컴퓨터 보안 등임