情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

정책기반의 새로운 공격 탐지 방법

김 형 훈*

요 약

컴퓨팅 환경이 보다 신뢰성 있고 실질적으로 사용되기 위해서는 보안이 필수적인 기능으로 요구된다. 알려진 공격의 패턴을 이용한 침입탐지는 공격자의 여러 가지 변형된 방법이나 새로운 공격 방법에 의해 쉽게 공격당할 수 있다. 또한 각각의 보안정책을 교묘히 회피하는 많은 공격 방법들이 수시로 개발되어 시도되고 있다. 따라서 침입에 성공하는 많은 공격들은 기존의 공격 패턴과 보안정책 사이의 허점을 이용하여 발생된다고 볼 수 있다.

본 논문에서 제안된 방법은 새로운 공격을 탐지하기 위해 이를 탐지하기 위한 특징값을 규칙집합을 통해 획득한다. 규칙집합은 알려진 공격, 보안정책과 관리자의 경험적 지식에 대한 분석을 통해 공격의 특징을 감지할 수 있도록 작성된다. 이러한 규칙집합에 의해 획득된 특징값들은 훈련단계에서 Naive Bayes 분류기법을 통해 공격에 대한 통계적 특징값으로 사용한다. 제안된 방법은 훈련단계에서 얻어진 공격에 대한 통계적 특징값을 이용하여 변형된 공격이나 새로운 공격을 탐지할 수 있다.

Ⅰ. 서 론

정보처리 기술의 눈부신 발전과 컴퓨터 네트워크의 급속한 확산은 우리의 생활을 더욱더 편리하게 만들고 있으며, 거의 모든 분야에 걸쳐 넓게 사용되고 있다. 그러나 이러한 컴퓨팅 환경이 보다 신뢰성 있고 실질적으로 사용되기 위해서는 보안이 필수적인 기능으로 요구된다. 침입탐지기술은 다양한 방어를 위한 보안 기법의 배후에서 마지막 보안에 대한 방어 방법이라 할 수 있다.

침입탐지방법은 오용침입탐지(misuse detection) 방법과 비정상행위침입탐지(anomaly detection)방법으로 나눌 수 있다. 오용침입탐지 방법은 기존에 알려진 공격 패턴을 모델화하여 이러한 패턴의 발생을 탐색하여 침입을 탐지하는 방법이다. 오용침입탐지 방법은 저장된 공격 패턴을 탐색하여 침입을 탐지하므로 낮은 거짓 경고율(false positive)을 가지면서 알려진 공격을 신뢰성 있게 탐지할 수 있다. 그러나 오용침입탐지 방법은 저장된 공격패턴들에 포함되어 있지 않는 새로운 공격들을 탐지할 수 없다는 문제점을 갖고 있다.

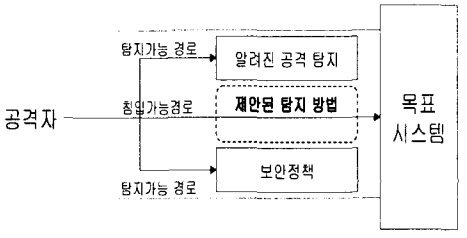
비정상행위침입탐지 방법은 새로운 공격을 탐지할 수 있는 방법으로써 과거에 학습된 정상적 행위에 대해 현재의 행위를 비교함으로써 침입을 탐지하는 방법이다. 그러나 비정상행위침입탐지 방법은 높은 거짓 경고율을 갖는 문제점과 탐지된 침입에 대해 실시간으로 적절한 대응 조치를 취하기 어려운 문제점이 있다.

침입탐지 방법의 연구에 있어서 주된 연구 대상은 알려진 공격보다는 알려지지 않은 새로운 공격을 탐지하기 위한 것이라 할 수 있다. 기존에 알려진 공격이나 보안정책에 직접적으로 위배되는 침입 행위는 다양한 침입방지 및 침입탐지 방법에 의해 해결되고 있다. 그러나 알려진 공격의 패턴을 이용한 침입탐지는 공격자의 여러 가지 변형된 방법이나 새로운 공격 방법에 의해 쉽게 공격당할 수 있다. 또한 시스템에 대한 각각의 보안정책을 교묘히 회피하는 많은 공격 방법들이 수시로 개발되고 시도되고 있다. 즉, 침입에 성공하는 공격들은 기존의 공격 패턴과 보안정책 사이의 허점을 이용하여 발생된다고 볼 수 있다.

따라서, 본 논문에서 제안한 방법에서는 "기존의 공격 패턴"과 "보안정책"에 의한 침입탐지는 해당 센서를 통해 탐지하는 것으로 간주하고 [그림 1]과 같

* 광주여자대학교 정보통신학과 (hhkim@mail.kwu.ac.kr)

이 이들 사이의 공백 부분에서 발생하는 새로운 공격들을 탐지하기 위해 정책 기반의 features에 대한 통계적인 정보를 이용하는 방법을 제안하였다.



〔그림 1〕 제안된 방법의 탐지 대상 공격

Ⅱ. 제안배경

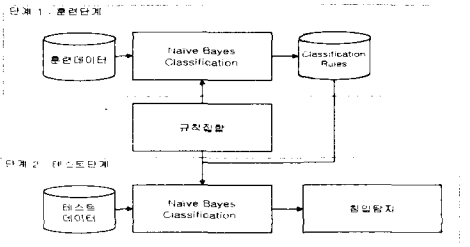
본 논문에서 제안한 이 방법은 전문가의 보안에 대한 경험적 지식을 활용함으로써 다른 침입탐지 방법에서 탐지하기 어려운 공격행위들을 보다 효과적으로 탐지할 수 있다. 알려진 공격 패턴들에 대한 전문가의 분석 경험을 밑바탕으로 이들 공격의 특징을 얻을 수 있는 규칙들을 만들었다. 이들 규칙들을 적용함으로써 공격 탐지에 필요한 특징을 효율적으로 계산하여 기존 공격의 변형된 공격이나 새로운 침입 공격을 보다 안정적으로 탐지할 수 있도록 하였다.

일반적으로 컴퓨터 시스템을 사용하는 각 기관과 컴퓨터 시스템에 따라 서로 다른 보안 전략을 요구할 수 있으며, 이러한 경우에도 본 논문에서 제안한 방법은 이에 적합한 규칙들을 구성하여 사용함으로써 각 기관이나 시스템에서 탐지하고자 하는 침입형태를 탐지할 수 있는 환경 적응성이 있다.

알려진 공격의 패턴이나 보안정책에 의한 침입탐지 방법은 새로운 공격을 탐지하기 어렵거나 쉽게 우회 당할 수 있는 문제점이 있다. 그러나 본 논문에서 제안한 탐지방법은 정책 기반의 특징들을 획득하고 이들 특징들의 통계적인 정보를 이용하여 침입을 탐지함으로써 변형된 공격이나 새로운 공격들을 탐지할 수 있고, 침입자의 다양한 우회 동작에 큰 영향을 받지 않고 이들 침입행위를 탐지할 수 있다.

Ⅲ. 정책기반 새로운 공격 탐지 방법

침입탐지 시스템을 연구, 개발함에 있어서 가장 큰 관심 사항은 하루에도 몇 개씩 발생되는 기존 공격의 변형된 공격이나 새로운 공격을 탐지할 수 있도록 하는 것이다. 여기에서 기술할 정책기반의 새로운 공격 탐지방법 또한 기존 공격의 변형된 공격과 새로운 공격을 탐지하기 위한 목적으로 제안하였다. 제안된 정책기반 새로운 공격탐지방법의 기능 구성도는 〔그림 2〕와 같다.



〔그림 2〕 정책기반 새로운공격 탐지 방법의 기능 구성도

제안된 침입탐지방법은 훈련단계와 테스트단계의 두 단계를 거쳐 실제 환경에 배치된다. 훈련단계는 우선 이 단계에서 사용될 특징값(features)을 추출하기 위한 규칙집합과 훈련데이터집합을 준비한다. 특징값을 추출하기 위한 규칙들을 작성하기 위해 알려진 공격들을 분석하고, 이 탐지모델이 배치될 시스템의 보안전략을 분석한다. 이러한 분석 작업은 침입탐지 분석 전문가에 의해 이루어지며, 분석 전문가의 경험적 지식을 함께 적용하여 규칙들을 작성한다. 또한 훈련단계에서 사용할 훈련데이터집합은 레이블된 데이터로써 정상적인 행위(benign behavior)와 공격행위(malicious behavior)를 포함하고 있다. 이렇게 규칙집합과 훈련데이터집합t이 준비되면 Naive Bayes classification방법을 적용하여 특징값 벡터를 기반으로 한 classification rules를 생성함으로써 훈련단계를 완료한다.

테스트단계는 훈련단계에서 분석한 규칙집합과 Naive Bayes classification에 의해 자동적으로 생성된 classification rules를 테스트 데이터에 적용하여 공격행위를 탐지한다. 테스트데이터는 기존 공격의 변형된 공격과 훈련데이터에는 포함되어 있지 않는 새로운 공격 그리고 정상적인 행위들이 포함되어 있다. 테스트데이터에 규칙집합이 적용되어 특징값들을 추출하고 classification rules를 적용하여 공격행위를 탐지한다. 다음은 제안된 탐지방법의 각 구성 요소에 대해 기술하였다.

1. 규칙집합

규칙집합은 알려진 공격들의 분석, 일반적인 보안 전략 및 시스템이 배치될 환경의 특수한 보안전략의 분석, 보안 분석 전문가의 경험적인 지식을 기반으로 발생될 공격의 특징을 가장 잘 획득할 수 있도록 구성한다. 규칙집합은 몇 개의 도메인으로 분류되어 구성될 수 있으며 도메인의 개수 및 도메인에 포함되는 규칙의 개수는 보안 분석 전문가의 분석에 따라 결정한다. 다음 [그림 3]은 각 도메인별 규칙의 구성 형식이다.

```
DName1 {
  R11: malicious<-SC(user32.EndDialog) ∧
       SC(kernel32.EnumCalendarInfoA) ∧
       MC(FAIL_LOGIN)
  ...
}

DName2 {
  R21: malicious<- SC(shell32.ExtractAssociatedIconA)
  ...
}
...
```

[그림 3] 규칙집합의 구성 형식예

규칙을 적용하여 검사된 결과는 malicious 여부를 True(malicious) 또는 False(benign)의 값으로 평가된다. 특정 도메인 Di에 대한 규칙들의 적용 결과를 해당 도메인의 features vector DFi = (f1, f2, .., fn)로 사용한다.

2. 데이터집합

데이터집합은 훈련단계에서 사용하기 위한 훈련데이터와 테스트단계에서 사용되는 테스트데이터로 구성된다. 데이터집합은 공격행위(malicious bahavior)와 정상적인 행위(benign bahavior)를 모두 포함하고 있다. 단 훈련데이터에 포함된 모든 행위는 그것이 공격행위인지 아니면 정상적인 행위인지가 표시된 레이블된 데이터이다. 훈련데이터에 규칙집합을 적용하여 각 도메인에 대한 feature vector를 평가하고, 이를 기반으로 classification rules를 생성한다.

3. Classification Rules

제안된 탐지방법에서는 Naive Bayes 방법을 이용하여 classification rules를 생성한다. Naive Bayes 방법은 기본적으로 features들이 상호 독립적이라는 것을 가정하고 있다. 제안된 방법에서 사용되는 features는 규칙집합의 각 규칙들로부터 계산된 값들이며, 각 규칙은 상호 독립적인 특징을 가지며 작성된다.

특정 도메인에 대한 규칙집합을 적용하여 features vector F=(f1, f2, ..., fn)가 만들어지고 해당 도메인에 대한 침입행위가 발생되었는지를 결정하기 위해 naive Bayes 방법을 사용한다. 즉, C가 정상적인행위(benign) 또는 공격행위(malicious)를 나타내는 변수라할 때 P(C|F)의 값을 평가하고자 한다. P(C|F)는 features vector F가 획득된 해당 도메인이 정상적인행위 또는 공격행위를 포함할 확률을 나타낸다. 이는 다음과 같은 naive Bayes 방법에 의해 계산된다.

$$P(Ci|F) = \frac{P(F|Ci)P(Ci)}{P(F)}$$

$$P(F|Ci) = \prod_{k=1}^{n} P(fk|Ci)$$

여기서 fi는 해당 도메인에 대한 규칙 Ri를 적용하여 계산된 값이고, Ci는 정상적행위 또는 공격행위를 나타낸다.

V. 결 론

다양한 분야에서 컴퓨터 및 네트워크를 기반으로 한 정보처리에 대한 요구가 늘어가고 있으며, 이와 함께 침입탐지 시스템에 대한 연구 또한 이러한 환경에 있어서 필수적인 기술로 요구되고 있다.

일반적으로 침입탐지 시스템은 오용침입탐지 시스템과 비정상행위침입탐지 시스템으로 분류할 수 있으며, 기존에 알려진 공격을 탐지하기 위한 오용침입탐지 시스템의 경우 상용화되어 안정적으로 사용되고 있는 상황이다. 그러나 하루에도 몇 건씩 발생되는 기존 공격의 변형된 공격이나 새로운 공격이 이루어지고 있다.

본 논문에서 제안된 침입탐지 방법은 알려진공격, 보안정책에 대한 전문가의 경험적 지식을 규칙화하

여 공격에 대한 효율적인 특징값을 획득하였다. 그리고 이 특징값을 기반으로 훈련데이터에 대한 naive Bayes 방법을 적용하여 classification rule을 생성하고 이를 통해 새로운 공격을 탐지할 수 있도록 하였다. 이러한 규칙집합은 점진적으로 추가, 수정될 수 있어 환경변화에 적응할 수 있도록 하였다. 향후 연구방향으로는 호스트기반공격, 네트워크기반공격 각각에 대한 특징을 분석하고 이를 위한 규칙집합을 분석하고 침입탐지분석가의 많은 경험적 지식을 수집, 분석할 필요가 있다.

참 고 문 헌

[1] Wenke Lee, SalvatoreJ. Stolfo, Philip K. Chan, Eleazar Eskin, Wei Fan, MatthewMiller, ShlomoHershkop, Junxin Zhang, "RealTime Data Mining-based Intrusion Detection", 2001 IEEE.

[2] Steven A. Hofmeyr, Stephanie Forrest, Anil Somayaji, "Intrusion Detection using Sequences of System Calls", August 18, 1998.

[3] Han, Kamber, "Data Mining Concepts and Techniques", Morgan Kaufmann Publishers, 2001.

[4] Matthew G. Schultz and Eleazar Eskin, Erez Zadok, "Data Mining Methods for Detection of New Malicious Executables", IEEE, 2001.

[5] Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick, "Intrusion Signatures and Analysis", New Riders, 2001.

[6] 손태식, 서정택, 은유진, 장준교, 이철원, 김동규, "Heap과 Stack 영역에서의 경계 체크를 통한 Buffer Overflow 공격방지 기법에 대한 연구", 정보보호학회지, 2001. 12.

[7] Wenke Lee, Dong Xiang, "Information Theoretic Measures for Anomaly Detection", IEEE, 2001.

[8] R. Sekar, M. Bendre, D. Dhurjati, P. Bollineni, "A Fast Automation-Based Method for Detecting Anomalous Program Behaviors", IEEE, 2001.

[9] Alfonso Valdes and Keith Skinner, "Probabilistic Alert Correlation", RAID 2001.

[10] Paul D. Williams, Kevin P. Anchor, John L. Bebo, Gregg H. Gunsch, Gary D. Lamont, "CDIS: Towards a Computer Immune System for Detecting Network Intrusions", RAID 2001.

〈著 者 紹 介〉

김 형 훈 (Hyung-Hoon Kim)
정회원

1986년 2월 : 전남대학교 계산통계학과 졸업(학사)
1988년 2월 : 한국과학기술원 전산학과 졸업(석사)
1995년 3월~현재 : 전남대학교 계산통계학과 박사과정
1994년 9월~현재 : 광주여자대학교 정보통신학과 교수
관심분야 : 시스템 및 네트워크 보안, 인공지능