AREIDS : 적응적인 실시간 침입탐지시스템 평가도구

정유석°, 조성배
연세대학교 컴퓨터과학과
{j8508, sbcho}@candy.yonsei.ac.kr

AREIDS : an Adaptive Real-Time Evaluation Tool for Intrusion Detection System

Yoo-Suk Jung° Sung-Bae Cho
Computer Science Department, Yonsei University

요 약

최근 몇 년간에 이루어 진 네트웍 및 인터넷 시장의 발전과 더불어 성장한 시스템에 대한 침입 등은 이를 방어하기 위한 여러 도구의 개발을 가져왔다다. 이러한 도구들 중 침입탐지시스템은 시스템 방어에 핵심적인 역할을 하는데, 현재까지 이를 평가하기 위한 자동화된 온라인 평가도구는 없는 실정이다. 보안관련 학문 및 시장이 발달한 미국에서는 DARPA의 지원아래 관련된 연구가 진행되어 1998년과 1999년 대규모의 침입탐지시스템 평가가 이루어졌으나, 이때의 평가들은 당시의 침입 수준만을 고려한 것으로 새로운 침입 환경에 대한 확장은 용이하지 않기에, 급속도로 발전하는 침입 기술에 대응하기 위한 새로운 방법이 필요하다. 본 논문에서는 새로운 침입 환경에 적응적이며 실시간으로 다량의 침입에 대한 정량적 탐지성능을 측정하고 결과를 통계적으로 분석하여 출력할 수 있는 통계적인 침입탐지 평가도구를 개발한다.

1. 서 론

최근 몇 년간에 이루어 진 네트웍 및 인터넷 시장의 급속한 발전으로 관련 시장에 대한 긍정적인 팽창 뿐 아니라 네트웍 시스템에 대한 침입이나 바이러스 웜 등의 부정적인 요소들이 증가하고 있다. 따라서 이를 방어하기 위한 도구들이 개발되기 시작했는데 그 중 침입탐지시스템은 시스템 방어에 핵심적인 역할인 침입을 감지하는 역할을 맡는다.

시스템 보안의 중요성이 커짐에 따라 다양한 침입탐지시스템이 등장하고 있다. 그러나 이에 대한 자동화된 온라인 평가도구는 아직 개발 단계에 머무르고 있으며, 대부분 수동적인 성능평가만이 이루어지고 있다. 국내의 침입탐지시스템에 대한 평가는 한국정보보호센터에서 이루어지고 있으나 현재는 초기 단계로 평가를 위한 각종 방안들이 마련되고 있는 상황이다. DARPA의 경우에는 1998년과[6] 1999년에[7] 대규모의 침입탐지시스템에 대한 평가가 이루어졌고, MIT Lincoln 연구소에서 자동화된 온라인에서의 평가에 대해 연구되고 있다.

현재 주된 연구의 방향은 공격들에 대한 다양한 환경에서의 대응 평가 및 단순한 통계적인 출력에 초점이 맞추어져 있다. 그런데 새로운 종류의 침입이 급속도로 증가하고 있는 현 상황에서는 특정 침입에 대한 다양한 상황에서의 탐지성능을 측정하는 것 뿐 아니라 다량의 침입에 대한 정량적 탐지성능을 측정하는 것과 탐지 결과에 대한 통계적인 분석 또한 중요한 문제이다.

본 논문에서는 새로운 침입 환경에 적응적이며 실시간으로 다량의 침입에 대한 정량적 탐지성능을 측정하고 결과를 통계적으로 분석하여 출력할 수 있는 통계적인 침입탐지 평가도구 개발에 대해 소개한다.

2. 관련 연구

초기의 침입탐지시스템에 대한 평가는 적은 수의 시스템에 대해 단순한 트래픽 상황에서 적은 수의 은닉기능이 없는 공격만으로 평가가 이루어졌으나[3, 4], 1998년 DARPA의 1차 평가에서는 10개의 시스템, 38개의 공격, 충분한 트래픽과 일부의 은닉화된 공격을 통한 평가가 이루어졌다[6]. 표 1은 침입탐지시스템에 대한 평가의 변화추이를 나타낸다.

표 1. 과거 침입탐지시스템 평가의 특징[7]

연구자	탐지수	침입수/시스템	은닉	비고
Puketza[3,4]	2	4/1	No	자동화공격. 단순한 텔넷 트래픽
Debar[2]	3	4/1	No	자동화공격. 단순한 FTP 트래픽
Shipley[1]	10	12/4	Yes	10개의 상용제품의 비교
Durst[5]	4	19/4	Yes	1998년 DARPA 실시간 평가
Lippman[6]	10	38/4	Yes	1998년 DARPA 오프라인평가

MIT Lincoln 연구소는 1998년부터 DARPA의 지원아래, 침입탐지 관련 연구를 위한 방향을 제시하고 기술에 대한 객관적 교정을 위해서 침입탐지 평가를 주제로 과제를 수행하였다. 각 과제에서 침입탐지시스템들은 훈련용 데이터를 통해 정보를 제공받고 검사용 데이터를 통해 성능을 평가받았다. 훈련용 데이터에 삽입된 공격에 대해서는 관련된 모든 정보가 제공되었으며, 검사용 데이터에 포함된 공격에 대해서는 어떠한 정보도 제공되지 않았다. 평가 방법은 검사용 데이터에 포함된 각 침입에 대한 탐지 정보에 점수를 부과하는 방식으로 이루어졌다. 부여된 점수는 해당 ID가 침입이라고 확신하는 정도를 나타낸다. 평가 점수를 위한 정보는 1) 공격 탐지와 식별여부 검사, 2) 공격 시작 시간 탐지여부 검사, 3) 공격 목표 탐지여부 검사였다.

1998년에는 침입탐지 시스템에 대한 최초의 포괄적인 평가가 이루어졌다. 이 평가에서는 네트웍 트래픽 및 유닉스 호스트에 대한 평가가 이루어졌으며, 최초로 False positive error를 측정

하였다. 평가 데이터에는 7주간 38종류에 대한 300번의 공격 정보가 포함되었다[6]. 1999년의 평가에서는 1998년의 평가를 확장한 것으로 윈도우 NT에 대한 평가와 새로운 공격 등을 추가했다. 또한, 새로운 공격들을 훈련 데이터에 삽입하지 않고 평가하여 해당 공격을 탐지할 수 있는지에 초점이 맞춰졌다. 평가는 탐지 결과의 ROC 곡선을 통해 탐지율과 false positive 오류율로 이루어졌다[7].

DARPA에서 이루어진 침입탐지시스템의 평가는 현재의 침입 수준에 초점이 맞추어져 있으므로 특정 공격들에 대한 다양한 환경에서의 적응이 주된 평가 방향이었고, 따라서 어떤 종류의 가상 환경을 만드는가에 대해 연구되어 왔다. 그런데 이제는 새로운 종류의 침입들이 증가하는 것과 관련된 침입패턴, 침입유형 등의 관리 및 결과에 대한 통계적 분석 관련 영역의 개발이 미흡함으로 이에 대한 보완이 필요하다.

3. AREIDS

AREIDS(adaptive real-time evaluator for intrusion detection system)는 연세대학교 소프트컴퓨팅 연구실에서 개발한 적응적 실시간 침입탐지 평가도구이다. 이것은 평가대상 침입탐지시스템에 대해 다양한 침입을 시도하고 통계적인 평가를 하는 것은 물론, 새로운 침입방법과 환경에 대한 추가가 용이하여 새로운 침입패턴에 대한 평가가 쉽게 이루어질 수 있으며, 탐지도구는 자바(Java)로 침입패턴은 이진실행파일로 독립적으로 구현하여 다른 운영체제에 쉽게 포팅이 가능하게 하였다.

3.1 평가관련 정보

침입탐지시스템 평가도구는 침입탐지기능의 성능을 분석하기 위해 침입패턴이나 침입유형 등의 척도를 사용하게 된다. 그런데 이 척도들은 일반적으로 통용되기는 하지만 그 뜻이 명확하지 않아 다음과 같이 제 정의한다.

정의 1. 침입패턴(Intrusion Pattern) : 알고리즘 상으로 구분되는 침입의 종류이다.

정의 2. 실행 침입패턴(Executable Intrusion Pattern) : 침입패턴을 통해 구현된 코드로 하나의 알고리즘으로부터 다수의 코드가 야기되듯 하나의 침입패턴으로부터 다수의 실행 침입패턴이 생성될 수 있다.

정의 3. 침입유형(Intrusion Type) : 다른 알고리즘을 갖는 유사한 형태의 침입의 종류이다.

정의 4. 시스템 취약성(System vulnerabilities) : 시스템 취약성은 시스템에서 침입 당하기 쉬운 논리적 물리적 장소를 의미한다.

AREIDS에서는 평가를 위한 기본 정보인 침입패턴, 실행침입패턴, 침입유형, 시스템취약성 등을 추가할 수 있지만, 기본적인 평가를 위한 정보는 표 2와 같이 제공된다. 침입유형은 CERT-CC에서 정의한 10가지 침입유형 중 평가도구에서 사용할 수 없는 사회 공학유형을 제외하고 선정했으며, 시스템취약성은 시스템 관점이 아닌 침입의 관점에서 일반적인 것들을 선정했다.

3.2 시스템 구조

AREIDS의 전체 구조는 그림 1과 같다. 침입패턴관리기는 침입패턴의 추가, 삭제, 정정 등의 관리를 담당하며, 침입유형관리기와 취약성관리기는 각각 침입패턴의 특성인 침입유형과 취약성 정보에 대해 관리한다. 성능평가기는 실행침입패턴 DB의 실행 침입패턴들 중 평가를 위해 선택된 것들을 평가대상 IDS가 설치된 호스트로 실행한다. 결과분석기는 IDS로부터의

표 2. 침입탐지시스템 평가를 위한 기본 정보

침입유형	시스템취약성
· 사용자도용	· 패스워드 및 계정관련
· SW보안오류	· 원격 파일접근 서비스 관련
· 버퍼오버플로우	· 원격지에서의 쉘 및 루트 권한 취득 관련
· 구성설정오류	· DOS 관련
· 악성프로그램	· 프로토콜 관련
· 프로토콜취약점	· NFS 관련
· 서비스거부공격	· CGI/Finger/NIS/RPC 관련
· E-Mail관련공격	· 포트 관련
· 취약점정보수집	

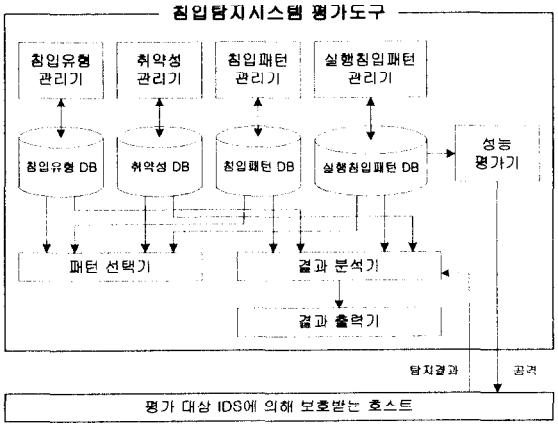

그림 1. 침입탐지 평가도구의 기본구조

탐지 결과를 받고 침입탐지시스템의 성능을 통계적으로 분석하며, 결과 출력기는 유형, 취약성별 탐지 결과를 그래프와 텍스트 형식으로 출력한다.

3.3 침입패턴 관련정보의 데이터베이스 스키마

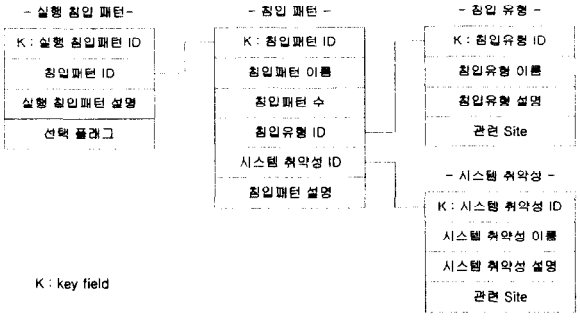

그림 2. 침입패턴 관련정보의 데이터베이스 스키마 관계

그림 2는 AREIDS의 기본 자료가 되는 침입패턴, 실행침입패턴, 침입유형, 시스템취약성을 위한 데이터베이스 스키마이다. 침입 패턴은 기타 정보들의 근간이 되는 정보로 스키마에는 키에 해당하는 침입패턴 ID와 침입패턴 자체의 정보를 포함하는 이름, 해당 침입패턴으로 구현된 실행 침입패턴의 총 수, 해당 침입패턴의 침입 유형 및 시스템 취약성 그리고 침입패턴 자체에 대한 설명으로 이루어진다. 실행침입패턴은 특정 침입패턴의 구현으로 키에 해당하는 실행 침입패턴ID와 해당 실행 침입패턴의 침입패턴 및 설명과 선택 플래그로 이루어진다. 선택

플래그는 침입을 실행할 때 해당 실행 침입패턴이 평가를 위한 침입에 사용되는지 여부를 나타낸다. 침입유형과 시스템 취약성은 각각 키에 해당하는 ID와 고유한 이름 및 설명 그리고 관련된 웹사이트 주소를 포함한다.

3.4 동작 시나리오

침입탐지 평가를 위한 시나리오는 표 3과 같다. ①의 침입유형, 시스템취약성, 침입패턴, 실행침입패턴의 등록은 기존의 정보(침입유형, 시스템취약성, 침입패턴, 실행침입패턴)의 변경이나 삭제, 새로운 정보의 추가가 발생할 때만 실행되며, ②의 대상 침입탐지시스템이 설치된 호스트에 대한 정보의 등록은 각 실행 침입 패턴이 실행되기 위해 필요한 호스트 관련정보를 설정하는 것이다. ③의 실행침입패턴의 선택은 각 정보의 관점에서 이루어지는데, 예를 들어 특정 침입유형을 선택한 경우 해당 유형의 모든 침입패턴으로 구현된 모든 실행침입패턴이 평가를 위한 침입으로 선택된다. ⑤의 침입탐지 결과는 표 2의 형식으로 정리되어 침입탐지시스템 평가도구로 전송된다. ⑥의 침입탐지 결과 분석은 각 정보에 따라 침입 시도 중 탐지수와 탐지 확률을 계산하여 ⑦의 결과 출력에서 그래프와 텍스트의 형식으로 제공된다.

표 3 침입탐지시스템 평가를 위한 시나리오

① 침입유형, 시스템취약성, 침입패턴, 실행침입패턴 등록
② 대상 침입탐지시스템이 설치된 호스트에 대한 정보 등록
③ 평가를 위해 침입을 시도할 실행침입패턴을 침입유형, 시스템취약성, 침입패턴, 실행침입패턴의 관점에서 선택
④ 시스템 침입
⑤ 침입탐지 결과 전송
⑥ 침입탐지 결과 분석
⑦ 침입탐지 결과 출력

3.5 AREIDS의 기능

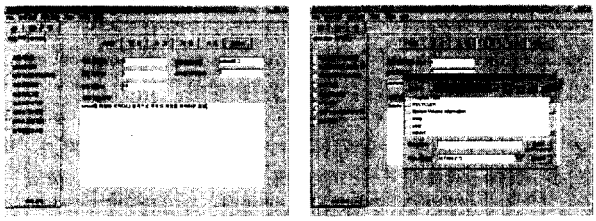

그림 3. 평가관련 정보 업데이트

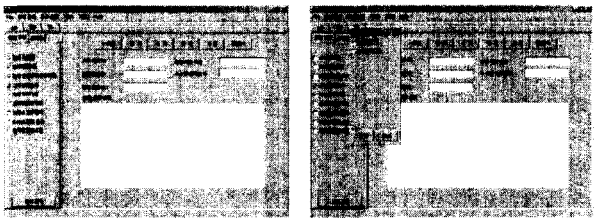

그림 4. 평가를 위한 침입패턴 선택

평가관련 정보 업데이트는 침입패턴[그림3.좌], 실행침입패턴[그림3.우], 침입유형, 시스템취약성의 추가, 변경, 삭제의 기능이 있으며, 이를 위해 검색 및 이동(이전, 다음)의 기능을 포함한다. 위의 기능은 모두 버튼으로 구성되어 있다.

평가를 위한 실행침입패턴은 침입유형, 시스템 취약성, 침입패턴 등의 척도를 기준으로 선택되거나 개별 실행침입패턴으로 선택된다. 실행침입패턴 선택을 위해 침입유형이나 시스템 취약성을 선택한 후 이중클릭을 하면 해당 침입유형이나 시스템 취약성을 갖는 모든 침입패턴들의 실행침입패턴이 선택되며[그림4.좌], 한번 클릭을 한 후 상세 선택 버튼을 누르면 개별 침입패턴을 선택할 수 있다[그림4.우].

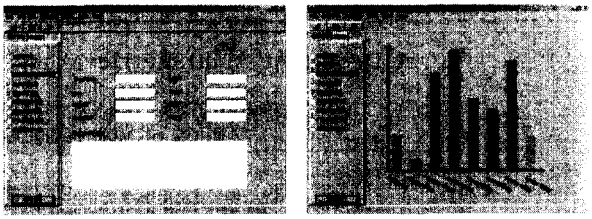

그림 5. 평가호스트 설정과 평가 결과

그림 5.좌는 평가대상 호스트 정보를 설정하는 화면으로 현재의 버전에서는 대상 호스트의 IP주소, 포트, 사용자 ID, 비밀번호이며 및 확장영역을 설정한다. 그림 5.우는 평가결과 출력의 화면으로 AREIDS에서는 이와 같은 그래프 형식의 결과와 텍스트형식의 결과를 제공한다.

4. 결론 및 향후과제

본 논문에서 소개한 AREIDS는 다량의 실행침입패턴을 통한 통계적인 평가는 물론, 새로운 침입패턴 및 관련 정보인 유형과 취약성을 추가함으로써 새로운 침입환경에 적응할 수 있다. 또한 평가 시스템 자체는 침입패턴과 구분되어서 자바로 구현되었기에 여타 운영체제로의 포팅이 용이하다. 그러나 본 논문에서 소개한 평가 시스템은 다량의 침입패턴을 통한 통계적인 분석과 새로운 침입 환경에의 적응에만 초점을 맞추고 개발되었기에 가상적인 환경의 생성을 통한 침입패턴들의 다양한 방향에서의 접근 방법 등을 보완할 필요가 있다.

참고문헌

[1] G. Shipley, "Intrusion detection, take two," Network Computing, 15 November 1999.

[2] H. Debar, M. Dacier, A. Wespi and S. Lampart, "An experimental workbench for intrusion detection systems, " Research Report RZ 2998(#93044), IBM Research Division, Zurich Research Laboratory, 8803 Ruschlikon, Switzerland, 9 March 1999.

[3] N. Puketza, K. Zhang, M. Chung, B. Mukherjee, and R. A. Olsson, "A methodology for testing intrusion detection systems," IEEE Transactions on Software Engineering, 22 719-729., 1996.

[4] N. Puketza, M. Chung, R. A. Olsson, and B. Mukherjee, "A software platform for testing intrusion detection systems," IEEE Software, 43-51, Sep./Oct. 1997

[5] R. Dust, T. Chanmpion, B. Witten, E. Miller, and L. Spagnuolo, "Testing and evaluating computer intrusion detection systems," Communications of the ACM 42 53-61, 1999.

[6] R. P. Lippmann, et. al, "Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation," Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX), vol. 2, IEEE Press, New York, January 2000

[7] Richard Lippmann, et. al, "The 1999 DARPA off-line intrusion detection evaluation," Computer Networks, Vol. 34, no. 4, pp. 579-595, October 2000.