가상 네트워크 환경에서의 공격자 추적 시뮬레이션

김상영° 최진우* 우종우* 황선태* 박재우** 남건우** 최대식**
*국민대학교 컴퓨터학부
**한국전자통신연구소 부설 국가보안기술연구소
cwwoo@kookmin.ac.kr, dschoi@etri.re.kr

Attacker Tracing Simulation in the Virtual Network Environment

Sangyoung Kim° Jinwoo Choi* Chongwoo Woo* Suntae Hwang* Jaewoo Park** Gunwoo Nam** Daesik Choi**
*School of Computer Science, Kookmin University
**National Security Research Institute

요 약

최근 인가되지 않은 컴퓨터에 대한 접근이 사회적으로 커다란 문제로 대두되고 있으며, 점차 파괴적인 상황으로까지 악화 되고 가고 있다. 따라서 이러한 침입 행위에 대해 침입자들을 추적하여 경고를 줄 수 있는 보다 능동적인 대응이 필요하게 되었다. 이 문제에 대한 많은 해결책이 제시 되었으나 완벽한 대안이 되지는 못하고 있는 실정이며, 오히려 대부분의 경우 숙련된 시스템 관리자의 경험에 의존하는 경향이다. 따라서 침입의 경우에 대비해 어떠한 새로운 상황이 발생하더라도 시스템을 유지할 수 있도록 시스템 관리자들을 훈련시킬 필요가 있다. 본 논문에서는 시스템 관리자들을 훈련하기 위하여 시뮬레이션 기반의 공격자 추적 시스템을 제안한다. 본 시스템은 가상의 지역 네트워크 환경에서 시스템의 간섭 없이 약속된 시나리오에 의한 공격 경로를 분석하고 다양한 형태의 공격 형태를 연습하고 배우는 기능을 제공한다.

이 시스템은 두 가지 주요 문제에 대해 학생들을 훈련시킨다. 첫째, 공격 형태를 발견하는 것이며, 둘째, 다양한 로그 데이터를 분석하여 공격이 이루어진 흔적을 발견해 내는 것이다. 시스템의 테스트 영역은 LINUX 기반의 환경으로 그 범위는 다양한 형태들의 로그 데이터들을 종합하여 분석하는 것으로 제한 한다.

1. 서 론

컴퓨터 통신 네트워크의 급속한 발전은 우리 사회 전반에 걸쳐 많은 이익을 가져왔으나, 한편으로 이러한 새로운 통신 기술은 악의적인 컴퓨터 침입의 증가라는 부작용을 초래하고 있다. 이러한 문제점을 해결하기 위하여 최근 침입탐지에 관한 많은 연구결과가 보고 되고 있다[4][5]. 침입 탐지 시스템(Intrusion Detection System : IDS)은 이러한 환경에서 유용한 도구로 사용되며, 보다 다양한 가능성들이 제시되고 있다[1][3]. 최근 IDS 관련 제품들은 공격자의 정보를 제공하는 등의 응답 메커니즘을 사용하지만, 대부분의 경우 공격자는 보다 영리한 방법으로 다수의 사이트들을 매개로 한 공격을 이용하여 자신의 위치를 숨기고 있다. 따라서 시스템 관리자는 이러한 침입 시 방어적인 성격의 대응이 아닌 보다 능동적으로 침입 경로 상의 손상된 컴퓨터들의 발견과 같은 대응이 항상 가능하도록 훈련할 필요가 있다.

이러한 분야의 연구는 대표적으로 AI의 계획기법을 적용한 ID-Tutor[6]가 있으며, ID-Tutor의 단점인 메뉴 위주의 학습 방식과 학습자 모델에 관한 문제점을 해결하기 위해서, 보다 실제와 유사한 가상 환경 내에서의 학습 가능한 시스템들이 연구 되고 있다[9][10].

본 논문에서는 시스템 관리자들을 훈련하기 위해 시뮬레이션의 개념이 적용되어진 공격자 추적 시스템을 제안한다. 학습자는 시스템 간섭 없이도 약속된 시나리오에 의한 공격 경로를 분석하고, 그 결과 다양한 형태의 공격 형태를 학습할 수 있는 기능을 제공한다. 또한, 효과적인 학습을 위해서 지능형 교육 시스템(Intelligent tutoring System)[2]의 구조에서 학습자의 문제 해결을 기록하는 학습자 모델을 적용하였다.

2. 시스템 설계

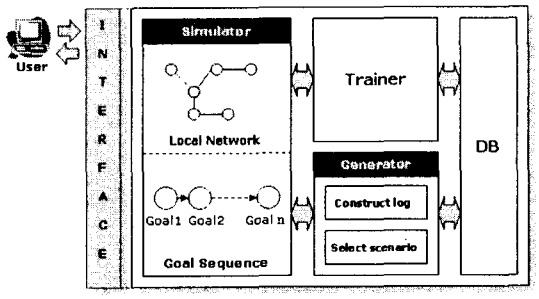
시스템은 학습자에게 지역 네트워크와 같은 가상 시뮬레이션 환경(Virtual Simulation Environment)을 제공한다. 학습자는 주어진 GUI 기반의 가상 시뮬레이션 환경에서 로그 정보를 가지고 현재의 침입 시스템을 분석하고, 침입이 이루어진 흔적들로 침입 경로를 역추적 해봄으로써 지역 네트워크 상의 침입 시나리오를 훈련한다.

이 시스템에서 로그 정보는 리눅스 시스템[8]을 기준으로 하며, 훈련 대상은 리눅스 관리자로 한정한다. 전체적인 시스템은 내부적으로 로그 제너레이터를 이용하여 가상의 네트워크를 구성하는 각각의 컴퓨터 내에 위치하는 로그들을 생성하고, 여기에 침입 시나리오를 적용하는 과정을 반복하여 가상의 네트워크 엔터티들로 이루어진 환경을 제공한다. 또한 새롭게 보고 되어진 사례들[7]을 이용하여 시나리오들을 시스템 내로의 추가 가능하도록 확장성을 고려하여 설계하였다.

이 연구는 ETRI 부설 국가보안 기술연구소 2002년 위탁 연구과제에서 지원 받았음

2.1 시스템 구조

시스템의 전반적인 구조는 [그림 1]과 같이 설계 하였다. 트레이닝 과정은 단위 시뮬레이션으로 시작하여, 단계적으로 종합적인 사고를 요구하는 연습 문제를 트레이닝 하게 된다. 단위 시뮬레이션은 침입 유형에 따라 다양한 개념에 대한 단위 학습과 가상의 네트워크 서버 연결을 기반으로 이루어지며, 학습자는 이 과정을 통해 침입 유형에 대한 로그 분석 능력을 기르게 된다.



[그림 1] 시스템 아키텍처

시뮬레이터는 학습자의 트레이닝에 도움을 주기 위한 가상 시뮬레이션 환경을 제공하며, 이러한 환경을 통해 학습자가 문제를 해결하게 된다. 시뮬레이터의 동작은 내부적으로 시뮬레이터 상에서 침입 흔적 발견을 위한 학습자의 행위를 트레이너에게 전달하며, 트레이너를 통해 데이터베이스에 저장된다. 외부적으로는 학습자의 행위에 따른 적절한 도움이나 반응을 보여주어 능동적인 학습이 이루어지게 한다.

제너레이터는 내부의 데이터베이스를 기반으로 시뮬레이터로부터 전달 받은 학습자의 행위를 가지고 시뮬레이션 할 수 있는 가상의 환경을 조성하는 역할을 수행 한다. 주요 기능은 현재 가상 네트워크 구조에 적합한 로그를 생성 하고, 침입 경로와 행위에 대해 적절한 시나리오를 선택 하여, 두 가지를 조합하여 침입 시나리오에 따른 로그를 생성하는 것이다.

트레이너는 내부적으로 학습자의 행위를 모델링 하는 역할을 수행한다. 사용자가 트레이닝을 할 때 이루어지는 행위는 트레이너를 통해 데이터베이스에 저장 되고, 트레이닝 후 결과에 대한 평가와 조언에 사용된다.

인터페이스는 브라우저 상에서 동작하며, 학습자의 행위에 따라 서버의 시뮬레이터와 상호작용하며 학습을 수행 한다.

2.2 시뮬레이션

시뮬레이션은 학습자에게 가상의 네트워크 환경을 제공하여 해커의 침입 유형과 행위를 학습자가 직접 분석하고 경유지로 사용된 시스템을 추적하는 과정이다.

시뮬레이션 과정은 다음과 같이 이루어진다.

① 학습자에 의한 환경 변수 입력

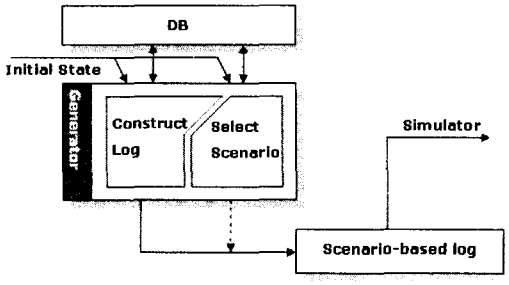
② 제너레이터를 통한 내부적인 가상 환경 구축

③ 학습자가 가상의 환경에서 침입 유형을 분석하고 침입 경로를 추적, 동시에 학습자의 행위는 트레이너를 통해 추적/저장

④ 트레이닝 과정이 끝난 후, 트레이너가 추적한 학습자의 정보를 가지고 학습 목표에 대한 평가와 도움을 제시

2.3 제너레이션

[그림 2]는 제너레이터에 의한 시뮬레이션 환경 생성 과정으로 써 그 목적은 학습자에 대한 정보를 바탕으로 침입 유형이 적용된 가상의 환경을 구성하는 것이다. 이 시스템에서는 시뮬레이션 과정이 로그를 분석하는 데 중점을 두고 있으므로, 시나리오에 따른 침입 행위가 반영된 로그를 생성하여 시뮬레이터에게 제공하는 역할을 수행한다.



[그림 2] 제너레이션 과정

초기에는 각 로그 테이블 구조 중 "ans, cnt" 필드들을 제외한 나머지 구조가 학습자에게 제공된다. 로그분석 시뮬레이션 학습 동안 학습자는 침입에 대한 정보라고 예상되는 부분을 각 라인에 포함된 체크박스에 표기함으로써 학습자가 침입 판별 기준으로 어느 부분을 사용하였는지를 명시하게 된다.

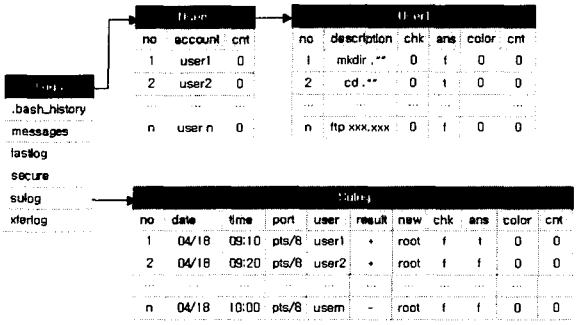
2.4 평가

학습과정은 기본적인 침입 유형에 따른 단위 시뮬레이션으로부터 종합적인 침입 유형이 조합된 종합적인 시뮬레이션에 이르기까지 단계적으로 이루어진다. 학습자는 단위 시뮬레이션에서 특정 침입 유형에 대한 기본적인 학습을 하게 되고, 이렇게 얻어진 지식을 바탕으로 가상 네트워크 환경에서의 종합적인 침입 분석 및 판단을 위한 훈련을 하게 된다. 시스템 내부에서는 트레이너를 통해 가상 환경에서의 학습자의 조작 과정을 모니터링 하게 되며, 현재의 침입 시나리오와의 비교를 통해서 학습자의 성취도를 평가하게 된다.

2.5 로그 데이터베이스

데이터베이스 내의 로그들에 대한 테이블 스키마는 [그림 3] 과 같은 구조로 구성된다. 각 로그에 대해서 표기가 완성된 답안은 시스템으로 전송되어 답안과 상응하는 테이블을 기준으로 비교하게 된다. 만약에, 적절하지 않는 라인이 발견되었을 경우 "color" 필드에 가중치 값을 기록하게 된다. 이 필드의 값은 학습자에게 피드백을 하는 용도로 사용되며,

학습자 인터페이스에서 해당 값에 따라 다른 색상으로 표현한다. 이러한 과정은 학습자가 학습을 종료할 때까지 반복하여 수행하게 되며, 종료 시까지 걸린 시간과 각 라인의 수정 횟수가 기록된다.

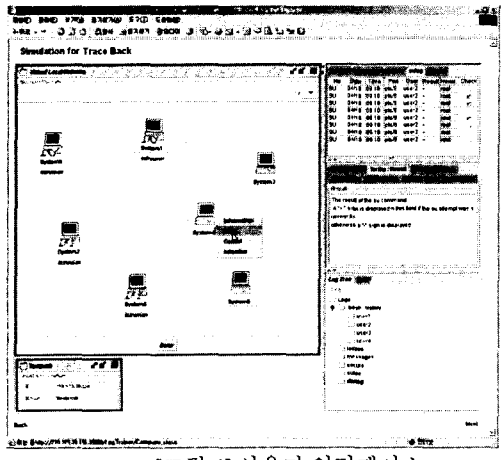


[그림 3] 로그 데이터베이스

이러한 기록들은 학습자 모델을 위한 데이터베이스로 사용되며, 각 학습자의 로그 분석 시의 취약한 부분에 대한 정보를 유지하게 된다.

3. 구현

이 시스템은 JDK1.3.1을 사용하여 구현되었으며, 서버는 Microsoft NT 4.0, 데이터베이스는 MS SQL Server5.0을 사용하였다.



[그림 4] 사용자 인터페이스

[그림 4]에서 좌측에 위치한 "Virtual Local Network" 패널은 시뮬레이션을 위한 가상 지역 네트워크를 나타낸다. 실선은 시스템 사이에 통신이 이루어졌음을 의미한다.

우측 프레임에서는 학습자가 선택한 시스템이 가지고 있는 여러 가지 종류의 로그들을 제공한다. 로그 테이블은 그 정보를 구조화하여 학습자에게 제시한다. 특정 컬럼을클릭하면 시스템은 우측 중앙부에 선택된 컬럼에 상응하는 도움말을 제공한다. 서버 시스템은 학습자 행위들에 관한 정보를 데이터베이스와 비교하게 되고, 만일 특정 로그 내에 잘못된 라인이 선택되었다면 피드백으로써 다른 색상으로 표현하여 학습자로 하여금 재학습이 가능하도록 지시한다.

4. 결론

본 논문에서는 시스템 관리자를 훈련시키기 위한 시뮬레이션 기반의 공격자 추적 트레이닝 시스템을 설계 및 구현하였다. 본 시스템은 주요한 두 가지 주요 문제에 대한 훈련을 제공한다. 첫 번째는 공격 유형을 파악하는 것이고, 두 번째는 다양한 로그 데이터를 분석하여 공격에 대한 흔적을 발견하는 것이다.

이 시스템의 장점은 다음과 같이 나타낼 수 있다. 첫째, 시스템 관리자가 원하는 만큼 다양한 추적 메커니즘을 연습할 기회를 제공한다. 둘째, 가상의 환경을 사용하기 때문에 시스템에 대한 간섭에 대해 걱정할 필요가 없다. 더불어, 웹 기반의 시뮬레이션 시스템이므로 학습자는 웹 브라우저를 이용하여 어디서든지 손쉽게 학습을 진행 할 수 있다. 셋째, 훈련 시에 학생의 특정 항목에 대한 체크여부에 따라 학생의 능력을 평가 할 수 있고, 필요할 때에 훈련에 도움이 되는 기본적인 힌트를 제공받을 수 있다.

참고문헌

[1] Anderson, D., Frivold, T., and Valdes, A., "Next-generation intrusion-detection expert system(NIDES)", Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, CA, 1995.

[2] Alpert, S., Singley, K., and Fairweather, P., "Porting a Standalone Intelligent Tutorin g System on the Web", Proceedings of ITS'2000 workshop, pp. 1-11, 2000.

[3] Garvey, T., and Lunt, T., "Model based intrusion detection", Proceedings of the 18th National Information Security Conference, pp. 372-385, 1995.

[4] Kumar, S., "Classification and Detection of Computer Intrusions", PhD thesis, Purdue University, 1995.

[5] Lunt, T., "Automated Audit Trail Analysis and Intrusion Detection: A Survey", Proceedings of the 11th National Computer Security Conference, pp. 74-81, 1988.

[6]. Rowe, N.C. and Schiavo, S., "An Intelligent Tutor for Intrusion Detection on Comput er Systems", Computers and Education, pp. 395-404, 1998.

[7] CERT Advisory CA-1991-18 Active Internet ftp Attacks, http://www.cert.org/advisories/CA-1991-18.html

[8] Understanding system log files on a Solaris 2.x operating system,http://www.cert.org/security-improvement/implementations /i041.12.html

[9] Woo, C., Choi, J., and, Evens, M., "Web-based ITS for Training System Managers on the Computer Intrusion", Proceedings of the ITS2002, pp. 311-319, 2002.

[10] Woo, C., and Choi, J., "Web-based tutoring system for computer security", Proceedings of the PRICAI2002, pp. 522-531, 2002.