웹 어플리케이션 IDS 평가를 위한 테스트 환경 설계 및 구축

서정석° ,이영석, 김한성, 차성덕
한국과학기술원 전자전산학과
{jsseo°, yslee, kimhs, cha}@salmosa.kaist.ac.kr

Evaluation Environment of Web Application Intrusion Detection Systems

Jeongseok Seo° ,Youngseok Lee, Han-Sung Kim, Sungdeok Cha
Div. of Computer Science, Dept. of EECS, KAIST and AITrc/IIRTRC/SPIC

요 약

최근 기업이나 국가 기관의 다양한 서비스 제공 요구와 함께 웹 서비스의 유용성과 용이성이 맞물려 웹 서비스 사용량은 꾸준히 증가하고 있으며, 웹 서비스 보안의 필요성은 매우 높아졌다. 그러나 다른 인터넷 서비스들에 비해 웹 서비스에 대한 보안은 연구 부족으로 인하여 기술적 수준이 낮으며, 오히려 웹 서비스에 특화된 보안 기술과 도구의 부족으로 인하여 웹 공격의 빈도와 피해는 점점 증가하고 있는 추세이다. 웹 서비스를 효과적으로 보호하기 위해서는 웹 서비스에 특화된 침입 탐지 기술이 필요하며, 이를 평가하기 위한 웹 IDS 평가 환경과 평가 기준이 필요하다. 본 연구에서는 웹 IDS 평가를 위한 평가 기준과 테스트 환경 설계에 대해서 알아보고자 한다.

1. 서 론

웹(World Wide Web) 서비스는 사용자간의 정보 전달에서부터 e-commerce, 인터넷 쇼핑몰, 인터넷 뱅킹(web-based banking)등 사용량이 점차 확대되어 가고 있다. 최근 웹은 개인, 기업, 국가의 정보와 서비스 제공의 요구와 맞물려 중요한 미디어로 부상하고 있다. 2002년 CSI/FBI에서 수행한 컴퓨터 보안 설문 조사를 보면 웹 서비스 오용과 불법적인 공격을 받고 있는 웹 사이트는 2001년 23%에서 2002년 38%로 증가하고 있다[1]. 기존의 방화벽이나 signature 기반의 IDS들은 증가하는 웹 공격에 효과적으로 대응할 수 없기 때문에 웹 어플리케이션에 특화된 침입 탐지 시스템(웹 IDS)과 보안 기술들의 필요성은 급격히 증가하고 있고[2, 3], 이에 관한 연구는 점차 많이 이루어지고 있다[4].

이에 따라 새로운 웹 IDS 연구의 효용성과 성능을 검증하기 위한 적절한 평가 환경과 기준의 부재에 따라 연구의 필요성이 나타나게 되었다. 기존의 침입 탐지 시스템을 평가하기위한 연구는 U.C. Davis, MIT Lincoln Lab., MITRE 등에서 많이 이루어져 왔다[5, 6]. 하지만 기존 Host-based/Network-based IDS 평가를 위한 연구이기 때문에, 데이터 소스 등의 문제로 웹 IDS 평가를 위한 적합한 평가 환경이 아니며, 웹 공격 데이터가 부족하여 IDS의 핵심 기술을 평가하기에 부적합하다.

웹 IDS를 사용하는 소비자와 연구하는 연구자에게 효과적인 평가기준이 되기 위하여 무엇보다도 과학적이고 정량적(quantitative)으로 웹 IDS의 성능을 평가할 수 있어야 하며, 따라서 객관적이고 보편적(general)으로 사용될 수 있는 웹 IDS 평가 기준과 테스트 데이터를 설계하는 일은 매우 중요하다.

침입 탐지 시스템을 평가하는 기준은 일반적으로 공격이 포함된 테스트 데이터를 사용해 공격 탐지율과 오 탐지율(false positive/negative)을 비교하는 ROC 분석 방법이 많이 사용되고 있다. 이러한 IDS 평가 데이터는 IDS를 연구하고 설계하는 일에 직접적으로 관련되어 있으며 평가 데이터가 편중되지 않도록 설계하여야 한다. 예를 들어 편중된 IDS 평가 데이터를 사용하여 높은 탐지율과 낮은 오 탐지율을 가지도록 IDS를 개선하면 시스템이 일반적인 환경에서 좋은 결과를 내지 못하는 경우가 발행할 수 있다. 따라서 훌륭한 IDS 평가 데이터는 개발되고 있는 IDS의 장점과 단점을 정확히 분석해 낼 수 있으며, 이를 통해 현재 시스템을 효과적으로 개선할 수 있게 하여야 한다. 또한 개발이 완료된 후 시스템 개발이 최종 목적에 부합되는지 객관적으로 판단할 수 있게 할 수 있어야 한다. 결국 좋은 IDS 평가 환경은 침입 탐지 시스템을 정확하게 평가할 수 있도록 객관적이고 보편화된 평가 데이터를 설계하는 일이 매우 중요하며, 평가 데이터가 침입 탐지 시스템의 핵심 기술을 잘 드러낼 수 있으며 목적에 부합되는 보안 문제를 해결할 수 있도록 일반성을 잃어버리지 않아야 한다.

2. Web IDS 평가를 위한 테스트 환경

이 장에서는 웹 IDS 평가를 위한 환경을 알아보자. 침입 탐지 시스템의 평가 프로세스는 평가하기 위한 공격 데이터와 정상 데이터를 수집하고 알고리즘의 성능 평가를 수행한 후 알고리즘을 개선하는 과정을 반복적으로 수행하게 되며, 만족할 수 있는 성능이 나올 때까지 위

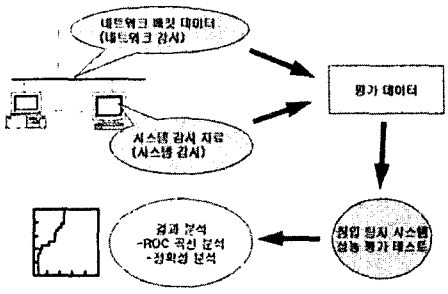

그림 1 IDS 평가 프로세스

과정을 반복하게 된다. 공격 데이터와 정상 데이터는 주로 네트워크 레벨의 패킷 데이터나 시스템 레벨의 감사 자료를 수집해 사용한다. 또한 웹 IDS의 평가를 위해 웹 서비스를 요청하는 URI(Uniform Resource Identifier)들을 수집하여 데이터로 사용할 수 있다. 본 연구에서는 네트워크 레벨에서 웹 서비스 요청 URI들을 수집하여 평가 데이터로 사용하였다.

침입 탐지 시스템이 정상적인 웹 서비스 요청을 공격으로 탐지할 수 있는 오 탐지율(false positive rate)을 측정하기 위해서는 정상적인 웹 서비스 요청 데이터를 수집하여 IDS의 평가 데이터로 사용해야 한다. 그림 2는 대량의 실제 웹 서비스 요청 URI들을 정상 데이터로 수집할 수 있는 환경을 보여준다. TCP replay에 의해 저장된 데이터 집합은 정상적인 웹 서비스 요청들로 이루어져 있음을 확인해야 하며, 관리자에 의해 웹 공격 데이터는 제거되어야 한다. 정상 데이터 수집은 100Mbps 이더넷 환경에서 포트 미러링(port mirroring)을 사용하였으며, 실험의 정확성을 위해 실제 사용 중인 인터넷 쇼핑몰과 학교 기관의 웹 서비스 요청 URI 데이터를 수집하였다. 이를 위한 모듈은 네트워크 패킷에서 웹 요청 URI들을 추출하여 저장하고, 설정된 웹 서버의 IP로 저장된 URI들을 이용하여 웹 서비스 요청을 할 수 있도록 TCP replay를 수정하였다.

침입 탐지 시스템이 웹 공격을 탐지하는 탐지율(detection rate)과 공격을 탐지하지 못하는 오 탐지율(false negative rate)을 측정하기 위해서는 의미 있는 웹 공격 데이터를 사용해야 한다. 이 때 성능 평가를 위해 사용하는 웹 공격 데이터들은 IDS의 핵심 기술과 탐지

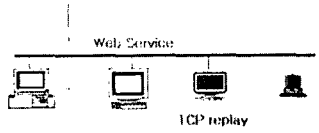

그림 2 정상 테스트 데이터 수집 환경

성능을 효과적으로 검증할 수 있도록 객관적이고 일반화된 데이터들로 이루어져야 한다. 그림 3은 웹 IDS 성능 평가를 위한 테스트 환경을 보여준다. 웹 IDS 평가 방법으로 ROC 분석 기법을 사용하고 평가 환경이 구축되었다면 가장 중요한 것은 적절한 웹 공격의 분류 기준에 따라 객관적인 웹 공격 데이터를 구성하는 것이다.

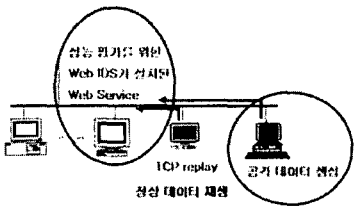

그림 3 Web IDS 평가를 위한 테스트 환경

3. 웹 공격 테스트 데이터

신뢰 있는 웹 IDS 평가 환경을 구축하기 위해서는 웹 공격 테스트에 대한 설계가 매우 중요하다. 표 1에서는 효과적인 웹 IDS 평가를 위해 웹 평가 공격 데이터를 네트워크 레벨의 웹 IDS에 대한 공격과 어플리케이션 레벨의 웹 서비스에 대한 공격으로 분류하였다.

표 1 웹 공격 테스트 데이터의 분류

어플리케이션 레벨	cgi 취약점 공격[7], 일반적인 웹 어플리케이션 취약점 공격[2, 3, 8]
네트워크 레벨	IDS 회피/삽입 공격, IDS DoS 공격

3.1 웹 IDS 회피(insertion) 공격

먼저 네트워크 레벨에서 웹 IDS가 회피(evasion) 공격을 탐지할 수 있는지 평가하며, cgi 스캐닝 공격 데이터 중 한 개를 임의로 선택하여 아래와 같이 HTTP 공격 패킷을 생성하여 테스트 한다.

- 8byte와 1byte 단위로 순서가 있도록 패킷을 분리
- 8byte와 1byte 단위로 순서가 없도록 패킷을 분리
- 8byte와 1byte 단위로 순서가 없도록 패킷을 분리하고 각각의 조각이 중복되도록 패킷을 생성

3.2 웹 IDS 삽입(insertion) 공격

이 공격을 통해 웹 IDS가 삽입(insertion) 공격을 탐지할 수 있는 지 평가하며, cgi 스캐닝 공격 데이터 중 한 개를 임의로 선택하여 아래와 같이 HTTP 공격 패킷을 생성하여 테스트 한다.

- 8byte와 1byte 단위로 순서대로 패킷을 분리하고 다

른 내용의 조각이 같은 순서에 중복되도록 패킷 생성
- 8byte와 1byte 단위로 순서 없이 패킷을 분리하고 다른 내용의 조각이 같은 순서에 중복되도록 패킷 생성

3.3 cgi 스캐닝 공격

대표적인 cgi 취약점을 이용하며, 이 공격은 whisker (웹 스캐닝 툴)에 포함되어 있는 공격들이다[7].

- URL encoding
- Directory insertion
- Premature URL ending
- Long URL
- Fake parameter
- TAB separation
- Case sensitivity
- Windows '₩' delimiter
- Session splicing

3.4 일반적인 웹 어플리케이션 취약점 공격

이 공격들은 일반적인 웹 서비스에서 자주 발생하는 취약점들로 웹 어플리케이션과 웹 서비스 컨텐츠에 따라 공격 방법이 다양하게 존재한다[2, 3, 8]. 따라서 이 공격들을 테스트 하기위해 가상의 취약점이 존재하는 웹 서비스를 가정하고 일련의 공격 데이터들을 구성하여 데이터베이스화 하였고, 평가하고자 하는 웹 IDS의 특징과 운용하고자 하는 웹 서비스의 특징에 따라 유연하게 사용할 수 있도록 구성하였다. 이 취약점을 이용한 웹 공격 테스트 방법들은 아래와 같다.

- 입력 값 검증 부재 공격
- 취약한 접근 통제 공격
- 취약한 인증 및 세션 관리 공격
- 크로스 사이트 스크립팅 취약점 공격
- 버퍼 오버플로우 공격
- 삽입 취약점 공격
- 부적절한 에러 처리 공격
- 취약한 정보 저장 방식 공격
- 서비스 방해 공격
- 부적절한 환경 설정 공격

3.5 웹 IDS DoS 공격

웹 IDS가 공격 탐지를 위해 사용하는 리소스가 한계를 넘어서면 웹 IDS는 더 이상 공격 탐지를 하지 못하고 마비되는 현상이 나타난다. 이 평가를 통해 웹 IDS가 사용될 수 있는 네트워크 환경을 평가할 수 있다.

- 매초 200개의 새로운 웹 연결을 시도하는 100byte의 웹 공격 패킷 생성
- 위 공격을 매 초당 10개씩 늘려가며 패킷 손실이 발생할 때까지 테스트
- 위 공격에서 패킷 크기를 100byte씩 늘려가며 패킷 손실이 발생할 때까지 테스트

4. 결론

침입 탐지 시스템을 평가하는 것은 침입 탐지 시스템을 연구하고 개발하는 것과 매우 밀접한 관계가 있다. 개발된 침입 탐지 시스템이 효과적이라는 것을 검증하기 위해서는 실제 공격을 가지고 해당 시스템을 테스트하는 것이 가장 쉽고 효과적인 방법이다. 하지만 평가 데이터들을 평가하기 위한 표준화된 비교 측정 기준이 없으며, 개인이나 기업, 조직의 중요한 정보 유출 문제로 인해 침입 탐지 시스템이 사용될 실제 현장 데이터를 수집하는 것이 쉽지 않기 때문에 보편적인 평가 데이터를 수집하는 것은 매우 어려운 일이다. 본 연구에서는 앞으로 연구되고 설계될 웹 서비스에 특화된 침입 탐지 시스템을 평가하고 검증하기 위한 테스트 환경을 소개하였고, 이 환경을 통하여 개발된 어플리케이션 침입 탐지 시스템의 테스트와 성능 향상을 위하여 노력할 수 있는 환경 구축이 이루어 졌다.

5. 참고 문헌

[1] 2002 CSI/FBI computer crime and security survey, Computer Security Institute and Federal Bureau of Investigation, Computer Security Issues and Trends 8(1), 2002.

[2] J.S. Seo, H.S. Kim, S.H. Cho and S.D. Cha, "Attack Categorization based on Web Application Analysis", Jounal of KISS: Information Networking, Vol. 30, No. 1, Feb. 2003.

[3] J.S. Seo, H.S. Kim, S.H. Cho and S.D. Cha, "Web Server Attack Categorization based on Root Causes and Their Locations", IEEE Information Assurance and Security (IAS 2004), Apr. 2004.

[4] S.H. Cho and S.D. Cha, "SAD: Web Session Anomaly Detection based on Parameter Estimation", Computers and Security, Vol. 23, No. 4, June 2004.

[5] Puketza N., Chung M., Olsson R.O., and Mukherjee B., "A Software Platform for Testing IDS", IEEE Software, Vol. 14, No. 5, 1997.

[6] Lippmann R.P., etc., "Evaluating IDSs: The 1999 DARPA OffLine Intrusion Detection Evaluation", Computer Networks, Vol. 34, No. 2, 2000.

[7] Rain Forest Puppy, A look at whisker's anti-IDS tactics, http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html

[8] The Open Web Application Security Project, Top Ten Most Critical Web Application Security Vulnerabilities, January 2004.