실시간 로그를 통한 지능형 웹 서버 침입 탐지 시스템에 대한 연구

선준호
고려대학교 컴퓨터정보통신대학원 미디어공학과
e-mail:korealover@empal.com

Real-Time Intellectual Invasion Detection Systems Using Log

Jun-Ho Sun
Dept. of Media Engineering.
Gradute School of Computer Infomation and Communications,
Korea University

요 약

웹 어플리케이션의 프로그래밍 오류를 이용한 침입이 대부분의 공격 수단으로 이용되고 있다. 본 논문에서는 웹 어플리케이션의 동작으로 인한 취약점을 분석 후 기계학습 기법을 이용하여 웹 해킹 공격 패턴을 비교, 분석하며 새로운 공격시도를 학습하는 지능형 침입 탐지 시스템 모델을 제안한다.

1. 서론

인터넷의 발달로 해킹의 공격의 유형도 변화하고 있다. 전통적인 공격(traditional attack) 방식은 주로 운영체제나 네트워크구조를 숙지하고 있어야 가능한 수준으로 시스템의 취약점을 찾아내는 것이 어려워 사회 공학(Social Engineering)과 같이 시스템이나 네트워크 관리자를 속여 중요 정보를 획득하는 것이 주요 기법이었다. 본 논문은 제안모델을 설계하고 구현한 과정에 대해 설명하고, 본 연구의 결론과 향후 과제에 대하여 기술한다.

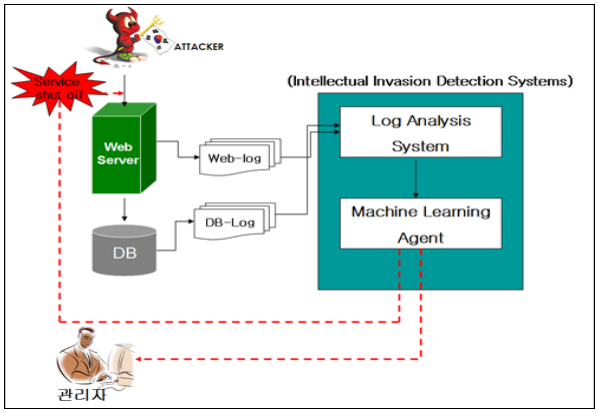
2. 제안 모델

2-1. 연구 배경

해마다 정보보호진흥원에서는 웹 해킹의 변화와 보안대책에 대한 자료를 배포하고 있지만 근본적으로 웹 어플리케이션 개발자 및 시스템관리자들의 보안에 대한 인식이 없이 기존의 개발 툴이나 습관에 의존하여 웹 어플리케이션을 제작하기 때문에 항상 취약점에 노출되어 있다. 이러한 웹 상에서 발생하는 여러 취약점들을 바탕으로 기존의 방화벽이나 IDS에 의존하던 방식에서 벗어나 웹 서버 전용의 실시간 Agent를 도입한 효과적인 지능형 침입 탐지 시스템을 제안하고자 한다.

2-2. 제안 모델의 구조

본 논문에서 제안하는 지능형 침입 탐지 시스템은 모델은 다음과 같다.



(그림 1) 지능형 침입 탐지 시스템

(그림 1)에서는 웹 공격(Attack)에 대응하는 프로세스를 보여주고 있다.

- **Log Analysis System:** 클라이언트로부터 접속 요청이 발생할 때마다 실시간으로 모아진 웹 로그와 데이터베이스 로그 정보를 Machine Learning Agent가 공격인지 아닌지를 결정할 수 있도록 로그 데이터를 가공하는 시스템이다.
- **Machine Learning Agent:** Log Analysis System에서 가공 되어진 데이터를 웹 공격인지 정상적인 접근 인지를 분류(Classification)하고 결정한다. 또한 새로운 웹 공격이 발생할 경우 새로운 공격행태에 대해 학습을 한다. 이는 기존의 침입 탐지 시스템이 공격형태의 룰(Rule)을 가지고 패턴을 비교 하는 방식과는 차별화된 에이전트(Agent)이다. 웹 공격이라는 결정을 내리게 되면 관리자에게 통보

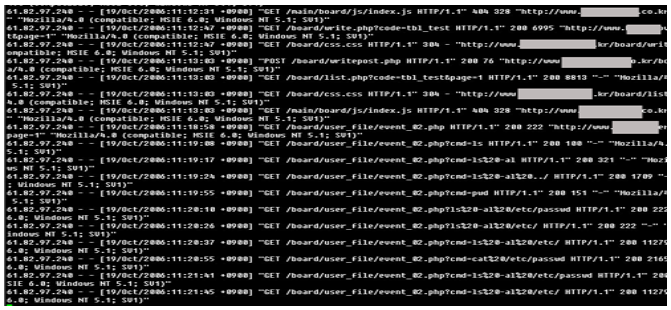
하게 되며 웹 공격을 시도한 공격자에게는 웹 서비스를 차단하게 된다.

2-3. 제안 모델의 장・단점

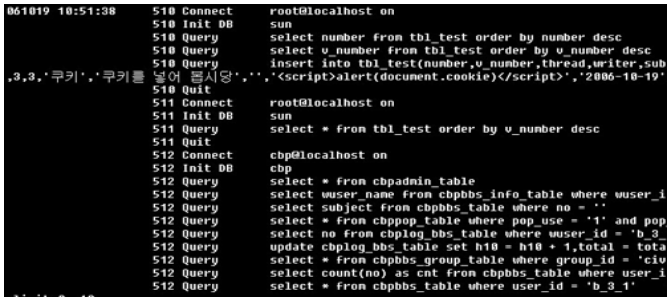
본 논문에서 제안한 에이전트(Agent) 모델은 침입이 이루어진 후에 로그 분석을 통해 실시간으로 판단하고 대처하는 방식으로 공격자가 남긴 로그 분석을 토대로 Machine Learning Agent가 즉각적인 의사결정이 가능하기 때문에 침입 탐지율이 높은 웹 서버 보안이 가능하다. 또한 기존에 연구 되었던 웹 로그를 통한 웹 서버 보안 연구 보다 다양한 공격행태도 대처할 수 있다. 기존 연구가 웹 로그에의 특정 패턴만을 데이터 마이닝하는 반면 본 논문은 웹 로그의 특정 패턴 뿐 만이 아니라 SQL Injection, XSS(Cross Site Script), Parameter Manipulation(파라미터 변조), User CGI Upload(사용자 CGI 업로드) 등의 공격 탐지도 가능하다. 그렇지만 접속자가 많은 대용량 서버의 경우 초당 몇 백 메가바이트의 로그가 기록되므로 실시간으로 로그를 분석하기에는 고성능의 하드웨어가 필요하며 이에 따라 다른 프로세스에 과부화 문제가 발생 할 수 있다.

3. 사례연구

(그림2)은 공격자가 프로그래밍 오류중의 하나인 파일 업로드 버그가 있는 게시판에 침입한 후 정보 수집을 위해 몇몇 시스템 명령어를 실행했을 때 웹 로그에 나타난 기록을 포착한 것이며, (그림3)은 DB 로그의 기록에서 html을 허용한 게시판에 XSS(Cross Site Script) 공격을 포착한 것이다.



(그림 2)시스템 명령어 사용한 웹 로그 기록



(그림 3) XSS(Cross Site Script) 공격을 포착

(그림3)에서와 같이 데이터베이스 로그는 XSS 공격뿐만 아니라 SQL Injection 탐지도 가능하다.

4. 결론 및 향후 과제

본 논문에서는 실시간으로 웹 로그와 데이터베이스 로그를 통해 기계학습 기반의 지능형 침입 탐지 시스템을 제안하였다. 기존의 방화벽이나 침입 탐지 시스템(IDS)으로는 실시간으로 이루어지는 웹 공격에 노출되어 있으므로 이를 해결하기 위해 웹 어플리케이션의 취약점을 분석하였다. 또한 웹 로그와 데이터베이스 로그를 분석하여 실시간 공격뿐만 아니라 새로운 공격에도 대비 할 수 있는 지능형 침입 탐지 시스템을 제안하였다. 본 논문에서 제안하는 방법을 확대하여 시스템의 로그 정보도 활용하여 웹 공격뿐만 아니라 다양한 공격 탐지를 위한 연구가 필요하다.

참고 문헌

[1] 황순일, 김광진, “웹 해킹 패턴과 대응”, 사이텍미디어, 2005

[2] 진홍태, 박종서, “웹 로그 마이닝을 통한 실시간 웹 서버 침입탐지”, 2004년도 한국정보과학회 봄 학술발표논문집 Vol.31, No.1

[3] 안정철, “시스템 로그분석”, 이비컴, 2005

[4] 정현철, “웹 해킹의 변화와 보안대책”, 한국정보보호진흥원, 2006

[5] 한은섭, 김명호 “웹 애플리케이션 취약성 정보를 제공하는 웹 서버 모니터링 시스템”, 한국정보과학회 2003년 추계학술대회

[6] 이재승, “웹어플리케이션 보안 기술 동향”, 한국전자통신연구원 정보보호연구단, 2005

[7] 김성열, 정수은, 박중길, 김상천, 한광택, “소스코드를 이용한 웹 응용 취약점 분석에 관한 연구”, 2003년도 한국정보보호학회 동계정보보호학술대회 논문집 Vol.13, No2

[8] 양대일, 김경곤 공저 “정보 보안 개론과 실습” 한빛미디어, 2007