웹 로그 데이터셋을 이용한 침입 상태 시각화 방안에 관한 연구

이수영 구본현 조재익 조규형 문종섭

고려대학교 정보경영공학전문대학원

{leesuyoung1, koo191, chojaeik, mathbank, jsmoon}@korea.ac.kr

Research on Intrusion Detection Visualization using Web Log Data set

Suyoung Lee Bonhyun Koo Jaeik Cho Kyuhyung Cho Jongsub Moon

Graduate School of Information Management and Security

요약

최근 인터넷 사용이 폭발적으로 증가함과 더불어 웹 어플리케이션에 대한 다양한 공격이 발생하고 있다 . 이런 다양한 웹 공격에 대해 방어를 위해서는 효율적인 침입탐지가 가능하여야 하며, 이상행위에 대해 신속하고 적절한 정보전달이 필요하다. 다양한 보안 이벤트들에 대한 시각화 시스템은 이를 만족시켜주는 수단이다. 본 논문에서는 선행 연구였던 웹 공격 기법에 대해 분석해보고 시각화 기법을 살펴본 후, 이를 개선하여 기존 시각화 기법으로는 표현하지 못했던 웹 로그 데이터셋에 기초한 웹 이상행위의 시각화기법을 제안한다. 웹 침입탐지 시각화 시스템을 바탕으로 다양한 웹 공격에 대한 시각화 실험결과를 제시한다.

1. 서론

DoS/DDoS와 같이 네트워크를 파괴시키는 공격은 크게 줄어들고 있다. 그러나 OWASP 10대 취약점 공격기법에 정의된 SQL-Injection, Cross-Site-Scripting(XSS) 등을 통해 웹 어플리케이션 공격이 급증하고 있다[1]. 일반적인 보안도구를 통한 분석 작업에 있어서 실시간으로 네트워크 상황을 알 수 있는 도구가 필요하다[2]. 보안도구의 효율적인 운용과 네트워크 보안상황을 인식하기 위한 기술로서 실시간 시각화 기술이 많이 연구되어왔다[3, 4, 5]. 보안 이벤트의 시각화를 통해 얻을 수 있는 장점은 다음과 같은 요소들이 있다. 첫째, 호스트 OS들은 시각화 인식에 의해 식별되어질 수 있다. 둘째, 기존(오용방식) 침입 탐지 시스템에서는 찾지 못하는 일부 공격들에 대해서도 시각화를 통해 식별이 가능하다. 셋째, 시각화기술은 적은 시간이나 상태만으로도 충분이 정보의 표현이 가능하다. 넷째, 오용방식에서의 탐지하지 못하는 Zero-day 공격을 시각화를 통해 나타낼 수 있다. 끝으로, 분산 스캐닝 혹은 슬로우 스캔 공격 식별이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 침입탐지관련 연구를 소개한다. 3장에서는 본 논문에서 제안하는 시각화 설계 내용을 살펴보며, 끝으로 4장에서는 결론을 맺도록 한다.

2. 관련 연구

이번 절에서는 웹 어플리케이션과 어플리케이션 서버에게 가장 취약한 부분과 공격 기법들을 살펴보고, 본 논문에서 초점을 맞추고 있는 시각화 기법에 관한 기존 연구들을 알아볼 것이다.

가. 웹 공격 기법 분석

정보보호 관점에서 웹 응용 제품의 침투 기법에 대한 시험 및 검증은 네트워크기반의 보안제품 및 취약점 분석을 통해 이루어지지 못했다. 이 논문에서는 이를 반영하므로 적합한 방법의 시각화를 위해 공격기법을 살펴보고자 한다. 공격 기법에는 관리자의 잘못된 설정과 개발자가 작성한 취약성을 가지는 코드 그리고 사용자의 부주의 때문에 발생 할 수 있다. 따라서 어떤 공격기법이 존재하는지 조사해보고 이 논문에는 이를 반영한 시각화 방법을 제안한다.

1) 입력 값 검증 부재

웹 어플리케이션은 응답하기 위해 입력 값으로 주로 HTTP 요청을 받아들인다. 공격자는 URL, 쿼리 문자열, HTTP 헤더, 쿠키, HTML 폼 인자, HTML 히든 필드 등 모든 HTTP 요청을 변조할 수 있으며, 이를 통해 사이트의 보안 메커니즘을 우회하고자 시도한다. 흔히 발생하는 입력 값 변조 공격은 URL 강제 접속, 명령어 삽입, 크로스 사이트 스크립팅, 버퍼 오버플로우, 포맷스트링 공격, SQL 구문 삽입, 쿠키 조작, 히든 필드 조작 등이 있다.

2) 취약한 인증 및 세션 관리

웹 어플리케이션은 개별 사용자들의 요청을 지속적으로 추적하기 위해 세션을 생성해야 한다. 하지만, HTTP 프로토콜은 연결 종속적 프로토콜이 아니기 때문에 세션에 관한 관리가 완벽 할 수 없다. 종종 웹 어플리케이션 환경이 세션 관련 기능을 제공함에도 불구하고, 많은 개발자들은 자체적으로 세션 토큰을 생성하여 사용하는 것을 선호한

다. 어느 경우든지 세션 토큰이 적절히 보호되지 않으면, 공격자가 현재 활성화된 사용자의 세션을 가로채 다른 사용자를 가장하여 접속할 수 있다.

3) 버퍼오버플로우

버퍼오버플로우 취약점은 개발자의 부주의 및 인식 부족으로의 응용프로그램 보안취약점중 하나이다. 프로그램에서 버퍼의 한계를 점검하지 않고 작성된 코드부분을 이용하여 악의적인 공격자 코드로 리턴 어드레스 등을 덮어쓰도록 한다. 그러므로 프로그램의 정상적인 동작을 변경하거나 프로그램이 다운되도록 하는 공격 방법이다. 버퍼오버플로우 취약점은 웹 서버 또는 웹 어플리케이션에 존재할 수 있다. 많이 사용되는 제품에 존재하는 버퍼오버플로우는 일반적으로 알려지게 되고 이로 인해 해당 제품의 사용자는 상당한 위험에 노출되게 된다. 자체 제작한 웹 어플리케이션의 경우 검증 부재 문제로 인해 버퍼오버플로우가 발생할 확률이 상대적으로 높다. 버퍼오버플로우의 취약점으로부터 시스템을 보호하기 위해서 개발자는 항상 주의를 기울여야 한다.

4) 서비스거부공격

정보시스템의 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 행위이다. 이는 주로 시스템에 과도한 부하를 일으켜 정보 시스템의 사용을 방해한다. 한 사용자가 시스템의 리소스를 독점하거나 모두 사용, 또는 파괴함으로써 다른 사용자들이 서비스를 올바르게 사용할 수 없도록 만드는 것을 말하며, 시스템의 정상적인 수행에 문제를 일으키는 모든 행위를 DoS라 할 수 있다. DoS 공격은 크게 Denial of Service(DoS), Distributed Denial of Service(DDoS), Distributed Reflection Denial of Service(DrDoS)로 나눌 수 있다. 세 가지 모두 서비스 거부 공격이며, 공격방법에 따라 차이를 보인다. 2000년 2월 아마존, 이베이, 야후 등 포털 사이트들이 DoS의 변종인 DDoS의 공격을 받아 운영이 불가능한 사건이 발생하면서 일반인들에게 알려지기 시작했다.

나. 기존 시각화 기법 분석

이 장에서는 네트워크 및 웹 이상행위에 대한 기존 시각화 연구들에 대해서 알아본다. John.R.Goodall은 침입탐지에 절차를 감시, 분석, 대응 3단계로 나누었다[6]. 첫째, 감시과정은 트래픽이나 감시 대상을 지속적으로 주시한다. 그리고 정의된 이벤트 발생 시 다음 단계로 전달하는 과정이다. 둘째, 분석단계는 감시과정으로부터 전달된 이벤트 발생기준을 어떻게 정의하고, 처리할지에 대한 정의 단계이다. 셋째. 대응단계에서는 분석과정에서 발생한 침입 정보를 어떻게 전달하고, 대응할 것인지 정의를 내리는 단계이다. 분석과정에서의 정보를 효과적으로 전달하기 위한 방법으로, 시각화를 통한 정보 전달 방법이 가장 효과적이고, 신속한 방법이 될 수 있다. 이는 생태학적 구조상 사람은 직관적으로 시각적인 패턴을 가장 잘 인식하기 때문이다[8]. 표1는 네트워크 및 웹상의 이상행위 시각화에 대한 기존 연구들의 특징이다.

<표 1> 기존 시각화 도구의 특징 비교

도 구	특 징	단 점
TNV [1]	시간에기반한 이상행위의 감시	장기간의 트래픽 수집이 요구됨.
VisAlert [2]	동심원을 이용한 오용탐지 시각화 표현	Snort 탐지 룰에 대한 시각화에 대한 국소적인 단점
PVF [3]	X,Y축을 이용한 이상 Port, IP의 시각화	1차원 데이터의 표현만으로 시각화를 구성하고 있는 단점.
WebViz [4]	웹 페이지들과 사용자들의 이동 경로를 시각화	효율적이지 못한 레이아웃구조
SAD [5]	웹로그 분석을 통한 웹 서버의 이상행위 감시	웹 접근 로그 기반의 시스템

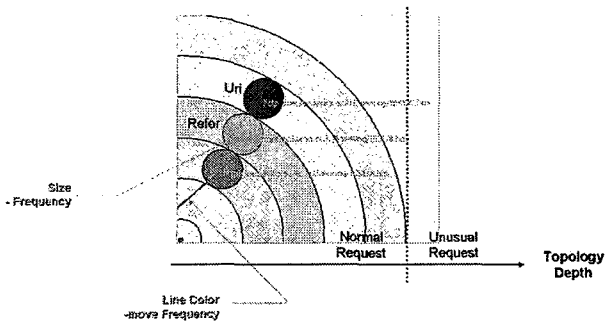
시각화에 사용되는 데이터의 측면에서 표1의 TNV를 제외한 나머지 도구들은 모두 웹 로그와 같은 감사파일에기반한 시각화 도구들이다. 이러한 로그파일에기반한 시스템은 로그파일의 보안상의 문제와 일정 시간이 경과한 다음에 시각화가 갱신되는 단점이 존재한다. TNV는 장기간의 시간이나 적어도 몇 시간 동안의 사용자들의 세션을 수집해야만 이상 행동에 대한 세션을 분석 및 확인할 수 있는 단점이 존재한다. 표1의 SAD에서 시도하였던 구조는 정적인 갱신과 이벤트의 중복 시각화로 인하여 감시 시간이 길어질수록 효율성이 크게 떨어지게 되었다[15].

3. 시각화 구현 및 실험

동심원 레이아웃 구조는 웹로그데이터 셋을 토폴로지상의 구조로 효과적으로 표현할 수 있는 레이아웃 구조이다[12]. 표 2는 제안하는 동심원 레이아웃 구조의 시각화 기준이며, 그림1는 이러한 정의 기준을 바탕으로 시각화를 표현한 인터페이스의 예시화면이다.

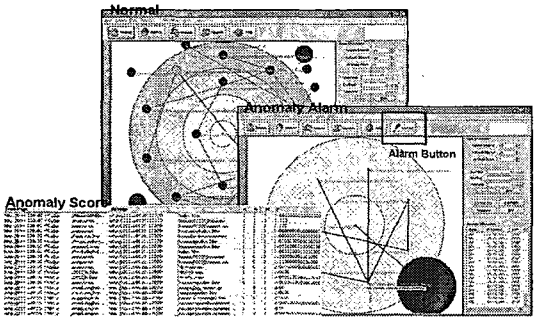
<표 2> 시각화 표현 기준 정의

Name	Method	Description
DC (Division Circle)	radius	웹 토폴로지 상의 깊이를 나타냄 (원의 외부는 존재하지 않는 요청을 표현)
RC (Request Circle)	color	정상과 비정상 여부와 최근의 요청을 표현 (이상탐지 알고리즘을 이용)
	size	HTTP Request에 대한 빈도수를 표현.
	degree	시간에 따른 순서를 표현. (상대좌표를 이용해 이벤트의 중복을 회피)
L_Line (Link Line)	color	Reffer와 Uri 사이의 정상관계 여부를 표현
	width	Reffer와 Uri 쌍의 빈도수를 표현



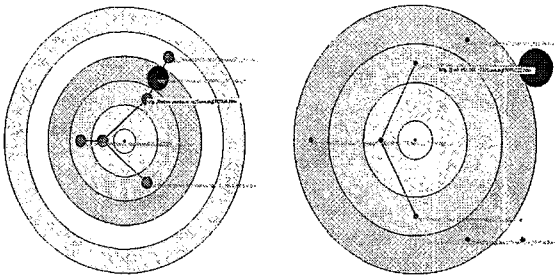
[그림 1] 동심원 인터페이스 시각화 구현 예시

시각화 기법의 기본적인 생각은 나무의 나이테 이다. Division Circle (DC)는 나이테와 같이 배경의 큰 원이다. 이것이 의미 하는 것은 웹 토폴로지 상의 깊이를 표현한다. 즉, DC 외부의 요청은 서버에 존재하지 않는 웹 페이지의 요청이다. 서버에 대한 페이지 요청 시 새로운 원 Request Circle(RC)이 생성되어진다. RC 의 색깔은 이 요청이 비정상적인지를 표현할 수 있으며, RC의 크기는 HTTP Request에 대한 빈도수를 나타낸다. 그리고 DC에 대한 RC의 상대 좌표를 이용해서 시간에 따른 순서를 표현 할 수 있다. 웹서버에 처음 접속 시에는 DC의 중심에 가깝지만, 세부 페이지로 내려 갈수록 분할 원의 바깥쪽에 위치한다. Link Line은 색깔과 폭으로 표현을 했으며 의미하는 바는 Reffer 와 URI 사이의 정상 관계 여부, 그리고 Reffer와 URI 쌍의 빈도수를 표현한다. 사용자의 행위가 비정상적인 것으로 판단될 경우, RC가 이상 색상으로 바뀌며, 경고 알람기능을 활성화되어 이상을 전달한다.



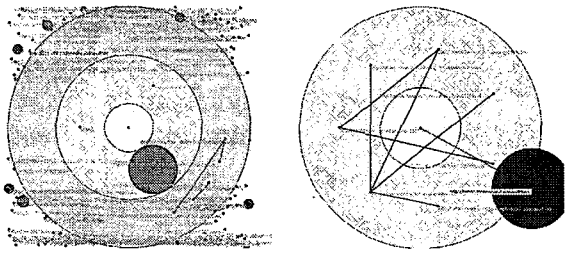
[그림 2] 시각화 인터페이스

그림3은 이러한 정상적인 시각화와 비정상 시각화 인터페이스를 보여주고 있다. 위의 그림은 정상적인 사용자 패턴의 그림으로 일반적으로 내부에 RC가 나타나게 된다. 그림 3(우)는 웹 토폴로지 내에 존재하지 않는 요청이 발생하였을 때, 혹은 오용탐지 룰에 존재하는 요청이 발생하였을 때, 분할원의 외부에 요청원이 생성되는 것을 확인할 수 있다. 본 논문의 시각화 방법에서는 침입 상태를 확인하기위해 오용탐지 기법인 Snort의 탐지 룰의 웹 공격 패턴과 이상 패킷을 DB화 하였다. 또한, 감시 프로세스로부터 받은 로그형식(*Log*)의 데이터 중 PostQuery와 UriQuery필드를 비교 하여 오용 탐지를 시각화 한다. 만약 공격패턴 DB로부터 일치되는 Query가 탐지되었을 때는, 그림3(좌)의 그림처럼 비정상의 시각화를 보여준다.



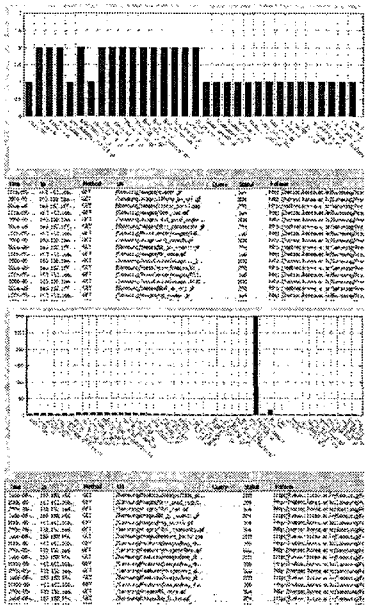
[그림3] 정상(좌)과 비정상 시각화(우)

공격실험을 하기위해 본 논문에서는 현재 가장 많이 사용되는 Nikto, BrutusAET2, Code Red 의 시각화를 제시한다. Nikto는 웹 서버와 어플리케이션에 대해 취약점을 찾아내는 웹 스캐너 도구이다[13]. Nikto 웹 스캐너를 이용한 공격 테스트 결과는 다음 그림 4(좌)의 그림과 같다. Normal인 경우는 대부분의 RC가 동심원의 내부에 위치한 것을 확인할 수 있는 반면, 스캐너를 통한 웹 어플리케이션을 스캔 시에는 대부분 존재하지 않는 페이지나 cgi관련 취약점을 확인함으로써, 동심원의 내부에 RC가 많이 분포하는 것을 확인할 수 있다. BrutusAET2는 사전파일을 이용하여, 인증 폼에 패스워드를 무작위로 대입하여 로그인을 시도하는 패스워드 해킹도구이다14]. 사전파일의 내용을 무차별로 대입하여 일치하는 값을 찾아낸다. 공격 시도에 대한 탐지화면은 그림4(우)와 같다. 그림 좌측의 정상적인 패턴에 비해 우측의 공격패턴은 분할 원 외부의 존재하지 않는 페이지 요청을 확인할 수 있다.



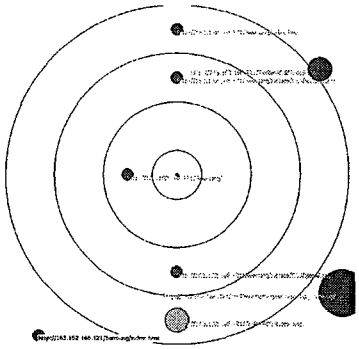
[그림 4] Nikto 웹취약점 스캔공격(좌)과 패스워드 무차별 대입공격 시각화(우)

공격 발생 시 그림 4(우)과 같이 정상 RC들이 상대적으로 매우 작아지고, 공격 RC가 급격하게 높은 비율을 차지하는 것을 확인할 수 있다. 공격 탐지시의 그림 5의 빈도확인 그래프는 공격 페이지가 다른 빈도들에 비해 상대적으로 급격하게 증가함을 확인 할 수 있다. 빈도수가 늘어날수록 그래프의 효율적인 표현을 위해 상대적으로 다른 페이지들의 크기는 줄어들도록 구현 하였다. 리스트 테이블에서는 대입되는 공격 문자열을 출력하여, 어떠한 문자열들을 대입하여 공격하는지 실시간으로 확인할 수 있도록 구성하였다.



[그림 5] 정상적인 패턴(상)과
패스워드 무차별 대입공격 빈도 그래프(하)

Code Red는 Windows 인덱스 서비스의 .ida 취약점을 이용하여 확산되며, 80번 포트(HTTP)를 이용하여 전파된다. 그 피해증상은 Windows 운영체제의 언어버전에 따라 다르게 나타나며, 한글버전인 경우 홈페이지 화면이 변경되지 않아 피해를 입고도 탐지를 하지 못하고 있는 경우가 많다. Code Red는 기존의 웜이나 바이러스처럼 특정 파일이 복사되는 형태가 아닌 메모리에 상주하는 형태로 감염된다. 그림 5은 코드레드 웜 공격에 대한 탐지 화면을 시각화를 통해 표현한 화면이다. 동심원 외부에 비정상적인 접근이 탐지되었고, HTTP의 메서드인 POST 쿼리 문자열로 나타내며, 그림6 과 같이 Code Red의 접근로그가 탐지되었음을 확인할 수 있다.



[그림 6] 코드레드 웜 공격 시각화

4. 결론

시각화 시스템은 보안 도구 관리자들에게 보다 빠르고, 이해하기 편리한 정보 전달 도구이다. 제안한 시각화 기법을 검증하기위해 실험을 통해 패스워드 무차별 대입공격, 웹 스캔 공격 등에 대해 어떻게 시각화 할 수 있는지 인터페이스 결과 화면을 보였다. 또한 일반적인 관리자가 다루는 로그 기반의 분석은 많은 텍스트의 분석으로 인하여 오용에 대한 탐지에 어려움이 크다. 시각화에서는 보다 편리하고 직관적으로 로그를 분석하고 인식할 수 있도록 설계 되었으며, 단순 텍스트 기반의 분석에 나타나지 않으며 분석하기 힘든 웹 토폴로지의 의미 있는 상태를 나타낼 수 있었다. 특히, 일반적이지 않은 공격을 인식하기 위해 본 논문의 시각화에서는 일반적으로 쉽게 인식하는 동심원구조로 표현 했으며 이는 사람의 인지과정에 시각적으로 매우 효과적이다. 하지만 차후 연구에서는 동심원의 거리에 더욱 의미를 부여해서 연구를 진행하고 아울러 표현해야할 데이터가 많아질 경우 생길 수 있는 중복 현상을 단편화와 웹 토폴로지의 의미를 부여하는 방안에 중점을 두어 야 할 것이다.

5. 참고 문헌

[1]Eugene Lebanidze, "Securing Enterprise Web Applications at the Source: An Application Security Perspective", OWASP Tech. Report, 2004

[2]J. McHugh, "Intrusion and intrusion detection," International Journal of Information Security, vol. 1, pp. 14-35, 2001

[3] M. Stolze, R. Pawlitzek, and A. Wespi, "Visual Problem-Solving Support for New Event Triage in Centralized Network Security Monitoring:Challenges, Tools and Benefits," GI-SIDAR Conf. ITIncident Management & IT-Forensics (IMF), 2003.

[4]R. Ball, G. A. Fink, and C. North, "Home-Centric Visualization of Network Traffic for Security Administration," ACM Workshop Visualization and Data Mining for Computer Security (VizSEC/DMSEC), pp. 55-64., 2004

[5]L. Girardin and D. Brodbeck, "A Visual Approach for Monitoring Logs," Proc. 12th Systems Admin. Conference (LISA), 1998, pp. 299-308.

[6]John R. Goodall, "User Requirements and Design of a Visualization for Intrusion Detection Analysis", IEEE Workshop on Information Assurance and Security, 2005

[7]Y. Livnat, J. Agutter, S. Moon, R.F. Erbacher, S. Foresti, "A Visualization Paradigm for Network Intrusion Detection", IEEE Workshop on Information Assurance and Security, pp17-19, 2002

[8]W. Yurcik, J. Barlow, K. Lakkaraju, and M.Haberman, "Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements," ACM CHI Workshop HCI and Security Systems HCISEC), 2003.

[9]The World Wide Web Consortium, http://www.w3.org/Protocols/rfc2616/rfc2616.html

[10]W3C Extended Log File Format, http://www.w3.org/TR/WD-logfile.html

[11]N. Friedman and Y. Singer. Efficient bayesian parameter estimation in large discrete domains, 1999

[12]B.H. Lee, S.H. Cho, S.D. Cha,"Real-Time Visualization of Web Usage Patterns and Anomalous Sessions", KIISC, Vol.14. no.4., p.97-110,2004

[13]Nikto-Web Scanner, http://www.cirt.net/code/nikto.shtml

[14]BrutusAET2-Password Cracking Tool, http://packetstorm.troop218.org/Win/index2.html

[15]Sang-hyun Sho Han-sung Kim Byung-hee Lee Sung-deok Cha, SAD:Web Session Anomaly Detection based on Bayesian Estimation , , 2003