韓國컴퓨터情報學會 論文誌
第16卷 第1號, 2011. 1.

2011-16-1-3-4

HTTP Outbound Traffic 감시를 통한 웹 공격의 효율적 탐지 기법

최 병 하*, 최 승 교**, 조 경 산***

An Efficient Detecting Scheme of Web-based Attacks through Monitoring HTTP Outbound Traffics

Byungha Choi*, Sung-kyo Choi**, Kyungsan Cho***

요 약

웹 기반 공격에 대한 대응책으로 계층적 웹 보안 시스템이 있지만 다양한 혼합 및 우회 공격에는 제대로 대응하지 못하는 실정이다. 본 논문은 웹 공격에 의해 발생하는 악성코드 유포, XSS, 웹쉘 생성, URL Spoofing, 개인정보유출 등의 증상을 HTTP outbound traffic의 감시를 통해 실시간으로 탐지하는 효율적인 기법을 제안한다. 제안 기법은 다양한 웹 공격에 의해 생성되는 HTML 태그와 Javascript 코드를 분석하여 설정한 시그너처를 outbound traffic과 비교 검색하여 웹 공격을 탐지한다. 실제 침입 환경에서의 검증 분석을 통해, 계층적 보안 시스템과 결합된 제안기법이 우회된 웹 공격에 대한 탐지능력이 탁월함을 보인다.

▸ Keyword : 웹 공격, Outbound Traffic, 탐지, 시그너처, 우회 공격

Abstract

A hierarchical Web Security System, which is a solution to various web-based attacks, seemingly is not able to keep up with the improvement of detoured or compound attacks. In this paper, we suggest an efficient detecting scheme for web-based attacks like Malware, XSS, Creating Webshell, URL Spoofing, and Exposing Private Information through monitoring HTTP outbound traffics in real time. Our proposed scheme detects web-based attacks by comparing the outbound traffics with the signatures of HTML tag or Javascript created by the attacks. Through the verification analysis under the real-attacked environment, we show that our scheme installed in a hierarchical web security system has superior detection capability for detoured web-based attacks.

▸ Keyword : Web-based Attacks, Outbound Traffic, Detection, Signature, Detoured Attack

• 제1저자 : 최병하 교신저자 : 조경산
• 투고일 : 2010. 09. 30, 심사일 : 2010. 10. 08, 게재확정일 : 2010. 10. 25.
* 단국대학교 대학원(Graduate School, Dankook University)
** 강원대학교 컴퓨터공학과(Dept. of Computer Engr., Kangwon University)
*** 단국대학교 컴퓨터학부(Div. of Computer, Dankook University)

Ⅰ. 서 론

다른 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 침해행위인 해킹은 시대별로 대상과 방식이 진화하였다. 80년대의 패스워드를 찾아 시스템의 취약점을 공격하는 기법에서, 90년대에는 네트워크를 사용한 공격 기법으로 변화하였다. 즉, 원격 사이트에서 OS의 취약 데몬 프로그램에 대한 공격과 TCP/IP 모델의 특성을 이용한 공격이 주를 이루었다. 2000년대에는 시스템 자체보다는 시스템이 제공하는 서비스를 공격하는 기법으로 발전하였다[1].

한국 인터넷 진흥원에 의하면 웜과 공격자에 의한 단순침입시도에 이어, 다양한 공격 기법으로 지속적인 증가를 보이는 웹 공격의 일종인 “홈페이지 변조”가 인터넷 공격의 주요 유형이다[2]. 이 유형의 공격으로 침입에 성공한 공격자는 침입 흔적과 이상 증상을 삭제하여 서버 관리자가 침해를 인지 못하고 계속 방치하게 함으로써, 웹서버에 접근한 다수의 사용자 컴퓨터에 악성코드 감염과 XSS에 의한 정보 유출 같은 비정상적인 증상을 일으킨다.

이들의 대응책으로 계층적 웹 보안 시스템이 제시되었지만, 이들 보안 시스템을 우회하는 새로운 공격 기법이 개발되어 기존의 웹 보안 시스템과 탐지 및 차단기법으로는 이들을 해결하기 어렵다. 결국 이들 공격의 탐지 및 차단 실패로 웹페이지 및 DB 변조로 이어지고 비정상적인 증상이 웹 서버가 출력하는 HTML(Hyper Text Markup Language) 문서에 Outbound Traffic을 통해 사용자 컴퓨터에게 전달되는 것으로 분석된다.

본 논문은 이러한 분석을 기반으로 HTML문서에서 비정상적인 증상을 일으키는 Javascript 코드 또는 HTML 태그 등을 시그너처로 설정하고, 침입 탐지 시스템에 정의된 규칙으로 설치한 후에, 웹서버의 HTTP outbound Traffic을 감시하여 공격의 침해 여부와 접속한 사용자에 전파되는 피해를 탐지할 수 있는 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장은 관련연구로 웹의 취약점 및 이를 방어하기 위한 계층적 웹 보안 시스템과 공격 탐지 및 차단 기법을 제시한다. 3장에서는 2장의 분석에 기반하여 우회 웹 공격과 그로 인한 피해 전파를 실시간으로 탐지하는 효율적인 기법을 제안한다. 4장에서는 제안 기법의 우회 공격에 대한 탐지 능력을 검증하고, 5장의 결론으로 본 논문을 마무리 짓는다.

Ⅱ. 관련연구

본장에서는 웹의 공격에 대한 취약점과 이를 방어하기 위한 기존의 탐지 및 차단 기법을 제시하고, 이들을 이용한 계층적 웹 보안 시스템을 분석한다.

1. 웹의 취약점 분석과 탐지 기법 관련 연구

웹 보안에 대한 연구와 결과에 권위가 있는 OWASP(the Open Web Application Security Project)에서는 웹의 대표적 취약점 10가지를 표 1과 같이 제시하였다[3]. 또한 국정원에서도 국내의 공격 기법과 공격 통계에 의거해 디렉토리 리스팅, 시스템 파일까지 노출되는 파일 다운로드 취약점, 크로스 사이트 스크립트 취약점, 악성파일에 대한 파일 업로드 취약점, 원격관리도구인 WebDav 취약점, 국내 공개 게시판인 테크노트, 제로보드 취약점, SQL Injection 취약점 등 8대 취약점을 제시하였다[4].

표 1. OWASP 웹 응용 프로그램 보안의 10가지 취약점
Table 1. OWASP TOP 10 Most Critical Web Application Security Risks

기법	내용	기법	내용
인젝션	질의문이나 명령문과 함께 악의적인 명령 입력	잘못된 보안 설정	응용 프로그램이나 프레임워크, 서버 등의 잘못된 설정으로 발생하는 취약점
XSS(1)	Script나 HTML 태그를 삽입하여, 웹 사이트를 손상시키거나 악성사이트로 이동	불안전한 암호화 저장	민감한 데이터를 암호화나 해싱으로 적절히 보호하지 못하여, 조작 또는 가로채기 함
취약한 인증 및 세션관리	비밀번호 또는 키 세션토큰을 가로채어 권한 및 계정 등의 정보 침해	URL 접속제한 실패	민감한 데이터의 URL을 노출
불완전한 직접 객체 참조	파일, 디렉토리 또는 DB 등이 노출됨	비효율적인 전송계층 보호	네트워크 트래픽의 무결성 보호 실패
CSRF(2)	인증 정보를 XSS 형태로 위조하여 HTTP요청을 하게 하여 주요정보 갈취	검증되지 않은 웹페이지 전송 또는 이동	검증 없이 다른 웹사이트로 전송 또는 이동
(1)크로스 사이트 스크립팅(Cross Site Scripting) (2)교차 사이트 위조 요청(Cross Site Request Forgery)			

따라서 이들 웹 공격을 탐지하고 차단하는 기법이 필요하게 되었고, 다음과 같은 기법들이 제시되었다.

첫째, 패킷의 송수신을 감시하며 페이로드에 관여하지 않는 규칙모음을 통해 접근을 통제하는 기법인 패킷 필터링과 응용 계층까지 감시하며 송수신되는 패킷을 동시에 추적하는 상태 기반 패킷 필터링 기법이 존재한다[5].

둘째, 웹 취약점과 네트워크의 유해트래픽에 대한 탐지 및 차단을 위해 인터넷, 트랜스포트, 응용 계층의 프로토콜을 분석하여 악의적인 행위에 대한 특정 패턴과 비교하는 시그너처 기반 탐지와 사용자 정보, 네트워크 트래픽 흐름, 애플리케이션 정보 등에 대한 정상행위의 모델과 비교하는 비정상 행위 기반 탐지가 제시되었다[6].

2. 계층적 웹 보안시스템 관련 연구

앞 절의 탐지 및 차단 기법에 대해 웹 공격은 취약점을 이용하는데 그치지 않고, 이들을 혼합하는 기법으로 발달하였다. 이의 대응책으로 다단계의 방어선을 구축하여 한 단계의 보안 시스템이 무너져도 다른 단계의 보안 시스템이 방어할 수 있는 다단계의 계층적 구조가 등장하였다[7].

그림 1. 계층적 웹 보안 시스템
Fig. 1. Hierarchical Web Security System

계층적 웹 보안 시스템은 일반적으로 그림 1과 같이 구성된다. 즉, 패킷 필터링과 상태기반 패킷 필터링 등으로 단순 침입 등을 방어하는 1단계의 방화벽, 시그너처와 비정상행위 기반 탐지기법으로 인터넷 계층에서 웹을 포함한 응용계층까지의 유해트래픽을 탐지하는 2단계의 침입 탐지 시스템, 그리고 패킷 필터링과 및 시그너처와 비정상행위 기반 탐지를 모두 사용하여 웹서버를 집중적으로 방어하는 3단계의 웹 방화벽으로 구성된다.

계층적 보안 시스템을 사용하여 보안 수준을 더 높이기 위해 여러 탐지 기법들을 보안 시스템에 분산 설치하여 서로 다른 시점에 적용할 수 있다. 즉 공격시점의 Inbound Traffic 감시, 침해여부를 탐지하기 위한 서버 시스템 감시, Outbound Traffic 감시의 3가지 유형이 적용될 수 있다[6].

보안시스템 관련 해외의 연구 사례는 다음과 같다.

보안 업체 등에 보고된 악성 URL 블랙리스트의 시그너처를 사용하여 악성 웹 페이지를 판단하는 기법을 구현한 Google의 안전 브라우징이 있다[8]. 또한 방화벽의 보안 수준을 높여 대부분의 취약점을 방화벽을 중심으로 방어하도록 외부의 HTTP 필터링 서버와 연동하여 HTTP Traffic을 감시하는 기법을 활용한 예로 Cisco 방화벽과 WebSense 필터링 서버가 있다[9]. 그리고 OWASP의 10가지 취약점에 대한 시그너처를 Mod Security 방화벽으로 사용될 수 있도록 OWASP에서 제공한다[10]

III. 효율적인 웹 공격 탐지 기법 제안

본 연구에서는 HTTP Outbound Traffic을 감시하여 계층적 웹 보안 시스템을 우회하는 공격 기법을 탐지하는 효율적인 기법을 제안한다.

1. 탐지 대상 선정과 제안 탐지 기법

계층적 웹 보안 시스템으로 보안 수준이 높아짐에 따라 직접 공격 보다는 그림2와 같이 보안 시스템을 우회하는 다양한 공격 기법이 등장하였다[11].

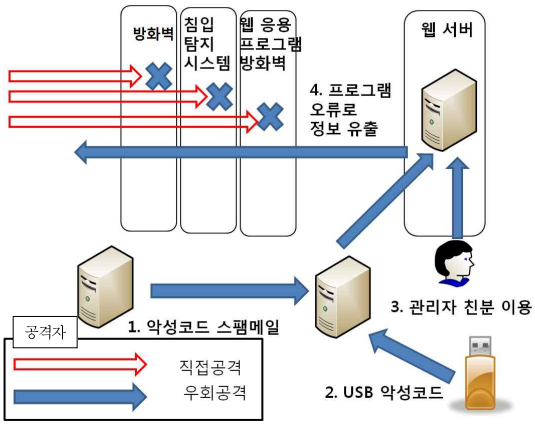

그림 2. 우회 공격기법
Fig. 2. Detoured Attacks

이들은 스팸메일의 악성코드 또는 USB의 악성코드를 이용해 원격의 관리자 컴퓨터에서 서버로 공격하거나, 관리자 친분을 이용하여 접근제어의 파악 후 공격 또는 웹서버 응용 프로그램의 프로그램 오류를 이용한 정보 유출 등이 있다.

이들 공격은 2장에서 제시된 대표적 웹 공격인 XSS와

Injection등의 대부분 취약점을 발생시키고, 또한 침입 성공 후 outbound traffic으로 악성코드 유포와 웹쉘로 인한 정보유출, XSS, 개인 정보 유출 등을 발생시킨다[3, 12].

따라서, 본 연구에서는 이러한 최근의 통계와 OWASP, 국정원에서 제시한 취약점을 고려하여 성공한 웹 공격 후 Outbound Traffic에 등장하는 웹 취약점으로 악성코드 유포, XSS(CSRF 포함), 웹쉘, URL Spoofing, 개인정보 유출의 5 유형을 탐지 대상으로 한다. 이들 탐지 대상의 공격은 Outbound Traffic으로 다수의 사용자에게 피해를 발생시키려는 목적과 다양한 정보유출을 위해 공격을 시도한다.

본 연구의 제안 기법은 어떤 경로로 침입할지 모르는 상황에서 시행된 우회 공격으로 DB나 웹 페이지가 악성으로 변조 또는 생성 되었을 때 외부로 유출되는 Outbound Traffic의 이상 증상을 검색하여 공격 여부를 탐지하는 기법이다.

본 제안 기법은 그림 3과 같이 웹 공격으로 침해받은 서버

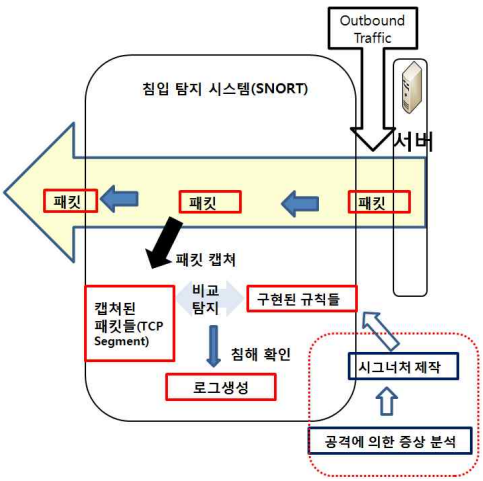

그림 3. 제안 기법의 동작
Fig. 3. Operation of the Proposed Scheme

가 HTTP로 유출하는 트래픽을 감시하여 침해를 탐지한다. 이를 위하여 웹 공격으로 침해된 서버가 유출하는 HTTP 트래픽에 포함되는 다양한 비정상적인 HTML 태그와 코드를 시그너처로 설정하고 이들을 실제 트래픽과 비교하여 침입 여부를 탐지하도록 한다. 또한, 탐지의 대상이 웹 서버에서 다양한 언어들로 구현된 DB의 정보와 프로그램들의 조합으로 실시간 출력하는 HTML 문서들이므로, 설정된 시그너처는 탐지 대상 시스템과 특정 프로그램 언어에 종속되지 않는다. 그러므로 제안 기법의 구현을 위해 이들 시그너처들을 침입 탐지 시스템 (본 연구에서는 Snort v2.8.6.1)에 적용되는 형식의 규칙으로 제작되어 설치된다.

본 제안 기법은 성공한 웹 공격 이후 외부로 5가지 탐지 대상이 유출되기 직전에 실시간으로 탐지하는 기법이므로, 웹 서버에 종속되지 않고 프로그램 언어와 운영체제에 독립적인 침입 탐지 시스템에 제안 기법을 설치하는 것이 적당하다. 이 때, 침입 탐지 시스템의 위치는 웹 서버와 방화벽인 게이트웨이 가까이 위치시켜 Outbound Traffic을 탐지하도록 한다. 즉, 서버로부터 유출되는 패킷 속의 비정상적인 HTML 태그나 Javascript 코드를 비교 탐지하여 본 연구의 대상인 5유형을 해당 시그너처가 발견되면, 로그 파일에 해당 규칙의 메시지와 함께 해당 패킷의 내용을 실시간으로 남기게 된다.

실제 본 연구에서 설정한 시그너처와 이를 구현한 규칙은 다음 절에 제시하며, 본 제안 기법이 설치된 실제 시스템의 구성은 그림 4와 같다.

2. 제안 기법의 시그너처와 규칙 구현

5가지 유형의 탐지 대상에 대해 HTTP outbound traffic에서 발견된 비정상적인 HTML 태그와 Javascript 코드를 분석하여 다음과 같이 시그너처로 제시한다.

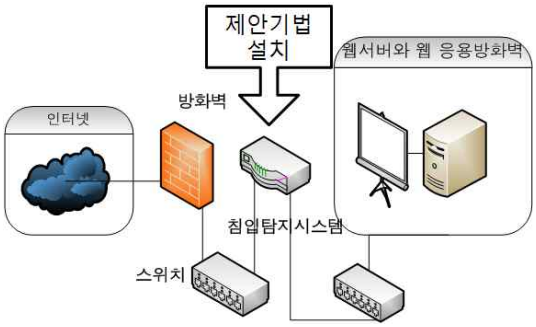

그림 4. 제안 기법의 설치 및 운영
Fig. 4.Installation of Proposed Scheme

1) 악성코드 유포 시그너처: 침해된 웹서버의 변조된 홈페이지는 악성코드 유포의 가장 좋은 경로가 된다. 본 연구팀은 선행 연구로 악성코드를 유포하는17 가지 태그와 코드들을 시그너처로 설정하였다[13]. 시그너처의 예로는 <iframe src=" 외부서버의파일" style =display:none>이 있다.

2) XSS(CSRF 포함) 시그너처: OWASP는 CSRF와 동일한 형태인 XSS에 의해 생성되는 태그와 코드를 정리하여 XSS Discovery Statements로 제시하였다[13]. 이를 바탕으로 제작한 시그너처의 예로는 <IMG SRC="이미지파일이 아닌 Javascript인 문자열">이 있다.

3) 웹쉘 탐지 시그너처: 웹으로 운영체제 악의적인 명령을 입력하여 실행하는 악성프로그램인 웹쉘은 OWASP의 취약점

대부분을 노출시킨다. 파일목록을 출력하는 명령을 통해 데이터베이스 접속 계정과 비밀번호 등의 파일을 찾을 수 있으며, 디렉토리 리스팅에 해당하는 문자열이 그림 5처럼 나타난다 [14]. 따라서 디렉토리 리스팅의 시그너처로 탐지할 수 있다.

그림 5. 웹쉘에서 디렉토리 표시
Fig. 5. Directory listing with WEBSHELL

4) URL Spoofing 시그너처: 특정 링크를 클릭했을 때 의도하지 않는 악성사이트로 이동하며, 시그너처의 예로는 <a href="정상도메인%01@악성도메인">이 있다.

5) 개인 정보 유출 시그너처 : 침해된 홈페이지에서 웹쉘이나 HTML 문서 속에 주민등록번호, 은행계좌번호, 핸드폰번호, 이메일, 신용카드 번호, 사업자 번호 같은 유형이 패킷 속에 포함되어 나타난다. 이러한 개인정보의 형태를 시그너처로 작성한다.

실제 탐지에 적용할 수 있도록 앞에서 제시된 시그너처의 정보를 탐지 시스템에서 정의한 형식으로 표현되는 규칙으로 변환하여야 한다. 본 연구에서는 앞서 제시된 시그너처를 정규표현식을 이용하여 그림 6과 같이 설정하여 탐지시스템인 Snort에 설치한다. 그림 6의 예는 서버에서 포트 80을 통해 전송되는 Outbound Traffic을 감시하여 "<iframe src="외부서버의파일" style=display:none>"라는 HTML의 태그를 다른 속성과 형식 등에 무관하게 검출할 수 있도록 시그너처를 정규표현식의 규칙으로 제작하여 침입탐지 시스템을 구현하는 과정이다.

본 연구에서는 악성코드 규칙 30개, 웹쉘 탐지 규칙 2개, URL Spoofing 2개, 개인정보유출 5개, XSS(CSRF 포함)의 88개 규칙을 제작하여 설치하였다.

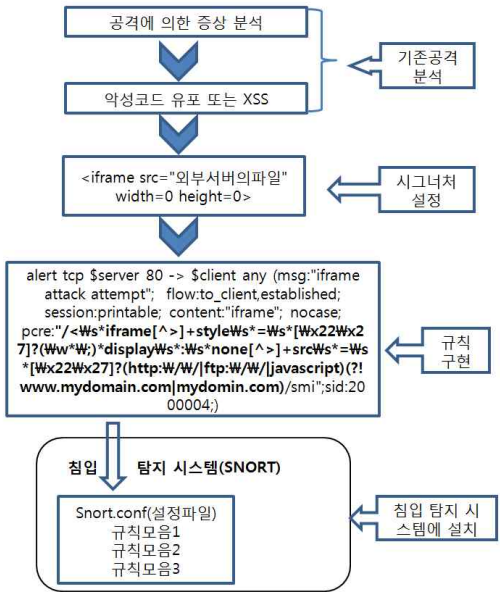

그림 6 제안 시스템 구현과정
Fig. 6. Implementation Process of the Proposed System

IV. 제안 탐지 기법의 검증 분석

1. 검증 환경의 구현

계층적 웹 보안 시스템은 표 2과 같이 침입 탐지 시스템 그리고 웹서버와 웹 방화벽을 MS Virtual PC 2대로, 그리고 방화벽과 스위치는 Dynamips 가상머신으로 구축하여 제안 기법을 검증한다. 제안 기법의 탐지 대상 시스템인 웹 서버는 윈도우 2000 서버의 IIS 5.0으로 ASP와 MS-SQL 2000의 실제 운용 중인 쇼핑몰 소스와 DB를 이용하여 동일하게 Virtual PC에 구축한다.

계층적 보안 시스템의 구성을 위해 웹 방화벽은 웹서버에 추가로 Webknight v2.3을 설치하고, 시그너처 기반의 침입 탐지 시스템은 Snort v2.8.6.1를 설치하고, 방화벽은 가상머신인 pemu를 이용하여 패킷과 상태기반 필터링을 설정한 Cisco PIX를 설치한다.

웹 서버와 침입 탐지 시스템, 방화벽 앞장에서 제시된 그림 4와 같이 연결한다. 탐지 및 차단 기법은 관련연구에 제시된 바와 같이 방화벽에는 패킷과 상태기반 필터링을 설정하고, 시그너처 기반 탐지 기법의 침입 탐지 시스템과 웹 방화벽을 구축한다.

표 2. 검증 시스템의 사양
table 2. Details of Verification System

서버	항목	내용
웹서버와 웹 방화벽	DB	MS - SQL 2000
	웹서버	IIS 5.0
	웹프로그램 언어	ASP
	침해 상태	SQL Injection 침해
	가상머신	MS Virtual PC
	웹 방화벽	ATRONIX Webknight
	웹 방화벽 버전	2.3
	운영체제	window 2000 서버
	웹 방화벽 규칙	한국인터넷진흥원 샘플규칙
	비고	IIS와 같은 컴퓨터에 설치
침입 탐지 시스템	침입탐지시스템	Snort 2.8.6.1
	운영체제	window 2000 서버
	Packet capture lib	winpcap 4.0
방화벽	가상 장비명	CISCO PIX Firewall 525
	메모리	128 M
	방화벽 운영체제	pix721

본 연구의 검증 환경은 계층적 보안 시스템의 검증을 함께 제시하기 위한 것이며, 시스템 사양과 무관하게 동일한 탐지가 가능하다.

2. 제안 시스템의 검증

계층적 보안 시스템에 대해 취약점 분석 도구인 Nessus, 웹을 집중적으로 분석하는 OWASP의 Joomla 스캐너, SQL Injection 공격 도구인 HDSI, 그리고 앞장에서 제시된 5 유형의 우회 공격에 대한 탐지기능 결과는 표 3과 같다.

표 3. 계층적 웹 보안 시스템의 취약점 방어 단계
Table 3. Detecting steps of Hierarchical Web Security System

취약점 분석 공격	취약점 검사항 목갯수	발견된 취약점 갯수	계층적 보안 시스템 방어		
			방화벽	침입탐지 시스템	웹방 화벽
Nessus(1)	38390	118	차단	(4)	(4)
Joomla(2)	466	7	차단못 함	탐지못함	차단
HDSI(3)	SQL Injection	침해됨	차단못 함	탐지못함	차단
우회 공격	5유형 (13개)	13	0개 차단	0개 탐지	0개 차단

(1) 출처 : http://www.nessus.org/nessus/
(2) 출처 : http://www.owasp.org/index.php/Category:OWASP _Joomla_Vulnerability_Scanner_Project
(3) 출처 : http://www.playes.net/Soft/106.asp
(4) 이미 공격이 차단되어 무의미함

계층적 보안 시스템은 직접적인 공격은 모두 탐지하는 우수한 보안 수준을 보인다. 그러나 표 3의 마지막 줄에 제시되는 바와 같이 이들을 우회하는 공격은 전혀 탐지하지 못한다. 여기서, 계층적 보안 시스템을 우회하는 공격은 그림 7과 같이 생성하였다.

이러한 우회 공격은 웹쉘을 생성하고 악성코드 유포와 XSS, URL Spoofing, 개인정보 유출 등을 가능케 한다.

계층적 보안 시스템만으로는 이들의 공격을 탐지 못하지만, 계층적 보안 시스템에 앞장의 그림 4와 같이 제안 기법을 설치하면 이들 우회 공격에 의한 다양한 증상을 표 4와 같이 모두 탐지할 수 있다.

또한 특정한 웹 응용 프로그램의 언어와 운영체제, 그리고 웹 서버와 무관하게 공격 이후 HTTP로 HTML 문서를 외부로 전송하는 모든 경우에 적용 가능하다.

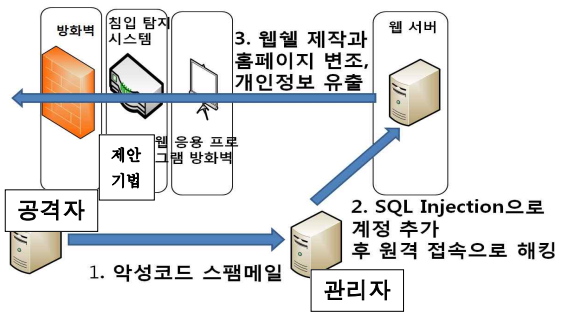

그림 7. 우회 공격 생성
Fig. 7. Generation of Detoured Attacks

표 4. 우회공격에 의한 증상 탐지
Table 4. Detection for Detour Attacks

웹 공격	계층적 보안시스템	침해건수(1)	제안시스템	탐지 시그니쳐	공격 방법
악성코드	탐지 못함	3	탐지	String.fromCharCode(	(2)
XSS	탐지 못함	6	탐지	String.fromCharCode(	(2)
웹쉘	탐지 못함	2	탐지	"<dir> ."	(3)
URL Spoofing	탐지 못함	1	탐지	<a href=...r@...	(2)
개인정보 유출	탐지 못함	1	탐지	주민등록번호, 핸드폰번호, 이메일, 사업자 등록번호	(4)

(1) 우회 공격으로 생성한 침해된 HTML 문서 갯수
(2) 침해된 사이트의 HTML 문서를 우회 공격으로 생성
(3) 실제 웹에서 존재하는 웹쉘 소스를 우회 공격으로 생성
(4) DB의 회원정보를 우회 공격으로 HTML 문서로 생성

Ⅴ. 결론

본 연구에서는 직접적인 공격뿐만 아니라 계층적 웹 보안 시스템에서 탐지하기 어려운 우회 공격에도 효율적인 대응방안을 제안하였다.

이는 외부에서 들어오는 공격보다는 공격 후의 증상을 HTTP Outbound Traffic을 감시하여 탐지하는 기법으로 기존의 Inbound 위주의 공격 탐지와는 탐지 시그너처와 탐지 대상 등에서 차이가 있다. 즉, 공격 받은 이후 실시간으로 유포되고 있는 악성코드, 개인정보, XSS(CSRF 포함), URL Spoofing, 개인정보 유출 등을 HTTP Outbound Traffic을 통해 탐지하는 제안기법은 계층적 웹 보안 시스템이 탐지 못한 우회 공격까지 탐지함을 보였다. 또한 이 기법은 외부로 전송되는 HTML의 태그와 코드를 탐지하는 것이므로 웹 응용 프로그램과 시스템의 사양에 무관하게 작동될 수 있다. 새로운 기법과 경로를 통한 공격이라도 제시된 증상을 모두 탐지할 수 있으므로 새로운 공격 기법에 대한 대응책도 될 수 있다.

웹서버의 환경과 HTML의 구성에 따라 정상적인 HTML 문서를 5가지 탐지 대상으로 처리하는 오탐 문제가 발생할 수 있다. 따라서 정규표현식으로 이루어진 시그너처의 오탐에 대해 예외 정규표현식을 적용하여 방지하였다. 이러한 오탐 문제는 정상 행위 모델을 비교하여 탐지하는 비정상 행위 기반 탐지로도 해결할 수 있을 것으로 분석된다. 본 연구의 향후 연구로 HTTP outbound traffic에 대한 비정상 행위 기반 탐지 기법을 제시한다.

참고문헌

[1] Mi-Sun Kim, Jin-Bo Kim, Hyoung-Cho Yang, Yong-Min Kim and Jae-Hyun Seo, “Web 2.0 and Ajax Security Vulnerabilities,” Communications of The Korea Information Science Society, Vol. 25, No. 10, pp. 43-48, Oct. 2007.

[2] Korea Internet & Security Agency, *"Korea Internet Incident Report of April 2010,"* Jul. 2010.

[3] OWASP, *"OWASP Top 10,"* Sept. 2009.

[4] National Cyber Security Center, *"Monthly Cyber Security,"* Jul. 2006.

[5] Hyeon Soo Kim, Young Dae Park and Seung Hak Kuk, "Development of Test Tool for Testing Packet Filtering Functions," Journal of The Korea Information Science Society, Vol. 13, No. 2, pp. 86-99, Apr. 2007.

[6] Sung-Min Jang and Yoo-Hun Won, "Design and Implementation of a Web Application Firewall with Multi-layered Web Filter," Journal of The Korea Society of Computer and Information, Vol. 14, No. 12, pp. 157-167, Dec. 2009.

[7] Maricel Balitanas, Min-kyu Choi and Tai-hoon Kim, “Duplex Defensive Approach in Network Infrastructure,” Procs. of The Korea Institute of Information Technology, pp. 926-929, Jun. 2009.

[8] Google, *http://code.google.com/intl/en/apis /safebrowsing*

[9] Cisco, *http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a008088517b.shtml*

[10] OWASP, *http://www.owasp.org*

[11] Teng Gao, Yue-wei Ding and Si-chong Da, “Research of Access Control of USB Storage Device with Information Security in Unauthorized Internet Access Monitoring System,” Procs. of Computational Intelligence and Software Engineering 2009(CISE 2009), pp. 1-5, Dec. 2009.

[12] Jin-Cherng Lin and Jan-Min Chen, “MUSIC: Mutation-based SQL Injection Vulnerability Checking,” Procs. of Quality Software International Conference 2008(QSIC '08), pp. 77-86, Aug. 2008.

[13] ByungHa Choi and Kyungsan Cho, " An Improved Detecting Schemes of Malicious Codes using HTTP Outbound Traffics," Journal of The Korea Society of Computer and Information, Vol. 14, No. 9, pp. 47-54, Sep. 2009.

[14] Korea Internet & Security Agency, *"Korea Internet Incident Report of March 2008,"* Mar. 2008.

저 자 소 개

최 병 하

2009 : 단국대학교 컴퓨터학과(박사과정)
관심분야 : 네트워크 보안
Email: notanything@hanmail.net

최 승 교

1982 : 단국대학교 전기공학과(학사)
1992 : 단국대학교전산통계학과(석사)
2001 : 단국대학교 대학원 전산통계학과(박사)
1994~현재 : 삼척/강원대학교 컴퓨터공학과 교수
관심분야 : 컴퓨터구조, 성능평가, 시뮬레이션
Email: skchoi@kangwon.ac.kr

조 경 산

1979 : 서울대학교 전자공학과(학사)
1981 : 한국과학원 전기전자공학과(석사)
1988 : 텍사스 대학교(오스틴) 전기전산공학과(Ph.D.)
1988~1990 : 삼성전자 컴퓨터부문 책임연구원, 실장
1990~현재 : 단국대학교 컴퓨터학부 교수
관심분야 : 네트워크시스템 및 이동통신보안, 컴퓨터시스템
Email: kscho@dankook.ac.kr