한국시뮬레이션학회 논문지
Vol. 19, No. 3, pp. 99-108 (2010. 9)

웹서비스 공격정보 분류 방법 연구

서진원[1] · 서희석[2] · 곽 진[3†]

A Study on Classification Method for Web Service Attacks Information

Jin Won Seo · Hee Suk Seo · Jin Kwak

ABSTRACT

The main contents of this paper is to develope effective measures for Internet Web service attack, classifying vulnerability of Web Service by network layer and host unit and researching classification method by attack range of type of services. Using this paper, we can accumulate analyzed Web service attack information which is key information of promote Web security strengthening business, and basis of relevant security research for detect and response Web site attack which can contribute to activation information security industry.

Key words : Put English key words here, Put English key words here

요 약

본 논문의 주요 내용은 인터넷의 웹서비스 공격에 대한 효과적인 대책을 수립하기 위한 연구로서, 웹서비스 대상으로 하는 공격 정보를 네트워크 계층 및 호스트 구성단위 별 취약점을 분류하며, 서비스 유형에 따른 공격범위 산정 및 분류방법에 대한 모색을 하고자 한다. 이 논문 자료를 이용하여 웹 서비스 공격 정보들의 분석정보를 축척을 통한 다양한 웹 보안 강화 사업 추진의 핵심 정보로 활용될 수 있으며, 웹사이트 공격 탐지 및 대응을 위한 관련 보안 연구의 기초자료 및 정보 보호 산업 활성화에 기여할 수 있다.

주요어 : 웹서비스 공격, 웹서비스 취약점, 공격분류방법

1. 서 론

총 34조 1,000억원(정부 1조 3,000억; 민간 32조 8,000억)을 투자하는 '방송통신 기반 고도화 및 융합서비스 활성화를 위한 방송통신망 중장기 발전계획'(2009~2013)에 의하면, 사업이 완료되는 2013년에는 인터넷의 속도가 10배 빨라지고, 대다수의 국민들이 현재 이용하는 50~100Mbps의 전송속도가 1Giga급으로 상승되는 등 인터넷 사용 환경은 비약적으로 발전하고 있다.

그러나 이와 같은 인터넷 인프라의 첨단화가 가속화 될수록 이를 악용하는 사이버 범죄 또한 비례하여 증가하고 있다. 특히 과거 공격 대상을 개별 시스템에 주안점을 뒀던 공격자들이 DDoS, 웹 공격, SQL Injection 등과 같은 웹사이트를 대상으로 공격 방법을 달리함에 따라 웹사이트의 보안이 중요한 이슈가 되고 있다. 이러한 다양한 웹사이트에 대한 공격들은 사회적으로 많은 혼란을 야기시키고 있는데 대표적인 예로 2003년 1.25 인터넷 대란, 2009년 7.7 DDoS 공격, 최근에 발생한 DDoS 공격 등이 있다. 이러한 사이버 침해사고의 피해에 따른 사회적 파장이 커지면서 웹사이트 보안의 중요성 및 사이버 테러 대응방안의 필요성이 대두되고 있으며, 사이버 위협은 21세기의 가장 심각한 위협요인 중 하나가 되었다.

사이버 공격에 따른 웹사이트의 피해 규모는 막대한데, 작년 7.7 DDoS 침해사고 때 국가 및 피해기관은 신뢰도에 커다란 손실을 입었으며, 경제적 피해 규모의 경우 현대경제연구원에 의하면 최소 363억원에서 최대 544억원으로 추정되었다. 이러한 피해액은 행안부에서 발표한 2008년 풍수해 피해액인 580억원에 거의 근접한 수치

2010년 7월 9일 접수, 2010년 8월 25일 채택
[1] 한국인터넷진흥원 웹보안지원팀
[2] 한국기술교육대학교 컴퓨터공학과
[3] 순천향대학교 정보보호학과
주 저 자 : 서진원
교신저자 : 곽 진
E-mail; jkwak@sch.ac.kr

여서 피해 정도는 심각하다고 할 수 있다.

따라서 본 논문에서는 웹사이트 대상 공격을 사전에 방지하거나 빨리 탐지하여 효과적으로 방어할 수 있도록, 웹사이트에서 발생할 수 있는 다양한 공격정보에 대한 분류 방법을 분석을 모색하였다.

2. 네트워크 계층별(TCP/IP) 취약점 및 공격 유형

TCP/IP는 컴퓨터 간의 통신을 위해 개발한 통신 프로토콜로써 현재 인터넷에서 사용되는 사실상의 통신 프로토콜 표준이다. RFC(Request for Comments)의 형태로 공개되고 발전되고 있으며 유닉스에서는 표준 프로토콜로 사용되고 있을 뿐만 아니라 거의 모든 운영 체계에서 구현되고 있다. 그러나 TCP/IP는 처음부터 보안성보다는 기능성에 중점을 두고 개발되었기 때문에 현대시대에 보안을 중요시 하는 전자상거래나 정보교환에 많은 취약점을 가지고 있다. 다음의 표 1은 TCP/IP의 계층별 공격 유형을 정리한 것이다.

2.1 네트워크 계층

① 케이블 단절 : 물리적인 공격 방법으로는 회선 단절이 있으며 이로 인한 네트워크 장애는 매우 심각한 상황이다. 네트워크가 연결된 클라이언트들은 모든 업무수행이 불가능한 상황으로 되며, 특히 OTDR(Optical Time Domain Reflectometer)과 같은 전송매체 테스트 장비가 없는 상태에서 이런 장애가 발생하면 문제점의 파악 및 복구에 많은 노력이 필요하다.

② MAC Flooding : MAC Flooding(Media Access Control Flooding) 공격은 한 포트에서 수천 개의 호스트가 스위치와 연결되어 있는 것으로 보이지만 실제는 변조된 MAC(Media Access Control) 정보를 공격 호스트에서 발생시키는 것이다. macof라는 공격 툴은 15만 5천개의 MAC Address를 발생 할 수 있으며, 짧은 시간 대량의 위장된 MAC Address를 특정 포트에서 발생시키면, 스위치는 발생된 MAC Address를 내부에 저장하게 되는데 스위치의 하드웨어 공각 제약으로 인한 최대 저장할 수 있는 MAC Address 공간이 위조된 MAC Address로 채워지게 된다. 공격이 진행되고 있는 상태에서 스위치와 연결된 정상적인 호스트가 통신할 때, 스위치의 MAC 정보에는 이미 공격자의 위조된 MAC Address만이 존재한다. 이때 Flooding 공격으로 데이터가 모든 호스트에 전달되므로 공격자는 자신의 호스트에서 스니퍼를 이용한 스니핑이 가능하다.

③ MAC 변조 : 모든 물리적인 장비에는 일련번호가 내장되어 있으며 이 같은 일련번호를 통해 장비 제조업체와 인터페이스 Address를 구분할 수 있다. NIC(Network Interface Card)의 경우 윈도우 계열 OS에서 고유의 MAC Address를 손쉽게 변경할 수 있다. 따라서 MAC Address를 변경 후 다른 컴퓨터의 MAC인 것처럼 속이는 ARP Spoofing(Address Resolution Protocol Spoofing) 공격이 가능하다.

④ ARP 공격 : ARP Spoofing 공격은 자신의 MAC Address를 타 시스템, 주로 게이트웨이의 MAC Address로 위조하여 타 시스템(게이트웨이, 서버, PC 등)으로 향하는 트래픽을 감염된 시스템으로 유도하는 방식이다. L2 장비인 스위치는 이더넷 프레임으로부터 MAC Address를 추출하여 Switch MAC Table을 작성하고 모든 트래픽을 MAC Address를 기반으로 전송하게 된다. LAN 상의 모든 호스트 IP-MAC Address 매핑은 ARP Request Broadcasting을 통해 쉽게 알아 낼 수 있다. 또한 ARP Reply 패킷을 각 호스트에 보내서 쉽게 ARP Cache를 업

표 1. TCP/IP 계층별 공격 유형

TCP/IP	전송단위	주소체계	장비	공격유형
어플리케이션	Message	Domain Name	Computer	Virus, 버퍼오버플로, DNS cache poisoning
전송	Segment/ Datagram	Port 주소	L4switch	Syn Flooding, 스캐닝
인터넷	Packet	IP 주소	Router, L3switch, IP공유기	DHCP 공격, ICMP 공격
네트워크	Frame	MAC Address	Switch, Bridge	MAC Flooding, MAC 변조, ARP 공격
	Bit/Signal		Hub, Repeater	케이블 단절

데이트하여 통신을 할 수 있다. 공격자는 이 과정에서 어떠한 인증도 요구하지 않는다는 취약점을 이용하여 모든 호스트 IP-MAC Address를 확인한 다음 각 호스트에 위조한 MAC Address 즉, 스니퍼의 MAC Address를 보내고 스니퍼의 Cache가 사라지지 않도록 변조된 ARP Reply를 지속적으로 보낸다. 일단 정상적인 통신이 이뤄지면 스니퍼는 피해 시스템에서 전송하는 모든 패킷을 캡처 할 수 있게 된다.

2.2 인터넷 계층

① DHCP 공격 : DHCP(Dynamic Host Configuration Protocol) 요청 클라이언트는 DHCP 디스커버 메시지를 브로드캐스트 형식으로 전송한다. DHCP 디스커버 메시지를 받은 DHCP 서버는 디스커버 오퍼(Discover Offer) 메시지로 응답한다. 이때 디스커버 오퍼 메시지에는 클라이언트 MAC, 할당될 IP Address, 서브넷, 대여 기간, 서버 식별자 IP 등을 포함된다. DHCP 서버로부터 메시지를 받은 클라이언트는 IP 리스 선택(Lease selection) 메시지를 서버에 브로드캐스트로 전송한다. 이 때 클라이언트들이 브로드캐스트 방식으로 메시지를 전송하는 이유는 DHCP가 다중으로 구성돼 있을 수도 있기 때문이다. 마지막으로 IP 리스 선택 메시지를 받은 서버는 DHCP ACK 메시지를 전송함으로써 DHCP의 IP 부여 과정을 마치며, 이 같은 동작 방식이 동일한 서브넷에 존재하는 공격자가 얼마든지 메시지를 가로채 오동작을 발생시킬 수 있다.

② ICMP 공격 : 대부분의 네트워크는 라우터나 게이트웨이가 한 개이지만 하나의 라우터로 감당할 수 없을 경우 두 개 이상 운영해서 로드 밸런싱(Load balancing)을 해야 하며 그중 ICMP 리다이렉트를 사용한다. ICMP (Internet Control Message Protocol) 공격은 공격자가 네트워크에 존재하는 또 다른 라우터임을 각 호스트에게 알린 후 특정한 목적지 주소를 가진 패킷만을 리다이렉트하여 스니핑 한다.

2.3 전송 계층

① Syn Flooding : SYN Flooding은 Spoofing 된 출발지 주소로부터 엄청난 양의 TCP SYN 패킷을 생성한 후 이를 특정 TCP 서버로 전달한다. SYN Flooding의 목적은 목표 TCP 스택이 SYN/ACK 패킷을 전송하는 데 자신의 자원을 모두 소비하고 절대 받을 수 없는 ACK 패킷을 기다리게 만들어서 서버가 본래 작업을 하지 못하게 하는 것으로 서비스 거부 공격이다.

② 스캐닝 : 포트 스캔은 특정 IP주소에서 어떤 TCP나 UDP 서비스가 접근 가능한지 알아보기 위해 호스트의 정보를 얻어내는 기술이다. 공격자는 시스템 스캔을 통해 접근이나 공격할 서비스의 정보를 얻기 때문에 이는 성공적인 침투의 중요한 단계이며 열려져 있는 포트로 트로이 목마와 같은 Virus 프로그램을 이용하여 공격 대상의 PC를 제어할 수 있다.

2.4 어플리케이션 계층

① 바이러스 : 어플리케이션에 내장된 매크로 혹은 스크립트 언어를 사용해서 매크로 Virus와 스크립트 Virus가 있으며, 운영체제와 상관없이 응용 프로그램을 플랫폼삼아 작동한다.

② 버퍼오버플로 : Buffer Overflow 공격은 어플리케이션 소스 코드에서 버퍼에 복사되는 데이터의 양을 충당하기에 버퍼의 크기가 충분하지 않은 부분에서 발생하는 프로그래밍 오류를 이용하는 공격이다. 그러므로 Overflow라는 용어는 인접한 메모리 위치가 덮어 쓰일 때 사용된다. 스택 기반 Buffer Overflow의 경우 성공적인 공격은 함수의 복귀 주소(스택에 존재)가 공격자의 코드를 가리키게 덮어 쓴다. 이를 통해 공격자는 그때부터 쭉 프로세스의 실행을 제어할 수 있다. 또 다른 분류의 Buffer Overflow 공격은 힙으로부터 동적으로 할당되는 메모리 영역에 적용된다.

③ DNS cache poisoning : 공격자는 취약한 DNS를 사용하는 시스템에 조작된 DNS query를 전송하여 Cache의 정보를 변경, 정상적인 사이트에 접속 시 다른 사이트의 IP로 변조 시키는 방법이다.

3. 호스트 구성단위 취약점

웹사이트를 이용하기 위해서는 사용자측에선 웹브라우저가 필요하며 서버 측에서는 웹서버가 구축이 되어 있어야 한다. 또한 웹 페이지를 표시하기 위해서 script preprocessor와 스토리지인 데이터베이스가 필요하며, 사용자가 웹 서버를 이용할 수 있는 웹 인터페이스가 필요하다. 이런 구성요소에 따른 취약점이 발견되고 있으며 여기에서는 각각의 취약점에 대해서 알아본다.

3.1 웹 브라우저

웹 브라우저는 널리 사용되는 웹 서비스 클라이언트 도구이다. 그 종류는 Microsoft Internet Explorer, Safari,

표 2. 웹브라우저별 URL Spoofing 취약점

번호	구분	취약점명
1	공통	여러 웹브라우저들이 프롬프트 다이얼로그 박스 출처 Spoofing 취약점
2	IE	마우스 이벤트를 이용한 IE 상태표시줄의 URL 변조 취약점
3		IE 팝업창 타이틀바 Spoofing 취약점
4		IE의 Window 로딩 시 경쟁 조건을 이용한 주소표시줄 Spoofing 취약점
5	Fire fox	Firefox 다운로드 다이얼로그 소스 Spoofing 취약점
6		Firefox 모달 다이얼로그 Spoofing 취약점
7		IE를 제외한 여러 웹브라우저들의 IDN 처리 관련 사이트 속성 Spoofing 취약점
8		Firefox chrome 윈도우 Spoofing 취약점

Firefox, Opera 등 매우 다양하다. 웹 브라우저는 사용하기 매우 쉽도록 설계되어 있다. 대부분의 사용자들은 보안에 관하여 초보이거나 훈련되지 않은 경우가 대부분이기 때문에 웹 공격을 막기 위한 효과적인 지식을 가지고 있지 못하고 웹 공격에 대한 위협을 모르는 사람들이 대부분이다. 실제 웹 공격을 수행하거나 정보를 얻기 위해 해커들이 많이 사용하는 클라이언트 도구로 가장 간단한 telnet을 들 수 있다. 대표적인 공격방법으로는 URL Spoofing이 있으며 이 공격 자체로는 시스템의 운영이나 동작에 영향을 미치지 않는다. 그러나 최근 빈발하고 있는 피싱과 결합하였을 경우에는 공격 대상자가 자신이 속고 있다는 것을 알아채기 힘들기 때문에 자신도 모르는 사이에 피해자가 될 수 있다.

3.2 웹 인터페이스

웹 서비스를 사용하는 사용자와 웹 서버가 상호작용하기 위해 사용되는 인터페이스 구성요소이다. 다른 구성요소 들이 프로그램으로 이루어져 있는 반면에 인터페이스 구성요소는 HTTP 프로토콜과 데이터, 코드로 구성된다. 즉, 클라이언트의 웹 브라우저를 통해 사용자에게 보이는HTML 코드와 client side scripts 코드, 세션 정보를 위한 쿠키(cookie)뿐만 아니라, 사용자가 웹 서버에 서비스를 요청하는 URI까지 포괄한다. 따라서 이 구성요소는 웹 서비스에서 클라이언트 영역을 제외하고는 사용자 측에 가장 가까운 구성요소이다. 웹 인터페이스의 특징은 사용자가 웹 브라우저를 통해 보고 있는 인터페이스의 클라이언트 소스 코드를 볼 수 있다는 특징이 있다.

때문에 악의적인 사용자는 클라이언트의 HTML 코드를 변경시켜 사용자가 원하도록 웹 요청(request)을 보낼 수도 있다. 따라서 Web Interface에서의 대표적인 취약점은 사용자들의 정보들이 저장되어 있는 쿠키를 볼 수 있는 쿠키 스니핑과, 로그인 부분의 입력 값을 이용하여 admin 계정을 얻을 수 있는 SQL 인젝션 공격이 가능하다.

3.3 웹 서버

웹 서버는 사용자의 웹 브라우저와 실제 사용자가 원하는 정보를 연결시켜 주는 역할을 하는 웹 어플리케이션에서 가장 중점적인 역할을 하는 구성 요소이다. 웹서버는 HTTP/HTTPS 요구를 관리하고, 사용자의 세션을 관리하며, 웹 서비스의 모든 과정을 처리할 수 있도록 담당하는 역할을 한다. 웹 서버의 종류로는 Microsoft IIS, Microsoft PWS, Apache, iPlanet, NCSA, CERN, JAVA Web Server, Netscape Enterprise Server, Oracle Web Server, O' Reilly Web Site, Stronghold, Spyglass 등 다양한 종류가 있으며 다음은 대표적인 데몬 중 IIS 취약점이다.

① 향상된 권한 획득 : 침입자는 이 취약점을 사용하여 시스템 수준 권한이 있는 취약한 서버에 있는 응용 프로그램을 불러와서 실행할 수 있다. IIS가 작동하고 있지 않은 응용 프로그램을 실행하도록 설정되어 있는 경우 이 취약점이 악용될 수 있다.

② 서비스 거부 : 원격지 침입자가 서비스 거부 상태를 초래할 수 있다. 이 취약점은 IIS가 WebDAV 요청에 대한 메모리를 할당하는 방법과 관련이 있다. 특히 정교하게 작성된 모든 WebDAV 요청으로 IIS는 서버에 매우 많은 용량의 메모리를 할당할 수 있다. 서버로 전송된 일부 잘못된 요청으로 인해 취약한 시스템은 서비스에 대한 올바른 요청에 응답하지 못할 수 있다.

③ 파일 업로드 공격 : 원격지 침입자가 취약한 서버에 파일을 업로드하고 이를 실행할 수 있다. 이 취약점은 IIS 5.0에 있는 스크립트 원본 액세스 권한에 따라 파일 종류를 잘못 나열한 결과 발생한다. 결과적으로 침입자는 악성 파일을 취약한 서버에 업로드하고 이를 실행할 수 있다.

3.4 Server side Scripts Preprocessor

사용자가 웹 서버에 요청한 query가 실제 OS나 database에 적용되기 이전에 프로그램 수행의 필요 여부에 따라 적용되는 과정이다. 실제로 이 과정은 기본적으로는 설치되지 않지만, 웹 서비스에서 필요에 의해 설치되는 모듈

이다. 현재 대부분의 웹 서비스에서는 웹 서비스의 기능을 확장하기 위하여 server side scripts preprocessor 모듈들을 사용하고 있다. 이러한 preprocessor의 종류로는 CGI(Common Gateway Interchange), JSP 또는 ASP등이 있다. CGI는 주로 PHP, Perl, C/C++, Python이나 shell scripts 언어로 주로 표현되어있으며, JSP는 Java scripts 언어로, ASP는 ActiveX로 작성된 스크립트 언어이다.

① ASP 코드의 SQL 삽입 공격 : ASP 코드의 Request.Form 또는 Request.Querystring 컬렉션에서 사용자가 제공한 데이터가 데이터 유효성 검사 없이 동적 SQL 문을 만드는데 사용되는 경우 공격자가 SQL 문에 삽입하고 악용할 수 있다. 이를 일반적으로 1차 SQL 삽입 공격 취약점 이라고 한다. 한 ASP 페이지를 사용하여 데이터베이스에 저장된 사용자 입력이 데이터베이스에서 검색된 다음 다른 ASP 페이지에서 동적 SQL 문을 만드는데 사용되는 경우 공격자가 SQL 명령을 SQL 문에 삽입하고 악용할 수 있다. 일반적으로 2차 SQL 삽입 공격 취약점이라고 한다.

② CGI 취약점 : CGI의 취약점은 CGI 그 자체가 아니라, HTTP 명세서와 다양한 시스템 프로그램의 취약점이다. 시스템을 공격하는 다른 방법들이 있는데, 예를 들어 안전치 못한 파일 퍼미션은 FTP나 Telnet으로 공격받을 수 있다. CGI는 다른 허점들을 공격할 수 있는 많은 기회를 제공한다. CGI 명세서는 파일을 읽고 쉘을 획득하고 서버 파일 시스템을 파괴 할 수 있는 기회를 제공하며 스크립트의 assumptions공격, 서버 환경 취약점 공격, 다른 프로그램과 시스템 콜의 취약점 공격으로 액세스를 획득할 수 있다.

3.5 데이터베이스

데이터베이스는 데이터들을 쉽게 입력하고, 검색하고, 관리할 수 있게 하기 위해서 만들어진 데이터들의 집합이다. 현재 대부분의 웹 서비스는 데이터베이스를 이용하여 이루어지고 있다.

가장 흔히 쓰이는 웹 어플리케이션용 데이터베이스로는 MySQL, Oracle, DB2, Microsoft SQL 서버 등이 있다. 데이터베이스 관리자는 해당 데이터베이스의 환경 설정에 주의를 기울여야 한다. 일반 사용자들에게는 보여서는 안 될 데이터가 관리자의 환경 설정 미숙으로 인하여 보이는 문제점이 발생할 수도 있기 때문이다.

① MySQL mysqld 권한 상승 취약점 : 공격자는 [mysqld] option section 하에서 user=root 라인을 포함한 DATADIR/my.cnf를 생성하여 공격할 수 있다. mysqld 서비스가 수행될 때, 디폴트 user 대신에 root 사용자 권한으로 수행될 수 있다. 이러한 취약점으로 인하여 변조된 시스템상에서 공격자는 상승된 권한을 얻는 것을 허락하게 된다.

② Oracle 로그인 접근 통제 취약점 : 오라클에서는 클라이언트와 서버 간 통신하는 과정 중 SQLPlus를 통해 DBMS 접속 시 인증 단계에서 SYS 권한으로 실행되는 유효한 SQL 구분이 포함되어 있다. 이러한 유요한 SQL 구문은 공격자에 의해 임의의 공격 SQL 구분으로 교체 조작됨으로써 서버에서 일반계정의 Oracle 유저가 SYS 권한으로 공격 SQL 구문이 실행할 수 있는 취약점이 발표되었다.

표 3. OWASP의 분류

공격방법	공격 경로	공격이 전파된 정도	취약점 탐지 용이도	기술적 영향
인젝션	쉬움	보통	보통	심각함
XSS	보통	널리 전파	쉬움	보통
취약한 인증 및 세션 관리	보통	보통	보통	심각
안전하지 않은 직접 객체 참조	쉬움	보통	쉬움	보통
크로스 사이트 요청 위조 (CSRF)	보통	널리 전파	쉬움	보통
보안 설정 오류	쉬움	보통	쉬움	보통
URL 접속 제한 실패	쉬움	드물게 전파	보통	보통
검증되지 않은 Redirect와 Forward	보통	드물게 전파	쉬움	보통
데이터를 암호화 하지 않고 저장	어려움	드물게 전파	어려움	심각함
전송 계층에 대한 불충분한 보호	어려움	보통	쉬움	보통

4. 웹 서비스 유형에 따른 공격범위 산정분류

4.1 웹 공격 분류

국제 웹 보안 표준기구인 OWASP(Open Web Application Security Project)에서 '2010년 가장 심각한 웹 어플리케이션 보안 위험 10가지' 보고서를 발표하였으며 위협원, 공격경로, 보안상 취약점, 기술적 영향으로 분류하였다.

① 인젝션 : 위협원은 시스템에 신뢰할 수 없는 데이터를 전송할 수 있는 사람이며, 공격경로는 목표 인터프리터의 구문을 익스플로잇 하는 간단한 텍스트 기반 공격을 전송한다. 보안상 취약점은 어플리케이션이 인터프리터로 신뢰할 수 없는 데이터를 보낼 때 발생한다. 인젝션 취약점은 아주 널리 전파되어 있고, SQL query, LDAP query, XPath query, OS 커맨드, 프로그램 Argument 등에서 자주 발견된다. 기술적 영향은 데이터 도난, 오염, 투명성 저하, DoS 공격의 결과를 가져올 수 있다. 인젝션은 호스트를 완전히 장악당하는 결과를 가져오는 경우도 있다.

② 크로스 사이트 스크립팅 : 위협원은 시스템에 신뢰할 수 없는 데이터를 보낼 수 있는 사람이며, 공격경로는 브라우저에서 인터프리터를 익스플로잇 할 수 있는 텍스트 기반 공격 스크립트를 전송한다. 내부 소스를 포함한 거의 모든 데이터 소스가 공격 경로로 사용될 수다. 보안상 취약점은 어플리케이션이 사용자가 제공한 데이터를 적절하게 검증하거나 Escape하지 않고 브라우저가 전송한 페이지에 포함시킬 때 발생한다. 기술적 영향으로 사용자 브라우저에 스크립트를 실행해 사용자 세션 하이재킹, 웹사이트 변조, 악성 콘텐트 삽입, 사용자를 Redirect, 멀웨어를 사용해 사용자 브라우저 하이재킹 등의 악성 행위를 수행할 수 있다.

③ 취약한 인증 및 세션 관리 : 위협원은 다른 사람의 계정을 훔치려고 하는 익명의 외부 공격자와 계정을 소유하고 있는 사용자로 악성 행위를 감추려고 하는 내부자이다. 공격경로는 인증 혹은 세션 관리 기능 노출 취약점을 사용해 사용자를 가장 한다. 보안상 취약점은 로그아웃, 패스워드 관리, 타임아웃, 로그인 상태유지 (Remember Me), 비밀 질문, 계정 업데이트 부문이 취약하다. 기술적 영향으로 공격에 성공하는 경우 공격자는 사용자가 할 수 있는 모든 것을 수행할 수 있기 때문에 권한이 부여된 계정은 더 많은 피해를 입는다.

④ 안전하지 않은 직접 객체 참조 : 위협원은 특정 유형의 데이터에 전체적이 아닌 부분적으로 접속할 수 있는 사용자이다. 공격경로는 시스템 접속권한을 가진 사용자는 시스템 객체를 직접 참조하는 Parameter값을 허가되지 않은 다른 객체를 참조하도록 변경해 접속한다. 보안상 취약점은 어플리케이션은 사용자가 객체에 대해 접속권한이 있는지 여부를 항상 검증하는 않기 때문에, 안전하지 않은 직접 객체 참조에 취약한 결과를 가져온다. 기술적 영향으로 Parameter로 참조 가능한 모든 데이터에 침입할 수 있다. 네임 스페이스가 희소(Sparse)하지 않는 한 공격자는 이런 유형의 데이터 전체에 쉽게 접속할 수 있다.

⑤ 크로스 사이트 요청 위조 : 위협원은 사용자를 속여 웹사이트에 요청을 제출하게 하는 사람이며, 공격경로는 위조된 HTTP 요청을 생성해, 사용자를 속여 이미지 태그, XSS, 등 다른 많은 기술들을 이용해 이 요청을 제출하도록 한다. 보안상 취약점은 Transaction 전체를 세부적으로 추정할 수 있는 웹 어플리케이션을 이용해 CSRF 공격을 수행한다. 브라우저는 세션 쿠키 등의 식별정보를 자동으로 전송하기 때문에, 공격자는 합법적인 요청과 구별이 되지 않는 가짜 요청을 생성하는 악성 웹페이지를 생성할 수 있다. 기술적 영향으로 공격자는 사용자로 하여금 사용자가 변경할 수 있는 데이터를 변경하도록 만들거나, 사용이 허가된 기능을 수행하도록 할 수 있다.

⑥ 크로스 사이트 요청 위조 : 위협원은 시스템 침입을 시도할 수 있는 계정을 소유한 모든 사용자와 익명의 외부 공격자이다. 공격경로는 허가받지 않은 접속을 획득하거나, 시스템 관한 정보를 알아내기 위해 디폴트 계정, 사용되지 않는 페이지, 패치 되지 않은 취약점, 보호되지 않은 파일과 디렉터리 등에 접속한다. 보안상 취약점은 잘못된 보안설정은 플랫폼, 웹 서버, 어플리케이션 서버, 프레임워크, 맞춤형 코드를 포함한 모든 차원의 어플리케이션 Stack에서 발생할 수 있다. 기술적 영향으로 공격자는 시스템 데이터나 기능에 부분적으로 허가받지 않고 접속할 수 있다. 이런 취약점들은 시스템 전체가 침입당하는 결과를 가져올 수 있다.

⑦ URL 접속 제한 실패 : 위협원으로 네트워크에 접속한 사람은 누구나 어플리케이션에 요청을 전송할 수 있는 사용자이다. 공격경로는 허가받은 시스템 사용자인 공격자는 권한이 있어야 접속할 수 있는 페이지 URL을 변경한다. 보안상 취약점으로 어플리케이션은 페이지 요청을 항상 적절하게 보호하지는 않는다. URL은 설정을 통해서 보호되는데, 시스템 자체가 잘못 설정된 경우가 있다. 기술적 영향으로 공격자는 이런 취약점들을 이용해 허가받지 않은 기능에 접속할 수 있다. 이런 유형의 공격은 관리

적 기능을 주된 목표로 한다.

⑧ 검증되지 않은 Redirect와 Forward : 위협원으로 사용자를 속여 웹사이트로 요청을 제출하게 만드는 사람이며, 공격경로는 사용자로 하여금 검증되지 않은 리다이렉트 링크를 클릭하도록 한다. 이 링크에는 유효한 사이트 주소가 포함되어 있기 때문에 사용자는 의심하지 않고 클릭하는 경우가 많다. 보안상 취약점으로 사용자를 다른 페이지로 Redirect하거나, 같은 방법으로 내부 Forward를 사용하는 경우가 많다. 검증되지 않은 Parameter에 타깃 페이지가 표시되는 경우, 공격자는 Destination 페이지를 선별할 수 있다. 기술적 영향은 멀웨어를 인스톨하거나 사용자를 속여 패스워드나 기타 중요한 정보를 노출하는 데 사용될 수 있으며, 안전하지 못한 Forward를 이용하면 액세스 컨트롤을 우회할 수 있다.

⑨ 데이터를 암호화 하지 않고 저장 : 위협원으로 시스템 사용자 접속 권한이 없는 보호된 데이터 파일에 접속하려는 시스템 사용자나 내부 관리자이다. 공격경로로 대부분 암호화를 크랙하는 대신에, 키를 찾아내고, 암호화되지 않은 사본을 획득하거나, 자동으로 암호해독을 하는 채널을 통해서 데이터에 접속한다. 보안상 취약점은 암호화가 적용되더라도 안전하지 않은 키를 생성, 저장, 키 로테이션을 시행하지 않거나, 약한 알고리즘을 사용하는 경우가 많다. 약하고 Salt되지 않은 Hash를 패스워드 보호에 사용하는 경우도 많다. 기술적 영향으로 데이터를 암호화하지 않고 저장하면 암호화되어야 하는 모든 데이터가 침입을 당하는 경우가 자주 일어난다. 암호화되어야 하는 정보는 식별정보, 개인정보 (PII), 시스템 설정 등이 있다.

⑩ 전송 계층에 대한 불출분한 보호 : 위협원으로 사용자 네트워크 트래픽을 감시할 수 있는 사람이며, 공격경로는 사용자 네트워크 트래픽 감시는 힘들 수 있지만, 쉬울 수도 있다. 사용자가 취약한 사이트에 접속하고 있는 동안에 적절한 네트워크 트래픽을 감시하는 것이 주로 힘들다. 보안상 취약점으로 대부분 어플리케이션들은 인증하는 동안에만 SSL/TLS을 사용하고, 다른 때는 사용하지 않기 때문에 세션 ID 인터셉트는 물론 전송된 모든 데이터를 노출할 수 있다. 어플리케이션은 만료되었거나 부적절하게 설정된 인증을 사용하는 경우도 있다. 기술적 영향은 개인 사용자들의 데이터를 노출해 계정을 도난당하는 결과를 초래할 수 있다. 관리자 계정이 침입당하는 경우 사이트 전체가 노출될 수 있다. 불충분한 SSL 설정은 피싱을 쉽게 만들어 줄 수도 있다.

표 4. 기존 분류법의 비교

종류	장점	단점
Howard	공격전체프로세스를 관찰하기 쉬움	구체적인 공격특성이 나타나 있지 않음
Lough	어떤 공격이든 분류에 포함시킬 수 있음	분류 자체가 구체적이지 않음
Simon	공격들이 자세히 되어 있음	새로운 공격 시 분류하기어려움

4.2 기존 웹 사이트 공격 분류 방법

네트워크에 연결된 어떤 단말기들도 Virus, 웜, 그리고 해커들의 공포로부터 안전하지 못하다. 비즈니스에 관련된 시스템뿐만 아니라 개인이 사용하는 시스템도 예외는 아니다. 따라서 피해 범위를 넓혀가는 네트워크 공격들을 방어하기 위해서 현재 사용되고 있는 네트워크 공격을 분류하는 방법을 알아본다.

① Howard의 분류법 : 광범위한 공격들을 포함할 수 있는 공격 프로세스 기반(process-based) 분류법으로써 공격자, 도구, 접근, 결과, 목적의 다섯 개의 카테고리로 되어 있다. 공격의 전체 프로세스를 관찰하기에는 적절하지만 구체적인 공격 특성이 나타나 있지 않다. 예를 들면, Code Red와 같은 공격을 이 분류법으로 나누기에는 어려움이 따른다.

② Lough의 분류법 : Lough는 공격의 특성에 기반을 둔 VERDICT(Validation Exposure Randomness Deallocation Improper Conditions Taxonomy)를 제안하였다. 공격의 특성에 기반 하였으므로 새로운 공격이나 혼합형(blended) 공격 등 어떤 공격이든지 분류에 포함시킬 수 있다. 그러나 모든 공격을 포함시키기 위해 분류 자체를 구체적으로 만들지 못했다는 단점이 있다. 예를 들면, 공격에 사용된 구체적인 기법(skill)뿐만 아니라, 이 공격이 흔히 알려져 있는 웜에 속하는지 Virus에 속하는지에 대한 결정도 모호해진다.

③ Simon의 분류법 : 앞서 얘기한 분류법들의 집합체로 생각될 수 있는 분류법으로, 현재는 공격 벡터(attack vector), 공격 대상(attack target), 취약성과 취약성에 대한 공격 기법(vulnerability and exploit), 혼합형 공격의 특징 설명(attacks having payloads or effects beyond themselves)의 네 개의 디멘전(dimension)으로 구성되어 있다. 공격들이 자세하게 나타나 있다는 것이 최대 장점이지만, 그 특징이 너무 자세하여 새로운 공격이 나온다면, 과거 공격들과 유사하게 분류되기가 힘들다.

4.3 공격 방법 및 공격 범위 분석

공격범위는 크게 6가지로 분류 할 수 있으며 인증, 인가, 클라이언트 측 공격, 명령어 수행, 정보유출, 논리적 공격으로 나눴다. 다음 표 5는 웹 서비스 유형에 따른 공격 방법을 분류하였다.

① 인증 : 인증은 대개 로그인시 암호의 사용을 통해 이루어지며 암호를 알고 있는 사람은 믿을만한 사용자라고 간주된다. 모든 사용자는 처음에 자신이 원하는 암호를 등록하고, 이후 계속 사용할 때마다, 사용자는 이전에 신고 된 암호를 잊지 않고 사용해야만 한다. 그러나 자금 교환 등이 수반되는 중요한 거래에서 암호가 종종 도난당하거나, 우연히 알려지거나 또는 잊혀 질 수 있다.

② 인가 : 웹사이트가 사용자, 서비스 어플리케이션에 대해 요청 된 동작을 수행하는 데 필요한 허가를 받았는지를 결정하는 웹사이트의 방식을 타깃으로 하는 공격에 대한 것이다. 예를 들어, 각 웹사이트는 특정 내용이나 기능에는 특정 사용자만을 허가해야 한다. 그렇지 않은 경우 다른 리소스에 대한 사용자의 액세스는 제한됨을 뜻한다.

③ 클라이언트측 공격 : 클라이언트 측 공격은 웹사이트 사용자에 대한 남용이나 악용에 초점을 맞춘다. 사용자가 웹사이트를 방문했을 때에 기술적, 심리학적으로 양자 간의 신뢰가 구축이 된다. 사용자는 방문한 웹사이트가 유효한 내용을 전달해줄 것으로 믿고 방문하는 동안 공격이 없을 것으로 기대한다. 이러한 관계적 기대치를 역이용하는 것이다.

표 5. 웹서비스 유형에 따른 공격 방법 분류

서비스 유형	공격 형태	사용 프로토콜	공격 대상	증상
인증	무차별 공격	Normal Brute Force Attack Reverse Brute Force Attack	웹 서버	사용자 계정 획득
	불충분한 인증	URL Attack	웹 서버	관리자 권한 획득
	취약한 비밀번호 복구기능 유효화	브루트 포스	웹 서버	패스워드 해킹
인가	자격증명/세션 예측	Session Hijacking	호스트	세션 공격
	불충분한 인가	URL Attack, Network Sniffer	웹 서버	숨겨진 디렉터리 접근 및 세션 공격
	세션 고정	HTTP request	호스트	쿠키 고정을 겨냥한 공격
Client측 공격	컨텐츠 스푸핑	Contents Spoofing	호스트	허위 컨텐츠 제공
	XSS	Cross-site Scripting	호스트	URL에 내장된 코드 에코
명령어 수행	버퍼 오버플로우	Buffer Overflow	웹 서버	DoS 공격 및 의도하지 않은 동작
	포맷 스트링 공격	Format String Attack	웹 서버	임의의 코드 수행 및 스택 외 값 읽기
	LDAP 인젝션	LDAP 프로토콜	웹 서버	LDAP 서버 접근 권한
	OS Commanding	OS Command	웹 서버	운영체제 접근
	SQL 인젝션	SQL	웹 서버	커스텀 SQL 문장 사용
	SSI 인젝션	SSI	웹 서버	루트 디렉터리 리스팅
	XPath 인젝션	Xpath	웹 서버	임의의 사용자 로그인
정보 유출	디렉터리 인덱싱	Directory Indexing	웹 서버	디렉터리 데이터 열람
	정보 유출	코드주석	웹 서버	SQL 인젝션을 위한 정보
	경로 유출	URL Attack	웹 서버	경로 유출
	예측 가능한 리소스 위치	URL Attack	웹 서버	숨겨진 파일 열람
논리적 공격	기능의 오남용		웹 서버	웹사이트의 특징을 이용해 액세스 컨트롤
	서비스거부	DoS	웹 서버	CPU 사용률을 최대화
	불충분한 반-자동화		웹 서버	자동화된 프로세스를 악용
	불충분한 프로세스 검증		웹 서버	트래픽 플로우 변경
	분산된 서비스 거부	DDoS	웹 서버	DoS와 동일

④ 클라이언트측 공격 : 클라이언트 측 공격은 웹사이트 사용자에 대한 남용이나 악용에 초점을 맞춘다. 사용자가 웹사이트를 방문했을 때에 기술적, 심리학적으로 양자 간의 신뢰가 구축이 된다. 사용자는 방문한 웹사이트가 유효한 내용을 전달해줄 것으로 믿고 방문하는 동안 공격이 없을 것으로 기대한다. 이러한 관계적 기대치를 역이용하는 것이다.

⑤ 명령어 수행 : 모든 웹사이트는 요청을 완수하기 위해 사용자가 제공하는 데이터를 이용한다. 사용자가 제공하는 데이터는 구조 명령(construct commands)을 창출하기 위해 쓰이며 그 결과 동적인 웹 페이지 컨텐츠가 나오게 된다. 이 과정이 안전하지 못하게 진행되면 공격자가 명령어 수행을 바꿀 수 있게 되는 것이다.

⑥ 정보 유출 : 시스템 특정 정보(System specific information)에는 소프트웨어 배포, 버전 번호, 패치 레벨이 포함되거나 정보가 백업파일이나 임시파일의 위치를 포함할 수도 있다. 대부분의 경우 사용자의 필요를 충족시키기 위해서 이 정보를 밝힐 필요는 없으며 웹사이트는 어느 정도의 정보를 나타나게 하지만, 가능한 한 데이터의 양을 제한하는 것이 최선이다. 공격자가 웹사이트에 대한 정보를 더 많이 얻게 될수록 시스템은 공격에 더 쉽게 노출되는 것이다.

⑦ 논리적 공격 : 어플리케이션 논리는 어떤 동작을 수행하기 위해서 사용되는 예상되는 절차 흐름으로 비밀번호 복구, 계정 등록, 경매입찰, 전자상거래 구매 등이 모두 어플리케이션 논리의 예이다. 특정 동작을 완성하기 위해 웹사이트에서 사용자에게 구체적인 여러 단계를 올바르게 수행할 것을 웹사이트에서 요구할 수도 있으며 공격자는 이러한 특징을 우회하거나 오용해서 웹사이트와 그 사용자를 해칠 수 있다.

5. 결 론

본 논문에서는 웹사이트 공격정보 수집 모델을 제시하기 위한 선행 연구로서 웹사이트 대상 공격정보 분류에 대한 연구를 수행하였다. 공격 시스템을 분석하기 위하여 TCP/IP 계층인 네트워크, 인터넷, 전송, 어플리케이션 각각에 대한 취약점을 분석하였다. 또한 호스트 구성단위로 웹브라우저, 웹 인터페이스, 데몬, 스크립트 언어, 데이터베이스의 취약점을 분석하였다. 기존 OWASP에서 발표한 공격 분류 방법과, 기존의 분류방법을 분석했으며, 웹서비스 유형에 따른 공격범위 산정에 관한 연구를 수행하였다.

추후 계획으로는 공격정보 수집을 위한 실제 웹사이트 샘플링 및 트래픽 확보 방안과 분석 결과에 대한 분류별 통계 산출 및 활용 연구를 수행할 계획이다.

참 고 문 헌

1. 고승철, 이강신, 고규만, 정기문, 조영득, 네트워크 취약점 점검도구 선정지침, 02-03, 정보통신산업진흥원, pp. 16-65, 2002년.
2. 고훈, “홈 네트워크 취약점 분석 및 인증분석,” 정보보호학회지, 16(6), pp. 42-47, 2006년 12월.
3. 서정석, 김한성, 조상현, 차성덕, 웹 어플리케이션 특성 분석을 통한 공격 분류, 정보과학학회, 한국정보과학지, 30(1), pp. 97~116, 2003년.
4. 윤준, 최신 웹 해킹기법에 대한 분석와 대응방법,한국인터넷진흥원, pp. 1-19, 2004년.
5. 조영복, 김동명, 이상호, “모바일 노드에서 ID기반의 AAA 인증 프로토콜,” 한국퍼지및지능시스템학회, 16(1), pp. 331~335, 2006년 5월.
6. 인터넷침해대응센터, 홈페이지 주요 취약점 및 보호대책, 한국인터넷진흥원, pp. 1-15, 2004년.
7. 지식경제부, 네트워크 위협의 제로데이 공격 대응을 위한 실시간 공격 시그니처 생성 및 관리기술 개발, 지식경제부, pp. 15-34, 2009년.
8. 한국인터넷진흥원, 인터넷 통계 월보, 제32901, 한국인터넷진흥원, p. 11, 2010년.
9. 한국인터넷진흥원, 웹브라우저 URL 스푸핑 취약점 정리, 2005년.
10. OWASP, 10대 가장 심각한 웹 어플리케이션 보안 취약점, 2007년.

서 진 원 (monopoly516@gmail.com)

1998 전북대학교 컴퓨터공학과 학사
2001 전북대학교 컴퓨터공학과 석사
2001 한국정보보호진흥원 정보보호 평가 연구원
2004 한국정보보호진흥원 인터넷침해대응센터 선임연구원
2010 한국인터넷진흥원 웹보안지원팀 팀장

관심분야 : 네트워크 & 어플리케이션 보안, 보안 시뮬레이션, Anti-DDoS

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과 학사
2002 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사
2005 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사
2005～현재 한국기술교육대학교 컴퓨터공학부 조교수

관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN

곽 진 (jkwak@sch.ac.kr)

2000, 2003, 2006 성균관대학교 학사, 석사, 박사
2006～2006 일본 큐슈대학교 방문연구원
2006～2006 일본 큐슈시스템 정보기술연구소 특별연구원
2006～2007 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007～2009 정보통신연구진흥원 집필위원
2007～현재 순천향대학교 정보보호학과 교수
2007～현재 정보통신산업진흥원 기술평가위원
2008～현재 디지털아이디관리포럼 운영위원
2009～현재 한국정보통신기술협회 JTC/SC27 분과 기술위원
2009～현재 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원
2009～현재 순천향대학교 정보보호학과 학과장
2009～2009 순천향대학교 공과대학 교학부장
2010～현재 순천향BIT 창업보육센터 소장
2010～현재 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원
2010～현재 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원
2010～현재 교육과학기술부 국가기술 수준 평가 전문위원
2010～현재 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원
2010～현재 지식경제부 지식경제기술혁신평가단 평가위원

관심분야 : 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안