웹 환경을 이용한 보안 취약점 점검 도구 개발에 관한 연구

장승주* · 최은석*

*동의대학교 컴퓨터공학과

A Study on Implementation of Vulnerability Assessment Tool on the Web

Seung-Ju Jang* · Eun-Seok Choi*

*Dept. of Computer Engineering, Dong-Eui University

E-mail : sjjang@deu.ac.kr

요 약

우리나라가 IT 강국으로 성장할 수 있었던 배경은 여러 이유가 있지만, 그 이유들 중에서 "Web"의 탄생을 생각하지 않을 수가 없다. "Web"이라는 매개체는 서비스를 제공자들 사이에서 상호연결을 쉽게 해주고, 새로운 직업과 기회를 주었다. 하지만 접근하기 쉬운 Application과 Application들 간의 통합이 됨에 따라 보안에 대한 문제가 발생한다. 이러한 보안상의 취약점을 점검하는 도구들이 존재하고 있다. 보안상의 취약점을 예방하는 차원에서 개발되어 졌지만, 악의적인 용도로 사용되어 질 수도 있다. 악성코드의 경우 전년도 동기 대비 50.9%, 스파이웨어의 경우 9.7%정도 증가했다고 밝혔다. 본 논문은 보안 취약점 점검 도구들을 이용하여 웹 상에서 사용자의 컴퓨터 시스템에 대한 점검을 통해서 결과를 보여주는 환경을 개발한다. 또한 공개된 보안 취약점 점검 도구의 융합을 통한 통합된 보안 취약점 점검 기능을 점검하는 웹 환경을 개발한다.

키워드

보안, 취약점, Vulnerability, 웹환경

Ⅰ. 서 론

우리나라가 IT 강국으로 성장할 수 있었던 배경은 여러 이유가 있지만, 그 이유들 중에서 "Web"의 탄생을 생각하지 않을 수가 없다. "Web"이라는 매개체는 서비스를 제공자들 사이에서 상호연결을 쉽게 해주고, 새로운 직업과 기회를 주었다. 또한 업무의 효율성을 거의 무한대로 제공한다. 하지만 접근하기 쉬운 Application과 Application들 간의 통합이 됨에 따라 보안에 대한 문제가 발생한다. 보안에 문제가 생김에 때라 일반적으로 해킹(hacking)으로 알려진 크래킹(cracking)이 빈번하게 일어난다. 이러한 보안의 문제는 보안상의 취약점(Vulnerability)을 크래커(cracker)들이 사용하기 때문이다. 보안 취약점(Vulnerability)은 시스템 및 네트워크의 보안정책을 위반하여 공격되어지는 시스템 및 네트워크 설계, 구현, 운영, 관리상의 약점이라고 할 수 있다. 이러한 보안상의 취약점을 점검하는 도구들은 공개되어 있는 프로그램들도 있지만 상용화된 프로그램들도 있다. 이러한 프로그램들은 보안상의 취약점을 검사하고 그 결과를 사용자에게 보여 준다. 이는 보안상의 취약점을 예방하는 차원에서 개발되어 졌지만, 악의적인 용도로 사용되어 질 수도 있다.

2003년 말 90개의 웹 사이트를 해킹하여 260만 명의 개인 정보를 유출한 사건이 있었다. 이 사건의 피의자가 "발표된 취약점에 대해 관계자가 패치하지 않을 경우 인터넷에 공개 되었을 때 5분이내면 해킹이 가능하다." 라고 말을 해 충격을 주었다.

본 논문은 웹 환경을 이용하여 보안 취약점을 점검해 줄 수 있는 점검 도구의 개발을 연구 하고자 한다. 사용자는 웹에 접속하여 보안 취약점 점검을 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 본 연구와 관련 있는 연구를 설명하였고, 3장에서는 보안 취약점 점검 도구의 설계에 대해 기술하였다. 4장에서는 널리 알려진 보안 취약점에 대하여 공개된 보안 취약점 점검 도구로 실험을 하였다. 5장에서는 본 연구의 결론으로 구성한다.

II. 관련연구

보안에 대한 중요성을 지속적으로 알리고 정보를 제공하고 있는 국내 Web site중 안철수연구소(www.ahnlab.com 대표 오석주)는 보안 취약점을 파고드는 신종 악성코드와 스파이웨어들에 대해 지난해인 2006년 1월부터 11월까지의 동향을 분석하였다. 악성코드는 바이러스, 웜, 트로이목마처럼 PC 정보를 손상하거나 유출하려는 악의적 목적으로 만들어진 프로그램을 통칭한다. 스파이웨어는 사용자의 인터넷 사용 습관, 즉 즐겨 검색하는 단어, 자주 클릭하는 배너 광고 등을 수집해 마케팅에 활용하기 위한 만든 프로그램이다. 최근에는 애초의 목적과 달리 악성 코드와 결합돼 부정한 방법으로 금전적 이익을 취하는 업자들에 의해 이용되고 있다. 표 2는 신종 악성 코드 발견 통계이다.

표 2. 악성코드발견 통계

월	악성코드	스파이웨어
1 월	258	426
2 월	132	202
3 월	241	250
4 월	240	1,079
5 월	413	661
6 월	233	542
7 월	247	516
8 월	306	476
9 월	703	506
10 월	565	652
11 월	693	857
합 계	4,031	6,167

표 2의 조사에서 시간이 지날수록 신종 악성코드와 스파이웨어가 증가함을 보여 주고 있다. 안철수연구소는 악성코드의 경우 전년도 동기 대비 50.9%, 스파이웨어의 경우 9.7%정도 증가했다고 밝혔다. 특히 허위 안티스파이웨어, MS 보안 취약점을 이용한 제로 데이 공격(Zero Day Attack) 등은 보안상의 취약한 부분을 공격하여 주요정보가 노출될 수 있는 위험을 갖고 있다. 제로 데이 공격(Zero Day Attack)은 취약점이 발견된 후 개발사의 공식적인 취약점 패치 발표 이전에 해당 취약점을 공격하는 악성코드나 스파이웨어가 제작되는 것을 말한다. 허위 안티 스파이웨는 사용이 무료라고 광고해서 사용자를 현혹시킨 후에 사용자 컴퓨터에 프로그램을 설치하게 된다. '악성코드'를 잡는다는 명분으로 주로 스파이웨어를 진단하며 정상적인 파일까지 진단하거나 사용자 PC의 파일을 암호화해 불안감을 자극한다. 문제를 해결하려면 비용을 지불하도록 유도한다. 프로그램 사용을 위해서 한번 결제하게 되면 반복적으로 결제가 되고, 이 프로그램은 삭제가 안 되는 경우도 있다. 또한 허위 안티스파이웨어의 경우 최근 일반 사용자 층, 즉 보안 비전문가들의 입장에서도 보안이 중요하다는 인식을 악용한 경우라 하겠다. 이러한 악성코드와 스파이웨어에 안전하기 위해서 서버 시스템이 보안에 얼마나 취약한지를 알아야 하며, 일반인도 손쉽게 자신의 컴퓨터 시스템이 보안에 취약한지를 인식하고 그에 대한 대비를 하는 것이 필요하다.

전 세계 운영체제의 대부분이 MicroSoft 사(이하 MS)의 Windows 운영체제 계열이다. MS의 Windows 와 Windows 용 응용프로그램도 보안 취약점이 발견되고 있다. 최근에 와서는 이러한 보안 취약점이 개발사에서 발견되어 패치 버전을 배포하기 전에 시스템을 공격당하는 일이 빈번하게 발생하고 있다. 이에 따라 MS는 보안관련 Web site를 운영하고 있다. 이 site는 보안관련 동향, 뉴스, 자체 개발 기술 등을 개시하여 이용에게 보안의 중요성을 알림과 동시에 컴퓨터 시스템의 보안 구멍을 매우는 역할을 하고 있다. MS는 STPP(전략적 보안지원 프로그램; Strategic Technology Protection Program)의 일환으로 일반적으로 틀리기 쉬운 보안 관련 설정을 간단히 확인하는 방법에 대한 고객의 요구에 따라 MBSA(Microsoft Baseline Security Analyzer)를 개발하여 제공하고 있다.

보안 취약점을 이용하는 공격자의 입장에서 시스템에 침입하기 위해 제일 먼저 하는 행위는 바로 해당 네트워크 및 시스템에 대한 보안 취약점 점검이다. 광범위한 보안 취약점 점검을 통해서 현재 어떠한 서버가 네트워크에 연결되어 있는지 또한 각각의 서버에서는 어떠한 서비스가 제공 중이며 이러한 서비스를 통해서 해당 시스템이 웹 서버인지, DB서버인지 혹은 메일 서버인지 등 어떠한 목적으로 운영되는지도 추측할 수 있게 된다. 반대로 서버 관리자의 입장에서는 자가 보안 취약점 점검을 통하여 자신이 운영하는 서버가 자신이 알지 못하는 사이 다른 포트가 열려 있는지 등을 확인할 수 있다.

초기의 보안 취약점 점검 툴 들은 자가 보안 취약점 점검을 목적으로 개발되었다. 이러한 보안 취약점 점검 툴 들이 해킹에 사용하고 있다.

III. 보안 취약점 점검 도구 설계

본 논문은 기존의 보안 취약점 점검 도구들을 이용하여 사용자 컴퓨터 시스템에 대한 보안 취약점을 점검한다. 본 논문에서 제안하는 보안 취약점 점검 도구는 보안 취약점 점검 결과를 사용자에게 알려준다. 본 논문에서 설계한 보안 취약점 점검 도구는 다음 그림 1과 같다.

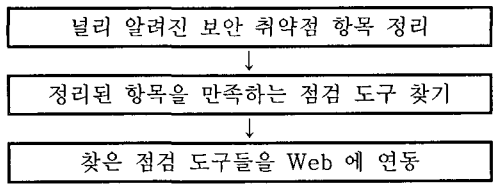

그림 4. 보안 취약점 점검 도구 설계 과정

그림 1은 보안 취약점 점검 도구 설계 과정을 보여준다. 보안 취약점 점검 도구를 설계하기 위하여 우선적으로 널리 알려진 보안상의 취약점에 대한 항목들을 정리한다. 기존의 보안 취약점이 어떤 것이 있는가를 정리하여 이 기능들을 중심으로 도구의 기능을 설계한다.

표 3. 기존 보안 취약점 항목

점검분야	항 목
네트워크 구조식별	- Ping 스캔 - TCP 포트 스캔 - UDP 포트 스캔 - SNMP 점검 - 백도어 점검
웹	- 웹브라우저 취약점 - 서비스 거부 취약점 - Filters, Proxies
사용자 관련 보안	- 계정 보안 - 로그인 파라미터 점검 - 사용자 파일 - 패스워드 관련 보안
파일 관련 보안	- 파일접근 - 파일시스템 무결성 - Database
시스템 설정 관련 보안	- 네트워킹 서비스 설정사항 - 특수 파일의 설정 점검 - 시스템 배치 작업 점검 - 로그분석 - 기타 유틸리티 점검 - 레지스트리 설정 점검
OS 관련 보 안	- 초기설정값 점검 - OS 패치 점검 - 바이러스 감염 점검

표 3은 기존 보안 취약점에 대해 정리한 항목들이다. 기존의 보안 취약점을 비슷한 분야별로 나누어 정리 하여, 본 논문에서 제안하는 보안 취약점 점검 도구 개발에 중요한 평가 기준으로 사용된다.

두 번째, 보안 취약점 항목을 만족하는 점검 도구들을 찾는다. 널리 알려진 보안 취약점에 대해서 정리한 항목에 만족하는 점검 도구를 찾아야 한다. 널리 알려진 보안 취약점에 대한 점검은 기본 사항이기 때문에 이를 만족하여야 한다. 본 논문에서 제안하는 보안 취약점 점검 도구는 이러한 항목들을 만족하도록 한다.

세 번째, 기존의 점검 도구들이 사용자 컴퓨터 시스템을 점검할 수 있게 구성한다. 보안 취약점 점검 툴 중 공개되어 사용가능한 툴을 중심으로 웹에서 동작이 가능하게 한다. 보안 취약점 점검 툴의 설치, 실행, 제거에 이르기 까지 모든 행위는 웹에서 이루어진다. 웹을 통하여 보안 취약점 점검 도구의 실행 결과를 출력한다.

웹의 구성은 기본이 되는 HTML 언어를 바탕으로 asp, java script등을 사용하여 사용자의 시스템 환경에 영향이 적은 범용 언어들을 사용하여 개발한다.

Ⅳ. 실험

본 논문에서 제안한 보안 취약점 점검 도구에 포함된 취약점 점검 항목을 점검할 수 있는 기존의 툴 중심으로 실험을 수행한다. 실험에 사용된 컴퓨터 시스템은 다음 표 4와 같다.

표 4. 실험에 사용된 컴퓨터 시스템

컴퓨터 시스템 Ⅰ	
CPU	Intel PentiumⅣ 2.8 GHz
RAM	512 MB
하드디스크	160 GB
운영체제	Windows XP Home Edition SP2
컴퓨터 시스템 Ⅱ	
CPU	Intel PentiumⅣ 2.0 GHz
RAM	512 MB
하드디스크	40 GB
운영체제	Windows XP Professional SP2

표 4에서와 같이 본 논문에서 제안하는 기능의 실험을 위하여 두 대의 시스템을 사용하였다.

본 논문에서 제안하는 웹 환경의 보안 취약점 점검 도구에 포함된 툴은 표 5와 같다.

표 5. 실험에 사용된 점검 도구

기존 보안 취약점 점검 툴	버 전
MBSA	1.2
Nmap	4.20
Ferret	1.11

본 논문에서 제안하는 보안 취약점 점검 도구에 대한 실험 방법은 실험용 컴퓨터 시스템에 표 5에 있는 보안 취약점 점검 도구들을 사용하여 본 논문의 3장에서 작성한 널리 알려진 보안 취약점 항목에 얼마나 만족하는지를 알아본다.

표 6. 보안 취약점 점검 항목에 대한 점검 도구의 만족(○ ; 항목에 대해 만족)

구 분	항 목	MBSA	Nmap	Feret
네트워크 구조식별	- Ping 스캔		○	
	- TCP 포트 스캔		○	
	- UDP 포트 스캔		○	
	- SNMP 점검			
	- 백도어 점검			
웹	- 웹브라우저 취약점	○		
	- 서비스 거부 취약점			
	- Filters, Proxies			
사용자 관련 보안	- 계정 보안			○
	- 로그인 파라미터 점검			
	- 사용자 파일			
	- 패스워드 관련 보안			○
파일 관련 보안	- 파일접근			○
	- 파일시스템 무결성			
	- Database			
시스템 설정 관련 보안	- 네트워킹 서비스 설정사항	○		
	- 특수 파일의 설정 점검			
	- 시스템 배치 작업 점검	○		
	- 로그분석			
	- 기타 유틸리티 점검	○		○
	- 레지스트리 설정 점검			○
OS 관련 보안	- 초기설정값 점검	○		
	- OS 패치 점검	○		○
	- 바이러스 감염 점검			

표 6은 기존 보안 취약점 점검 툴들이 널리 알려진 보안 취약점 항목에 대하여 얼마나 만족하는지를 보여준다. 각 툴들은 나누어진 하나 또는 두 개의 분야의 항목에 대해서 점검함을 알 수 있다.

표 6의 실험 결과에서 보는 바와 같이 특정한 보안 취약점 점검 도구는 특정한 취약점 항목에만 적용가능 함을 알 수 있다. 따라서 본 논문에서와 같이 통합된 보안 취약점 점검 도구의 제공이 필요하다. 이러한 툴의 제공은 사용자에게 하나의 툴을 이용하여 시스템 내에 존재하는 보안 취약점을 점검 가능하도록 해준다.

V. 결론

널리 알려진 보안 취약점들은 일반인들도 손쉽게 접할 수 있는 부분이 많은 만큼 서버를 관리하는 입장에서는 위험하다. 보안에 대한 비 전무가도 간단한 프로그램 몇 가지로 중요한 시스템에 접근이 가능하다.

보안 전문가라도 여러 점검 도구로 무장을 하더라도 하나 혹은 그 이상의 취약점을 다 점검할 수 없다. 본 논문에서는 이러한 일을 방지하고자 알려진 보안 취약점들을 정리 하였다. 그리고 여러 점검도구들을 연동하여 마치 하나의 점검 도구로 점검하는 효과를 가져 오고자 본 연구를 제안한다.

본 논문에서 제안하는 보안 취약점 점검 도구는 특정한 보안 취약점만이 아닌 널리 알려진 보안 취약점을 전체적으로 점검할 수 있다. 또한 웹 환경을 이용하기 때문에 사용자 플랫폼에 관계없이 보안 취약점을 점검 할 수 있다.

본 논문에서 제안하는 보안 취약점 점검 도구의 실험 결과에서 널리 알려진 보안 취약점이라도 단 하나의 점검 프로그램으로는 모두 점검할 수 없음을 알 수 있다.

본 연구를 통하여 국제적인 크래커들의 경유지인 서버들을 보호한다. 본 논문의 연구가 마무리되면 여러 점검도구들이 하나의 점검 도구인 것처럼 서로가 연동이 되어 외부의 크래커들로부터 컴퓨터 시스템을 안전하게 보호할 수 있다.

참고문헌

[1] 기반보호팀, "네트워크 취약점 점검도구 선정 지침", p120-142, 한국정보보호진흥원

[2] 보안관리팀, "공개용 보안프로그램을 활용한 취약성 점검", p14-24, 한국정보보호진흥원

[3] http://microsoft.co.kr/

[4] YTN 김세호, "전문 해커 조직 적발, 국세청도 해킹", 2003.11.19

[5] http://home.ahnlab.com/

[6] http://sourceforge.net/

[7] http://itfind.or.kr/

[8] http://nilesoft.co.kr/

[9] 전계현, "웹 애플리케이션을 위한 보안 감리 점검항목", 강원대학교 정보과학석사학위논문 2006. 8

[10] Matin Tamizi, "Automated Checking for Windows Host Vulnerabilities", ISSRE'05, 2005

[11] Anil Sharma, Jason R. Martin, "A Host Vulnerability Checking Tool" DARPA

[12] 한국정보보호진흥원, "취약성 분석·평가 품질관리 연구", 한국정보보호진흥원, 2003

[13] 기반보호팀, "시스템 취약점 점검도구 선정 지침", 한국정보보호진흥원, 2002

[14] 한국정보보호진흥원, "공공기관 정보보호 수준 제고 사업", 한국정보보호진흥원, 2003

[15] Fanglu Guo, Yang Yu, "Automated and Safe Vulnerability Assessment", ACSAC, 2005.