개인 사용자를 위한 실시간 취약점 분석 및 보완도구의 설계와 구현

이종민*, 황성철**, 강흥식**
*인제대학교 컴퓨터공학과
**인제대학교 전산학과
e-mail:jmlee@nice.inje.ac.kr mslove1@nate.com
hskang@nice.inje.ac.kr

Design and Implementation of a Realtime Vulnerability Analysis and Complement Tool for Personal User

Jong-Min Lee* Sung-Chul Hwang** Heung-Seek Kang**
*Dept of Computer Engineering, Inje University
**Dept of Computer Engineering, Inje University

요약

현재 IDS, Firewall과 같은 정보보호 시스템이 활발히 연구되고 있지만 근본적인 취약점을 보완할 수는 없다. 해커들의 해킹을 위한 사전 작업은 우선 취약점 수집으로부터 시작된다. 해킹을 차단하기 위한 근본적인 해결책은 취약점을 찾아내고 취약점을 보완하는 것이다. 기존의 취약점 분석 도구들은 네트워크 관리자들에 맞춰 일정 네트워크의 취약점을 찾아내고 알려주는 역할만 했었다. 본 논문에서는 개인 사용자를 위한 취약점 분석 및 발견된 취약점을 실시간으로 알려주고, 보완해주는 도구를 제안한다.

1. 서론

현재 개인 사용자의 인터넷 활용이 급증함에 따라 해커들의 공격 가능성도 점차 높아지고 있다. UI의 발전으로 누구나 쉽게 컴퓨터를 사용하고 있지만 대부분 자신이 가지고 있는 정보를 보호하는 방법을 모르거나 무관심 한 것이 사실이다. 기존의 취약점 분석도구가 정보 보호를 위한 대안이 될 수 있지만 개인 사용자들이 사용하기에는 어렵고 기능이 네트워크 관리자 위주로 맞추어져 있으며 취약점 보완 또한 이루어지지 않는 것이 사실이다. 본 논문에서 제안하는 개인 사용자를 위한 취약점 분석 도구는 컴퓨터를 잘 다루지 못하는 사용자들도 쉽게 설치 및 취약점 검사를 할 수 있으며 스마트 업데이트를 이용하여 실시간 패치 파일 전송이 가능하도록 하였다.

본 논문의 형식은 다음과 같다. 2장에서는 취약점, 스마트 업데이트에 대해서 알아보고 3장에서는 본 논문에서 제안하고 있는 개인 사용자를 위한 취약점 분석 도구의 설계에 대해 서술된다. 이어 4장에서는 실험 결과를 보인 후 마지막으로 5장에서 결론 및 향후 발전 방향에 대해서 서술한다.

2. 관련연구

2.1 취약점 설명

취약점(Vulnerability)이란 시스템 및 네트워크의 보안 정책을 위반하여 공격되어지는 시스템 및 네트워크 설계, 구현, 운영, 관리상의 약점이라고 정의할 수 있다. 취약점은 크게 운영체제 버그 취약점, 프로토콜 취약점, 응용프로그램 버그 취약점, 백 도어를 이용한 방법으로 분류할 수 있다. 현재의 인터넷망의

표준 프로토콜인 TCP/IP는 보안을 염두 한 프로토콜로 설계되지 않았기 때문에 구조상 취약점을 가지고 있고 운영체제 또한 자체의 취약성을 가지고 있다. 응용프로그램의 경우 누구나 만들 수 있고 특히, 백 도어 등의 프로그램을 내부에 포함시킬 수 있기 때문에 항상 위험성을 내포하고 있다.

2.2 스마트 업데이트 소개와 대표적인 프로그램

스마트 업데이트란 사용자의 간단한 조작으로 자동업데이트를 해주는 것을 말한다. 스마트 업데이트는 많은 분야에서 활용되고 있다.

대표적으로 백신 프로그램인 바이로봇과 네이트온 메신저를 소개 하겠다. 바이로봇은 하우리에서 개발된 백신 프로그램으로 신종 바이러스에 보다 효과적인 대응을 위해 스마트 업데이트를 통해 사용자는 최신 버전의 엔진을 유지하여 피해를 최소화 시켜준다. 네이트온 메신저는 SK Communications에서 만든 메신저로써 최근 사용자가 가장 급증하고 있는 메신저이다. 이 프로그램은 프로그램 실행 시 업데이트 서버로 접속하여 버전을 확인한 후 새로운 버전이 있을 경우 자동으로 새 버전을 다운 받도록 하여 최신 버전을 유지하도록 해준다.

이상으로 스마트 업데이트를 이용하는 대표적인 프로그램에 대해서 알아보았다.

3. 개인 사용자를 위한 취약점 분석도구의 설계

3.1 개인 사용자를 위한 취약점 분석도구의 구성도

다음 [그림 1]은 전체적인 구조를 보여준다.

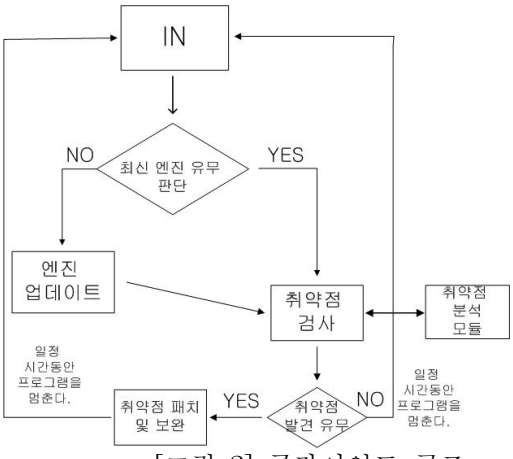
[그림 1] 전체적인 구조

취약점 분석 도구는 클라이언트 부분과 서버, 그리고 패치와 업데이트를 담당하는 파일 서버로 나뉜다.

사용자가 서버로 접속하면 최신버전의 엔진인지 확인하고 최신버전이 아닐 경우 서버에서 가장 트래픽이 덜한 파일 서버와 연결 시켜주어 최신 버전의 엔진을 다운 받도록 한다. 그리고 클라이언트가 취약점을 발견하고 패치가 필요할 경우 파일 서버로 접속하여 패치를 다운 받도록 한다.

3.2 클라이언트 설계

클라이언트의 구조는 [그림 2]와 같다.



[그림 2] 클라이언트 구조

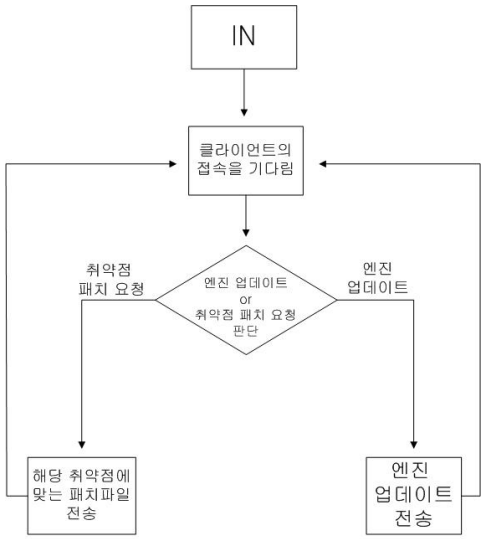
[그림 2]를 설명해 보면 클라이언트는 최신 엔진을 유지하면서 취약점을 검사하고 취약점이 발견되었을 경우 취약점에 따라 알맞은 대응을 하도록 한다. 취약점은 패치를 해야 하는 취약점과 패치를 하지 않아도 되는 취약점으로 나뉜다. 클라이언트에서 취약점을 검사한 후 패치를 해야 하는 취약점일 경우 서버에서 파일서버와 연결 시켜주고 패치를 다운 받도록 한다. 그리고 패치를 하지 않아도 되는 취약점일 경우, 예를 들어 백도어 프로그램이 실행되고 있을 경우 경고 메시지와 확인 절차를 걸쳐 프로세스를 종료 시키도록 하는 것과 같이 취약점에 맞는 대응을 하도록 해 준다.

3.3 서버 설계

서버는 간단하게 설계 및 구현이 이루어진다. 파일서버와 통신 하면서 파일 서버에 접속 해 있는 사용자들을 파악하고 클라이언트의 업데이트 요청이 이루어 질 경우 가장 트래픽이 적은 파일 서버와 클라이언트를 연결 시켜주어 효과적으로 업데이트가 이루어 질 수 있도록 한다.

3.4 파일 서버 설계

파일 서버의 구성은 [그림 3]과 같다.

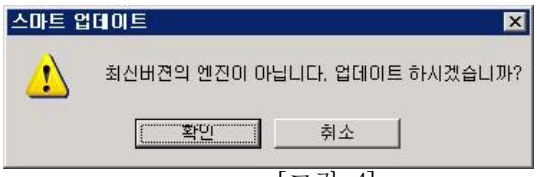


[그림 3] 파일 서버의 구성

클라이언트에서 파일 서버로 접속이 이루어지면 파일 서버는 클라이언트의 요청에 따라 엔진 업데이트, 혹은 취약점 패치를 해준다. 클라이언트 사용자가 늘어나면 파일 서버를 증설할 수 있도록 분산 서버로 설계를 하였다.

4. 실험 결과

[그림 4]는 클라이언트 프로그램 실행 시 스마트 업데이트가 이루어지는 그림이다.



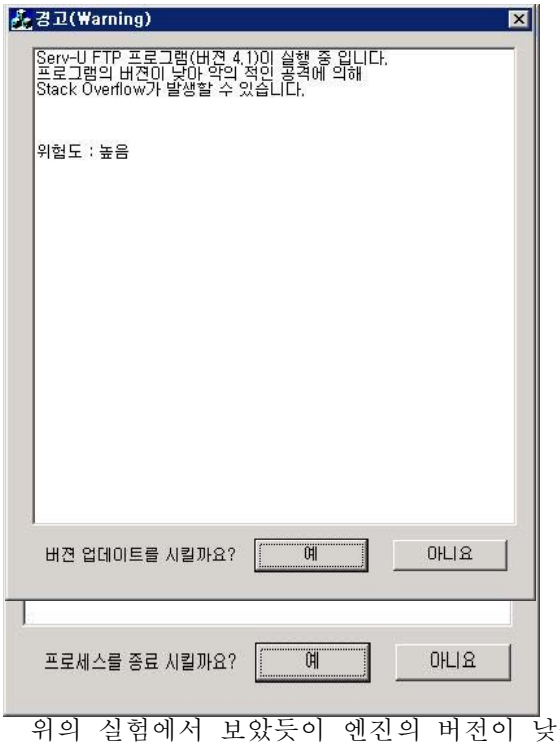
[그림 4]

[그림 5]는 VNC라는 원격 제어 프로그램이 실행되고 있을시 의 경고 메시지와 프로세스를 종료 시킬 것 인가를 묻고 있다.

[그림 5] 취약점 발견 및 보완 I

[그림 6]은 Serv-U라는 FTP 프로그램의 버전이 낮을 경우 스마트 업데이트를 통해 패치 여부를 묻는 그림이다.

[그림 6] 취약점 발견 및 보완 II



위의 실험에서 보았듯이 엔진의 버전이 낮을 경우와 취약점을 분석하고 취약점 보완 및 패치가 효과적으로 이루어짐을 알 수 있다.

5. 결론 및 향후 연구

인터넷이 널리 보급되고 사용되고 있음에도 불구하고 다수의 사용자들이 보안에 대한 무관심과 번거로운 업데이트 때문에 취약점이 보완되지 않아 해킹 사례가 점점 증가하고 있는 실정이다. 따라서 본 논문에서는 컴퓨터를 잘 다루지 못하는 개인 사용자들을 위한 취약점 분석 및 실시간 보완 도구를 제안하여 효과적으로 취약점을 보완할 수 있도록 하였다. 하지만 본 논문에서 제안한 시스템은 MS Windows용 버전만 연구되어 Linux 사용자들을 위한 취약점 분석 및 보완에 관한 연구는 이루어 지지 않았다.

향후 연구과제로는 Linux용 버전도 연구하여 양 플랫폼에서 효과적인 보안이 이루어 질 수 있도록 할 것이다.

참고문헌

[1] http://www.nessus.org
[2] http://www.securityfocus.com
[3] http://msdn.microsoft.com
[4] 김용성 저 "Visual C++ 완벽 가이드" 영진출판사 2002
[5] Richard M. Jones 저 "Introduction to MFC

Programming with Visual C++" Prentice Hall 2002
[6] Addison Wesley 저 "TCP/IP Illustrated Volume 1: The Protocols", 1994
[7] 석원홍, "스마트 업데이트를 이용한 리눅스 보안 시스템" 한국정보과학회 2002. 10
[8] Anthony Jones, Jim Ohlund 저 "NETWORK PROGRAMMING FOR MICOROSOFT WINDOWS" 2003