웹기반 사용자 정보 키로그해킹 방지를 위한 입력 시스템

장 욱*, 최현영**, 민성기**
*고려대학교 컴퓨터정보통신대학원
**고려대학교 컴퓨터학과
{james,neongas,sgmin}@korea.ac.kr

An Input System to Prevent Keylog-Hacking for User Information Based on Web

Uk Jang*, Hyon-Young Choi**, Sung-Gi Min**
*Graduate School of Computer & Information Technology, Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

최근 고객의 컴퓨터와 개인 정보를 보호하기 위하여 개인용 컴퓨터 방화벽과 바이러스 백신의 사용이 점차 증가하고 있다. 그러나 개인용 컴퓨터 방화벽과 바이러스 백신은 이미 존재하거나 발견된 해킹 툴과 바이러스에 대해서만 개인 정보를 보호하기 때문에 한계가 존재한다. 따라서 원천적으로 개인 정보의 유출을 막을 수 있는 솔루션이 필요하다. 그 대표적인 것이 키로그(Keylog) 해킹방지 시스템이다. 이 시스템에서는 키보드의 입력을 암호화하거나 별도의 키보드 드라이버를 생성하여 개인 정보를 보호한다. 하지만 암호화하기 전 단계인 하드웨어 단계에서 개인 정보 유출과 오류로 인한 시스템의 미설치의 문제점이 여전히 존재한다. 본 논문에서는 웹사이트에서 발생하는 이러한 문제점들을 극복하기 위한 하나의 방법으로 KLD(Keyboard Logger Defense) 시스템을 제안하였다. 이 시스템은 키보드 사용으로 발생되는 근본적인 문제점을 해결하기 위하여 웹기반 마우스 입력방식을 사용하였고, 테스트 결과 기존 키로거(Keylogger) 프로그램에 대해서 입력한 키 데이터가 보호됨을 알 수 있었다.

1. 서론

개인용 컴퓨터 보급이 확대되고 인터넷이 일상화되면서 인터넷을 통한 전자상거래의 중요성이 높아지고 있고, 그 규모에 있어서도 급격하게 확대되고 있다. 통계청 발표에 의하면 2005년 2/4분기 우리나라 전자상거래 총 규모는 89조 3,990억원으로, 전년 동분기보다 15.1%가 늘었다[1]. 그러나 전자상거래의 확대는 개인 정보 유출과 같은 정보화 역기능에 대한 문제를 야기시키고 있다. 그래서 이전에는 서버 중심 즉, 서비스 제공 업체의 서버나 네트워크에 대한 보호에 중점적으로 관심을 가졌으나 이제는 이용 고객들의 개인 정보의 안전을 더 생각하게 되었다[2].

이러한 요구에 부응하기 위하여 최근 고객의 컴퓨터와 개인 정보를 보호하는 솔루션이 점차 증가하고 있다[3]. 그 중에서 개인용 컴퓨터 방화벽과 바이러스 백신이 대표적이다. 그러나 개인용 컴퓨터 방화벽이나 바이러스 백신은 이미 존재하거나 발견된 해킹 툴과 바이러스에 대해서만 개인 정보를 보호하기 때문에 한계가 존재한다[4]. 따라서 원천적으로 개인 정보의 유출을 막을 수 있는 솔루션이 필요하다. 그 대표적인 것이 키로그(Keylog) 해킹방지 시스템[4]이다. 이 시스템에서는 키보드의 입력을 암호화하거나 별도의 키보드 드라이버를 생성하여 개인 정보를 보호한다. 하지만 암호화하기 전 단계인 하드웨어 단계에서 개인 정보 유출과 오류로 인한 시스템 미설치의 문제점이 여전히 존재한다. 또한 이런 문제점들은 키보드 사용으로 인한 근본적인 문제점을 가지고 있기 때문에 기존과 다른 입력 방식이 필요하다.

본 논문에서는 웹사이트에서 이러한 문제점들을 극복하기 위한 하나의 방법으로 KLD(Keyboard

Logger Defense) 시스템을 제안하고자 한다. 제안 시스템은 키보드 사용으로 발생하는 근본적인 문제점을 해결하기 위하여 웹기반 마우스 입력 방식을 사용한다. 대표적인 키로거(Keylogger)[4] 프로그램을 사용하여 KLD 시스템에서 입력한 정보의 유출 여부를 테스트하고, 결론 및 향후 연구에 대하여 논의하고자 한다.

2. 관련 연구

다음은 키로그 해킹방지 시스템을 살펴보기 이전에 원인이 되는 키로거 프로그램과 문제점에 대하여 살펴보기로 한다.

2.1 키로거(Keylogger) 프로그램

키로거 프로그램은 사용자가 입력한 키 입력 정보를 특정한 위치에 저장하여 개인 정보를 읽어가는 방식으로 되어 있으며, 이는 크게 어플리케이션(Application) 레벨에서 수행되는 방식과 디바이스 드라이버(Device Driver) 레벨에서 수행되는 방식으로 나누어 볼 수 있다.

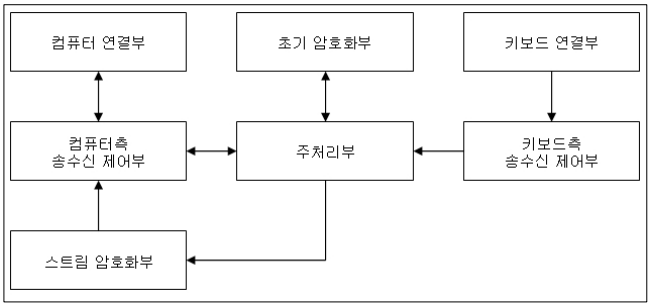
어플리케이션 레벨에서 수행되는 방식은 특정 어플리케이션과 동일한 UI(User Interface)를 이용하여 로그인 아이디와 패스워드 같은 개인 정보를 알아내는 방식과 운영체제가 키보드의 키를 읽어 어플리케이션 레벨로 전달하는 과정에서 키를 가로채는 방식으로 되어있다.[5]. 디바이스 드라이버 레벨에서 수행되는 방식은 악의적인 프로그램 수행 시, 키보드의 디바이스 드라이버와 운영체제의 중간에 키로거 디바이스 드라이버를 위치시킴으로써, 키보드로부터의 입력을 가로채는 방식으로 되어있다.

키로거 프로그램들은 인터넷상에서 쉽게 구입할 수 있으며, 일반적으로 공식 판매되는 키로거 프로그램들은 보안을 목적으로 하고 있다. 즉, 키 입력에 대한 로그를 기록하여 컴퓨터 범죄 조사의 목적, 비인가 접근 모니터링, 감사 로그의 저장, 그리고 아이들에 대한 채팅 감시 등을 목적으로 한다는 것이다. 그 종류로는 KEY GHOST, KeyLog Pro, ProBot 등이 있다[6]. 그에 반해 버그베어 웜(Bugbear Worm)이라는 단지 해킹을 목적으로 만들어진 키로거 프로그램도 있다[5].

키로거 프로그램은 관리자의 시스템 보안을 목적으로 개발되었기에 유용하게 사용한다면 아무런 문제가 되지 않으나, 악용될 경우 개인 정보가 유출되는 등 심각한 금전적 손실을 가져오게 된다. 따라서 이러한 문제를 예방할 수 있는 해킹방지 시스템이 필요하다.

2.2 키로그(Keylog) 해킹방지 시스템

키로그 해킹방지 시스템은 크게 3가지로 구분할 수 있다. 즉, 하드웨어 방식, 소프트웨어 방식, 그리고 PKI[7] 연동 보안서비스가 그것이다.



(그림 1) 하드웨어 키로그 해킹방지 시스템

첫째, 하드웨어 방식의 대표적인 키로그 해킹방지 시스템은 (그림 1)과 같다. 이 시스템은 키보드로부터의 키 코드 입력정보를 컴퓨터 시스템으로 전달하는 보안 어댑터로서, 키보드 또는 컴퓨터 시스템으로부터 보안모드 설정 명령을 받은 경우에는 키보드로부터의 키 코드 입력정보를 암호화하여 컴퓨터 시스템에 전달하고, 보안모드 해제 명령을 받거나 보안모드 해제 상태에서는 키보드로부터의 키 코드 입력정보를 암호화하지 않고 컴퓨터 시스템으로 전달하는 구성으로 되어 있다[8].

둘째, 소프트웨어 방식의 키로그 해킹방지 시스템으로서, 키보드 필터 드라이버를 이용하거나 Windows 95 계열의 경우 키보드 Input 서비스인 VKD Filter Keyboard Input을 Hook하여 구현되었다[9].

키보드 필터 드라이버로 구현할 경우, 키로거 프로그램 또한 동일한 드라이버로 구현될 수 있기 때문에 키보드 입력 데이터 보호 시스템의 드라이버가 Load될 때 항상 동일한 드라이버가 존재하는지 검사를 하여, 존재할 경우는 시스템을 재부팅하고 보호 시스템 드라이버를 먼저 Load해야 한다. 이렇게 동일한 키보드 필터 드라이버 중에서 가장 먼저 Load됨으로써 다른 필터 드라이버들보다 먼저 키보드 입력 데이터를 받을 수 있게 된다. 그래서 키보드 입력 데이터가 보호된다. 키보드 Input 서비스인 VKD Filter Keyboard Input을 Hook할 경우 Windows 95가 키보드 데이터를 처리하기 전에 먼

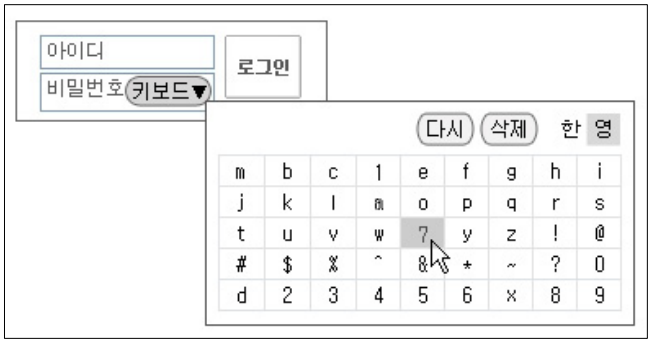
저 드라이버가 키보드 데이터를 받을 수 있기 때문에 키보드 입력 데이터가 보호된다.

셋째, PKI 연동 보안 서비스는 사용자의 신원확인을 위하여 아이디와 패스워드를 사용하지 않고 이미 발급받은 공인 인증서와 인증서 비밀번호를 사용하여 보안 서비스를 제공하고 있다. 또한 네트워크로의 송/수신에 대한 위험을 방지하기 위하여 SSL 또는 TLS을 이용한 보안 서비스를 사용하고 있다[10].

그러나 기존의 키로그 해킹방지 시스템과 PKI 연동 보안 서비스는 문제점들을 가지고 있다. 하드웨어 방식의 시스템의 경우 인터넷 뱅킹이나 증권을 거래하는 모든 고객에 적용하기는 현실적으로 불가능하다. 소프트웨어 방식과 PKI 연동 보안 서비스는 하드웨어 방식보다 해킹에 취약하며, 하드웨어적으로 구현된 키로거 프로그램이 설치되어 있을 경우 그 기능을 상실하게 된다. 그러므로 이와 같은 문제점들을 해결하고자 새로운 입력방식의 키로그 해킹 방지 시스템을 제안하고자 한다.

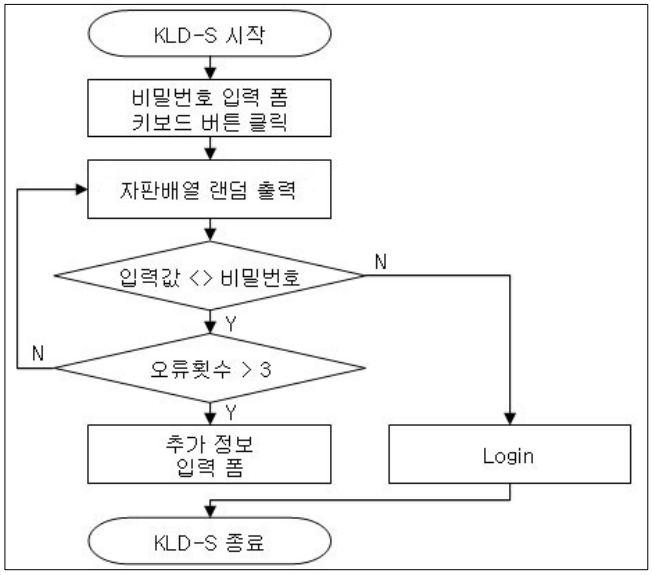
3. KLD(Keyboard Logger Defense) 시스템

기존의 키로그 해킹방지 시스템은 키보드를 사용한 입력방식에 초점을 맞추어 왔다. 하지만 이런 방식은 하드웨어적인 문제점이 발생하기 때문에 개인 정보 유출을 막는 데는 한계가 존재한다. 이로써 키보드를 사용하지 않고 개인 정보를 입력할 수 있는 새로운 입력 시스템인 KLD 시스템을 제안한다.



(그림 2) KLD 시스템 사용자 인터페이스

KLD 시스템은 키보드 사용으로 인한 근본적인 문제점을 해결하기 위하여 마우스를 이용하는 입력방식을 사용한다. (그림 2)와 같이 비밀번호 입력 폼 안에 있는 키보드 버튼을 클릭하면 가상 키보드가 생성되며 생성 시 랜덤 배열 방식으로 구성된 자판이 생성된다. 랜덤 배열 방식의 자판 생성은 마우스 클릭 시 마우스의 위치를 저장하여 비밀번호를 유추하는 방식을 방지하기 위함이다. 생성된 자판을 사용하기 위하여 마우스를 자판위로 위치시키면 마우스 포인터가 가리키는 키만 색이 반전된다. 사용자는 반전된 키를 클릭 함으로서 비밀번호를 입력할 수 있으며, 이로 인하여 입력 오류를 방지할 수 있게 된다.



(그림 3) KLD 시스템 처리 절차

(그림 3)은 KLD 시스템의 처리 절차를 나타내고 있다. 비밀번호 입력 폼에서 키보드 버튼을 클릭하면 랜덤 배열 형식의 자판이 생성된다. 비밀번호를 입력할 때 오류 입력 시 오류 횟수를 3회로 제한하여 그 이상이면 추가 정보 입력 폼으로 이동한다. 랜덤 방식의 자판 배열임에도 불구하고 저장한 마우스 위치를 사용하여 모든 경우를 시도하는 해킹을 방지하기 위하여 오류 횟수 지정은 필요하며 지정한 오류 횟수 이상이면 추가 정보 입력 폼으로 이동하는 동시에 관리자에게 오류 정보가 전달된다. 추가 정보 입력 폼에는 주민등록번호, 성명, 비밀번호 등과 같은 본인만이 알 수 있는 요소로 구성한다.

KLD 시스템은 자바(Java) 프로그래밍 언어를 사용하여 구현하였다. 그렇기 때문에 키로그 해킹방지 시스템의 미설치로 개인 정보가 유출되는 문제점을 미연에 방지할 수 있으며, 웹사이트에 시스템을 삽입하는 방식으로 이루어져 있어서, 시스템 설치로 인한 시간을 낭비하지 않게 한다. 또한 사용자 입장에서의 추가 업데이트도 필요하지 않고, 기존 시스템을 변경할 시에는 웹사이트에 시스템을 추가하는 방식이므로 인터넷상에서 작업 및 유지 보수가 가능한 장점도 있다.

4. 시스템 테스트 및 결과

KLD 시스템을 평가하기 위하여 간단한 테스트를 실시하였다. 테스트는 Windows 2000 Server SP4, Intel Pentium 4 1500MHz, 256MByte 메모리의 환경으로 구성된 PC를 사용하였으며, KLD 시스템은 자바(Java) 프로그램 언어를 사용하여 구현하였다.

KLD 시스템의 평가는 <표 1>과 같은 대표적인 키로거 프로그램을 사용하였고, 테스트 방법은 각각의 키로거 프로그램 실행 후 구현 시스템으로 키 데이터를 입력한 후 키 입력이 로깅(Logging)되었나를 확인하는 것이다.

<표 1> 테스트용 키로거 프로그램

키로거 프로그램	출처
STARR Pro	www.iopus.com
ProBot SE	www.nethunter.cc
Spy Agent	www.spytech-web.com
Red Hand	www.redhandsecurity.com
IK Stealth	www.amecisco.com
Ghost Keylogger	www.keylogger.net
KEYSPY	www.kings.co.kr
TestKeyLog	www.anti-keylog.com

키로거 프로그램에 대하여 키보드 키 데이터가 노출되지 않는지를 테스트한 결과는 <표 2>와 같다. 테스트한 결과 기존의 키로깅에 대해서 완벽하게 차단하는 기능을 보여주고 있다.

<표 2> 테스트 결과

키로거 프로그램	키 보호 여부
STARR Pro	보호
ProBot SE	보호
Spy Agent	보호
Red Hand	보호
IK Stealth	보호
Ghost Keylogger	보호
KEYSPY	보호
TestKeyLog	보호

5. 결론 및 향후 연구

본 논문에서는 기존의 키로그 해킹방지 시스템이 가지고 있는 문제점인 암호화하기 전 단계인 하드웨어단계에서 개인 정보 유출과 오류로 인한 시스템의 미설치로 개인 정보의 유출 방지를 해소하기 위하여 KLD 시스템을 제안하였다. 제안한 시스템은 키보드 사용으로 발생되는 근본적인 문제점을 해결하기 위하여 웹기반 마우스 입력 방식을 사용하였다. 그리고, 대표적인 8가지 키로거 프로그램을 사용하여 테스트한 결과 입력한 데이터 정보에 대한 보호가 매우 뛰어남을 확인할 수 있었다.

제안한 KLD 시스템은 증권 거래 시스템, 은행 계좌 입력 및 로그인(Login), 인증서 비밀번호 입력 등의 키보드 보안이 필수적으로 요구되는 시스템에 적용될 수 있을 것이다.

향후에는 마우스를 사용하여 가상 키보드에 입력하는 방식으로 인한 사용자가 느끼는 불편함을 좀 더 보완해야 하겠다.

참고문헌

[1] 통계청, “2005년 2/4분기 전자상거래통계조사 결과” 통계청 보도자료, 2005. 9.

[2] 재정경제위원회, “전자금융거래법” 제정안입법예고, 2004. 8.

[3] 한국정보보호진흥원, “2005정보보호실태조사”, 보고서자료, 2005. 6.

[4] 유영일, “해킹 할 것인가 해킹 당할 것인가”, 삼각형프레스, 2000. 5.

[5] 안철수연구소, “안티키로거를 이용한 개인 정보 보호(1)”, http://www.ahnlab.com/securityinfo/tech_view.jsp, 2003. 3.

[6] http://www.keylogger.org, KEYLOGGER.ORG.

[7] 김동준, “온라인 증권거래에 PKI 기반 인증을 적용하기 위한 방법”, 서강대학교 정보통신대학원 석사학위논문, 2001.

[8] 주식회사 세이프텍, "보안기능을 갖는 어댑터 및 이를 이용한 컴퓨터 보안시스템", 특허청, 특허번호 10-2001-7003927, 2001. 3.

[9] Mark Russinovich, "Ctr2lCap for Windows 95", "http://www.sysinternals.com/win9x/utilities/ctrl2cap95.shtml".

[10] 류현우, “공개키와 SSL을 이용한 전자상거래 사용자 인증시스템 설계 및 구현”, 명지대학교대학원 석사학위논문, 2000.