White Paper

AhnLab Online Security,
간편하고 안전한 통합 온라인 보안 서비스

Revision Version: AhnLab Online Security White Paper ver. 1.0.1
Release Date: November 14, 2008

AhnLab, Inc.
6th Fl., CCMM Bldg.
12 Yeouido-dong,
Yeongdeungpo-gu, Seoul 150-869,
Korea
82-2-2186-6000
www.ahnlab.com

Table of Contents

Ⅰ. Introduction ---------- 3

Ⅱ. 해킹의 패러다임 변화와 공격 유형---------- 3

해킹 패러다임의 변화 ---------- 3
웹 해킹 프로세스 ---------- 5
웹 해킹의 유형 ---------- 6
웹 해킹 대응의 어려움 ---------- 7

Ⅲ. AhnLab Online Security(AOS)란 ---------- 8

Ⅳ. AhnLab Online Security(AOS) Technology ---------- 9

AOS Smart Update i ---------- 9
AOS Anti-Keylogger ---------- 10
AOS Firewall ---------- 15
AOS Anti-Virus&Spyware ---------- 16
AOS SecureBrowser ---------- 17
AOS SecureBrowser 보안 기술 ---------- 17
보안 전용 브라우저 및 AOS SecureBrowser의 장점 ---------- 19

Ⅴ. Conclusion ---------- 21

I. Introduction

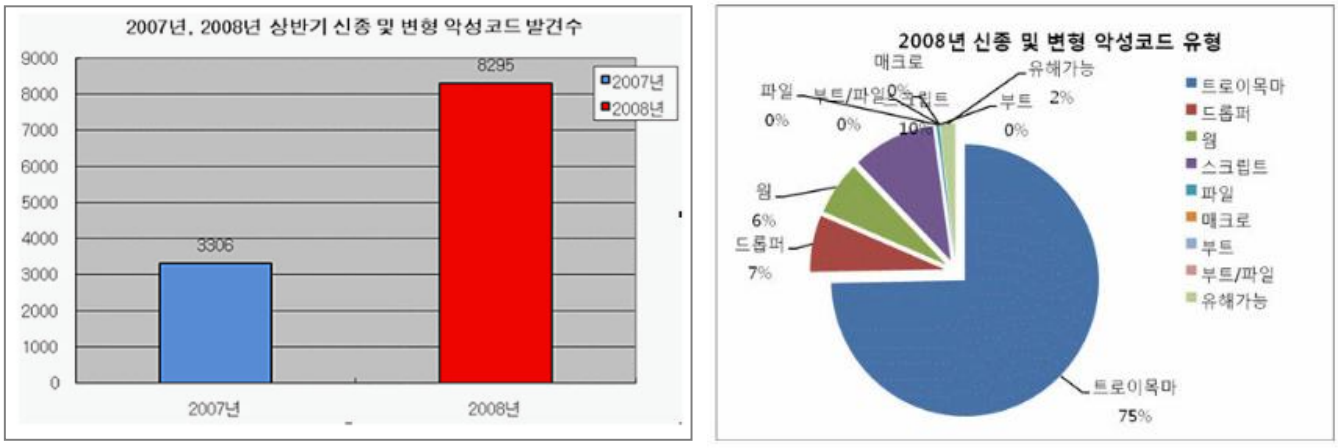
인터넷의 발달은 개인은 물론 전 산업 분야에 걸쳐 커다란 패러다임의 변화를 가져왔다. 인터넷 포털/온라인 게임/온라인 쇼핑몰 등 새로운 산업을 태동시켰으며, 온라인 은행거래/증권거래/교육 등 기존 오프라인 산업과 결합해 새로운 부가가치를 창출하고 있다.
하지만 인터넷이 비즈니스의 중심으로 자리잡으면서 각종 보안위협 및 그로 인한 피해가 기하급수적으로 늘어나고 있다. 특히, 금전적 이익을 목적으로 하는 해킹 범죄가 급증하고 있으며, 이에 따라 해킹의 유형 또한 특정 대상을 목표로 하는 전문화•조직화•국지화 경향을 띠고 있다. 이러한 해킹의 패러다임 변화 속에서 안전한 인터넷 서비스 제공은 기업들에게 있어서 매우 중요한 과제가 되고 있다. 즉, 개인정보 보호와 전자금융거래의 안정성 확보를 위해 보안 기술에 있어서도 새로운 변화를 수용해야 할 시점이 된 것이다.

본 문서에서는 전자금융거래 및 개인정보 수집 단계에서 발생할 수 있는 해킹 유형의 확인을 통하여 현재 보안 환경에서 취약한 부분을 살펴보고, 이를 보완할 수 있는 온라인 통합 보안제품인 AhnLab Online Security(이하 AOS)에 대해 기술하고자 한다.

II. 해킹 패러다임의 변화와 공격유형

1. 해킹 패러다임의 변화

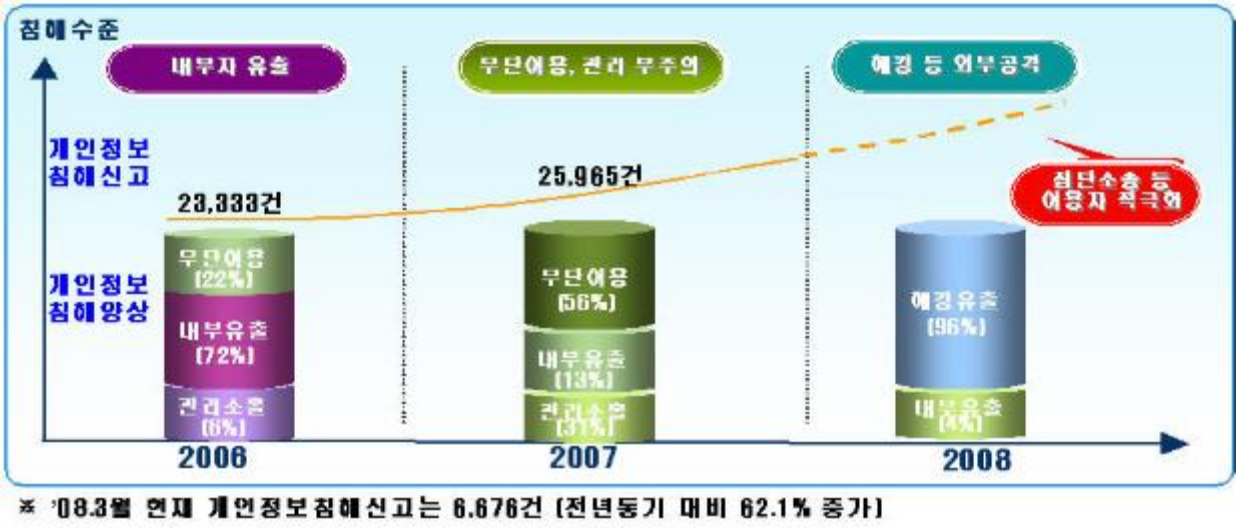
최근 한국의 악성코드 동향을 보면 중국 발 해킹과 함께 일반 클라이언트를 대상으로 매우 국지적으로 발생하였다는 뚜렷한 특징을 가지고 있다. 특히 악성코드들의 변형 발견 시간은 점점 짧아지고 있으며, 그에 따른 악성코드의 수는 폭발적인 증가를 기록하고 있다.



출처: "2008년 상반기 ASEC 리포트", 안철수연구소, 2008.07.22

<그림 1> 2007 년, 2008 년 상반기 신종 및 변형 악성코드 발견 수 / 변형 악성코드 유형

<그림 1>을 살펴보면 2008년 상반기 악성코드 발견 수는 전년 동기 대비 무려 151%가 증가하였으며, 특히 트로이목마와 스크립트 유형이 가장 많은 비중을 차지하고 있음을 확인할 수 있다. 이러한 결과는 스크립트를 이용한 악성코드의 배포와 트로이목마를 이용해 사용자 정보를 탈취하려는 목적이 크기 때문이다.



출처: "인터넷상 개인정보 침해방지 대책", 방송통신위원회, 2008.04.

<그림 2> 개인정보 침해신고 및 침해양상 변화

이러한 상황을 반영하듯 <그림 2>와 같이 개인정보 침해 신고 또한 지속적으로 증가하고 있다. 특히 주목해야 할 사항은 2008년 개인정보 침해 신고의 96%가 해킹에 의한 유출이었다는 점이다. 이는 '사이버 블랙마켓'을 통한 대가성 범죄가 증가하고 있다는 것을 의미한다.

이렇듯, 해킹 범죄가 자기 과시나 시스템 마비 목적에서 금전적 이익을 추구하는 쪽으로 바뀌면서, 해킹에 대한 패러다임 또한 함께 변화하고 있다. 이러한 해킹 패러다임 변화의 특징을 종합해 보면 다음과 같다.

1) 공격 형태가 단순하지 않고 다수의 기법을 악용하는 복합 공격이 늘어나고 있다.
2) 공격 대상이 전세계 불특정 다수에서 한 회사, 한 커뮤니티 등으로 국지화되고 있다.
3) 개인 범죄에서 글로벌화 된 조직범죄로 집단화되고 있으며, 해킹의 분업화가 이루어지고 있다.
4) 공격 유형이 음성적인 형태로 변화해, 해킹 유무를 쉽게 알아차릴 수 없다.

이러한 해킹의 패러다임 변화 속에서 개인정보 보호와 전자금융거래의 안정성 확보는 매우 중요한 과제라 할 수 있다. 그리고, 해킹 패러다임의 변화는 전자금융거래 보호 기술에 있어서도 새로운 변화를 요구하고 있는 것이다.

2. 웹 해킹 프로세스

웹 해킹(Web Hacking)이란 웹을 통해서 발생되는 해킹을 말한다. 이는 복잡하고 상위 개념의 기술에 의존적인 시스템 해킹과 구분하기 위해서 부르는 것으로 웹의 중요성과 더불어 웹 서비스에 특화된 해킹 기법을 가리킨다.

초기 해킹 기법은 운영체제나 네트워크 구조를 숙지하고 있어야 가능한 수준으로 시스템의 취약점을 찾아내는 것이 어려워 사회 공학(Social Engineering)과 같이 시스템이나 네트워크 관리자를 속여 중요 정보를 획득하는 것이 중요 기법이었다. 하지만 2000년대부터는 분산 서비스 공격 또는 트로이 목마와 같은 유형의 공격들이 나타나게 되었으며, 현재는 바이러스와 해킹의 경계선까지도 모호해지고 있는 상황이다.

<그림3 > 일반적인 웹 해킹 프로세스

이러한 웹 해킹 실행 프로세스는 <그림 3>에서와 같이 크게 4단계로 구분해 볼 수 있다.

첫 번째 단계는 해킹할 대상 즉, 특정 시스템 또는 애플리케이션 등에 대하여 디버깅(Debugging)이나 리버스 엔지니어링(Reverse engineering)과 같은 분석 기술을 사용하여 시스템의 취약점을 찾아내는 단계이다.
이 단계에서 해커는 공격에 필요한 정보를 수집하고, 수집된 정보를 목록화하며, 공격 목적에 따라 애플리케이션 공격 또는 시스템 계정 획득을 위한 악성 스크립트의 제작, 서비스 장애 유발 등 다양한 공격 시나리오를 구성할 수 있다. 하지만 다양한 보안 장치를 갖추고 있는 전자금융거래 시스템에서의 취약점 분석은 쉽지 않은 일이며, 분석을 위해 많은 시간과 비용이 투입된다. 그러나 최근에는 전문 해킹그룹을 통해 조직적으로 분석을 진행하거나, 운영체제 제작사에서 발표하는 보안 패치를 적용하지 않은 사용자를 타깃으로 한 취약점 분석이 일반화 되고 있다.

두 번째 단계는 분석된 취약성을 바탕으로 공격자가 세운 공격 시나리오대로 점검해 나가는 단계이다.
이때 각종 공격 코드와 공격 기법들을 바탕으로 시나리오에 의해 하나씩 시도하게 된다. 이 단계에서 해커는 시나리오의 오류를 수정하고, 해킹툴 제작을 위한 준비를 마치게 된다.

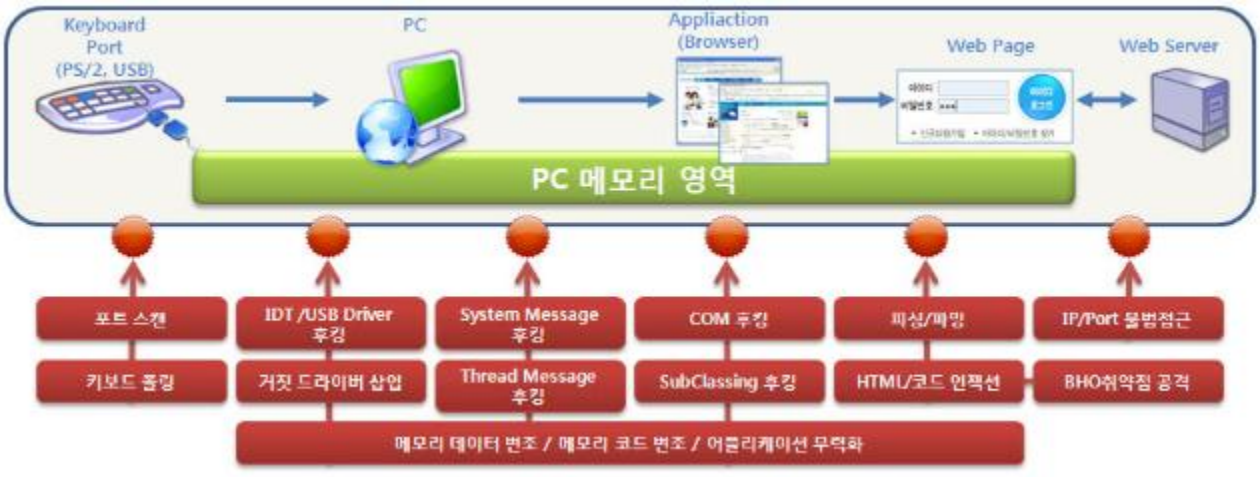
세 번째 단계는 분석 및 수정한 결과를 바탕으로 해커가 원하는 기능을 수행하는 해킹툴을 제작하는 단계이다.
해커는 공격 대상 및 배포 방법을 고려하여, 스크립트 형태나 트로이 목마, 웜, 바이러스의 형태로 제작한다.

마지막 단계는 제작한 해킹툴을 이용하여 해킹을 실행하거나 해킹툴을 배포하는 단계이다.
최근에는 해킹 실행조직 또는 개인에게 프로그램 및 해킹 방법을 판매하고, 이를 유지 보수해 주는 사례까지 발견되고 있다. 크로스사이트 스크립팅(XSS), ARP스푸핑, 스플로그(Splog) 등을 이용해 대량의 사용자를 일시에 감염시키는 사례 또한 증가하고 있다. 이와 함께 최근에는 다운로더를 이용한 패키지 형태의 해킹툴 제작이 늘어나고 있다.

3. 웹 해킹의 유형

앞에서 살펴본 것처럼 취약점을 분석하여 이를 공격할 목적으로 제작 배포된 해킹툴이 일반적인 웹 프로세스 환경에서 어떻게 구현되어 해킹이 일어나는지 알아보자.

웹 서비스에 필요한 요소를 생각해 보면, 웹 서버와 사용자 인증 모듈, 웹 브라우저와 같은 애플리케이션, 애플리케이션을 구동시키기 위한 PC 시스템, 그리고 Input 장치인 키보드 등이 있다. 문제는 이러한 모든 구성요소들에 각각 다른 취약점과 위협 요소가 존재한다는 것이다.



<그림 4 > 웹 해킹의 유형

<그림 4>는 전자금융거래 프로세스와 각 구성 요소 별로 발생할 수 있는 해킹 위협 요소를 보여주고 있다. 이를 통해 전자금융거래 트랜잭션이 진행되는 모든 단계에서 해킹이 발생할 수 있음을 알 수 있다.
이때 간과하지 말아야 할 것은 해킹의 패러다임 변화 속에서 해커는 해킹의 난이도를 따지지 않으며, 목적한 이익을 위해 끊임없이 취약점을 찾아내기 위한 분석을 진행한다는 것이다. 더욱이 해킹의 패러다임 변화가 가져온 전용 해킹툴의 생산과 판매는 기존에 상급 이상의 해킹 지식이 있어야만

가능했던 웹 해킹을 돈만 있으면 누구나 쉽게 시도할 수 있게 되었다. 이는 안정적인 전자금융거래 서비스에 큰 위협요소로 작용하고 있다.

4. 웹 해킹 대응의 어려움

기업들의 많은 노력에도 불구하고 웹 프로세스를 구성하는 각각의 요소에 끊임없이 해킹이 일어나는 이유는 아래와 같다.

1) 웹 해킹의 대상이 되는 사용자PC는 항상 취약하다.

고객사의 웹 서비스를 이용하는 사용자 PC 환경은 천차만별이다. 또한 기본적인 안티바이러스 제품과 OS 공급업체에서 제공하는 보안 패치조차도 적절히 활용하지 않는 사용자가 상당히 많다. 또한 해킹 패러다임의 변화와 함께 폭발적으로 증가하고 있는 트로이목마 및 다운로더 등의 악성코드는 보안상 취약한 이러한 PC들을 기반으로 웹 해킹에 활용되고 있다.

2) 공용 프로세스, 즉 웹 브라우저는 자체 보안의 한계점을 가지고 있다.

웹 트랜잭션에 사용하는 웹 브라우저, 그 중에서 국내에서 90% 이상의 시장을 점유하고 있는 인터넷 익스플로러(Internet Explorer)는 대표적인 범용 웹 브라우저이다. 하나의 웹 브라우저를 통해서 모든 일을 처리한다. 웹 서핑, 인터넷 뱅킹, 게임 등은 물론이고, 쇼핑몰을 통한 결제를 진행하기도 한다.

가령 현실 세계에서 하나의 그릇에 밥도 먹고, 물도 마시고, 얼굴도 씻고, 손발도 씻는 용도로 사용한다고 가정해 보자. 이 경우 관리를 아무리 철저히 한다 하더라도 위생상 문제점이 생길 수 밖에 없을 것이다. 마찬가지로 웹 브라우저 또한 이렇게 범용적인 목적으로 사용하다 보니 웹 브라우저가 사용하고 있는 각종 컴퓨터 자원 보호에 문제가 생기기 마련이다. 해커들은 이러한 문제점을 악용해 불특정 다수를 공격하고 있는 것이다.

이러한 웹 브라우저는 운영체제에서 사용하는 대부분의 파일 및 애플리케이션을 로드할 수 있다. 따라서 웹 브라우저를 공격 대상으로 하는 공격코드는 웹 브라우저 내에 존재하는 취약점뿐만 아니라 취약점이 존재하는 다른 애플리케이션을 공격대상으로 삼을 수 있다. 또한 범용 웹 브라우저로 사용하고 있는 인터넷 익스플로러는 액티브엑스(ActiveX) 취약점, 컴(COM) 후킹과 스크립트(Script) 조작, BHO(Browser Helper Object) 기능을 이용한 정보 탈취 등 많은 구조적 취약점을 가지고 있다.

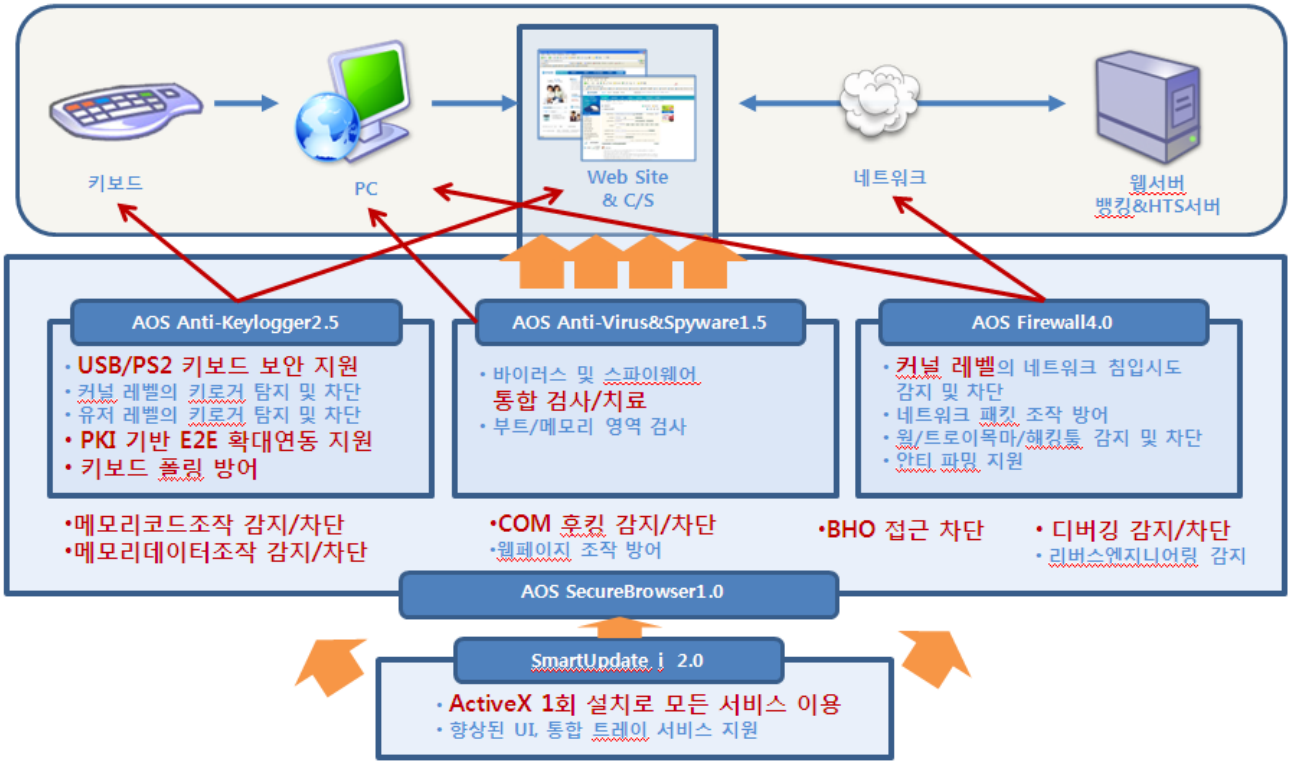
더욱이 인터넷 익스플로러와 같은 범용 웹 브라우저에서의 해킹 사고 발생 시에는 정보 조작 여부를 판단하는데 많은 어려움이 있다.

3) 우리가 일반적으로 사용하고 있는 PC 및 Windows OS는 메모리 영역을 보호해 주지 않는다.

현재 우리가 사용하고 있는 PC는 모두 '폰 노이만 구조'를 따르고 있다. 이는 데이터 메모리와 프로그램 메모리가 구분되어 있지 않고 하나의 버스를 가지고 있는 구조를 말하며, 모든 데이터와 코드가 메모리를 거쳐 처리됨을 의미한다.

우리가 일반적으로 사용하고 있는 32bit Windows OS는 각각의 프로세스마다 4기가의 가상 메모리를 할당한다. 하지만, 이는 관리를 목적으로 한 주소 공간의 격리이지 보안을 목적으로 하고 있지 않으며, OpenProcess, VirtualProtectEx, ReadProcessMemory, WriteProcessMemory 등 타 프로세스의 메모리에 접근할 수 있는 다양한 함수를 제공한다.

III. AhnLab Online Security(AOS)란



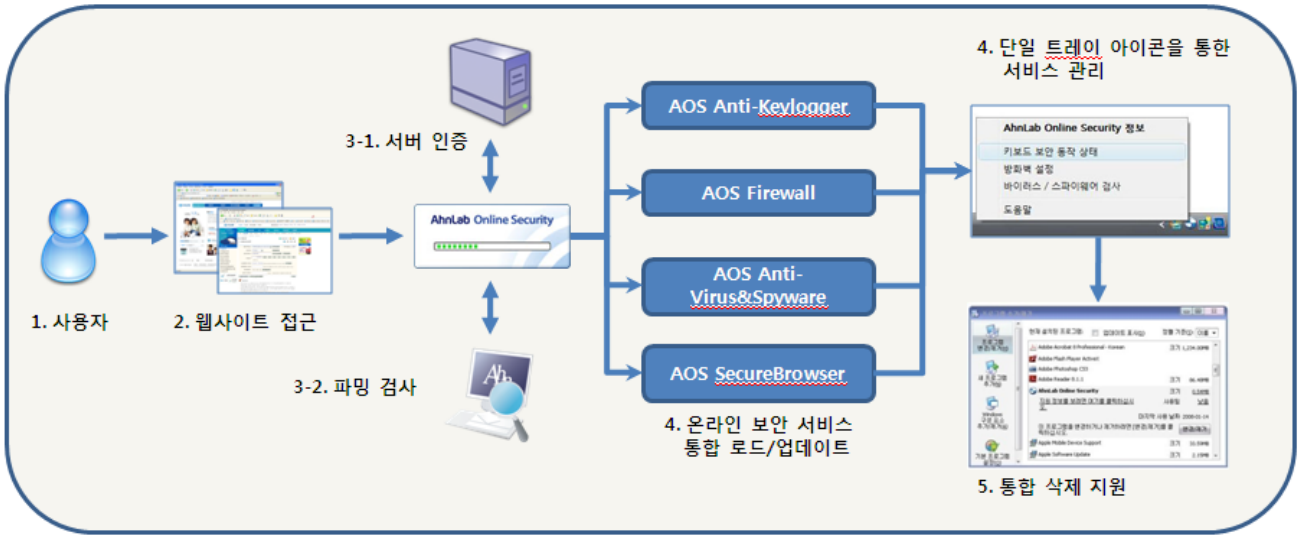
<그림 5 > AhnLab Online Security 서비스 개요

AhnLab Online Security(이하 AOS)는 해킹 패러다임 변화에 능동적으로 대처하기 위해 개발된 온라인 통합 보안 서비스이다. AOS는 키보드보안, PC 방화벽, 안티-바이러스/스파이웨어, 시큐어브라우저 등으로 구성되어 있다. 모듈화를 통해 단 한번의 프로그램 설치로 모든 서비스 이용이 가능하다.

AOS Anti-Keylogger는 키보드를 통한 정보 유출을 방지하며, AOS Firewall은 네트워크 침입 시도를 감지 및 차단한다. 안철수연구소의 V3 엔진을 사용하는 AOS Anti-Virus&spyware는 바이러스와 스파이웨어를 통합 검사/치료해주며, AOS SecureBrowser는 메모리 해킹을 포함한 전방위적인 해킹 감지 및 차단이 가능한 전용브라우저이다.

IV. AhnLab Online Security (AOS) Technology

1. AOS Smart Update i



<그림 6> AOS Smart Update i 의 특징 및 장점

AOS는 웹사이트에 접근하는 모든 사용자를 보호하는 것이 이 프로그램의 근본 목적이다. AOS는 사용자의 웹사이트 접근 또는 고객사가 지정한 이벤트 발생시 의무적으로 프로그램을 설치/동작하게 되며, 사용자가 고객사의 웹사이트를 벗어나거나 이벤트 종료 시 자동으로 프로그램 실행을 종료하게 된다.

AOS Smart Update i(이하 SUI)는 <그림 6>과 같이 AOS의 설치/삭제, 안티파밍, 서비스 모듈 연동, 통합UI 기능을 제공하는 launcher로서 동작 프로세스 별로 아래와 같은 특징 및 장점을 가지고 있다.

- **제품 통합 설치 및 인증:** AOS는 Internet Explorer가 제공하는 ActiveX 및 Firefox의 Plug-in 기술을 통해 설치되며, SUI는 서버 인증을 통해서 사이트에 필요한 ActiveX 및 Plug-in을 등록•업그레이드 해준다. 사용자는 최초 SUI의 설치 만으로 AOS의 모든 서비스를 이용할 수 있어, 타사 온라인 보안 서비스와 같이 여러 번 프로그램을 설치해야 하는 번거로움을 줄일 수 있다.

- **다국어 지원:** AOS에 해당되는 모든 서비스는 인증파일에 기술된 언어코드로 작동하게 되어 있어, 제품의 변경 없이 한국어 이외에 영어, 일본어, 스페인어, 포르투갈어 등을 추가로 사용할 수 있다.

- **설치 장애에 대한 대응:** SUI 및 AOS는 설치 프로세스는 기본적으로 암호화 되어 있으며, 설치 파일 삭제 및 위변조 방지를 위한 체크 기능이 포함되어 있다. 만약, 최초 설치 시 파일 검증실패로 설치장애가 발생하면, 에러 메시지와 함께 AOS Anti-Virus&Spyware로 치료를 유도하며, 기존에 설치된 적이 있는 경우에서 파일검증 실패 시, '바이러스/스파이웨어 감염 가능성'을 알리고 치료를 유도한다. 또한, 기타 설치 장애 발생시, 자동으로 에러 메시지를 표시하고 에러코드에 해당하는 FAQ 링크를

표시해 주어, 사용자가 스스로 문제 해결을 할 수 있도록 한다.

- **안티 파밍 대응:** 파밍으로 해당 사이트에 접속이 안 되는 경우라고 하더라도 AOS 서비스가 적용된 다른 사이트로 접속 시에 잘못된 정보가 Hosts 파일에 있는지 검증하고 삭제한다.

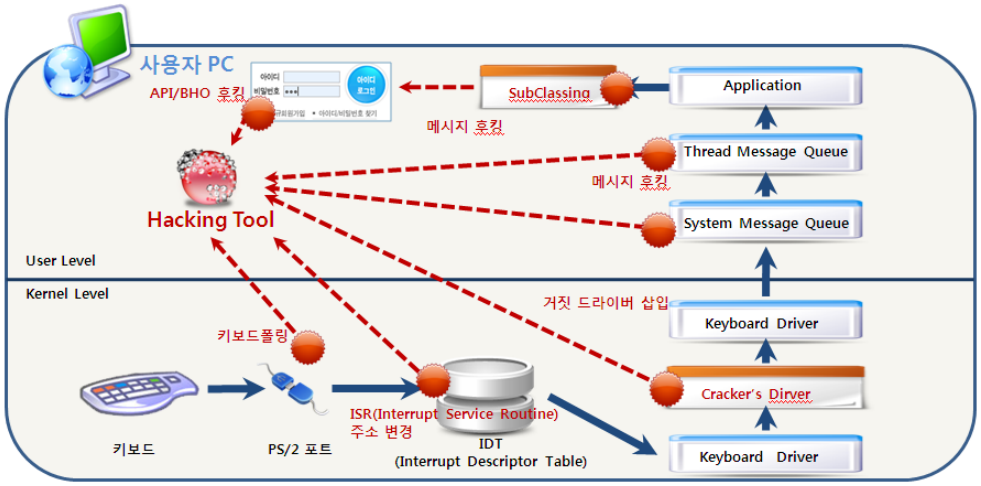
- **통합 UI 및 통합 삭제 지원:** AOS는 트레이아이콘 1개와 툴팁, 메뉴로 모든 서비스 상태를 알려주며, 그 역할을 SUI가 담당한다. 또한AOS 설치 시, 제어판에 'AhnLab Online Security'라는 이름으로 등록 되며, 삭제 시 AOS에 포함된 모든 서비스가 함께 삭제 된다.

2. AOS Anti-Keylogger

AOS Anti-Keylogger는 키보드를 통해 입력되는 중요한 개인정보(비밀번호, 계좌번호, 주민등록번호 등)를 암호화해 보호해주는 프로그램으로, 키로거(Key-logger) 프로그램이나 해킹 툴의 공격으로부터 개인 정보가 유출되는 것을 차단해 주는 서비스이다.

일반적으로 사용하는 키보드는 PS/2와 USB 방식으로 나뉘며, 접속 방식에 따라 입력 절차상에 아래와 같은 취약점을 가지고 있다.

1) PS/2 키보드 동작 방식 및 보안 취약점



<그림 7> PS/2 방식의 키보드 보안 취약점

PS/2 포트는 IBM이 개발한 키보드 및 마우스 전용 접속용 포트로서 장치제어를 위해 PC 내부에 Intel 8042(i8042) Keyboard Controller를 사용한다. <그림 7>은 PS/2 방식의 키보드 입력 처리 절차 및 발생 가능한 해킹 위협요소를 표시한 것으로 구체적인 내용은 아래와 같다

[Kernel Level의 해킹 위협 요소]

Port Monitoring (PS/2 방식 키보드): 사용자의 키 입력 후 키보드 Port 에 쓰여진 입력 값은 일정 시간 메인보드의 키보드 Port 에 남아있게 된다. 악성프로그램이 메인보드의 키보드 Port 에 남아있는 키보드 데이터를 읽어갈 수 있으며, 이를 Port Scanning/Monitoring 이라고 한다

IDT Hooking (PS/2 방식 키보드): IDT (Interrupt Descriptor Table)은 인터럽트(interrupt)를 처리하는 루틴인 ISR (Interrupt Service Routine)의 주소를 저장하고 있으며, 악성 프로그램은 사용자의 키보드 인터럽트가 발생했을 때 입력을 가로채기 위해 IDT 에 저장된 ISR 의 주소를 자신의 ISR 의 주소로 변경할 수 있다.

Filter (Client) Driver Hooking/Filtering (PS/2, USB 타입 키보드): Windows OS 커널은 키보드 입력 데이터를 제어하기 위해 Filter Driver (Client Driver)의 형태로 사용자의 키 입력을 얻을 수 있도록 지원한다. 악성 프로그램은 일반적인 키보드 Filter Driver 나 Client Driver 의 하단에 설치되어 사용자의 입력 값을 획득할 수 있다.

[**User Level의 해킹 위협 요소]**

Message Hooking(PS/2, USB 타입 키보드): 악성 프로그램이 윈도우에서 사용하는 메시지 큐 (System Message Queue, Thread Message Queue)를 후킹(hooking)하여 사용자의 키 입력 값을 획득할 수 있다.

SubClassing(PS/2, USB 타입 키보드): 각 윈도우 어플리케이션은 메시지 처리를 위해서 Windows Procedure 를 가지고 있다. 악성 프로그램은 이 Windows Procedure 를 재 설정하는 방법으로 사용자의 키보드 입력 값을 획득할 수 있다.

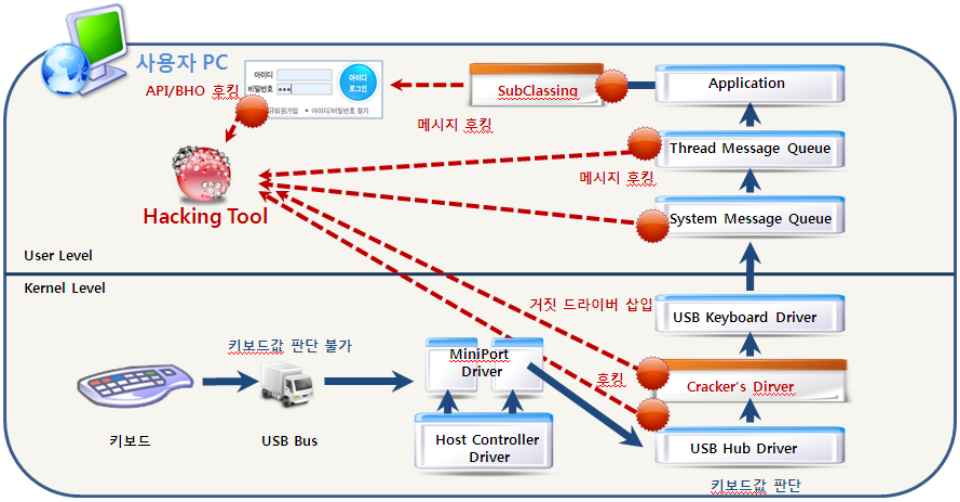
BHO Hooking(PS/2, USB 타입 키보드): BHO (Browser Helper Object)는 브라우저 구동 시 동시에 로딩되어 브라우저에서 일어나는 일을 감시할 수 있도록 IE 가 지원하는 기능을 사용하는 모듈이며, 악성 프로그램은 BHO 의 형태로 IE 에서 사용자의 키보드 입력 값을 획득할 수 있다.

API Hooking(PS/2, USB 타입 키보드): 실행중인 프로세스에 인잭션(Injection) 한 후 키보드 입력 처리에 관련된 windows API, 즉, DrawText, DrawTextEx, ExtTextOut 등의 함수를 Hooking 하여 입/출력 파라미터를 모니터링 하는 방식으로 사용자의 키보드 입력 값을 획득할 수 있다.

Memory Scan(PS/2, USB 타입 키보드): 실행중인 프로세스의 메모리를 스캔(Scan)하여 메모리 상에 저장된 사용자의 키보드 입력 값을 획득할 수 있다.

Screen Capture(PS/2, USB 타입 키보드): 사용자의 입력 값이 Text 인 경우 화면에 입력된 값을 screen capture 기능을 통해서 획득할 수 있다.

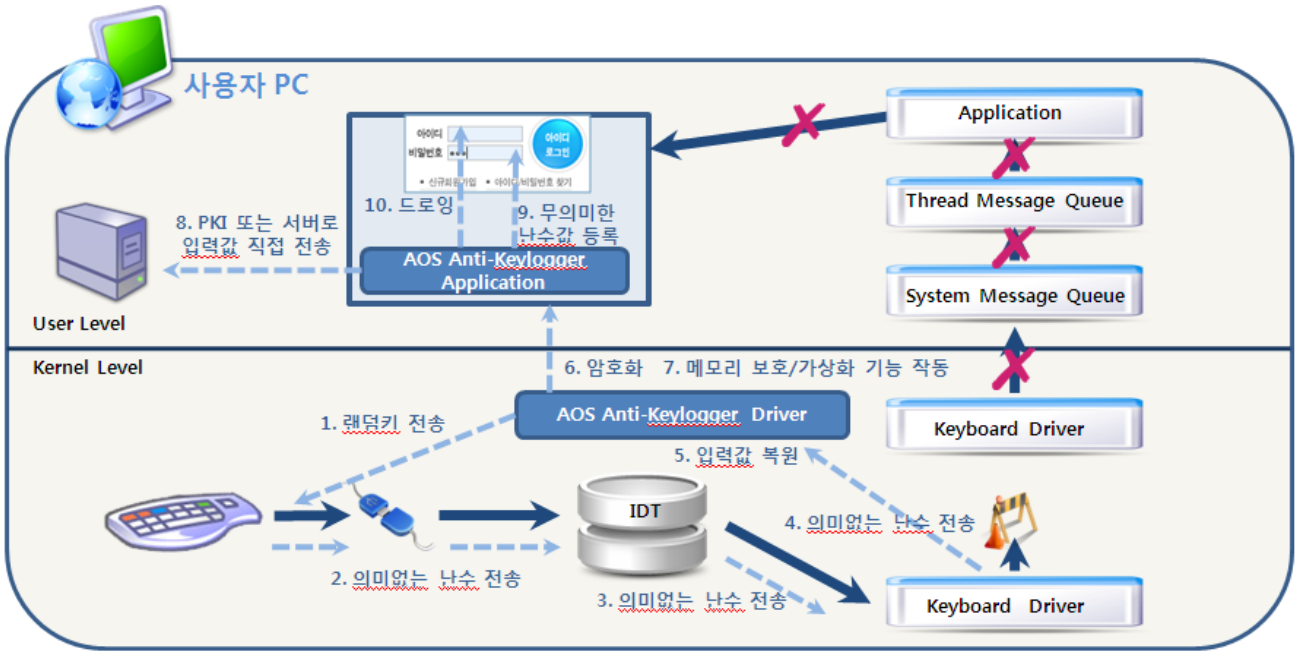
2) USB 키보드 동작 방식 및 보안 취약점



<그림 8> USB 방식의 키보드 보안 취약점

USB는 PC 관련 업체들이 참여한 USB-IF (USB Implementers Forum)에 의하여 현재 2.0 버전이 상용화되어 있으며, PnP (Plug and Play) 기능 강화와 함께 장치제어를 위하여 PC 내부에 USB Host Controller를 사용한다. USB에서는 사용자가 입력한 값이 USB Hub Driver로 값이 전달되기 전까지 키보드 값 인지를 판단하기 힘들며, 이에 관련된 대부분의 보안 취약점도 Driver 구간부터 발생하게 된다. 이점을 제외하고는 유저/커널 레벨에서 발생하는 보안 취약점은 PS/2방식의 키보드와 동일하다.

3) AOS Anti-Keylogger의 보안 기술 - PS/2

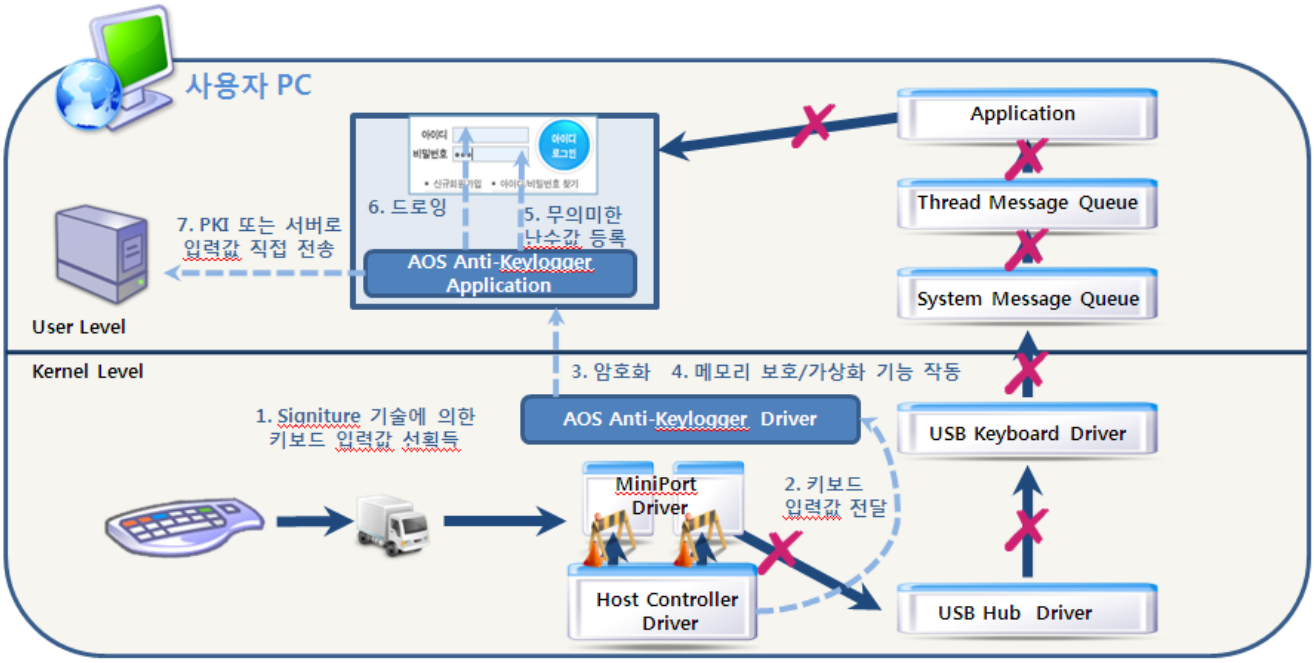


<그림 9> AOS Anti-Keylogger 의 보안 기술(PS/2)

PS/2 방식에서 AOS Anti-Keylogger의 보안 방식은 아래와 같다.

① 보호하려는 키 입력 항목에 Focus가 발생하면 AOS Anti-Keylogger Keyboard Driver는 S/KEY를 생성하여 1초에 20~40개 정도의 속도로 PS/2 Port에 난수를 Write 한다.
② AOS Anti-Keylogger Keyboard Driver는 난수와 사용자 입력 값이 혼합된 값에서 S/KEY를 제거하고 사용자의 입력 값 만을 암호화 하여 AOS Anti-Keylogger Application에 전달한다. 이 과정에 메모리 보호를 위해 가상화 기능이 함께 동작해 보호한다.
③ AOS Anti-Keylogger Application은 암호화된 값은 내부 메모리에 저장하고 사용자 입력 창에는 의미 없는 값을 출력한다. 이때 Password 처리와 일반 Text 처리가 다르며, 일반 Text의 경우 드로잉 방식으로 Text를 이미지화 하여 보여준다.

4) AOS Anti-Keylogger의 보안 기술 - USB



<그림 10> AOS Anti-Keylogger 의 보안 기술(USB)

USB 방식에서 AOS Anti-Keylogger의 보안 방식은 PS/2 방식과 커널 레벨 보안에 있어 상이한 부분이 있으며 USB 보호의 핵심 기술은 USB 패턴 중 키보드 데이터 패턴을 정확하게 추출하여 보호하는 기술로서 현재 특허출원 중이다. ('USB 장치의 입출력 패킷 보호방법')
이 내용은 아래와 같다.

① 보호하려는 키 입력 항목에 값이 입력된 값은 USB Bus를 통해 Host Controller 드라이버로 전달된다.
② Host Controller Driver는 USB Driver Stack의 가장 최하위 단. Port driver와 miniport 드라이버(들)로 구성되며, 시스템이 USB Device (H/W)를 발견하면 적당한 miniport 드라이버를 로드한다.
③ 이때 AOS Anti-Keylogger는 자체 패킷 추출 기술을 이용하여, Host Controller Driver에서 키보드 입력 값

을 구분하고, 사용자 입력 값을 AOS Anti-Keylogger Driver로 전송한다.

④ 이후의 과정은 PS/2 방식과 동일하다.

6) AOS Anti-Keylogger 서비스 확장

AOS Anti-Keylogger는 한국의 금융감독원 지침사항인 E2E(End to End) 보안을 지원한다. E2E는 암호화 기술을 이용해 금융기관에서 서비스하고 있는 공인인증서(PKI) 프로그램 및 금융기관 웹 서버까지 암호를 풀지 않고 직접 전달하는 기술을 말한다. 또한, AOS Anti-Keylogger는 기존의 ID/Password 항목 이외에 계좌번호, 주민등록번호, 이체금액 등까지 함께 E2E로 보안할 수 있는 확장 E2E 기술을 지원하고 있다. 여기에 증권사에서 서비스하고 있는 HTS(Home Trading System) 또는 은행에서 서비스하는 Application 방식의 뱅킹 프로그램 지원을 위해 SDK(Software Development kit)를 함께 제공하고 있다.

7) AOS Anti-Keylogger의 특징 및 장점

AOS-Anti-Keylogger는 타 키보드 보안 프로그램과 비교하여, 아래와 같은 특징 및 장점이 있다.

첫째, 커널/유저 레벨에서 발생 가능한 모든 보안취약점에 대응 가능하다.

AOS Anti-Keylogger는 앞서 기술한 바와 같이 PS/2 및 USB 방식의 키보드 환경에서 발생하는 보안위협에 대해 전방위적인 보안이 가능하다.

둘째, PS/2 방식에서의 키보드 폴링 대응이 가능하다.

S/Key 방식의 기술을 사용하는 AOS Anti-Keylogger는 사용자 입력 값이 최초로 저장되는 키보드 포트 구간부터 보호가 가능하며, 키보드 폴링 위협에 대응이 가능하다.

셋째, 자체 특허 기술로 제품간 충돌 위험성 및 장애요인을 제거하였다.

현재 시장에 제공되고 있는 대부분의 키보드 보안 제품들의 경우 PS/2방식의 경우 IDT hooking 방식 또는 이와 유사한 방식을 통하여 키보드 보호를 진행하고 있다. 이로 인해 두 개 이상의 유사 방식을 이용하는 키보드 보안모듈이 구동되는 경우(이러한 경우는 웹 환경에서는 흔히 발생한다) IDT hooking 시에 인터럽트 핸들러를 Anti-Keylogger의 ISR로 변경 한 이후에도 타사에 의해 교체되는 일이 발생할 수 있으므로 키보드 보안 모듈간 자사 모듈의 ISR이 구동될 수 있도록 경합이 발생하며 이로 인하여 시스템 안정성에 문제가 발생하는 경우가 있다. 또한, USB방식에 있어서도 일반적인 키보드보안 프로그램의 경우 USB miniport 드라이버를 후킹하는 방식으로 처리되고 있다.

AOS Anti-Keylogger 기술력의 우위는 후킹 방식이 아니라 USB 데이터를 구분해 내는 방식에 있다. 타 업체의 경우 정확히 USB 패턴에서 키보드 패턴을 추출해 내는 것이 아니라 통상적으로 사용되는 키보드 패턴(USB 데이터 헤더 크기 등)에 입각하여 USB 키보드 데이터 처리를 진행하고 있어 장애가 발생할 수 있으며, PS/2 방식과 마찬가지로 경합에 의한 충돌 위험성을 내포하고 있다.

넷째, Password 이외의 항목에 대한 보호 및 서비스 확장이 가능하다.

현재 국내외 상용키보드 보안 업체 중 일반 Text 항목에 Image Drawing 기법을 사용하는 곳은 없으며, Drawing 기술 적용으로 상시적으로 BHO 에 쉽게 노출되는 것을 방어할 수 있다. 또한, E2E 지원 및 SDK 제공으로 웹뿐만 아니라 어플리케이션 프로그램까지 다양한 환경에 적용이 가능하다.

3. AOS Firewall

AOS Firewall은 각종 보안 위협으로부터 개인을 보호하기 위한 온라인 PC방화벽으로, 허락되지 않은 네트워크를 통한 침입과 외부의 해킹을 감지하여 각종 암호나 개인 정보의 무단 유출 및 데이터 손상의 위협을 사전에 차단하는 역할을 수행하는 제품이다.

개인 컴퓨터(PC)에서 사용자가 원하지 않는 외부로의 정보 유출은 주로 트로이목마 등의 해킹툴이 PC에 침입한 경우에 발생하게 된다. 해킹툴이 PC에 침입하여 시스템에서 작동되면 사용자의 정보를 가로채서 미리 설정되어 있는 FTP 계정이나 E-mail을 통해서 외부(해커)로 유출하게 된다. AOS Firewall은 해킹툴 전용 엔진이 프로세스상의 해킹툴 존재여부를 항상 검사하므로 이를 미리 차단할 수 있다. 또한 알려지지 않은 해킹툴의 경우 외부로의 연결을 요청하는 프로그램을 감지하여 사용자에게 알려주어 사용자가 적법한 연결인가를 판단할 수 있도록 한다.

1) AOS Firewall의 주요 기능

▪ 개인 방화벽

AOS Firewall은 사용자의 PC에서 외부와 통신하는 프로그램의 실행을 감지하여 사용자에게 알려주는 기능이 제공되고, 프로그램별 감지 시 유저 레벨 및 커널 레벨에서의 IP 주소와 Port 별로 세부적인 감지 및 허용/차단 설정이 가능하다. 사용자가 직접 특정 IP/Port를 지정하여 허용/차단하는 기능도 함께 제공된다. 특히, 커널 레벨에서의 IP/Port 감지/허용/차단 기능은 커멘드창 등을 통해 불법 접근하는 행위까지 차단 가능하다. 또한 외부 통신을 위해 열어 놓은 TCP/UDP 정보를 사용자에게 보여주는 기능과, 검출이 어려운 자기위장 및 은닉형 해킹툴에 대한 자기대처 기능이 포함되어 있다.
AOS Firewall의 방화벽 기능은 사용자가 허용하게 되면 이후로는 '계속 허용'이 되어 사용자가 다시 설정하지 않아도 되어 불편을 주지 않는다.

▪ 공유폴더 제어/모니터링

네트워크에 연결되어 있는 사용자 시스템(컴퓨터)에 공유되어 있는 폴더를 관리하고 이에 접근하는 다른 사용의 접근을 허용 또는 차단할 수 있어 해킹툴이나 프로그램을 통한 접근이 아닌 네트워크를 통한 침입을 막을 수 있다. 그리고 AOS Firewall의 보안등급을 '높음'으로 설정하면 외부 사용자가 공유 폴더 접근 시에 감지하여 접근 허용 또는 차단할 수 있다.

▪ 실시간 해킹툴 감지/차단

AOS Firewall의 해킹툴 감지 전용 엔진이 최신 해킹툴 정보를 가지고 실시간으로 항상 실행되므로 사용자 시스템을 외부의 위협으로부터 보호할 수 있다. 엔진은 프로그램 실행 시 업데이트 되므로 사용자의 특별한 조작 없이 AOS Firewall을 실행해 놓는 것만으로도 보안이 가능하다
AOS Firewall은 안철수연구소의 해킹툴 전용 감지/차단 엔진이 탑재되어, 실시간 감지를 통해 프로세스에 접근하는 Key Logging 전용툴 및 Console 방식의 해킹툴, Back Orifice Hidden Process 등의 해킹툴을 감지/차단할 수 있다.

▪ **보안등급 설정 및 로그 보기**

AOS Firewall의 세부 기능들을 사용자가 원하는 등급에 따라 설정할 수 있다. '낮음'의 경우에는 해킹툴 감지를 주로 하며, '보통'에서는 해킹툴 감지, 프로그램 접근관리 등이 가능하다. '고급'에서는 공유폴더 접근 감지와 벡터 필터링(Vector Filter)을 하여 알려지지 않은 해킹의 위험을 감지하여 알려주는 기능이 추가 된다.

AOS Firewall의 실행, 중지, 종료에 대한 기록과 해킹툴 차단 기록, 그리고 프로그램 접근 허용 및 차단에 대한 정보를 조회할 수 있는 기능이 함께 제공 된다.

2) AOS Firewall의 특징 및 장점

인터넷 접속만으로 실행부터 엔진 업데이트까지 자동으로 실행되는 AOS Firewall은 아래와 같은 특징 및 장점을 가지고 있다.

첫째, AOS Firewall은 유저 레벨뿐만 아니라 커맨드창 또는 Driver를 통한 IP/Port의 불법적인 접근 시도에 대한 대응이 가능하다.

둘째, AOS Firewall은 안철수연구소의 최신 TS엔진을 탑재함으로써 트로이목마 및 해킹툴에 대해 기존 방화벽 제품보다 좀더 빠르고 정확한 대응이 가능하다.

셋째, AOS Firewall은 인터넷 웹 페이지 접속시 자동으로 실행되며, 1일 1회 이상 최신 악성코드 및 해킹툴 엔진이 자동 업데이트되므로 이용이 매우 간편하다.

넷째, AOS Firewall은 인터넷에 익숙한 사용자들을 위해 웹 페이지 형식의 화면으로 구성되어 있으며, 메뉴의 직관성을 높여 사용자들이 친숙하게 사용할 수 있다.

4. AOS Anti-Virus&spyware

AOS Anti-Virus&spyware는 20여 년 동안 축적된 안철수연구소의 기술과 노하우가 담겨있는 온라인 방역 프로그램이다. 별도의 방역 프로그램이 설치되어 있지 않아도 인터넷이 연결된 컴퓨터라면 언제 어디서나 사용자가 직접 바이러스와 스파이웨어를 진단하고 치료할 수 있다.

인터넷 접속만으로 실행부터 엔진 업데이트까지 자동으로 실행되는 AOS Anti-Virus&spyware는 아래와 같은 특징 및 장점을 가지고 있다.

첫째, 1988년 이후 20여 년간 추적해 온 V3 기술을 기반으로 안티바이러스와 스파이웨어를 동시에 진단/치료 할 수 있다. 또한 최신의 TS 엔진을 탑재해 검사와 업데이트에 소요되는 시간을 단축하였다.

둘째, 365일 신종 바이러스 및 해킹툴, 웜 차단을 위한 글로벌 대응 조직인 시큐리티대응센터(ASEC)을 통해 신속한 업데이트를 제공하며, 긴급 시에도 민첩한 대응력을 발휘할 수 있다.

셋째, AOS anti-virus&spyware는 휴리스틱 스캔 기능을 통한 유사 악성코드, 알려지지 않은 유해가능 코드까지 검출해 악성코드로 인한 피해를 최소화 할 수 있다.

넷째, 복잡한 환경설정 없이 클릭 한번으로 다양한 프로그램 검사/치료가 가능하며, 직관적인 UI(User Interface)로 초보자들도 손쉽게 사용할 수 있다.

5. AOS SecureBrowser

AOS SecureBrowser는 알려지지 않은 해킹 위협요소에 대해 직접 감지/차단이 가능한 솔루션으로서 메모리해킹 대응은 물론 자체 방어(Self Protection) 영역에 대한 보호가 가능한 전문 안티 해킹(Anti-Hacking) 서비스이다.

해킹 패러다임의 변화에 좀더 적극적으로 대응하기 위해서는 다음의 6가지 조건을 충족시켜야 한다.

첫 번째, 전자금융거래만을 위한 전용 플랫폼이 제공되어야 한다.
두 번째, 해커가 정상적인 웹 해킹 프로세스 절차를 진행할 수 없도록 해야 한다.
세 번째, 보안프로그램 자체가 해킹에 의해 무력화 되거나, 변조되지 않도록 자기보호(Self Protection) 기능을 갖추고 있어야 한다.
네 번째, 구간별 감지/차단 가능한 보안 프로세스 구현으로 사용자가 해킹 사실을 인지하고 후속 대응을 할 수 있도록 하여야 한다.
다섯 번째, 전통적인 웹 취약점에 대응 할 수 있어야 한다.
여섯 번째, 쉽고 신속하게 적용하고 기존 비즈니스 로직이 손상되지 않도록 해야 한다.

AOS SecureBrowser는 이 6가지 조건을 완벽하게 충족시키는 새로운 개념의 보안 서비스라고 할 수 있다. .

1) AOS SecureBrowser의 보안 기술

▪ 전용 플랫폼의 제공 및 전통적 웹 취약점 제거

공용 웹 브라우저는 많은 보안 취약점을 내포하고 있으며, 웹 해킹의 주요 도구로 활용되고 있다. 이에 안전한 웹 서비스 환경 구현을 위해서는 보안이 강화된 전용 플랫폼이 제공되어야 할 필요가 있다. 하지만 절대 다수의 사용자가 Internet Explorer를 사용하고 있는 현 상황에서, MS사의 웹 표준을 따르고 있는 전자금융거래 서비스 환경과의 호환성을 유지하면서, 보안성을 확보한 브라우징 서비스를 제공하는 데에는 많은 어려움이 있다.

이에 AOS Secure Browser는 다음과 같이 전용 플랫폼을 구성한다.

첫째, 마이크로소프트(Microsoft)사가 제공하는 인터넷 익스플로러 6 버전의 핸들을 사용한 전용 브라우저를 제공하여 별도의 가상메모리를 할당한다.

인터넷 익스플로러 6 버전은 퀵스 모드(Quirks Mode)로 렌더링되어 국내 대부분의 금융 웹사이트를 지원하고 있으며, 인터넷 익스플로러 7 버전에 비해 메모리 점유율이 낮아 상대적으로 전자금융서비스에 적합한 부분이 있다. 또한, 전자금융거래 시 필요한 보안 프로그램들에 대해서도 이미 검증이 완료된 상태이다.
다만, 향후 브라우저간 지원 범위를 넓히기 위해 CSS2.1을 정식 지원하는 인터넷 익스플로러 8 버전의 핸들로 교체하는 방안을 추가로 검토하고 있다.

둘째, 전용 브라우저에는 전자금융거래에 필요한 기능만을 포함한다.

기존 인터넷 익스플로러 내에 내장되어 있는 BHO(Browser Helper Object) 기능을 제거해, BHO를 악용한 해킹을 차단한다. 이와 함께 브라우저 로딩 시 인증서버와의 통신을 통해 사전에 인증된 IP로만 접속을 허용함으로써, 피싱(Phishing) 및 파밍(Pharming) 공격에 대응할 수 있다. 여기에 전자금융거래 시 해킹에 악용될 수 있는 주소창 및 기본 툴바 등의 활용 범위를 제한해 전자금융거래 및 개인정보 서비스 용도 이외에 전용 브라우저가 사용될 수 없도록 한다.

셋째, 외부 모듈 접근에 의한 해킹 위협에 대응하기 위해 화이트 리스트(White List) 기반의 접근 제어 기술을 사용한다.

이를 통해 내부적으로 인잭션(Injection) 되는 모듈들에 대해 사전에 화이트 리스트에 등록된 모듈만을 처리함으로써, 전자금융거래에 불필요한 애플리케이션이 접근할 수 없도록 할 수 있다. 또한 블랙 리스트(Black List)를 함께 운영하여, 디버깅 프로그램과 같이 일반적인 안티-멀웨어(Anti-Malware) 제품에서 탐지하지 않지만, 해킹에 활용될 수 있는 애플리케이션을 추가로 감지할 수 있도록 해 아래 기술할 안티 디버깅 기능을 보완할 수 있다.

▪ 웹 해킹 프로세스의 차단

위에서 기술한 바와 같이 대부분의 전문 해커는 해킹툴 제작을 위하여 해킹 대상에 대한 분석 및 테스트를 수행한다. 이때 사용되는 가장 유용한 기술들이 바로 디버깅과 리버스 엔지니어링이다. 따라서 만약 해커가 이러한 디버깅이나 리버스 엔지니어링 기술을 사용하지 못할 경우 해킹 대상 프로그램을 분석하기는 매우 힘들어지게 된다. AOS Secure Browser는 자체적으로 안티 디버깅 기능과 안티 리버스 엔지니어링 기능을 포함하고 있어, 해킹을 위한 분석단계부터 보안을 시작한다.

이와 같은 안티 디버깅 기술과 안티 리버스 엔지니어링 기술을 통해 웹 서비스에 사용되는 프로그램들에 대한 취약점을 외부로 쉽게 노출시키지 않음으로써, 좀더 안전한 보안 환경을 구축할 수 있다. 특히, 종단간(End to End) 암호화 방식에 있어서 키보드 보안프로그램이 암호화하기 직전 디버깅 프로그램에 의한 암호화 전 평문 노출 취약점에도 대응 할 수 있는 장점이 있다.

▪ 자기 보호(Self Protection) 구현

AOS SecureBrowser는 EXE 및 DLL과 같은 실행파일들에 대해 패킹(Packing) 및 파일 위변조 방지 기술을 활용하여 파일 변조 및 프로그램 무력화에 의한 해킹을 방지할 수 있다. 패킹 기술을 이용하는 이유는 개발된 프로그램의 코드를 크랙으로부터 보호하기 위해서이다. 패킹을 하게 되면, 본래의 코드는 팩킹이라는 포장지에 의해 감춰지기 때문에 먼저 언패킹(Unpacking) 작업을 해야 바이너리의 내부를 들여다 볼 수 있게 된다. 그러므로 만일 해커가 패킹을 벗겨 내지 못하면 바이너리 분석이 대단히 어려워져 해킹을 위한 분석이나, 파일 변조를 통한 프로그램 실행 조작, 프로그램 무력화를 시도할 수 없게 되는 것이다.

또한 파일 삭제 등을 통한 프로그램 무력화 시도를 막기 위해서는 프로그램 실행 및 업데이트 시 마다 실행파일의 변조 여부를 체크하고, 변조 시 복구할 수 있는 기능을 갖추고 있다.

▪ 메모리 보호 기술

애플리케이션에서 사용되는 모든 데이터 및 코드는 메모리를 통해 처리되며, 이를 악용한 다양한 메모리 해킹이 이루어질 수 있다. 이에 다양한 메모리 해킹 공격에 대응은 위에서 기술한 안티 디버깅과 안티 리버스엔지니어링, White List 및 Black List를 이용한 모듈 제어, 패커를 이용한 방법으로 어느 정도의

보안이 가능하다.
그러나 여기서 한 가지 주의 깊게 살펴봐야 할 것이 바로 패커의 실행 구조상의 제약이다. 패커는 실행파일을 압축 또는 암호화 등의 기법을 이용해 원본 실행파일과는 다른 형태로 변형을 가하는 프로그램이다. 이 변경된 실행파일(또는 패킹된 파일)이 실행될 경우 실행파일 내에 있는 패커의 로더가 먼저 실행이 된다. 이 로더는 메모리에 원본 파일의 내용을 메모리에 적재하는 역할을 수행하며, 메모리에 적재가 완료되면 원본 프로그램을 실행함으로써 그 역할을 다하게 된다. 다시 말해서 패커의 실행 구조상 보안 영역은 변형된 파일이 실행되어 원본 코드가 메모리에 적재되어 실제 프로그램이 실행되기까지이며, 프로그램이 실행된 후부터는 아무런 능력을 발휘하지 못한다.
따라서, 좀더 완벽한 전자금융거래 보호 환경 구현을 위해서는 구간별 감지/차단 가능한 보안 프로세스 구현으로 사용자가 해킹 사실을 인지하고 후속 대응을 할 수 있도록 하여야 한다.

이러한 시점에서 보았을 때 해커에 의해 상기 보안 기술들이 무력화 되거나 애플리케이션이 실행되어 패킹 프로그램으로 패킹된 코드가 실행 되어 메모리에 등록된 상황에서의 접근을 감지하기 위하여, 별도의 메모리 조작 감지 및 차단 기능을 추가로 제공할 필요가 있다.
AOS SecureBrowser는 유저/커널 레벨에서의 메모리 조작 감지 및 차단 기능을 가지고 있으며, 해커가 쉽게 메모리를 분석할 수 없도록 메모리 상에 존재하는 데이터를 암호화하여 저장하거나 데이터를 쪼개 저장되는 위치를 랜덤(Random)하게 변경시키는 방법을 함께 사용하고 있다.
이러한 메모리 보호 기능은 전용 브라우저 자신뿐만 아니라, 전용 브라우저의 차일드 프로세스(Child Process)로 동작하는 AOS 모든 서비스에 함께 적용될 수 있어, 보안성을 한층 더 높일 수 있다.

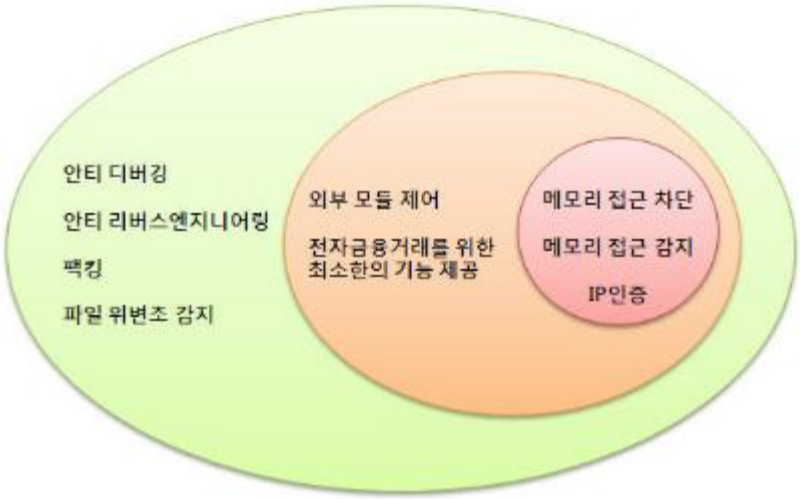
2) 보안 전용 브라우저 및 AOS SecureBrowser의 장점

일반적으로 보안성과 편의성은 서로 반비례하는 부분이 있다. 보안성이 향상되면 프로그램의 용량이 커지게 되거나, 메모리 사용량이 늘어나게 된다. 또한 사용자에 대한 제약사항이 늘어나게 되며 구축에 필요한 시간과 비용도 더 많이 소요된다.

이러한 부분에 있어, 전용 웹 브라우저를 이용한 보안은 다음과 같은 장점을 가질 수 있다.

① 전자금융거래에 필요한 기능만을 포함한 웹 브라우징 서비스가 제공되므로, 동일한 보안 기능이 적용되었다고 가정하였을 때, 공용 웹 브라우저 대비 높은 성능을 유지할 수 있다.
② 보안 기술 적용을 위해 기 구축된 전자금융거래 시스템 및 웹 페이지의 변경을 최소화 할 수 있다.
③ 전자금융거래를 이용하기 위한 사용자 교육 비용과 불편함을 유발할 수 있는 제약사항을 최소화 할 수 있다.
④ 일반 실행파일 및 ActiveX 방식의 설치뿐만 아니라, HTS(Home Trading System)과 같은 전용 애플리케이션에 대해 SDK(Software Development Kit)로 적용이 가능하다.
⑤ 브라우저 내 모듈화된 보안기술 적용으로, 신규 해킹기술에 대해 신속한 제품 패치 및 업그레이드가 가능하다.

안철수연구소의 보안 전용 브라우저인 AOS SecureBrowser의 특징 및 장점은 다음과 같다.



<그림11> AOS Secure Browser 보안 로직

첫째, AOS SecureBrowser는 <그림 11>과 같이 전자금융거래 프로세스 단위 별로 다중 보안 기술 적용해 해킹을 위한 취약점 분석 및 실행을 방지할 수 있으며, 해킹 사실을 사용자가 확인할 수 있다. 또한 새로운 해킹 기법들에 의해 몇 개의 보안 기술들이 무력화 되더라도 중요 정보 해킹을 진행하기 전에 추가 대응에 필요한 시간을 확보할 수 있다는 것이 장점이다.

둘째, 기존 전자금융거래 보안 프로그램들과의 상호 보완을 통해 보안성을 높일 수 있다. AOS SecureBrowser는 인터넷 익스플로러와 같은 독립 브라우저로서, 브라우저 내에서 구동되는 어플리케이션은 AOS Secure Browser와 동일하게 메모리 보호를 받을 수 있어, 강력한 보안성을 갖게 된다.

셋째, 한국 금융감독원 의무 지침 사항인 메모리 데이터 변조에 대응이 가능하다.
AOS SecureBrowser 는 2007 년 금융감독원의 의무 지침 사항인 '메모리 데이터 변조 및 COM 후킹 대응' 조건을 만족시키는 제품으로서, ID/Password 뿐만 아니라 계좌번호, 주민등록번호, 이체 금액 등 다양한 영역에서의 메모리 보호가 가능하다.

Ⅴ. Conclusion

국내 인터넷의 폭발적인 확산과 전자금융거래의 보편화는 해커들에게 새로운 수익모델을 제공하였고, 이에 따른 전자금융거래 보안 환경에도 새로운 변화가 요구되고 있다. 이러한 변화와 함께 이제 안전한 전자금융거래 서비스 제공 및 개인정보 서비스 제공은 기업의 항목이 되었으며, 서비스의 경쟁력을 평가하는 새로운 지표로 자리 잡았다. 관련 서비스를 제공하는 업체는 통합 보안 서비스 제공을 통해 안전한 비즈니스 환경을 조성할 수 있게 된다. 또한 IT 서비스의 신뢰도 향상을 통해 좀더 효율적인 고객관리를 할 수 있게 될 것이다.

온라인 통합 보안 서비스는 이제 금융시장뿐만 아니라, 공공/포탈/게임/쇼핑/커뮤니티 시장까지 제공하는 기본 서비스가 되었다. 웹의 발전과 함께 안전한 개인정보 보호 및 금융거래 서비스 제공이 시장에 이슈가 되면서 시장이 계속 확대되어 가고 있으며, 그러한 움직임은 향후에도 지속될 것으로 보인다.

안철수연구소가 제공하는 AOS를 통해 웹 서비스의 보안성이 더욱 강화되고, 사용자와 서비스 제공자 모두 만족할 수 있는 안전한 비즈니스 환경이 조성될 것으로 기대한다.