情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

국내 상용 제품의 인증 취약성 분석

전 웅 렬*, 원 동 호, 김 승 주

요 약

초고속 인터넷이 널리 보급되면서 오프라인에서만 가능했던 많은 서비스들을 이제 온라인에서도 사용할 수 있게 되었다. 온라인 서비스는 상대방을 대면하지 않기 때문에 적절한 사용자 인증과정이 반드시 필요하다. 현재 사용자 인증은 패스워드를 비롯하여 공인인증서, 보안토큰 등 다양한 방법을 사용하여 구현되고 있다. 그러나 공격방법이 다양화되고 지능화되면서 인증과정 역시 많은 취약점을 드러내고 있으며, 이를 극복하기 위한 개선방안에 대한 연구가 현재까지 활발하게 진행되고 있다. 따라서 본 고에서는 성균관대학교 정보보호 인증기술 연구센터가 지난 2008년 12월 종료된 ITRC 과제를 수행하면서 발표한 다양한 인증 프로토콜 취약점과, 취약점 발표 이후 대응 결과에 대해 서술한다. 본 고에서 다루어진 모든 취약점들은 발표 후 모두 패치되어 해결되었다.

Ⅰ. 서 론

초고속 인터넷이 널리 보급되면서 오프라인에서만 가능했던 많은 서비스들을 이제 온라인에서도 사용할 수 있게 되었다. 초창기 이메일 서비스를 시작으로 현재에는 온라인 메신저, 전자민원, 온라인 주식거래 등 다양한 서비스가 온라인으로 제공되고 있다. 온라인 서비스와 오프라인 서비스의 가장 큰 차이점은 상대방을 대면하지 않고 서비스를 제공하는 점이다. 따라서 온라인에서는 정당한 서비스를 위한 사용자 인증과정이 필수적이다.

보편적으로 사용되는 인증 방법은 패스워드를 사용한 사용자 인증이다. 대부분의 온라인 서비스는 패스워드를 사용한 사용자 인증을 채택하고 있다. 이외에도 공인증서, 보안토큰 등 다양한 인증 방법이 사용되고 있다. 그러나 공격자의 공격방법이 다양화되고 지능화되면서 이러한 인증과정에서 많은 취약성이 드러나고 있다. 특히 해킹이나 악성 프로그램 또는 내부적인 문제점에 의해 발생하는 개인정보 유출 사고는 이러한 인증 프로토콜의 안전성에 많은 영향을 미친다.

최근에는 이러한 인증 프로토콜의 취약성을 해결하기 위한 개선방안에 대한 연구가 활발하게 진행되고 있다.

따라서 본 고에서는 성균관대학교 정보보호 인증기술 연구센터가 지난 2008년 12월 종료된 ITRC 과제를 수행하면서 발표한 다양한 인증 프로토콜 취약점과, 취약점 발표 이후 대응 결과에 대해 서술한다. 본 고에서 다루어진 모든 취약점들은 발표 후 모두 패치되어 해결되었다.

Ⅱ. 네이트온 메신저 취약성 분석

2.1 요약

성균관대학교 정보보호 인증기술 연구센터는 지난 2006년 11월 국내에서 사용되고 있는 네이트온 메신저의 취약점을 분석하여 발표하였다. 네이트온 메신저는 인증 시 전송되는 사용자 정보를 암호화하여 전송하는 방법을 사용하고 있었다. 그러나 동일한 사용자에 대해서 동일한 인증정보를 생성하는 문제점과 인증 정보가 ID와 패스워드 조합의 해쉬로 되어 있어서 패스워드를 추출해 낼 수 있는 문제점이 있었다[1].

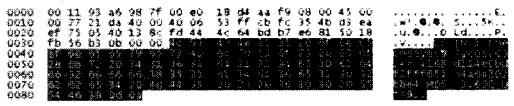
2.2 네이트온 인증과정 취약성 분석

2.2.1 네이트온 메신저 재전송 공격

당시 네이트온 인증 메커니즘을 분석하기 위해

* 성균관대학교 (wrjeon@security.re.kr)

Etherial Packet Capture 프로그램을 사용하였다. 패킷 캡쳐를 통해 분석한 네이트온 인증과정은 [그림 1]과 같다. 네이트온 메신저는 사용자가 인증을 받고자하는 인증 서버와 연결한 후, 사용자 개인정보를 바탕으로 인증정보를 생성하고 이를 인증서버에 전달한다. 네이트온 메신저가 전달하는 인증정보는 한 명의 사용자에 한해 동일했기 때문에 이를 활용하면 재전송 공격이 가능하였다. 아래 그림은 당시 네이트온 메신저가 인증서버에 전송하는 인증정보를 나타낸다[1].



〔그림 1〕 네이트온 메신저 인증정보

2.2.2 네이트온 메신저의 패스워드 해킹

당시 네이트온에서의 사용자 인증정보는 ID(또는 이메일 주소)와 패스워드의 조합에 MD5 해쉬 알고리즘을 적용한 값이었다. 따라서 해쉬값을 분석하면 사용자의 패스워드를 검출할 수 있다.

당시 상용 프로그램인 Passwordpro를 사용하여 네이트온 메신저 패스워드 해킹한 결과는 다음 그림과 같았다.

Password	Comments	Hash type
98734234oneoneeyes@lycos.co.kr		MD5

〔그림 2〕 네이트온 메신저 비밀번호 해킹결과

위 그림에서 나타난 바와 같이 해킹한 사용자의 네이트온 비밀번호는 "98734234"이고 사용자의 아이디는 "oneoneeyes@lycos.co.kr"인 것을 확인할 수 있었다[1].

2.3 대응결과

본 장에서 설명한 네이트온 메신저 재전송 공격 및 패스워드 취약점은 지난 2007년 2월 한국정보보호학회 논문지를 통해 발표되었다. 이후 업체의 네이트온 메신저 보안 업그레이드를 통해 해당 취약성이 보완되었으며, 현재는 본 절에서 설명하고 있는 공격이 불가능하다.

Ⅲ. 홈트레이딩 시스템 취약성 분석

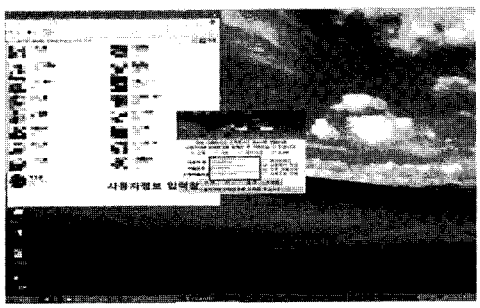
3.1 요약

지난 2007년 7월 성균관대학교 정보보호 인증기술 연구센터는 홈트레이딩 시스템(Home Trading System, 이하 HTS)의 인증 취약성에 대해 분석한 결과를 발표했었다. 연구센터는 당시 HTS의 인증과정 취약성 분석을 위해 28개의 증권사를 대상으로 선정하여 조사를 진행 하였으며, 키로깅이나 스니핑을 통해 개인 정보가 노출될 수 있는 문제점을 발견하였다[4].

3.2 HTS 인증과정 취약성 분석

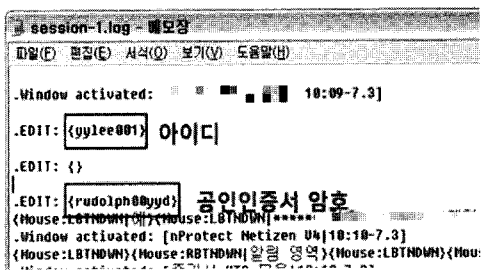
3.2.1 키로깅을 통한 개인정보 해킹

HTS는 일반적으로 키보드 보안솔루션을 함께 제공한다. 그러나 당시 키보드 보안솔루션이 설치되어 있는 경우에도 키로깅을 통한 개인정보의 해킹이 가능하였다. 아래 그림은 HTS의 일반적인 로그인 창을 나타낸다.



〔그림 3〕 HTS 사용자 인증정보 입력창

사용자가 입력하는 정보는 아이디, 패스워드 그리고

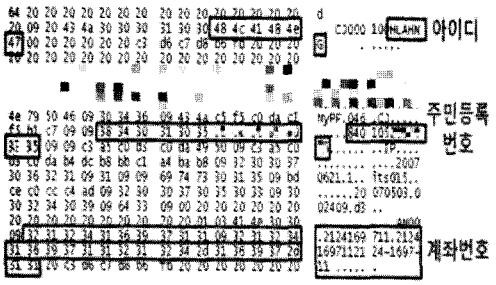


〔그림 4〕 키로깅 화면

공인인증서 패스워드이다. 만약 공격자가 백도어 프로그램을 사용자의 컴퓨터에 몰래 설치해둔 경우, 공격자는 키로깅을 통해 개인정보를 해킹할 수 있다[4].

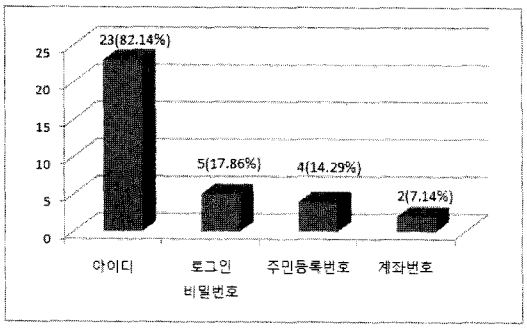
3.2.2 스니핑을 통한 개인정보 해킹

증권거래정보는 금전과 관련된 중요한 정보로 암호화되어 전송되어야 하지만 분석을 수행한 2007년 당시 실제 암호화가 완벽하게 적용되지는 않았다.



〔그림 5〕 스니핑

위 그림에서 나타난 것과 같이 스니핑을 통해 사용자의 ID, 주민등록번호, 그리고 계좌번호를 획득할 수 있었다. 2007년 당시 28개 증권사에 대한 조사결과는 아래와 같았다[4].



〔그림 6〕 2007년 스니핑 결과

3.2.3 대응결과

본 장에서 설명한 HTS의 보안 취약성은 2008년 2월 한국정보보호학회 논문지를 통해 발표되었으며, 조사한 28개 증권사 모두 추후 소프트웨어 업그레이드를 통하여 취약성을 보완하였다. 따라서 현재에는 본 절에서 설명한 공격이 가능하지 않다.

Ⅳ. 공인인증서 취약성 분석

4.1 요약

지난 2007년 2월 성균관대학교 정보보호 인증기술연구센터는 공인인증서의 취약성과 관련한 논문을 정보보호학회 논문지를 통해 발표하였다. 당시 논문에서는 공인인증서 관리 소프트웨어에서 정상적으로 삭제된 공인인증서와 개인키 저장 파일이 포렌식 툴을 이용하면 얼마든지 복구가 가능한 사실을 지적 하였다. 그리고 복구된 공인인증서와 개인키 저장 파일을 이용하여 오프라인에서 개인키 암호화 패스워드를 밝혀낼 수 있음을 설명하였다[5].

4.2 공인인증서 취약성 분석

4.2.1 포렌식 툴을 사용한 공인인증서 복구

2006년 당시 조사해본 결과 모든 소프트웨어에서 정상적으로 삭제된 공인인증서 파일이 포렌식 툴을 이용하면 아무런 제약 없이 복구가 가능하였다.

더욱이 사용자가 공인인증서를 이용한 서비스를 사용하기 위해서 설치되는 여러 파일들 중에서 공인인증서와 개인키 저장 파일을 제외한 다른 파일들은 새로운 공인인증서를 설치하더라도 변화가 없는 고정된 파일들이었다. 그러므로 공격자가 공인인증서와 개인키 저장 파일을 복구할 수 있다면, 사용자의 공인인증서를 도용하여 사용할 수 있는 문제점이 있었다[5].

〔표 1〕 공인인증서 삭제

삭제방법	하드디스크	USB 드라이브
공인인증서 소프트웨어를 사용하여 삭제	O	O
하드디스크 포맷	O	O
운영체제 상에서의 일반적인 삭제	O	O

4.2.2 공인인증서 패스워드 해킹

당시 공인인증서 소프트웨어에서는 일반적으로 5회

이상 패스워드를 잘못 입력하면 더 이상 해당 공인인증서를 사용할 수 없게 하는 등의 보안장치에도 불구하고 공인인증서 개인키 암호화에 사용되는 SEED 블록 암호 알고리즘의 패딩을 이용하여 공인인증서의 개인키 암호화 패스워드를 검출할 수 있었다.

당시 패스워드가 SEED 암호 알고리즘의 블록크기의 배수가 되지 않으면 부족한 부분을 채우기 위해, 공인인증서 소프트웨어는 PBES1에서 정의한 패딩을 사용하였다. 이러한 패딩을 이용하여 패스워드를 계산해 낼 수 있었다. 공격자는 임의의 패스워드를 생성하여 암호화된 키를 복호화 한 후, 복호화 된 값에 PBES1에서 정의된 패딩이 존재하는지 확인한다. 이 패딩이 존재하지 않는다면 다른 임의의 패스워드를 생성하여 이 작업을 반복하고, 이 패딩이 존재한다면 현재 사용한 임의의 패스워드가 공인인증서의 개인키 암호화 패스워드임을 알 수 있다[5].

4.2.3. 대응결과

본 장에서 설명한 공인인증서 관련 취약성은 2007년 2월 한국정보보호학회 논문지를 통해 발표되었으며, 한국정보보호진흥원을 주축으로 대응협의체를 구성하여 설명한 취약성을 해결하였다. 따라서 현재에는 본 절에서 설명하고 있는 공격이 가능하지 않다.

V. 주민등록번호 대체수단 취약성 분석

5.1 요약

지난 2007년 4월 성균관대학교 정보보호 인증기술 연구센터는 한국정보보호학회 논문지에 I-PIN 서비스에서 개인정보가 평문으로 전송되는 문제점을 발견하여 이를 발표하였다[3].

5.2 주민등록번호 대체수단 취약점 분석

5.2.1 스니핑을 이용한 개인정보 노출

2007년 당시 I-PIN 서비스를 이용할 때 스니핑 공격을 적용하게되면 전송되는 데이터에서 개인정보가 노출되는 것을 확인할 수 있었다. 아래 그림은 당시 사용자가 I-PIN 서비스를 제공하는 A 홈페이지에 접속하여 I-PIN 서비스를 사용할 때 통신내용을 분석한 결과이다.

〔그림 7〕 가상주민번호 유출화면

표시된 부분의 데이터는 발급기관이 사용자에게 발급한 가상주민번호로 통신상 평문형태로 전송되고 있음을 확인할 수 있었다.

2007년 당시 총 17개의 I-PIN 서비스 도입 사이트를 대상으로 조사한 결과 가상주민번호 뿐만 아니라 가상주민번호를 식별하는 ID, 그리고 비밀번호까지 유출됨을 확인할 수 있었다[3].

5.3 대응결과

본 장에서 설명한 I-PIN 관련 취약성은 2007년 4월 한국정보보호학회 논문지를 통해 발표되었으며, 이후 한국정보보호진흥원을 주축으로 협의체를 구성하여 취약성을 보완하였다. 이와 더불어 방송통신위원회에서는 올해 7월 7일부터 기존에 발견된 취약점 보완 및 기타 편의성 제고를 위한 여러 요구사항을 반영하여 I-PIN 2.0 서비스를 제공하고 있다. 이러한 I-PIN 2.0에서는 아래와 같은 정책을 통해 해당 서비스의 안전성 강화를 도모하고 있다.

〔표 2〕 I-PIN 2.0 서비스 안전성 강화 정책 내용

주체	점검 내용
본인확인기관 안전성 점검	· 서비스 안전성 정기점검 실시 · 정기점검 항목 이외의 웹사이트 취약성 점검 · 신용정보의 이용 및 보호에 관한 법률, 전자서명법에 근거한 안전성 점검
I-PIN 도입 웹사이트의 안전성 점검	· 암호화 전송을 위한 보안서버 적용 확인 · 웹사이트의 기술적, 관리적 보호조치 이행 여부 점검

VI. 보안 USB 메모리 취약성 분석

6.1 요약

지난 2007년 6월 성균관대학교 정보보호 인증기술 연구센터는 보안 USB 메모리의 취약성을 분석하여 발표하였다. 2007년 당시 보안기능이 탑재된 USB 플래

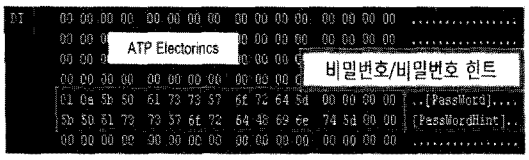
시 드라이브를 판매되고 있었다. 보안기능이 탑재된 제품은 저장되는 데이터를 암호화해서 저장하거나 비밀번호를 이용하여 USB 플래시 드라이브의 접근을 제한하는 기술 등이 적용되어 있었다[2].

6.2 보안 USB 메모리 취약성 분석

6.2.1 사용자 패스워드 해킹

2007년 당시 USB 통신을 스니핑할 수 있는 프로그램인 BusHound를 이용하여 USB 플래시 드라이브와 컴퓨터의 통신 내용을 분석하였다.

당시 USB 접근제어 프로그램은 사용자가 보안프로그램을 실행하면 USB 플래시 드라이브에 비밀번호와 비밀번호 힌트를 요청하였다. 이러한 요청이 발생하면 플래시 드라이브는 비밀번호와 비밀번호 힌트를 접근제어 프로그램으로 전송하게 되는데, BusHound를 이용하여 주고받는 데이터를 스니핑한 결과 비밀번호와 비밀번호 힌트는 암호화되었거나 해쉬되어 있는 형태가 아니라 평문 그대로 전송됨을 알 수 있었다. 아래 그림은 당시 비밀번호와 힌트가 노출되어 있는 BusHound로 데이터를 분석한 결과를 나타낸 것이다[2].



〔그림 8〕 ATP사의 접근제어 프로그램에서의 비밀번호 노출

6.2.2 패스워드 초기화 오류

당시 보안 USB 플래시 드라이브는 사용자가 접근제어용 비밀번호를 잊어버렸을 경우를 대비하여, 접근제어용 비밀번호 및 저장되어 있는 데이터를 모두 지우는 초기화 기능 역시 제공하고 있었다. 이미 널리 알려져 있듯이 일반적인 포맷은 하드디스크 및 메모리에서 데이터의 완전한 삭제를 의미하지 않는다. 포맷을 했어도 데이터 복구 유틸리티를 이용하면 대부분의 파일들을 복구할 수 있다. 분석을 진행할 당시 이러한 점을 이용하여 보안 USB 플래시 드라이브를 고의로 데이터와 비밀번호를 초기화하고, 복구 유틸리티를 사용하여 대부분의 파일들을 복구할 수 있었다. 다시 말해 패스워드를 모르더라도 USB의 해당 데이터에 접근 할 수 있었다[2].

6.2.3 대응결과

본 장에서 설명한 USB 플래시 드라이브 관련 취약성은 2007년 12월 한국정보보호학회 논문지를 통해 발표되었다. 이후 업체에서 접근제어 프로그램을 업그레이드 하여 취약성을 보완하였다.

Ⅶ. 결 론

초고속 인터넷이 널리 보급되면서 오프라인에서만 가능했던 많은 서비스들을 이제 온라인에서도 사용할 수 있게 되었다. 예를 들어 이메일, 메신저 등 개인의 연락수단으로 사용되는 것에서 비롯하여 전자민원, 온라인 주식거래 등 실생활 전반에 걸친 다양한 서비스가 이제 온라인으로 가능하다. 온라인 서비스와 오프라인 서비스의 가장 큰 차이점은 상대방을 대면하지 않고 서비스를 제공하는 점이다. 따라서 온라인에서는 정당한 서비스를 위한 사용자 인증과정이 필수적이다.

안전한 사용자 인증을 위해 현재 패스워드, 공인인증서, 보안토큰 등 다양한 방법이 사용되고 있고 연구되고 있다. 그러나 그럼에도 불구하고 보안사고는 빈번히 발생하고 있는 것이 현실이다.

이에 본 고에서는 성균관대학교 정보보호 인증기술 연구센터가 ITRC과제를 수행하는 동안 발표한 보안 취약점들에 대해 다루었다. 여기서 다루어진 모든 취약점들은 현재 모두 패치가 되어 해결되었다.

참고문헌

[1] 신동휘, 최윤성, 박상준, 김승주, 원동호, "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석", 한국정보보호학회 논문지, pp. 67-80, 2007. 02.

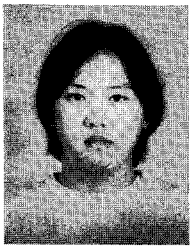
[2] 정한재, 최윤성, 전응렬, 양비, 김승주, 원동호, "보안 USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발", 한국정보보호학회 논문지, 제17권 6호, pp. 99-119, 2007. 12.

[3] 최윤성, 이윤호, 김승주, 원동호, "주민번호 대체수단에 대한 구현 취약점 분석", 한국정보보호학회 논문지, 제17권 2호, pp. 145-184, 2007. 04.

[4] 이윤영, 최해랑, 한정훈, 홍수민, 이성진, 신동휘, 김승주, 원동호, "홈트레이딩시스템의 보안 취약점 분석 및 평가기준 제안", 한국정보보호학회 논문지, 제18권 1호, pp. 115-137, 2008. 02.

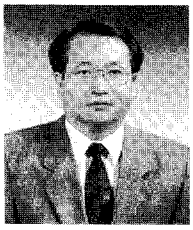
[5] 최윤성, 이영교, 이윤호, 박상준, 양형규, 김학범, 김승주, 원동호, "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출", 한국정보보호학회 논문지, 제17권 1호, pp. 41-56, 2007. 02.

〈著者紹介〉



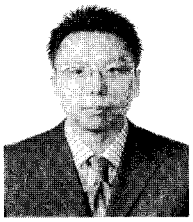
전 웅 렬(Woongryul Jeon)

2006년: 성균관대학교 정보통신공학부 졸업(학사)
2008년: 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(공학석사)
2008년~현재: 성균관대학교 대학원 전자전기컴퓨터공학과 박사과정 재학 중
<관심분야> 정보보호, 보안성평가



원 동 호 (Dongho Won)
정회원

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
2002년~현재: 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT감사 자문위원
2007년~현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장
<관심분야> 암호이론, 정보이론, 정보보호



김 승 주 (Seungjoo Kim)
정회원

1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: 한국정보보호진흥원(KISA) 팀장
2004년~현재: 성균관대학교 정보통신공학부 교수
2001년~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현재: 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET