情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

인터넷 뱅킹 해킹 유형과 대응 기술

강 신 범*, 정 현 철**

요 약

인터넷 뱅킹의 활성화와 더불어 그로 인한 문제점들이 제기되고 있다. 최근 고객의 실제 계좌에서 해커가 지정한 특정 계좌로 현금 이체가 이뤄지는 인터넷 뱅킹 시스템 해킹사고가 발생해 금융 정보보호 인프라 보안에 경종을 울리고 있다. 본고에서는 인터넷 뱅킹의 활성화와 함께 금융 정보보호 인프라의 새로운 사고 유형으로 등장한 인터넷 뱅킹 해킹 사고를 중심으로 점차 진보되는 해킹 기법들의 유형을 살펴보고 이에 대처하기 위한 해결 방법들에 대해 고찰해 본다.

Ⅰ. 서 론

인터넷의 발달과 더불어 이에 기인한 각종 서비스의 활성화로 미국 및 유럽의 금융 시장을 비롯한 전세계 은행의 인터넷뱅킹 사용자 수는 꾸준한 증가 추세를 보이고 있으며, 인터넷 뱅킹을 이용한 금융 거래 수요도 꾸준히 증가하고 있다. 국내의 경우도 이와 마찬가지로 인터넷 뱅킹 사용자의 수가 2005년 6월 기준, 2,290만명으로 증가하였으며,[1] 아래 그림 1의 표를 보면 2005년 6월을 기준으로 모든 은행들의 각 채널별 업무처리 비중 중 기존 업무의 대다수를 차지했던 창구 및 CD/ATM 기의 업무 처리 비중보다 인터넷 뱅킹이 차지하는 비율이 매우 큰 것을 알 수 있다.[1] 그림 2의 표를 통해 2002년 6월부터 2005년 6월까지의 금융서비스 전달 채널별 업무 처리 비율의 증감치를 비교해 보면 인터넷 뱅킹의 업무 처리 비율이 꾸준히 증가하는 추세임을 확인할 수 있다.[1]

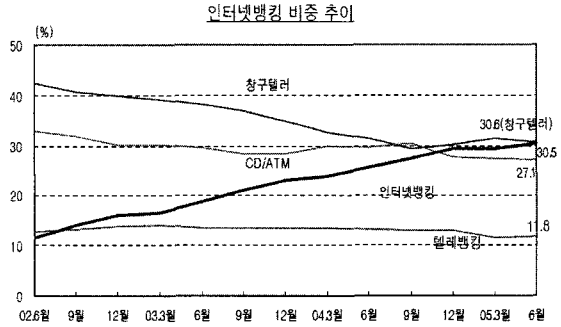
이와 같은 인터넷 뱅킹 수요의 증가는 사용상의 편리함이라는 이점 이면에 새로운 부작용을 일으키게 되었다. 지난 6월에 발생한 인터넷 뱅킹 해킹 사고와 최근에 분석된 인터넷 뱅킹 해킹 가능성에 대한 분석 보고서를 보면, 해킹의 유형이 인터넷 뱅킹 서비스 상의 취약점과 PC 보안상의 취약점 등에 대한 기술적인 분석을 토대로 바이러스, 웜 제작툴과 같은 전문적인 해킹 프로그램을 사용하는 등 수법이 점차 지능화 되고 있다. 이러한 인터넷 뱅킹의 보안상 취약점들은 비단

금융서비스 전달채널별 업무처리 비중
(2005. 6월중)

(건수 기준, %)

은행명		창구텔러	CD/ATM	텔레뱅킹	인터넷뱅킹	합계
시중은행(8개)	05. 3월	26.6	29.1	11.1	33.2	100.0
	05. 6월	26.1	28.3	11.6	34.0	100.0
지방 및 특수은행(10개)	05. 3월	34.7	26.2	13.6	25.5	100.0
	05. 6월	33.1	26.3	13.7	26.9	100.0
전은행(20개)	05. 3월	31.4	27.5	11.6	29.5	100.0
	05. 6월	30.6	27.1	11.8	30.5	100.0

〔그림 1〕 금융서비스 전달채널별 업무처리 비중



〔그림 1〕 인터넷 뱅킹 비중 추이

* 소프트포럼(주) 전략기획실 (sogoc@softforum.com)
** 소프트포럼(주) 대표이사 (hcchung@softforum.com)

우리나라의 문제뿐만이 아니라 인터넷 뱅킹을 운영하는 전세계 IT 금융 인프라의 공통적인 문제이기도 하다. 미국과 유럽 등 인터넷 뱅킹이 활성화 되어 있는 선진국들도 보안상의 문제를 해결하지 못하여, 많은 문제점들을 야기하고 있으며, 사용자들에게 100% 신뢰를 주지 못하고 있는 현실이다.

우리나라의 경우, 이번 인터넷 뱅킹 사고 이후 정보통신부는 한국정보보호진흥원 등 정보 보호 및 인터넷 뱅킹 관련 기관, 업체들과 함께 "전자거래 해킹방지대책"을 마련하기 위해 공동 작업반을 구성하여 "전자거래 시스템 안정성 분석", "해킹 프로그램 분석", "공인인증서 관리체계 개선"의 3개 분야로 나누어 운영하고 있다. 하지만, 이러한 노력들이 정책적으로 자리 잡지 못하고, 인터넷 뱅킹 사용자에게 제대로 인지되지 못한다면 미래 정보화 사회를 향한 금융 정보보호기술의 발전에 제약이 될 것이다.

본고에서는 인터넷 뱅킹 사용 시 발생한, 또는 발생 가능한 해킹 방법들과 이에 대응 가능한 기술들에 대하여 살펴본다.

II. 인터넷 뱅킹 해킹 유형

2.1 키보드 입력 정보 취득

국내 키보드 보안 제품들은 대부분 정상 동작시 공격에 대한 방어가 잘 이루어지고 있으나 지난 6월에 발생한 해킹 공격에서 고객 정보를 해킹 툴로부터 보호하지 못했던 것은 평문 관리를 허술하게 한데서 기인했다.

이번 사건 발생으로 인해 밝혀진 대부분의 문제중에는 운영상의 보강만으로도 대응 가능한 부분들이 많았다. 즉 내부에서 핸들링 되는 평문에 대한 관리시에 Key Logger 프로그램들로부터 방어가 필요하며, 일부 제품에서는 제품이 제대로 동작하는지 여부를 제대로 점검하지 않은 상태에서 입력을 받아 평문이 유출되는 현상을 나타냈는데 이 역시도 동작 상태를 점검하는 로직만을 추가 하면 거의 완벽하게 대응이 가능하다. 물론 내부적으로 키관리를 안전하게 하는 것도 필요한 것으로 파악됐다. 또 다른 우려상황은 BHO (Browser Helper Object)와 같이 기술을 악용하는 경우로 키보드입력 정보를 브라우저 단으로 넘겨 서버로 전송되기 전에 가로채는 방법들이 사용되었는데 이는 키보드로부터 입력된 정보를 평문으로 넘기지 않고 서버에서 풀 수 있는 키로 암호화 하여 바로 서버로 전송하는 방법(E2E)으로 대응할 수가 있다. 특히 해커가 이 BHO기술을 악용하면 사용자가 원하는 사이트가 아닌 음란 사이트 등으로 강제 이동을 시키거나 피싱(Phishing)에 사용할 수도 있기 때문에 인터넷을 사용하는 사용자라면 백신이나 스파이웨어 제거 툴을 사용하여 원치 않는 BHO 모듈은 반드시 제거해야 할 것으로 파악됐다.

이번 사건으로 인해 키보드를 통한 입력 값은 신뢰할 수 없으므로 이를 보강하기 위해 E2E 보안 기술을 적용해야할 것으로 보인다. E2E보안을 적용하기 위해서는 키보드 보안 제품과 켄텐츠 암호 제품과의 연동을 필요로 하는데 각각의 제품들의 구현 기술들이 서로 상이한 점이 많아 일괄적인 연동에는 어려울 것으로 보인다.

2.2 보안카드 공격

키보드 보안이 뚫린 경우 이체 등을 위해 사용하는 보안 카드 정보가 그대로 유출될 수밖에 없는데 근본적으로 랜덤성이 없는 까닭으로 한번 유출되면 방어 자체가 불가능하다. 이러한 이체시 요구되는 보안카드 값의 일회성을 높이기 위해서는 OTP(One Time Password)를 쓰는 방법이 제안 되고 있기는 하나 실제 동시 사용자 수가 많은 인터넷 뱅킹에 적용이 가능한 가는 검증이 되지 않은 상태이며 이를 적용하기 위한 비용이 다른 방법에 비하여 너무 높다는 문제가 있다. 또 다른 대안으로서 진보된 보안카드를 활용하는 방법을 고려해 볼 수가 있는데 SMS와 연계하여 서버에서 묻는 보안카드 번호를 전송하면 사용자는 그에 해당하는 인증 번호를 입력하는 방법을 사용하는 경우 저렴하면서도 안정적인 방법으로 사용될 수 있다. 기존에 보안카드가 공격을 받았던 이유를 보안카드 번호와 인증 번호가 같이 노출 되어서 생긴 문제라고 보면 이전에 100% 노출이 되었던 부분이 이와 같은 방법을 사용할 경우 35개의 숫자열을 지닌 보안카드의 경우 35*35의 가지 수가 생기게 되고 오류를 3번까지 허용할 경우 모든 번호가 노출 된 경우 대략 1/408의 성공 가능성을 지닌 공격이 되어 비용대비 엄청난 보안 강화 효과를 볼 수도 있다. 노출된 번호가 적을수록 가능성은 더 낮아지고 오류 허용횟수를 2회로 할 경우는 더욱 보안이 강화된다. 10개의 보안카드 번호가 노출된 경우를 확률적으로 계산해 보면 1/(35*35)*10/35*2가 되어 약 0.047%의 확률이 된다. 즉 적은 비용으로 굉장히 높은 보안 강도를 제공하게 된다. 추가적으로 보안카드를 1~2년에 한 번씩만 바꾸도록 한다면 굳이 OTP를 도입할 필요도 없을

것으로 보인다.

2.3 개인키 유출

키보드 보안과 관계없이 개인키는 쉽게 유출 가능하다. 패스워드가 유출된 경우는 저장된 개인키 파일만 가져가면 되고 그렇지 못한 경우는 API Hooking을 통하여 서명관련 함수를 모니터링 함으로써 손쉽게 취득할 수가 있다. 개인키 유출만으로 인터넷 뱅킹이 불가할 수는 있지만 인증서 만을 통하여 이루어지는 많은 서비스의 근간이 무너지기 때문에 근본적인 대책이 필요한데 이를 방어하기 위한 방법으로는 외부로 키가 유출되지 않는 가상 스마트 카드나 물리적인 스마트 카드/USB 토큰을 사용하는 방법 외에는 없다. 얼마 전까지만 해도 국산이 없어 너무 고가였으나 현재는 대형 업체들이 표준 스펙에 맞는 시제품 구현에 성공함으로써 가격이 많이 하락하여 도입이 좀 더 용이하게 되었다. 최근 각 은행이나 카드사에서 도입한 IC 카드에는 내부 연산 기능이 없어 키가 외부로 유출될 수 밖에 없는 상황이다.

가상 스마트카드와 같은 로밍 기술은 주로 KMI의 키로밍 기술을 사용하는데 일반적인 사용자들과 같이 보안의식이 없는 상태에서 사용자가 직접 개인키를 관리하는 것보다 오히려 편리성 및 보안성이 높다고 사료된다. 키로밍 기술은 네트워크를 통해 인증서 이동이 있기 때문에 이러한 환경에 대한 보안기술의 검증이 무엇보다 중요하다. 최근 핸드폰에 인증서를 저장하는 기술이 허용되었는데 이는 사용자에게 통신비용에 대한 부담과 동시에 보안프로그램과의 인터페이스가 일반 하드디스크에 저장된 인증서를 접근하는 방식과 다르지 않아 일반 하드디스크를 사용하는 경우와 같은 문제를 가지고 있다. 이외에도 게시판 기술 등을 활용하여 키로밍을 구현하는 경우가 있는데 이는 핸드폰을 사용하는 경우보다도 오히려 취약하다고 볼 수 있다. 핸드폰의 경우는 자신의 핸드폰에 보관을 하지만 서버에 인증서를 보관할 경우에는 서버 측에 적절한 보안 기법을 사용하여 서버 운영자도 인증서를 가져갈 수 없도록 해야 하기 때문이다.

Ⅲ. 해킹방법과 대응

해킹(Hacking)이란 국가나 기업 등의 단체 및 개인의 정치적, 사회적 물질적 이득을 위해 컴퓨터나 네트워상에 있는 데이터를 불법적인 방법으로 취득하는 것을 말한다. 해킹의 방법은 컴퓨터와 네트워크상에서 할 수 있는 모든 가능한 방법으로 시도가 가능한 것들로, 그 범위를 한정 지을 수 없으며 알려진 해킹의 방법 또한 셀 수 없이 많다.

본고에서는 이들 해킹 방법 중 금융 정보 획득을 위한 해킹 및 인터넷 뱅킹 상에서 가능한 해킹 방법들과 이에 대한 방지책을 제시한다.

3.1 피싱 (Phishing)

피싱(Phishing)이란 물질적 이득을 위해 개인 정보를 불법적으로 획득하고자 하는 사람이 이메일을 이용하여 불특정 다수에게 금융 기관임을 사칭하여 개인 정보의 업데이트 및 수정을 요구하여 개인의 카드 혹은 계좌 정보를 빼내어 불법적으로 이용하는 방법이다.

피싱을 이용한 대표적인 해킹 사례로는 eBay, Citibank 등 유명한 대기업을 대상으로 한 피해 사례가 많았다. 피싱을 이용한 해킹의 대표적인 방법은 아래와 같다.

단계 1: 고객 정보 확인을 요청하는 메일을 불특정 다수에게 보냄
단계 2: 고객이 메일상의 링크를 클릭하면 해커가 만든 위장 사이트에 접속됨
단계 3: 고객을 확인하기 위해 아이디, 패스워드로 로그인해야 한다는 메시지를 보여줌
단계 4: 아이디, 패스워드를 입력하면 아이디, 혹은 패스워드가 틀렸다는 경고 메시지를 보여주고 고객 아이디 확인을 위해 계좌 번호를 입력하는 페이지로 이동함
단계 5: 계좌 번호를 입력하면 고객이 확인되었다는 확인 메시지를 보여줌
단계 6: 입력받은 아이디와 패스워드, 계좌 정보를 해커의 이메일 주소로 전송

피싱을 막지 못하는 이유 중에 가장 근본적인 이유는 웹브라우져나 Outlook Express 등이 보안상 취약점들을 가지고 있기 때문이다. 피싱 공격을 당할때, 웹브라우저 주소창의 URL 과 링크가 스푸핑 되어 실제 기관과 매우 유사한 주소를 보여주기 때문에 메일을 받은 사용자가 웹사이트의 진위 여부를 바로 판단하기는 어렵다. 또한 사용자가 URL 정보가 맵핑되어 있는 이미지를 클릭했을 때 웹브라우져 하단에 보여주는 링크 정보도 잘못된 URL을 보여주기 때문에 사용자들이 쉽게 속을 수 있다. Outlook Express는 실제 링크된 URL과 다르게 링크가 표시될 수 있다는

취약점 때문에 이와 같은 피싱 공격을 막기는 쉽지 않다. 이와 같은 이유로 현재 피싱을 확실하게 막기 위한 보안 프로그램 혹은 보안툴이 제공되지 못하고 있는 실정이다. 현재 피싱을 막기 위해서는 사용자가 피싱으로 의심되는 메일을 받았을 때 조심하는 방법밖에 없다. 국내의 경우, 아직 외국처럼 피싱에 의한 사고 사례가 많은 편은 아니지만, "인터넷침해사고대응지원센터"와 같은 기관에서 피싱에 의한 피해를 막기 위한 방법을 제시하고 있으며, 신고도 접수하고 있다. 외국의 경우 영국에서는 "뱅크세이프온라인"[2]라는 이름으로 "영국은행 공동 피싱 범죄 대응 웹사이트"를 구축하여 운영하고 있다. 피싱을 막기 위하여 이러한 관련 기관들의 운영은 권장할만 하나 아직 미비한 점이 많다.

피싱을 막기 위해서는 우선 사용자에게 피싱 피해에 대해 인식시키고, 주의를 주는 것이 가장 중요하다. 이를 위해서는 관련 기관들의 운영뿐만이 아니라, 금융기관들의 적극적인 동참이 절대적으로 필요하다. 또한, 관련 보안 소프트웨어 개발업체들의 참여로, 피싱을 막기 위한 프로그램 개발도 병행되어야 할 과제로 남아있다.

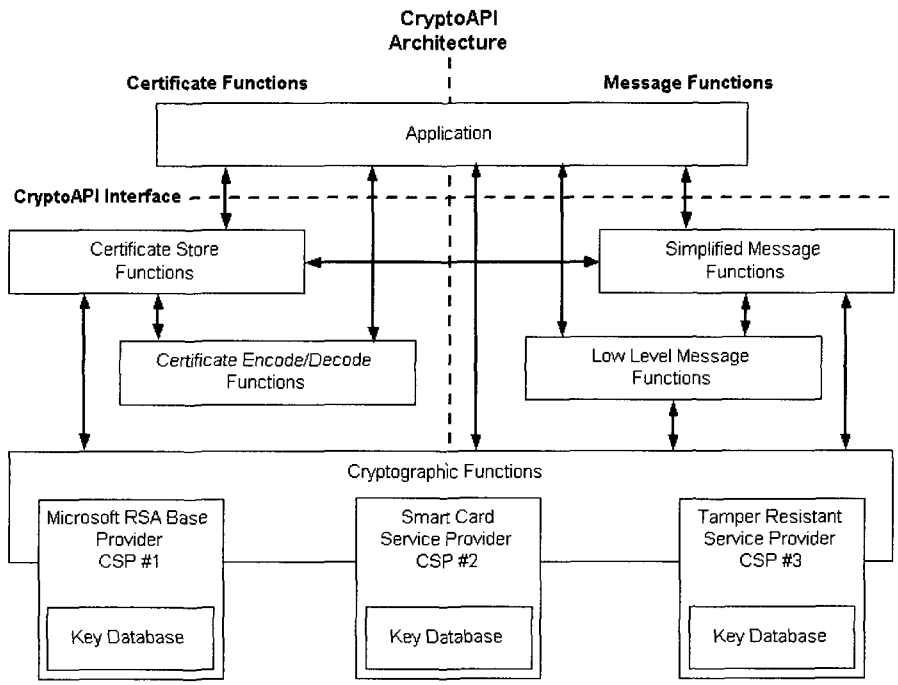
3.2 보안 카드

금융기관들은 인터넷뱅킹 사용시 계좌 이체 등 중요한 거래시에 거래자의 신원을 확인할 수 있는 방법으로 보안카드를 사용하고 있다. 보통 보안카드는 규칙성이 없는 난수 4자리 숫자가 하나의 비밀번호를 구성하고 있으며, 보안카드당 30~35개의 비밀번호를 가지고 있다. 그리고 이체 거래와 같은 주요 서비스 발생시에 인증서의 제출과 더불어 제2의 방어막으로 본인의 신원을 확인하기 위해 30~35개로 구성된 보안카드의 비밀번호 중 하나를 질의 받게 된다.

만약 인터넷 뱅킹을 사용하는 사용자의 컴퓨터가 해커가 설치한 바이러스 혹은 웜에 감염되어 키-스트록(key-stroke) 방식이나 키-로거(key-logger)에 의해 노출되었다 하더라도, 매 거래 시점마다 입력하는 값이 단순한 반복시도에 의해 알아내기 어려운 확률 분포도 안에 존재한다면, 보안카드는 제2의 방어막 역할을 충실히 수행할 수 있을 것이다. 또한, 보안카드 입력의 '재시도'를 방지할 수 있는 거래 절차가 확립된다면, 제2의 방어막을 좀 더 강화할 수 있을 것이다.

보안카드를 강화하는 방안으로, 개인 인증을 보강하기 위해 휴대폰을 활용하는 두 가지 방법이 있다. 일반적으로 휴대폰은 개인소유 성향이 무척 강한 것으로, 개인 인증의 한 방편으로 다른 서비스에서 많이 활용되고 있다.

첫번째 방법으로 현재 사용하는 보안카드와 더불어



〔그림 3〕 CryptoAPI Architecture

휴대폰의 SMS 서비스를 이용하는 방안이 있다. 이는 생성된 난수 입력을 두 번 하게 함으로써, 전체 비밀번호를 알아내는 확률을 낮추고 개인 인증을 강화할 수 있다는 효과가 있지만, 금융 기관의 입장에서 볼 때, 거래시 매번 지출되는 비용적인 측면을 고려하지 않을 수 없다.

두번째 방법으로 휴대폰에 보안카드 기능을 가진 칩을 내장하고, 해당 휴대폰을 은행 서버에 등록하여, 은행이 원하는 시점에 임의적으로 보안카드의 내용을 바꾸는 것이다. 이는 오프라인을 통해 보안카드를 교체해야 된다는 불편함과 보안카드가 가지고 있는 보안적 취약점을 극복할 수 있지만, 보안카드 기능을 가진 칩이 내장된 휴대폰의 인프라가 먼저 선행되어야 한다는 문제점을 가지고 있다.

위와 같은 휴대폰을 사용한 인증 이외에 좀 더 현실적인 대안으로 OTP(One-Time Password)를 사용하는 방법이 있다. OTP 란 일회성 비밀번호를 사용하는 것으로, 시스템에 접속할때마다 한번씩 새롭게 비밀번호가 부여되므로, 키-스트록(key-stroke), 키로거(key-logger) 등의 해킹으로부터 비밀번호가 노출되더라도 해당 비밀번호가 한 번의 사용 이후에 무효화 되므로, 안전하게 사용할 수 있다.

위에서 언급한 보안카드를 강화하기 위한 방법들은 정책적인 부분들이 먼저 선행되어야 한다. 물론 보안카드 강화를 위한 투자 비용에 대한 해당 금융기관들의 투자도 요구된다.

3.3 인증서와 개인키

인터넷 뱅킹 사용시 개인 인증의 핵심이 되는 것은 인증서와 개인키이다. 국내의 경우 인증서는 각 공인인증기관 및 연계된 금융기관을 통해 인증서를 발급받을 수 있으며, 각 인증서 및 개인키는 개인 컴퓨터의 하드디스크 및 공인 인증서를 저장할 수 있도록 규정된 저장 매체에 저장할 수 있다. 개인키는 저장될 때에 사용자가 입력한 비밀번호로 암호화되어 PKCS#7[3] 규격으로 저장된다.

가장 낮은 단계의 보안설정으로 볼 때, 인증서와 개인키가 쉽게 노출되는 경우는 하드디스크에 저장되었을 경우이다. 국내 공인 인증서는 파일 시스템상의 정해진 위치에 각 공인인증기관 및 인증서 단위의 파일로 저장되기 때문에, 컴퓨터에 대한 깊은 지식이 없는 사용자라 할지라도, 컴퓨터상에 저장되어 있는 인증서와 개인키 파일들을 쉽게 찾을 수 있다. 이것은 곧 해커의 입장에서는 어느 컴퓨터에 있는 인증서라도 쉽게 빼내올 수 있는 해킹 프로그램 제작이 무척 용이하다는 것이다.

가장 최근에 발생한 인터넷 뱅킹의 해킹 사고 사례만 보더라도, 가해자는 사용자의 컴퓨터에서 인증서 및 개인키를 손쉽게 빼내와 재발급 받아 사용했음을 알 수 있다. 개인키의 유출은 해킹 프로그램 제작을 통해 피해자의 컴퓨터의 하드디스크에서 파일의 형태로 직접 획득할 수도 있지만, 이것이 불가능한 경우에는 API Hooking을 통해 서명관련 함수를 모니터링 함으로써 쉽게 획득할 수 있다. 물론 개인키는 사용자가 입력한 비밀번호로 암호화 되어 있지만, 비밀번호는 사용자가 금융거래 이용시에 입력하는 비밀번호를 키-스트록(key-stroke) 방식이나 키-로거(key-logger) 등의 프로그램을 이용하여 획득할 수 있다.

많은 사용자들이 편리한 사용을 위해서 인증서를 집과 사무실 등에 각각 두거나 웹 메일이나 웹하드에 올려 놓고 이동시 편리하게 사용하는 경우가 많다. 이로 인하여 인증서의 유출 가능성이 대단히 높다. 이는 사용자의 자유이기 때문에 사실상 제한이 불가한 상태이다. 근본적으로 인증서를 하드디스크, 플로피 디스크, IC 카드 등에 저장 하는 한 이를 막을 수는 없다. 뿐만 아니라 인증서를 복사해 가는 것도 해킹 유형중의 하나이기 때문에 결국 해킹되어 유출된 인증서가 사용되어도 개인이 복사해서 사용하는 인증서와 구분되지 않기 때문에 막을 방법이 없게 된다.

근본적인 방법으로는 HSM 형태의 저장매체를 사용하여 한번 저장된 인증서의 개인키를 외부로 꺼낼 수 없게 하는 방법을 통하여 인증서 복제/복사를 방지할 수 있다. 물론 이 방법은 현재까지 알려진 기술로는 완벽한 복제/복사 차단 방법이다. 그러나 이 방법 역시 인증 프로그램에서 PKCS#11이나 MS CSP와 같은 표준 인터페이스를 지원해야 하나 지원하는 업체나 제품이 거의 없는 상황이다. 게다가 편리하게 사용가능한 USB형태의 토큰은 가격이 고가이고 저렴한 카드 형태는 리더기가 별도로 필요하고 그 비용 또한 만만치 않기 때문에 그 보급 방법에 문제가 있다.

하드디스크와 같이 특정 PC에 귀속된 경우와 같은 경우 인증서 자체에 식별번호와 같이 시스템 정보(CPU Serial, 보드정보, 바이오스 정보 등)를 포함시켜 인증서를 발급하는 것을 고려할 수는 있으나 이 기술을 적용하는 것이 시스템 종속적이고 부품 변경 등으로 인한 시스템 변경 시 인증서가 무효하게 되는 현상이 발생하며 또한 보안의 보장 여부는 검증 되지 않았다. 그러나 이 기술도 인증서를 IC Card나 이동 저장 장치에 담을 경우에는 의미가 없기 때문에 적절

한 방법으로 고려 될 수는 없을 것 같다.

위에서 언급했듯이 인증서와 개인키의 보안성을 위협하는 가장 큰 요소는 컴퓨터의 하드디스크에 저장되어 있을 경우이다. 본고에서는 이를 막기 위한 방법으로 소극적 대응 방법, 적극적 대응 방법, 진보적 대응 방법으로 설명한다.

먼저, 소극적 대응 방법으로는 이동성을 가진 저장 매체를 활용하는 것이다. 국내에서 공인 인증서를 저장하기 위한 이동성을 가진 표준 매체로는 이동식 디스크(floppy disk, USB Token)와 스마트카드가 있다. 물론 하드디스크에 인증서를 저장하는 것 보다는 안전하지만, 이동식 디스크 같은 경우, windows system 과 동일한 파일 포멧을 가지고 있어서, 이동식 디스크가 컴퓨터에 연결되어 있을 경우, 하드디스크에 인증서를 저장했을 때와 동일한 보안적 취약점을 가지고 있으며, 스마트카드의 경우, 스마트카드 리더기가 필수적으로 필요하기 때문에, 이동성에 제약을 가지게 된다.

적극적인 대응 방법으로는 저장 매체 자체가 key-pair 생성, 암호 및 서명 능력을 가진 칩을 탑제한 매체를 사용하는 것이다. 현존하는 매체로는 스마트카드 타입과 USB Token 타입 두 종류가 있으며, 외부 Interface로는 MS 에서 제공하는 CSP(Cryptographic Service Providers)[4] 와 PKCS#11 을 사용한다. 이러한 기술들은 개인키가 저장매체 외부로 유출되는 것을 막아주는 기본적인 로직들로 설계되어 있다.

국내에서는 현재 K 은행에서 MS CSP를 적용한 제품을 사용하고 있으며, PKCS#11 의 경우, KISA 에서 2003년 9월 국내에서 표준적[5]으로 사용할 수 있도록 규격을 정리해 놓았으나, 금융기관 및 업체, 사용자들의 인지도가 낮아 사용되지 않고 있다.

진보적인 대응 방법으로는 온라인상에 인증서와 개인키를 안전하게 위탁하여 사용하는 로밍 서비스 방식과 핸드폰 등과 같은 모바일 기기에 인증서와 개인키를 저장하는 방법이 있다. 온라인상에 인증서와 개인키를 보관하는 방법은 타인이 임의로 가져갈 수 없다는 매우 큰 장점이 있으나, 네트워크를 통해 데이터를 안전하게 전달할 수 있는 기술과, 관리자들도 인증서와 개인키를 열람해 볼 수 없도록 하는 암호화 기술, 암호키 분산 기술, 키로밍 기술들이 반드시 요구되는 기술집약적인 서비스이다. 이러한 로밍 기술의 경우 2000년 이후 미국을 중심으로 키복구 기술이 개인의 프라이버시를 침해한다는 맹점을 극복하기 위해 보다 강력한 암호 기술이 적용되어 발전된 기술로 국내에서도 2003년 정보통신부 산업기술개발사업의 일환으로 실제 운영 가능한 시스템이 개발되어 그 기술의 안정성이 입증되었다. 그리고, 핸드폰상에 인증서와 개인키를 저장하는 경우에는 휴대성이 보장되는 장점이 있으나, 휴대폰의 분실로 인한 보안적 위험 요소는 인증서와 개인키를 하드디스크에 저장한 것과 비슷한 위험요소를 가지고 있으며, 네트워크를 통해 데이터가 전달되므로, 데이터를 안전하게 전달할 수 있는 암호화 기술이 선행되어야 한다. 또한 인증서와 개인키가 저장 가능한 휴대폰을 배포해야 하므로, 비용적인 부분들도 해결되어야 될 과제로 남아있다.

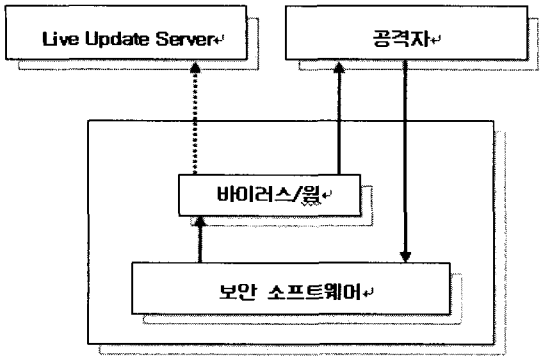
위에서 언급한 과제들 이외에도, 인증서 재발급시에 본인 확인을 위한 절차를 강화하는 등 정책 수립의 과제들이 아직 남아있다.

공인인증서 재발급의 이슈는 해킹을 통하여 인증서를 제외한 중요 뱅킹 정보가 유출되어 인터넷을 통하여 인증서를 재발급 받아 이를 사용할 수 있게 됨으로써 발생한다. 이를 보완하기 위해서 인증서 재발급이나 중요 정보 변경 등을 할 경우에는 SMS 또는 유선전화를 통한 통화 확인을 실시하도록 보완할 수가 있으나 고객 DB내의 휴대폰 정보나 전화 정보가 신뢰도가 떨어져 그다지 유효하지 못하다. 이런 이유로 재발급으로 인하여 발생하는 문제를 해결하는 어렵다. 결국 재발급 자체를 막는 것만이 재발급 문제를 근본적으로 해결하는 방법이다.

3.4 모듈 관리

현재 대부분의 보안 소프트웨어들은 MS(Microsoft)의 운영체제(OS:Operation System)상에서 동작하고 있으며, 이것은 곧 보안 소프트웨어들도 그 자신의 보안적 취약점 이외에 운영체제가 가지고 있는 보안적 취약점에 기인한 취약점들을 동일하게 가지고 있다고 볼 수 있다.

이러한 취약점들 중에 가장 큰 문제점은 역공학(Reverse Engineering)이 가능하다는 것이다. 역공학은 상품의 품질(quality)을 향상시키고 자원(resource)의 효율적인 관리를 위한 과정[6]을 위해 발전된 기술이지만, 소프트웨어 분야에서는 크랙(crack) 등과 같은 분야에 악용되는 현실로 나타나게 되었다. 보안 소프트웨어가 해커에 의해 분석되었을 때, 해커는 buffer overflow, memory attack 등의 방법을 동원하여 소프트웨어의 기능을 정지시키거나, 파괴할 수 있다. 현재는 상용화된 carck 가능한 제품들도 있으



〔그림 4〕 소프트웨어 모듈 변조 과정

며, 인터넷상에서 쉽게 구할 수 있는 crack 프로그램들도 있기 때문에, 이를 막기 위해서는 보안 소프트웨어 개발 업체들의 보안 소프트웨어 모듈에 대한 각별한 주의가 필요하며, 관련 기관들의 안전성 검증 작업도 필요하다.

이와 더불어 취약한 문제로는 라이브 업데이트(Live Update)중에 해커에 의해 변조된 모듈이 설치될 가능성이 매우 크다는 것이다. 아래 그림 4에 보안 소프트웨어의 모듈 변조 과정을 도식하였다.

단계 1: 공격자는 Live Update 서버에서 모듈을 다운 받음
단계 2: 공격자는 역공학을 이용하여 원본 모듈에 인증서를 추출하여 전송하는 기능을 추가
단계 3: 공격자는 바이러스/웜을 배포하여 라이브 업데이트시 자신의 서버로 접속하도록 유도
단계 4: 피해자는 공격자가 배포한 바이러스/웜에 의해 변조된 모듈을 설치함
단계 5: 공격자가 변조한 모듈에 의해 피해자의 인증서가 공격자의 서버로 전송됨

이러한 일련의 과정을 통해 피해자의 중요 정보가 해커에게 유출될 수 있다.

현재 이러한 공격에 의한 큰 피해 사고 사례는 접수되고 있지 않으나, 이러한 문제들에 대해 공공연하게 논의되고 있다. 라이브 업데이트의 보안성을 강화하기 위하여 보안 소프트웨어 개발 업체들은 라이브 업데이트 모듈의 투명성을 보장할 수 있도록 강화해야 할 것이다.

3.5 IE (Internet Explore)

최근들어 IE(Internet Explore)의 기능을 이용한 해킹 사고가 발표되어 많은 관심을 끌고 있다. 이 해킹 사고는 IE(Internet Explore)의 고유한 기능인 BHO(Browser Helper Objects)의 기능을 사용하여 웹브라우져에 입력된 데이터를 가로채는 방법이다.

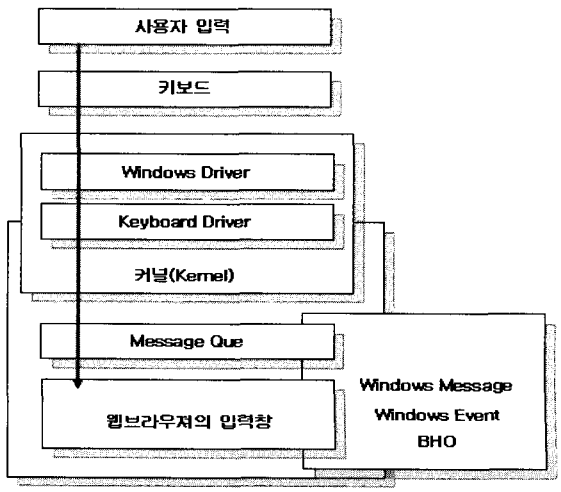
BHO(Browser Helper Objects)의 기능을 활용하면, 웹브라우져의 URL을 사용자가 의도하지 않은 곳으로 강제로 이동시키거나, 특정 프로그램을 실행시킬 수도 있다. 이러한 BHO(Browser Helper Objects)의 기능을 활용한 대부분의 해킹 프로그램들은 애드웨어나 스파이웨어로 제작되어, 피해자가 인지하지 못하는 사이에 피해자의 컴퓨터에 설치된다.

이를 막기 위해서는 사용자들의 각별한 주의가 필수적이다. 주기적으로 안티 바이러스 프로그램이나, 안티 애드웨어/스파이웨어 프로그램을 업데이트하고, 실행하여, 이러한 피해가 발생하지 않도록 주의해야 한다. 또한, 중요한 데이터가 암호화되지 않은 채 평문으로 웹브라우져를 통해 입력되는 것을 방지하는 것이 중요한데, 이 방법은 아래 '키보드 입력' 단락에서 제시한다.

3.6 키보드 입력 보안

키보드의 입력을 통한 중요 데이터의 획득은 앞서 말했듯이 키-스트록(key-stroke) 방식이나 키-로거(key-logger) 등에 의해 가능하다. 이러한 해킹 프로그램들이 기본적으로 사용하고 있는 기술은 윈도우 드라이버(driver) 기술이다.

아래 그림 5에 키보드를 통해 사용자가 입력한 데



〔그림 5〕 키보드를 통한 입력 데이터의 전달 Flow

이터가 해당 웹브라우져의 입력창(혹은 응용프로그램의 입력창)에 전달되기까지의 과정을 도식하였다. 이 중 하드웨어에서 운영체제를 거쳐 응용프로그램으로 이어지는 컴퓨터의Layer 중에서 가장 낮은 Layer에서 키보드를 통해 입력되는 데이터를 해킹하는 방법은 아래와 같이 3가지로 분류된다.

① 키보드 포트 해킹 (Keyboard Port Hacking)

키보드의 포트를 모니터링 하여 입력되는 데이터를 추출하는 방법

② 필터 드라이버 해킹 (Filter Driver Hacking)

Windows Driver 를 제어하여 키보드를 통해 입력되는 데이터를 추출하는 방법

③ 드라이버 후킹 (Driver Hooking)

키보드 드라이버를 후킹하여 키보드를 통해 입력되는 데이터를 추출하는 방법

이와 같은 방법들은 운영체제(OS)상의 가장 낮은 Layer 상에서 실행되기 때문에, 이를 막기는 쉽지 않다. 현재 이러한 해킹을 막기 위한 방법은 키보드 드라이버를 대체하는 이른바 "보안 드라이버"를 개발하여, 기존의 키보드 드라이버 대신에 키보드를 통해 입력되는 데이터를 받는 것이다. "보안 드라이버"는 키보드에서 전달된 데이터를 받아 암호화하여 자체 API를 통해 웹 브라우져나 응용프로그램에게 전달하기 직전에 복호화하여 전달한다.

이런 "보안 드라이버" 방식의 안티 키-스트록(key-stroke) 제품이나 안티 키-로거(key-logger) 제품들이 가지는 공통의 문제점들 또한 적지 않다. 가장 큰 문제점으로는 윈도우 드라이버의 불안정성으로 사용자 컴퓨터의 하드웨어 구성에 따라 완벽한 호환성이 유지되는 "보안 드라이버"를 개발하기 어렵다는 것이다. 이는 간혹 사용자의 컴퓨터상에 블루 스크린(Blue Screen)을 유발하는 요인이 되기도 한다. 또 다른 문제점으로는 "보안 드라이버"에서 암호화 된 데이터가 복호화되는 시점이 웹브라우져나 응용프로그램에 데이터가 넘어가기 직전이기 때문에, 순간적으로 암호화되지 않은 평문이 전달되게 된다. 결국, 암호화를 유지하는 구간이 제품의 성능을 평가하는 잣대가 되기도 한다.

다음으로, 응용프로그램 layer 에서 키보드를 통해 입력된 데이터를 가로채는 방법은 Windows 운영체제(OS)가 가지고 있는 'Windows Message'와 'Windows Event'를 이용하는 것이다. 키보드가 눌렸을때는 커널의 키보드 드라이버에서 이벤트를 발생시키며 어느 키가 눌렸는지에 대한 메시지를 전달한다. 해킹 프로그램은 이벤트를 감지하고 있다가 키보드가 눌렸음을 나타내는 이벤트가 들어오면 메시지를 캡쳐하여 키보드를 통해 어떤 키값이 입력되었는지 알 수 있다. 이런 해킹 프로그램 또한 "보안 드라이버"에서 키보드의 키가 눌렸을 때, 윈도우 이벤트와 메시지를 운영체제상으로 전달하지 않음으로써, 데이터를 안전하게 전달할 수 있다.

위에서 언급한 키보드 보안 제품들을 보완하기 위하여 본고에서는 두 가지 방법을 제시한다.

첫번째는 End-to-end 암호화이며, 두번째는 '가상 키보드'이다.

End-to-end 암호화란 키보드 보안 제품의 "보안

〔표 1〕 키보드 보안 솔루션과 가상 키보드 기능 비교

	키보드 보안 솔루션	가상 키보드
공격 방법	Port 해킹, Filter Driver, Driver Hooking Memory Attack, BHO, Dynamic HTML Hacking	좌표 추출, Screen Capture Memory Attack, BHO, Dynamic HTML hacking
End to End 암호화	PKI 솔루션과의 연동을 통해 적용 가능 하나, 완벽한 E2E암호화에는 일정한 한계가 있음	적용 가능
공격 대응 방안	BHO, Dynamic HTML Hacking → E2E 암호화를 통해 대응 가능 Port 해킹, Filter Driver, Driver Hooking, Memory Attack → 취약함	좌표 추출, Screen Capture → Shuffling 기능으로 대응 가능 Memory Attack, BHO, Dynamic HTML hacking → E2E 암호화를 통해 대응 가능
편리성	편리함	상대적으로 불편할 수 있음
안정성	드라이버 설치 문제로 시스템(OS)에 따라 불안정함	일반 Application으로 안정적임

드라이버"에서 암호화된 데이터가 웹브라우져나 응용프로그램에 전달되기 직전 복호화되는 hole을 막기 위함이다. 이를 위해 검증된 암복호 모듈을 클라이언트와 서버에 탑재하여, 키보드 보안 모듈에 의해 데이터가 복호화 되는 순간, 새로이 검증된 암호화 모듈로 데이터를 암호화하여 전달한다. 서버에서는 암호화된 데이터가 전달될 것이며, 서버에 탑재된 검증된 복호화 모듈을 이용하여 원본 데이터를 추출할 수 있을 것이다.

가상키보드는 데이터를 입력할 때에 키보드를 통한 입력 자체를 부정하는 방법이다. 가상키보드는 Windows 상에 키보드의 GUI 를 가진 응용프로그램을 실행시켜, 마우스를 통한 데이터 입력을 처리하는 방식이다. 이 방식은 데이터 입력시에 키보드 드라이버를 거치지 않으므로, 위 그림 5에서와 같은 layout에 대한 보안은 필요 없지만, Windows Event 확인에 의한 응용프로그램의 좌표를 스니핑할 수 있는 위험성을 가지고 있다. 이를 막기 위해, GUI 상의 키보드 자판을 열단위로 랜덤하게 섞는 'shuffle' 기능을 추가하는 방안이 있을 수 있다.

표 1에 키보드 보안 솔루션과 가상키보드간의 차이점을 요약하였다.

Ⅲ. 결 론

본고에서는 인터넷 뱅킹 시스템의 해킹 가능성에 대한 기술적 분석과 대응방법에 대하여 각각 시술하였다. 최근 발생한 인터넷 뱅킹 해킹 사건에서 볼 수 있듯이 아무리 좋은 보안 솔루션을 이용해 금융 정보보호 시스템을 구축했더라도 적절한 유지보수와 지속적인 기술갱신이 따르지 않으면 언제든지 치명적인 보안 사고의 가능성은 열려 있다. 최첨단 보안 기술의 집약이라도 말할 수 있는 인터넷 뱅킹 시스템의 취약점 발견으로 인해 국민의 우려가 증폭되었지만 이를 불식시키기 위한 적절한 대안은 아직 제시되지 못하고 있다. 원천적으로 보안성이 결여된 시스템(OS) 위에 아무리 좋은 솔루션을 올려놓아도 허점이 있기 마련이라는 벤더들의 볼멘소리도 있다. 본고에서 살펴본 바에 의하면 기술적으로 모든 분야를 아울러 아주 완벽한 보안 솔루션을 구축하기란 그리 쉬워 보이지만은 않는다. 완벽한 보안 솔루션의 도입으로 인한 사회적 비용 발생, 사용자들의 사용 불편 등에 대한 대응 또한 만만치 않은 저항일 것이다. 현재 국내의 인터넷 뱅킹 시스템은 PKI 기반의 인증 기술이 적용된 막강한 보안 솔루션으로 구축되어 있다. 이 시스템의 보안도는 결국 개인키가 안전한 장소에 저장되어 사용되고, 사용자가 입력하는 패스워드에 에이징(Aging)이 완벽하게 적용될수록 높아지게 된다. 본고에서 사고 방지를 위한 진보적인 대응책으로 소개된 로밍서비스의 경우 전문적인 보안 지식이 부족한 사용자들을 대신하여 보다 강력한 보안시스템이 구축된 로밍서비스 센터가 개인키를 안전하게 관리해 주며 사용자 입력하는 패스워드에 에이징 기법과 키보드 보안기술이 적용되어 있어 인터넷 뱅킹 해킹 방지를 위한 좋은 솔루션이 될 수 있을 것으로 사료된다.

참 고 문 헌

[1] 한국은행 홈페이지(http://www.bok.or.kr) 보도 자료 중 "2005년 6월말 현재 국내 인터넷뱅킹 서비스 이용현황"

[2] http://banksafeonline.org.uk/

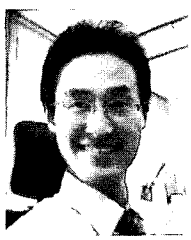
[3] http://www.rsasecurity.com의 PKCS section

[4] http://msdn.microsoft.com의 Security section

[5] 한국정보보호진흥원(http://www.kisa.or.kr) 자료 중 2003년 09월 "암호토큰을 위한 PKCS #11 프로파일 규격" PKCS#11 Conformance Profile Specification for Cryptographic Token

[6] Reverse Engineering-Kathryn A. Ingle, McGraw Hill,1994

〈著 者 紹 介〉



강 신 범 (Shinbeom Kang)

1997년 2월 : 전북대학교 정보통신공학과 졸업

1999년 2월 : 전북대학교 정보통신공학과 석사

1997년 2월~1999년 4월 : 미래산업(주) 보안기술연구소

1999년 4월~현재 : 소프트포럼(주) 전략기획실 실장

〈관심분야〉 해킹, 정보보호, 정보보호표준, 전자상거래 보안

정 현 철 (Hyoncheol Chung)
종신회원

1991년 2월 : 경북대학교 대학원 컴퓨터공학과 졸업(공학석사)
2003년 8월 : 경북대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 2월~1998년 10월 : 한국전자통신연구원 선임연구원
1998년 10월~현재 : 소프트포럼(주) 대표이사
〈관심분야〉 정보이론, 정보보호, 정보보호표준, 보안성 평가