情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구

이 원 철*, 이 석 래**, 이 재 일***, 김 인 석****

요 약

전자금융거래를 포함하여 안전한 전자거래 기반 마련을 위해 1999년 7월 1일 전자서명법의 시행과 더불어 시작된 공인인증서비스는 비대칭형(공개키) 암호기술을 기반으로 하는 전자서명(Digital Signature)에 법적 효력을 부여하여, 온라인 전자결제 등 전자거래를 위한 안전한 기반을 마련하여 왔다. 그러나, 최근 정보화의 급속한 발전으로 일반인도 쉽게 해킹툴을 접할 수 있게 되어, 인터넷뱅킹 해킹사고 등 전자금융거래의 안전성이 위협을 받고 있다. 본고에서는 전자금융거래에서 중요한 역할을 담당하는 공인인증서비스의 취약점을 분석하고 공인인증서비스 안전성 강화 방안에 대하여 기술한다.

Ⅰ. 서 론

정보화의 진전으로 e-비지니스 환경에서의 안전한 전자거래를 위해 공개키기반구조(Public Key Infrastructure, PKI) 도입의 필요성이 제기됨에 따라 국내에서는 1999년에 전자서명법을 시행하고 최상위인증기관(Root CA) 구축 및 공인인증기관 지정 등 전자서명인증체계를 설립하여 안전한 공인인증서비스를 시행하여 왔다. 전자서명법은 비대칭형(공개키) 암호기술을 기반으로 하는 전자서명(Digital Signature)에 법적 효력을 부여함으로써, 온라인 전자결제 등과 같은 전자적 거래를 촉진코자 하는 제도적 기반이며, 이를 통해 2005년 6월말 현재 1,134만 명이 공인인증서비스를 이용하고 있는 것으로 추정되고 있다.

그러나, 해킹기술의 발전과 초고속 인터넷의 확산으로 일반 사용자들도 쉽게 해킹툴을 접할 수 있게 됨에 따라 안전하다고 여겨왔던 전자금융분야에서의 공인인증서비스도 해킹의 위협에 노출될 수 있다. 특히, 지난 5월에는 한 초보 해커가 인터넷에서 쉽게 구할 수 있는 키보드해킹 프로그램으로 타인의 PC를 해킹하여 5천만원을 인출해가는 사고가 발생하기도 했다.

본 고에서는 전자금융거래 시 공인인증서비스의 취약점을 분석하고 전자금융거래의 안전성 및 신뢰성을 제고하기 위한 방안을 제안하고자 한다. 제 2절에서는 공인인증서비스의 안전성을 위협하는 취약점들에 대해 살펴보고, 제 3절에서 공인인증서비스의 안전성 제고를 위한 방안을 제안하고자 한다.

Ⅱ. 전자금융거래에서의 공인인증서비스 취약점 분석

전자금융거래를 포함하여 안전한 전자거래 기반 마련을 위해 1999년부터 국내에서 시작된 공인인증서비스는 전자거래서비스에서의 안전성 및 신뢰성을 제공하기 위한 수단으로 사용되어 왔고, 2005년 6월말 1,000만 명 이상이 이용할 정도로 급속히 확산되었다. 그러나, 지난 5월에는 인터넷뱅킹을 해킹하여 타인 계좌에서 5천만원을 인출하는 사고 발생 및 인터넷뱅킹서비스에서 사용되는 「공인인증서 관리 프로그램」의 취약점 발견 등으로 공인인증서비스의 안전성에 대한 검토가 필요하게 되었다. 이에 본 절에서는 현재 공인인증서비스에서 제기되고 있는 여러 취약점들을 살펴보고자 한다.

* 한국정보보호진흥원 인프라보호단 인증관리팀 (lwc@kisa.or.kr)
** 한국정보보호진흥원 인프라보호단 인증관리팀 (sllee@kisa.or.kr)
*** 한국정보보호진흥원 인프라보호단 (jilee@kisa.or.kr)
**** 금융감독원 IT업무실 (inskim@fss.or.kr)

2.1 해킹 사례를 통해 본 공인인증서비스 취약점

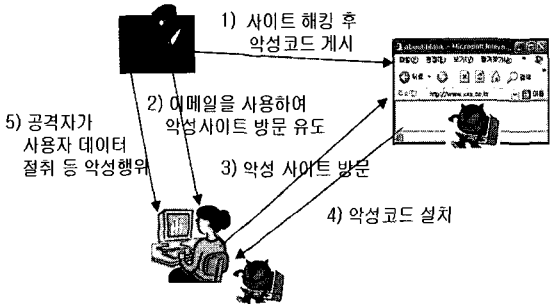
지난 5월 타인의 PC를 해킹하여 계좌에서 5천만원을 인출하는 인터넷뱅킹에 대한 해킹사건이 국내에서 처음으로 발생하였다. 범인은 타인 PC의 키보드 입력 내용을 볼 수 있는 키보드 해킹프로그램을 인터넷게시판을 통해 피해자의 PC에 설치하고, 이를 통해 피해자가 인터넷뱅킹을 이용하면서 입력한 계좌 비밀번호, 보안카드 번호 등 개인정보를 입수하고, 이러한 정보를 이용하여 피해자의 인증서를 자신의 PC에서 재발급 받아 인터넷 뱅킹에 사용하였다.

해당 사건 발생이 가능했던 원인으로 여러 가지 취약점을 들 수 있다. 첫째, 인터넷뱅킹 사이트에서 해킹방지 프로그램의 이용이 미비하였다는 점이다. 인터넷뱅킹에서 입력되는 비밀번호 등 개인정보의 보호를 위해서는 사용자 PC에 해킹 방지프로그램이 자동 설치되어야 하나, 일부 금융기관에서는 이용자 편의를 이유로 해킹방지 프로그램을 이용자가 선택적으로 설치토록 하였다. 이로 인해 사용자 PC에 해킹 방지프로그램이 설치되지 않은 경우, 비밀번호 등 개인정보는 쉽게 해커에게 유출될 수 있었다.

둘째, 인터넷뱅킹의 안전성 확보를 위한 주요 수단으로 활용되는 보안카드의 이용 상 취약점이다. 보안카드는 30여개의 4자리 숫자 표로 구성된 카드로 인터넷 뱅킹 이용 시 일회용 비밀번호처럼 사용된다. 그러나, 30여개로 구성된 보안카드의 비밀번호는 동일한 번호의 재 사용률이 높아 일회성 비밀번호로서의 가치가 떨어진다. 또한, 보안카드는 이용자가 3회 이상 입력 오류 시 거래가 정지되도록 운용되고 있으나, 일부 은행의 경우, 재접속 시에는 해당 기능이 올바르게 적용되지 않는 등 관리가 미흡하였다.

마지막으로 해킹한 정보로 공인인증서 재발급이 가능하였다는 점이다. 공인인증서 이용자가 전자서명키를 분실·훼손하거나 또는 도난·유출당한 경우, 해당 공인인증서를 폐지하고 새로운 공인인증서를 재발급 받아야 한다. 공인인증서를 재발급 받기 위해서는 해당 은행 등을 직접 방문하여 본인 여부를 확인받아야 한다. 그러나, 이는 이용자에게 상당한 불편을 초래하기 때문에 이를 해소하기 위해 온라인 본인확인을 통한 공인인증서 재발급을 일부 허용하였고, 해커가 이를 악용하여 피해자의 공인인증서를 자신의 PC에서 재발급 받아 이용하였다는 점이다.

즉, 사용자 편의성을 위해 허용한 여러 기능들이 오히려 취약점으로 작용하게 되었다.



〔그림 1〕 액티브엑스 취약점을 이용한 공격

2.2 공인인증서 관리프로그램의 취약점

사용자 PC의 공인인증서 관리 프로그램에서 인터넷 뱅킹 접속 시 액티브엑스의 취약점으로 인해 악성코드가 설치 될 수 있다. 이로 인해 다음과 같이 공격자가 의도하는 악의적인 프로그램이 사용자 PC에서 실행될 수 있다.

① 공격자는 사전에 악성 프로그램을 유포할 사이트를 해킹하거나, 게시판 등을 통해 악성 프로그램을 설치한다.
② 공격자는 사용자를 악성 프로그램 유포 사이트로 유도하기 위하여 사용자에게 E-Mail을 보내 사용자의 접속 유도 또는 특정 웹 게시판 사이트로 접속을 유도한다.
③ 공격자가 사전에 만들어놓은 악성 프로그램 유포 사이트에 사용자가 접속한다.
④ 이때, 악성프로그램이 사용자 PC에 자동 설치되어 작동한다.
⑤ 공격자는 PC에 대한 제어권한을 획득하여 사용자의 데이터 절취한다.

물론, 이러한 문제는 공인인증서비스 자체의 취약점에 의한 것은 아니며, 공인인증서 관리를 위한 프로그램이 가지는 취약점이며, 이를 이용한 해킹은 다음과 같은 사전 조건이 모두 만족되어야만 가능하다.

첫째, 사용자의 PC에 취약점이 존재하는 프로그램이 설치되어 있어야 한다.

둘째, 해커는 사용자를 공격하기 위하여 E-Mail 또는 게시판으로 대상자를 유인하는 메시지를 전달하여야 한다.

셋째, 사용자는 해커가 사전에 만들어 놓은 악성사이트로 접속해야 한다.

따라서, 보안프로그램과 금융기관 홈페이지 등을 이

용하는 공인인증서비스에서는 이러한 해킹의 발생 가능성은 낮다고 볼 수 있으나, 이와 유사한 여러 방법을 통해 해커에게 사용자의 전자서명키, 공인인증서, 패스워드가 유출될 수 있다.

현재, 대부분의 공인인증서비스 이용자는 자신의 전자서명키를 패스워드로 암호화하여 공인인증서와 같이 하드디스크에 저장하여 사용하고 있으며, 이에 따라 다양한 해킹 수법으로 사용자의 암호화된 전자서명키 및 공인인증서 유출이 가능하다.

플로피 디스켓이나 USB 저장장치와 같은 이동식 저장매체에 전자서명키를 저장하여 사용하더라도 100% 안전한 것은 아니며, 이동식 저장매체 종류에 따라 안전성의 정도 차이만 존재한다.

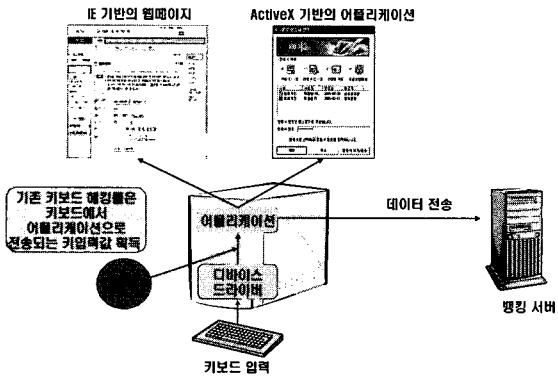
2.3 키보드 해킹을 통한 개인정보 유출

웹사이트 이용자가 인터넷에 접속하여 주민번호 등 중요한 개인정보를 입력할 때, 트로이목마, 백도어, 스파이웨어, 악성코드, 애드웨어, 키로거와 같은 여러 해킹 프로그램으로의 위협이 도사리고 있다.

현재, 개인정보 획득을 위한 방법은 크게 키로거와 같은 키보드 해킹 프로그램을 이용하는 방법과 피싱 등이 있는데, 피싱 문제는 공인인증서비스 측면보다 사용자 측면에서의 대책 마련이 더 중요한 부분이므로 본 고에서는 키보드 해킹에 대해서만 살펴보기로 한다.

키보드 해킹 프로그램은 앞서 인터넷 뱅킹 해킹 사례에서 언급한 바와 같이 타인 PC의 키보드 입력내용을 볼 수 있도록 해준다.

그림 2와 같이 사용자가 인터넷 이용 시 키보드 해킹이 이루어지는 영역은 크게 5가지 영역으로 하드웨어 레벨, 커널(Kernel) 레벨, 시스템 레벨, 어플리케이션 클래스(Class) 레벨과 인터넷 익스플로어(Internet Explorer) 레벨로 나눌 수 있다.



〔그림 2〕 키보드 해킹

하드웨어 레벨에서의 키보드 해킹은 키보드 컨트롤러 칩의 키보드 포트를 직접 모니터링하는 방법, 인터럽터 컨트롤의 취약성을 이용하는 방법, 인터럽터를 후킹(Hooking) 하는 방법 등이 있다. 커널 레벨에서는 키보드 드라이버를 후킹하는 방법과 USB 키보드의 USB HID(Human Interface Devices)를 후킹하는 드라이버 방법이 있다. 시스템 레벨에서는 시스템에서 호출되는 메시징(Messaging)을 후킹하는 방법으로 CBT(Core Based Tree) 메시지나 GET 메시지 등을 후킹하여 키입력을 가로채는 방법이다. 어플리케이션 클래스 레벨에서는 어플리케이션이 종속클래스, 슈퍼클래스 등의 윈도우 클래스를 호출하는 것을 후킹하게 된다. 마지막으로 익스플로어의 취약점을 이용하는 방법으로 익스플로어의 웹 브라우저 입력창에서 개인 정보를 입력하는 경우 MSHTML의 취약점, DHTML를 이용한 KEYPRESS 취약점, CHANGE 취약점, SUBMIT 취약점을 이용하여 개인정보를 유출하는 방법이 있다.

이러한 키보드 해킹을 방지하기 위하여 은행 등과 같은 전자거래 사이트에 서비스 이용 시 백신이나 키보드 해킹 방지 프로그램이 설치되고 있으며, 백신이나 키보드 해킹방지 프로그램 등과 같은 보안 솔루션을 이용하여 개인정보를 보호할 수 있으며, 이 경우, 보안 솔루션의 해킹 탐지 능력이 개인정보 보호의 중요한 키포인트로 작용된다.

Ⅲ. 공인인증서비스 안전성 제고 방안

3.1 전자서명키 저장매체 안전성 강화

일반적으로 공인인증서비스 이용자는 공인인증서와 전자서명키 저장매체로서 하드디스크를 주로 이용하고 있고, 일부 이용자의 경우 이동성을 확보하기 위해 플로피디스켓 또는 USB 저장장치 등을 이용하고 있다. 물론, 개인정보, 전자서명키, 공인인증서 등의 안전한 저장·관리를 위한 스마트카드나 USB 토큰도 일부 사용되고 있다.

그러나, 국내 전자서명인증체계에서는 공인인증기관 간 인증서 상호연동을 위해 공인인증서 저장위치를 통일하여 공개하고 있어 해커들의 표적이 되고 있다. 비록, 전자서명키는 암호화가 되어 저장되어 있지만, 키보드해킹 등으로 인해 패스워드의 획득이 가능하므로 하드디스크나 이동형 저장장치에 저장된 사용자의 공인인증서와 전자서명키는 해킹에 쉽게 노출될 수 있다.

또한, 전자서명키 등의 안전한 저장·관리를 위해 스마트카드나 USB 토큰을 이용하더라도 저장장치 내에 자체 전자서명기능이 없는 경우, 전자서명을 하기 위해서는 저장매체에 저장된 키를 가입자 PC의 메모리에 로딩하여야 하며, 이 때 메시지 후킹, 메모리 덤프 등의 해킹으로 전자서명키가 유출될 수 있는 가능성이 존재한다.

따라서, 사용자의 전자서명키의 유출없이 안전한 공인인증서비스를 이용하기 위해서는 암호 연산이 가능한 마이크로프로세서 칩이 탑재되어 자체 키생성, 전자서명, 검증 등을 수행할 수 있는 암호기능이 내장된 스마트카드나 USB 암호토큰 등을 사용할 필요가 있다. 이들은 보안기능을 갖춘 장치 내부에서 모든 연산이 이루어지기 때문에 키가 외부로 누출될 가능성이 없으므로 안전하게 전자거래서비스를 이용할 수 있다.

전자서명키 및 공인인증서 저장을 위한 스마트카드 또는 USB 암호토큰을 이용할 경우, 이들 장치를 이용하기 위한 다양한 종류의 디바이스드라이브를 지원 문제를 해결하여야 한다. 먼저, 공인인증서 관리 프로그램과 이들 장치간의 인터페이스를 PKCS #11과 같은 표준 규격으로 통일하여야 한다.

3.2 공인인증서 재발급 시 안전성 강화

공인인증서 이용자가 전자서명키를 분실·훼손하거나 도난·유출당한 경우에는 해당 공인인증서를 폐지하고 새로운 공인인증서로 재발급받아야 한다. 이 경우, 이용자의 본인 확인을 위해 이용자가 직접 은행 등의 등록대행기관을 방문하여야 하는데, 이러한 번거로움을 해소하여 이용자의 편의성을 증대하고자 온라인 본인확인을 통한 신원확인을 허용하고 있다.

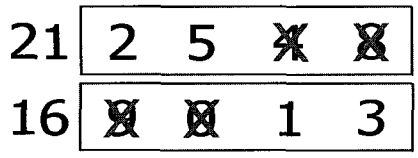
온라인 신원확인을 통한 재발급에는 공인인증서 재발급 신청자가 본인임을 확인하기 위해 계정번호, 비밀번호, 계좌번호, 주민등록번호 등의 개인정보와 일회용 비밀번호를 이용한다. 그러나, 이러한 정보들은 키보드 해킹 등으로 인해 해커에게 쉽게 노출될 수 있다.

특히, 비밀성이 가장 요구되는 일회용 비밀번호의 경우, 현재 대부분 보안카드를 사용하고 있으나, 가입자당 사용할 수 있는 번호는 30개 정도이며, 한 번호당 4자리의 숫자로 이루어져있어 일회성 정보로서의 가치가 떨어진다. 즉, 보안카드의 번호가 30개 정도이므로 동일 번호의 재사용 빈도가 높으므로 보안카드 중 하나의 번호가 노출될 경우, 전체 안전성은 취약할 수 있다.

따라서, 안전한 전자거래서비스 제공을 위해서는 공인인증서의 온라인 재발급 시, 주기적인 직접대면을 통해 신원확인을 강화하거나 이용자의 편의성을 해치지 않는 범위 내에서 보안카드의 비밀번호 수를 증가하여 해커에게 노출되는 정보량을 최소화하는 방안 마련이 필요하다.

현재, 일회용 비밀번호로 사용되고 있는 보안카드의 비밀번호 개수는 30가지 정도로 한정되어 있다. 그러나, 현재 발급된 보안카드의 30가지 비밀번호 중 2가지 이상의 비밀번호를 선택하여 조합하여 사용한다면 비밀번호 경우의 수를 증가시킬 수 있어 일회성 비밀번호가 가지는 랜덤 특성을 가질 수 있다.

다음 그림과 같이 4자리의 숫자 30개로 구성된 보안카드 이용 시 해당 보안카드의 비밀번호 중 2개(지시번호 21번 및 16번)를 선택하고 각 비밀번호에서 고정된 위치의 두 숫자를 조합하여 새로운 비밀번호를 생성할 수 있다.



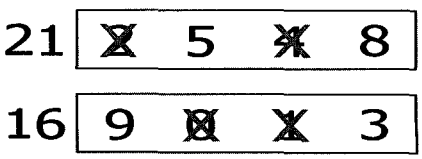
〔그림 3〕 2개의 비밀번호의 고정위치 선택 예

그림 4와 같이 30개의 보안카드 비밀번호 중 21번째 비밀번호 '2548'의 앞자리 수 2개와 16번째 비밀번호 '9013'의 뒷자리 수 2개를 조합함으로써 새로운 비밀번호 '2513'을 만들어 낼 수 있다. 이와 같은 방법으로 수식 1과 같이 총 870가지의 비밀번호가 사용 가능하므로 동일한 비밀번호의 재사용 빈도는 낮아진다.

$$\text{경우의 수} = N \times (N-1) = 870 \quad (1)$$

N : 보안카드의 비밀번호 수, 30

또한, 고정된 위치의 비밀번호를 사용하지 않고 랜덤 위치의 비밀번호를 사용하는 경우에는 그림 5와 같이 총 31,320가지의 4자리 수의 비밀번호가 생성 가능하지만, 중복되는 숫자를 고려하면 4자리의 최대 경우의 수 10,000 가지의 비밀번호 생성이 가능해진다.



〔그림 4〕 2개의 비밀번호 비고정위치 선택 예

$$\text{경우의 수} = (N \times 4C2) \times ((N-1) \times 4C2) \quad (2)$$
$$= 31{,}320$$

N : 보안카드의 비밀번호 수, 30

이와 같은 방법으로 기존에 발급된 보안카드를 그대로 이용하면서 안전성을 강화할 수 있으나, 이용자는 보안카드 이용 시마다 기존 비밀번호 이용하여 새로운 비밀번호를 조합하여야 하는 것이 불편할 수 있으므로 이용자의 편의성을 고려하여 안전한 비밀번호 생성 방안을 고려하여야 한다.

3.3 액티브엑스(ActiveX) 취약점 등 대응 체계 마련

지난 5월 공인인증서 관리 프로그램에서의 액티브엑스 취약점이 보고된 직후, 정보통신부, 한국정보보호진흥원, 공인인증기관, PKI 솔루션 업체 등으로 구성된 취약점 대응 TFT가 구성되었으며, 전체 전자거래서비스 기관(업체) 중 약 32%에 대한 보안 패치가 신속히 이루어진 바가 있다.

액티브엑스 취약점 등을 이용해서 이용자의 PC에서 악성의 프로그램을 실행시키는 등의 해킹방법은 비단 공인인증서비스 뿐만 아니라, 인터넷을 사용하는 모든 응용 프로그램이 산재하고 있는 문제라고 볼 수 있다. 또한, 이러한 사용자 소프트웨어의 취약점은 앞으로도 지속적으로 발생될 수 있다.

그러므로, 사용자 소프트웨어의 취약점에 대응하기 위해서는 지속적인 예방과 업데이트가 필수적이며, 이후 발생되는 취약점에 대해 체계적으로 대응할 수 있는 대응체계를 정비할 필요가 있다. 이를 위해서는 다수의 이용자가 사용하는 인터넷뱅킹 등과 같은 서비스를 대상으로 하는 해킹 프로그램의 수집·분석 능력을 강화하여 민·관이 공동으로 사고를 예방하는 체계를 구축해 나가야 한다.

3.4 개인정보 등 유출 방지를 위한 키보드 해킹방지

키보드 해킹을 방지하기 위하여 은행 등과 같은 전자거래 사이트에 서비스 이용 시 백신이나 키보드 해킹 방지 프로그램이 설치되고 있으며, 백신이나 키보드 해킹방지 프로그램 등과 같은 보안 솔루션을 이용하여 개인정보를 보호할 수 있다.

따라서, 키보드 해킹방지 프로그램 등과 같은 보안 솔루션의 해킹 탐지 능력이 중요한 키포인트로 작용된다. 국내 키보드 해킹방지 프로그램의 경우, 하드웨어 레벨의 해킹이나 메시지 후킹 등은 방지할 수 있으나, 웹 브라우저 입력창에 대한 해킹 방지는 제공되지 못하는 경우가 있다. 이러한 웹 브라우저 입력창에 대한 방지를 위해서는 기존 인터넷 익스플로러 및 사용자 소프트웨어 브라우저에 사용되는 일반 텍스트 입력창을 보안개체인 보안입력창으로 치환하여 사용자 거래정보 암호화하는 전송하는 방안이 고려되어야 한다.

Ⅳ. 결 론

1999년 전자서명법 시행과 함께 시작된 공인인증서비스는 비대칭형(공개키) 암호기술을 기반으로 하는 전자서명(Digital Signature)에 법적 인감과 동일한 효력을 부여하여, 온라인 전자결제 등 안전한 전자거래를 위한 기반을 마련하여 왔다.

최근 정보화의 급속한 발달로 일반인도 쉽게 해킹툴을 접할 수 있게 되어, 인터넷뱅킹 해킹사고 발생 등 공인인증서비스의 안전성이 위협을 받고 있다. 이에 자체서명기능을 가지는 스마트카드 등의 사용과 같은 전자서명키에 대한 안전한 관리 대책, 공인인증서 온라인 재발급 절차 개선, 공인인증체계의 안전성과 가용성 강화를 위한 장애발생 대응 체계 마련 등을 통해 공인인증서비스 안전성에 대한 신뢰 회복이 중요한 시점이다.

이러한 공인인증서비스의 신뢰 회복을 위해서는 현재 공인인증서비스의 문제점을 해결하고, 향후 발생할 수 있는 취약점에 대비할 수 있는 발판을 마련하여 민·관이 유기적으로 협력하여야 한다. 또한, 일반 이용자들에게도 해킹방지 프로그램의 설치나 비밀번호 관리 방법 등에 대한 전자거래 이용 가이드라인을 제공하여 보안 의식 제고의 기반을 마련하여야 한다.

참 고 문 헌

[1] 최영철, 오경희, 이재일, 홍기웅, 이홍섭 "전자서명 인증관리센터 구축 및 운영", *통신정보보호학회지*, 1999.

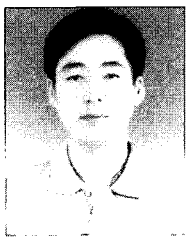
[2] 마이크로소프트, "'브라우저 프린트 템플릿'과 '폼을 통한 파일 업로드' 취약점에 대한 패치 제공", *Microsoft Security Bulletin MS00-093*, 2002.

[3] RSA Laboratories, "PKCS #11: Cryptographic Token Interface Standard", *RSA Security*, 2004.

[4] Sachin Shetty, "Introduction to Spyware Keyloggers", http://www.securityfocus.co

m/infocus/1829. 2005.
[5] KBS, "인터넷 인증서 비밀번호 샌다" 2005. 5. 보도자료.
[6] 연합뉴스, "해킹에 구멍 뚫린 인터넷 뱅킹", 2005. 6. 보도자료

〈著 者 紹 介〉

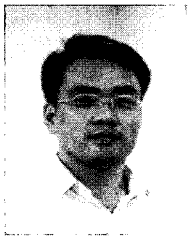


이 원 철 (Lee Won Cheol)

1995년 2월 : 경북대학교 전자공학과 공학사
1997년 2월 : 경북대학교 전자공학과 공학석사
1999년~2001년 : (주)웰컴정보시스템 근무
현재 : 한국정보보호진흥원 인프라보호단 인증관리팀

이 석 래 (Lee Seok Lae)

1992년 한양대학교 전자통신공학과 공학사
1994년 한양대학교 전자통신공학과 공학석사
1994년~1999년 LG전자 근무
현재 : 한국정보보호진흥원 인프라보호단 인증관리팀장



이 재 일 (Lee Jae Il)

1986년 2월 : 서울대학교 계산통계학 이학사
1988년 2월 : 서울대학교 계산통계학 이학석사
1991년~1996년 : 한국 IBM 소프트웨어 연구소 근무
현재 : 한국정보보호진흥원 인프라보호단장

김 인 석 (Kim In Seok)

1973년 2월 : 홍익대학교 전자계산학과 이학사
2003년 2월 : 동국대학교 국제정보대학원 정보보호학과 이학석사
2004년~현재 : 고려대학교 정보보호대학원 박사과정
1980년~1998년 : 한국은행 근무
현재 : 금융감독원 IT감독팀장