인터넷뱅킹 클라이언트 보안 강화를 위한 새로운 마우스 이용 비밀번호 입력 기술

°김영환 °°김성진 °이영록 °노봉남
°전남대학교 정보보호협동과정 °°광주은행 IT 업무부
°yhkim@kjbank.com °°sjkim100@kjbank.com °dogu@jnu.ac.kr °bongnam@jnu.ac.kr

A New Technology for Enhancing the Security of Client of Internet Banking by Using the Mouse used to Input Password

°YoungHwan Kim °°S.J. Kim °Y.L Lee °B.N. Noh
°Dept. of Information Security, Chonnam National University
°°IT Dept. of KwangJu Bank,

요 약

본 논문에서는 인터넷뱅킹의 클라이언트 측에서 마우스로 비밀번호를 입력하는 새로운 기술을 제안한다. 제안하는 기술은 웹 페이지의 입력 창에 있는 내용을 가로채기하는 것과 PKI 암호 모듈로 위장한 모듈이 사용자 정보를 가로채기하는 것으로부터 안전하도록 구현되었으며, 기술 자체는 키 스트로크와 훔쳐보기로부터 안전한 특징을 갖는다. 제안하는 기술은 현재 인터넷뱅킹에 탑재 가능한 상용 제품 수준으로까지 구현된 상태이다.

1. 서 론

인터넷뱅킹은 사용자들에게 공간적 이동을 하지 않아도 되도록 하였고, 이로 인해 시간과 비용을 절약할 수 있도록 해주었다. 이러한 장점 때문에 인터넷뱅킹 가입자 수는 2005년 9월말 현재 2천 543만명에 이르고 있으며, 2005년 3/4분기 중 인터넷뱅킹을 이용해 조회, 자금이체 및 대출을 포함한 금융 서비스 이용건수는 일평균 1,127만건에 달하고 있다 [22].

한편, 인터넷뱅킹의 클라이언트 측에서 보안사고가 발생하면 이는 바로 사회적 이슈가 되고 있다. 대표적인 예로서 2005년 6월의 키 스트로크(Key stroke) [23]를 이용한 계좌이체 사건은 TV의 헤드라인 뉴스를 장식하였고, 일간지의 1면 톱기사로 다루어졌다.

사건사고의 영향으로 현재 시중은행들은 인터넷뱅킹의 클라이언트 보안 강화를 위해 전력하고 있으며, 그 결과로 인터넷뱅킹의 클라이언트 측은 보안 기술의 집합체라 해도 지나침이 없을 정도가 되었다. 시스템적인 것으로는 백신과 방화벽 등이 설치되고, 기술적으로는 SSL 프로토콜 [1, 2] 및 PKI(Public Key Infrastructure; 공개 키 기반구조) [3-5]가 적용되고 있다. 마우스를 이용한 비밀번호 입력과 같은 새로운 기술이 도입되고 [6, 7], OTP(One Time Password; 일회용 패스워드) [8] 와 같이 기존에 알려져 있는 개념을 현실에 적용하고자 하는 등의 시도가 진행되고 있다.

본 논문에서는 인터넷뱅킹의 클라이언트 측에서 마우스를 이용해 비밀번호를 입력하는 기술을 제안한다. 제안하는 기술은 구현 측면에서 웹 페이지 입력 창에 있는 내용의 가로채기 및 PKI 암호 모듈로 위장한 모듈의 사용자 정보 가로채기에 안전하며, 기술적 측면에서는 키 스트로크와 훔쳐보기 [9-12]로부터 안전하다. 제안한 기술은 현재 상용 제품 수준으로까지 개발되어, 있어 현재 바로 인터넷뱅킹에 탑재 가능하다.

논문의 구성은 다음과 같다. 2 장에서는 인터넷뱅킹의 클라이언트 측에서 발생 가능한 보안위협들에 대해 살펴보고, 보안강화를 위한 기술 동향 등에 대해 기술한다. 3 장에서는 보안 강화를 위한 현재 기술들의 문제점을 지적한다. 3 장에서는 마우스로 비밀번호를 입력하는 새로운 기술을 제시하고, 제시한 기술의 안전도와 효율성을 분석한다.

2. 관련연구

2.1 인터넷뱅킹 클라이언트측 보안위협

온라인과 오프라인에서 발생 가능한 다양한 보안위협들이 인터넷뱅킹의 안전성을 해치고 있다.

온라인에서 인증서의 사용은 통신망의 안전도를 크게 향상시켰고, 서버에도 실시간 모니터링을 포함한 다양한 시스템의 도입이 그 실효를 거두고 있다. 반면에 클라이언트에서는 다양한 악성 코드들이 활개치고 있는 상황이다.

클라이언트에서 발생한 대표적 악성 코드가 키 스트로크이다. 키 스트로크는 키 보드에서 입력된 정보를

가로채는 것으로 주로 백신을 통해 방어하고 있다.

인터넷뱅킹 입력 창에 있는 정보를 가로채는 악성 코드가 있다. 이 악성 코드는 웹 페이지를 파싱하여, 그 구조를 트리로 나타낸 후, 입력 창에 대응하는 단말 노드에 있는 정보를 가로챈다. 비밀번호가 입력 창에 *로 표시된다 하더라도, * 뒤에 비밀번호가 히든되어 있으면 웹 페이지 파싱을 통해 이를 가로챌 수 있다. 현재는 중요한 정보가 웹 페이지를 거치지 않고 바로 PKI 암호 모듈로 전달되도록 하여 방어하고 있다.

사용자가 입력한 정보는 PKI 암호 모듈에 의해 암호화되어 서버로 전송된다. 이때, PKI 암호 모듈로 위장한 가짜 PKI 암호 모듈이 있다면, 사용자 정보를 PKI 암호 모듈로 전달하는 모듈은 어디로 사용자 정보를 전달해야 할지 모르게 된다. 이는 사용자 정보가 가짜 PKI 암호 모듈로 전달될 가능성이 높다는 것을 의미하며, 현재 시중은행의 인터넷뱅킹에서는 이러한 점을 고려하지 않고 있다.

사용자들은 다소 폐쇄된 공간에서 자신의 컴퓨터로 인터넷뱅킹 서비스를 이용하고 있기 때문에, 오프라인 보안위협은 심각하지 않은 면이 있으나 결코 소홀히 간주되어서는 않된다.

온라인 추측 공격은 비밀번호일 가능성이 높은 것들을 하나씩 반복 입력해 보는 방법이다 [13-15]. 온라인 추측 공격은 비밀번호 공간이 작아지면 강력한 보안위협이 되나, 일반적으로 잘못된 비밀번호 입력 횟수를 제한하면 안전한 것으로 간주하고 있다. 인터넷뱅킹에서는 잘못된 통장비밀번호를 세 번 입력하면 이를 재설정하도록 하도록 하고 있다. 또한 보안카드번호는 통신로 상에 적재되는 정보가 항상 다르게 하는 역할도 하지만, 온라인 추측 공격과 관련하여서는 통장비밀번호의 키 공간을 늘려주는 역할도 하고 있다.

오프라인에서 가장 손쉬우면서도 강력한 보안위협은 사용자가 비밀번호를 입력하는 걸 지켜보아 이를 알아내는 훔쳐보기이다. 훔쳐보기를 이용하면 다른 사람의 비밀번호를 쉽게 알 수 있고, 일단 비밀번호를 알게 되면 카드나 통장을 획득하는 후속 행위들로 이어질 수 있다. 이러한 이유로 인터넷뱅킹 사용자들은 주변에 누군가 있으면 사용을 중지하거나 빠르게 타이핑을 하는 방법으로 훔쳐보기를 방어하고 있다.

2.2 인터넷뱅킹 백신

2005년 6월에 키 스트로크를 이용해 계좌이체를 한 사건은 시중은행들이 백신의 기능을 강화하는 노력으로 이어졌다. 이러한 노력은 두 가지로 요약할 수 있다. 하나는 백신이 사용자 정보를 키 스트로크보다 먼저 가져오는 것이고, 다른 하나는 가져온 정보를 입력 창이나 PKI 암호 모듈로 전달하는 과정에서 악성 코드가 이를 가로채지 못하게 하는 일이다. 이를 위해 현재의 백신은 키보드 버퍼 단에 최대로 근접하여 사용자 정보를 가져오는 한편, 사용자 정보가 입력 창이나 PKI 암호 모듈로 전달되는 과정에서 이를 가로채려는 악성 코드가 있으면 사용자 정보가 아닌 다른 정보를 악성 코드에 전달하는 방식으로 동작하고 있다.

키보드를 통해 입력된 정보를 백신이 가지고 있기 때문에, 백신은 가져온 정보에 대한 제어권을 가지고 있다. 이러한 이유로 현재의 백신은 키 스트로크 방어 기능뿐 아니라 사용자가 입력한 정보를 웹 페이지를 거치지 않고 바로 PKI 암호 모듈로 전송하는 기능도 갖추고 있다. 즉, 현재의 백신은 키보드를 통해 입력된 정보를 키 스트로크가 가로채기 전에 먼저 가져와서, 중요정보를 웹 페이지에 전달하지 않고 바로 PKI 암호 모듈로 전달하고 있다.

2.3 마우스를 이용한 비밀번호 입력 기술

백신이 아무리 강화되어도 모든 키 스트로크를 방어할 수 없기 때문에, 시스템적이 아닌 기술로서 키 스트로크를 방어하고자 하는 노력도 전개되고 있다. 그리고 이러한 노력 중 하나가 마우스로 비밀번호를 입력하는 것이다.

마우스로 비밀번호를 입력하는 기술은 상용 및 연구 목적으로 오래 전부터 많은 연구가 진행되어 오고 있다 [6, 7]. 한편, 인터넷뱅킹에서는 마우스로 비밀번호를 입력하도록 하면 기본적으로 키 스트로크에 안전하기 때문에 이를 도입하는 은행들이 늘어나고 있다. 예를 들어, 그림 1은 현재 한 시중은행 인터넷뱅킹에서 사용 중인 마우스로 보안카드번호를 입력하는 기술의 인터페이스이다. 인터페이스에는 일정한 규칙으로 숫자들이 나타나고, 사용자는 이러한 인터페이스에서 마우스로 숫자를 눌러 보안카드번호를 입력한다. 인터페이스에 나타나는 숫자들의 배열이 인터넷뱅킹을 접속할 때 마다 다르다는 것이 하나의 특징이다.

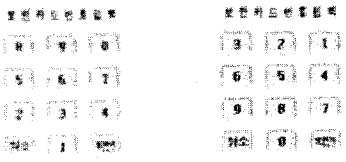


그림 1: 현재 한 시중은행 인터넷뱅킹에 탑재된 마우스를 이용한 보안카드번호 입력 기술의 인터페이스 예

2.4 OTP

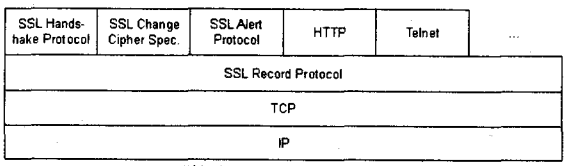
금융감독원에서는 인터넷뱅킹의 클라이언트측 안전성을 확보하는 가장 확실한 방법의 하나로 OTP(One Time Password; 일회용 패스워드)를 주시하고 있다 [22]. 그리고 이를 실현하기 위해 은행 및 증권사를 회원으로 하는 OTP 센터 설립을 추진하고 있다. 즉, 기업에 대해서는 이미 일반화되어 있는 OTP 를 개인으로 확대하고자 하는 것이다.

OTP를 사용하기 위해서는 클라이언트와 서버의 OTP 동기화가 필요하다. 현재 기업용 OTP는 시간을 이용해 동기화가 이루어지고 있는데, 개인용도 동일한 방법이 사용될 것으로 보인다.

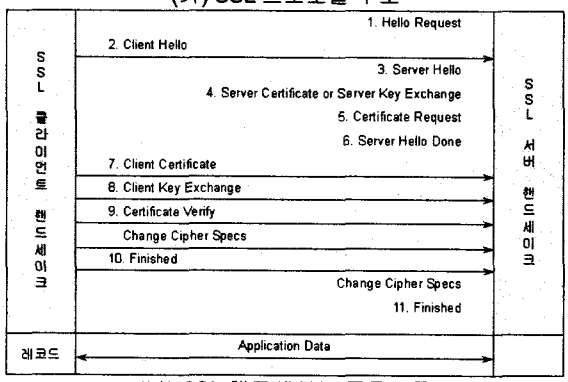
OTP 센터가 설립되면 인터넷뱅킹 사용자는 계좌이체를 하기 위해 OTP를 입력해야 한다. OTP를 입력하기 위해서는 OTP 생성기를 구입해야 하는데, 이에 따른 사용자 부담을 줄이기 위해 보조금을 주는 방안이 검토되고 있다. 한편, OTP 사용 저변 확대를 위해 OTP 사용자와 그렇지 않은 사용자 사이에 계좌이체 금액을 다르게 하는 등의 서비스 차별화가 고려되고 있다.

2.5 SSL 프로토콜 및 PKI

인터넷뱅킹에서 사용자가 로그인을 하면, SSL 프로토콜이 동작한다 [1, 2]. 그리고 그 결과로서 서버와 클라이언트는 관용 키 알고리즘의 키를 공유하게 된다 (그림 2 (나) 참조).



(가) SSL 프로토콜 구조



(나) SSL 핸드세이크 프로토콜

그림 2: SSL 프로토콜

실제 계좌이체 서비스는 PKI 하에서 이루어진다 (그림 3 참조).

클라이언트는 사용자가 정보를 입력하면, 입력된 정보의 해쉬 값을 구하고, 공개 키 암호 시스템의 개인 키로 해쉬 값을 암호화하여 전자서명을 한 후, 사용자가 입력한 정보와 전자서명 값을 접합하여 관용 키 암호 알고리즘으로 암호화한 후, 그 결과를 서버로 전송한다.

서버는 수신한 정보를 관용 키 암호 알고리즘으로 복호화하여 사용자가 입력한 정보와 전자서명 값을 구한 후, 전자서명 값을 공개 키 암호 시스템의 공개 키로 복호화한 결과와 사용자가 입력한 정보의 해쉬 값이 일치하는가를 비교하고, 일치하는 경우에 비밀번호 등을 확인하여 확인하고자 하는 정보들이 서버에 저장되어 있는 정보들과 일치하면 계좌이체를 한다.

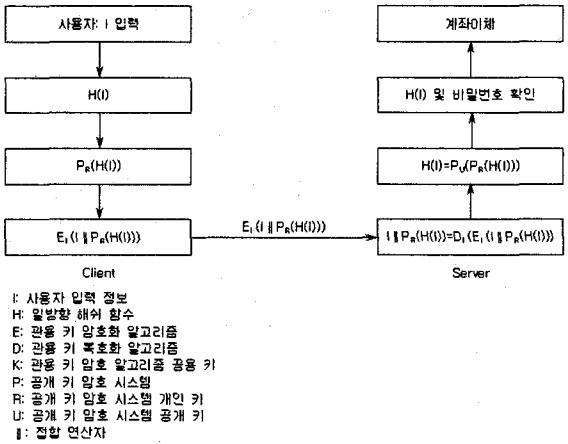


그림 3: PKI 하에서 동작하는 인터넷뱅킹 계좌이체 서비스

3. 문제점

3.1 백신 기능의 강화

백신은 키 스트로크를 막기 위해 도입되었으나, 현재는 키 스트로크 뿐 아니라 웹 페이지 입력 창에 있는 내용의 가로채기를 방어하는 기능도 갖추고 있다. 현재의 추세라면, 백신은 인터넷뱅킹 클라이언트 측에서 발생 가능한 모든 악성 코드를 방어하는 수준으로까지 그 기능이 강화될 정도이다.

한편, 백신의 기능 강화에 대한 우려의 목소리도 커지고 있다. 그리고 이러한 우려는 백신은 기술적인 해결책이 아니라 시스템적인 해결책이기 때문에, 그 기능이 아무리 강화되어도 키 스트로크 하나도 제대로 방어하지 못한다는 점에 기초하고 있다.

백신의 기능이 강화되면서 시중은행들은 만만찮은 비용을 감내하고 있다. 코드 사이즈가 큰 백신에 새로운 기능을 추가하다 보니 단일 모듈 개발보다는 많은 비용이 발생하고 있는 것이다. 또한, 백신의 기능 강화는 사용자의 불편을 가중시키고 있다. 백신의 모듈 크기가 커지면서 이를 다운로딩하는데 소요되는 시간이 갈수록 길어지고 있는 것이다.

3.2 마우스를 이용한 비밀번호 입력 기술

마우스로 비밀번호를 입력하게 하면 키 스트로크로부터 안전하다는 장점이 있다. 그러나 마우스로 비밀번호를 입력하는 기술을 도입하고자 하는 경우에는, 키 스트로크 뿐 아니라 2.1 절에서 기술한 다양한 보안위협들을 고려하여야 한다. 즉, 마우스를 이용해 입력된 비밀번호가 웹 페이

지를 거치지 않도록 구현되어야 하며, 사용자 정보가 가짜 PKI 암호 모듈로 전달되지 않도록 구현되어야 한다.

새로운 기술을 도입하고자 하는 경우에는, 기존의 방법이 방어하고자 하였던 보안위협에 대한 내구성이 보다 높아야 하는 한편, 새로운 기술의 도입으로 인해 보안강도가 취약해진 보안위협은 없는지를 살펴보아야 한다. 마우스로 비밀번호를 입력하면 키보드를 이용하는 것 보다 취약해지는 보안위협이 있다. 즉, 마우스로 비밀번호를 이용하면 거리가 있는 곳에서도 훔쳐보기로 비밀번호를 알 수 있다. 따라서 마우스로 비밀번호를 입력하도록 하는 기술을 탑재하려고 하는 경우에는 훔쳐보기에 대한 안전도 분석이 있어야 한다.

세계적으로 개인, 회사, 연구소 등이 상용 및 연구 목적으로 훔쳐보기로부터 안전한 비밀번호 입력 기술을 개발하고자 하는 노력을 오래 전부터 진행해 오고 있다 [9-12, 16]. 예를 들어, 그림 4는 미국의 리얼유저사가 현재 상용화하고 있는 기술의 인터페이스를 나타내고 있다. 리얼유저사 기술의 경우, 인터페이스에 숫자 대신 사람의 얼굴이 무작위 추출된 순서로 나타나는 것을 특징으로 하고 있다. 이는 숫자를 외우는 것 보다는 사람의 얼굴을 기억하기 어렵다는 점에 착안한 것으로, 미국에서 이 기술을 탑재한 곳이 점차 많아지고 있다.

그림 4: 마우스로 비밀번호를 입력하는 기술의 인터페이스 예

한편, 훔쳐보기에 대한 안전도의 이론적 토대는 인지 심리학 분야에서 많은 연구가 진행되어 오고 있다 [17-21]. 가장 대표적 이론으로는, 사람이 순간적으로 무작위로 나타난 숫자를 기억할 수 있는 개수의 범위가 7±2개라는 것이다 [18]. 최근에는 7±2개가 아닌 3개라는 이론이 발표되어 인지 심리학 분야의 큰 이슈가 되었다 [20].

결과적으로 마우스로 비밀번호를 입력하는 기술을 탑재하는 경우에, 탑재하고자 하는 기술의 안전성은 백신보다 나아야 하며, 오프라인에서는 훔쳐보기로부터 안전하여야 하고, 구현의 용이성을 포함한 효율성 평가척도에 대해서도 만족스러워야 한다.

4. I-DAS

4.1 필요성

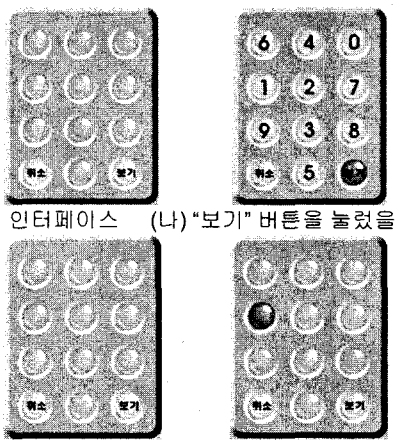
인터넷뱅킹의 클라이언트 측에서 마우스로 비밀번호를 입력하도록 하는 기술은 키 스트로크에 대한 궁극적인 해결책이 될 수 있다.

한편, 마우스로 비밀번호를 입력하도록 하는 기술을 사용하고자 하는 경우에는, 웹 페이지 입력 창에 있는 내용을 가로채거나 PKI 암호 모듈로 위장한 모듈이 사용자 정보를 가로채지 못하도록 구현되어야 한다. 또한 마우스 사용으로 인해 취약해질 수 있는 훔쳐보기로부터 안전한 기술이 탑재되어야 한다.

4.2 I-DAS를 이용한 비밀번호 입력 방법

인터넷뱅킹에서 마우스로 비밀번호를 입력하는 기술인 DAS를 예로서 설명하고자 한다. 설명의 용이를 위해 DAS 버전 1에 대해 기술하고, 버전 1의 비밀번호 입력 시간을 대폭 단축시킨 버전 2에 대해 기술하고자 한다.

먼저, DAS 버전 1에 대해 기술하고자 한다. 비밀번호가 1234라 하자. 사용자는 인터페이스에 있는 "보기" 버튼을 누른다(그림 5 (가) 참조). 그러면 "보기" 버튼을 제외한 버튼들에 0부터 9까지의 숫자가 무작위 추출된 순서로 나타난다 (그림 5 (나) 참조). 사용자는 비밀번호 1234의 첫 번째 숫자인 1이 나타난 버튼을 확인하다. 그리고 나서 "보기" 버튼 누름을 해지한다. 그러면 숫자들이 인터페이스에서 사라진다(그림 5 (다) 참조). 사용자는 숫자들이 사라진 상태에서 확인한 버튼(1이 나타났던 버튼)을 누른다 (그림 5 (라) 참조). 그러면 1이 입력된다. 비밀번호의 나머지 숫자인 234를 입력하는 방법은 1을 입력하는 방법과 동일하다.



(가) 초기 인터페이스 (나) "보기" 버튼을 눌렀을 때의 예

(다) "보기" 버튼 누름 해지 (라) 1의 입력

그림 5: DAS 버전 1에서의 비밀번호 입력 방법을 설명하기 위한 인터페이스 예

이제, DAS 버전 2에 대해 기술하고자 한다. DAS 버전 1 에서는 "보기" 버튼을 누르고, 입력하고자 하는 숫자가 나타난 버튼을 확인하고, 인터페이스에서 숫자가 사라진 상태에서 확인한 버튼을 누르는 과정을 반복하였다. 즉, 입력하고자 하는 숫자와 무관하게 비밀번호 길이만큼 "보기" 버튼을 눌러야 하였다. DAS 버전 2 에서는 "보기" 버튼을

누르고, 입력하고자 하는 숫자가 나타난 버튼을 확인한 후, 확인한 버튼을 누르면 현재 누르고 있는 버튼을 제외한 버튼들에 숫자들이 무작위 추출된 순서로 나타난다. 즉, DAS 버전 2는 입력하고자 하는 숫자가 나타난 버튼을 확인한 후, 확인한 버튼을 누르면 이 버튼(현재 누르고 있는 버튼)이 "보기" 버튼 역할을 한다. 따라서 DAS 버전 2를 이용하면 DAS 버전 1을 이용하는 경우와 비교하여 비밀번호 입력 시간을 대폭 단축시킬 수 있다.

4.3 구현

DAS 버전 2는 실제 인터넷뱅킹에 바로 탑재 가능하도록 구현되었으며(그림 6 참조), I-DAS는 인터넷뱅킹용 DAS 버전 2를 의미한다.

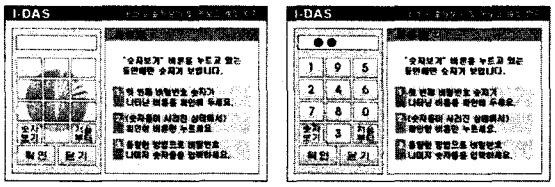


그림 6: I-DAS(인터넷뱅킹용 DAS 버전 2) 인터페이스 예

I-DAS를 인터넷뱅킹에 구비시키는 방법에는 두 가지가 있다. 첫 번째는 비밀번호 입력 창 옆에 별도의 버튼을 두고, 사용자가 이 버튼을 누르면 I-DAS가 구동되도록 하는 방법이다. 다른 하나는 비밀번호 입력 창에 마우스 커서가 위치하면 I-DAS가 자동으로 구동되도록 하는 방법이다. 두 방법 모두에서 I-DAS 인터페이스는 팝업 형태로 나타난다. 본 논문의 I-DAS는 비밀번호 입력 창 옆에 별도의 버튼을 구비하는 방식이 채택되었다.

I-DAS는 웹 페이지 입력 창에 있는 내용을 가로채지 못하도록, I-DAS를 통해 입력된 정보가 웹 페이지를 거치지 않고 바로 PKI 암호 모듈로 전달되도록 하였다. 즉, I-DAS로 비밀번호를 입력하면, 비밀번호가 입력 창으로 전달되지 않으며, 따라서 * 뒤에도 비밀번호가 히든되지 않는다.

I-DAS로 입력된 값이 PKI 암호 모듈을 위장한 가짜 PKI 암호 모듈로 전달되는 것을 방지하기 위하여, I-DAS는 I-DAS와 메모리를 공유하는 PKI 암호 모듈에만 입력된 값이 전달되도록 구현되었다.

인터넷뱅킹에서 I-DAS가 구동되도록 하기 위해서는 기존 인터넷뱅킹 모듈에 하나의 컴포넌트로 임베딩되어야 한다. 이를 위해 I-DAS에는 다음의 서브 모듈들이 포함되어 있다.

- PKI 인증서 연동 모듈
- 엑티브 X 페이지 제어 모듈
- 자동 업그레이드 모듈
- 웹 페이지 연동 모듈

4.4 I-DAS의 안전도

키 스트로크는 키보드에서 입력된 정보를 가로채는 악성 코드이다. I-DAS는 마우스로 비밀정보를 입력하기 때문에 기본적으로 키 스트로크로부터 안전하다.

웹 페이지의 입력창에 있는 내용을 가로채는 악성 코드가 있다. I-DAS를 통해 입력된 비밀번호는 웹 페이지 입력 창으로 전달되지 않고, 바로 PKI 암호 모듈로 전달된다. 따라서 I-DAS는 웹 페이지의 입력 창에 있는 내용을 가로채는 악성 코드로부터 안전하다.

클라이언트에 진짜 PKI 암호 모듈과 가짜 PKI 암호 모듈이 있다면 사용자 정보가 가짜 PKI 암호 모듈로 전달될 가능성이 높다. I-DAS는 사용자가 입력한 정보를 받아 그 정보를 I-DAS와 메모리를 공유하고 있는 PKI 암호 모듈에만 전달한다. 따라서 I-DAS는 PKI 암호 모듈로 위장한 모듈에 사용자 정보가 전달되지 않는다.

I-DAS를 이용하여 비밀번호를 입력하면 비밀번호를 입력하는 사용자는 누르고자 하는 버튼을 시각적으로 확인하지만, 비밀번호를 알려고 하는 사람은 (숫자들이 사라진 상태에서 비밀번호가 입력되므로) 무작위 추출된 순서로 나타난 수들을 순서대로 모두 기억하고 있어야 비밀번호를 알 수 있다. 따라서 I-DAS는 훔쳐보기로부터 안전하다.

I-DAS가 훔쳐보기로부터 안전하다는 이론적 근거는 [17-20]에 기초하고 있다. 한편 100명을 대상으로 한 모의실험 결과, I-DAS로 입력된 비밀번호가 훔쳐보기에 의해 노출될 확률은 평균 1.3%였다. 이는 실험에 참가한 사람들이 I-DAS 인터페이스를 주시하도록 한 상태에서 실험한 것으로, 일상적 환경에서 I-DAS로 입력된 비밀번호가 훔쳐보기에 의해 노출될 가능성은 0%에 가깝다는 것을 의미한다.

표 1: 훔쳐보기에 의한 비밀번호 노출율(평균±표준분산, 최소, 최대)

Traditional Password	I-DAS
92.4±1.8, 89, 96	1.3±2.5, 0, 10

4.5 I-DAS의 효율성

비밀번호를 입력하는 기술의 효율성을 평가하는 다양한 척도가 있다. 이들 중 비밀번호 기억 용이성, 비밀번호 입력시간, 기술의 단순성 등이 I-DAS와 관련이 있다.

비밀번호 기억 용이성: 비밀번호로 어떤 정보를 입력하는가에 의해 평가된다. 그림 4에 있는 리얼유저사 기술의 경우에는 사람의 얼굴을 기억하여야 했다. I-DAS는 숫자로 이루어진 비밀번호를 입력하기 때문에 기억의 용이성이 좋다.

비밀번호 입력시간: I-DAS 의 경우, 안전성이 담보되는

대신 비밀번호 입력시간이 길어지는 단점이 있다. 100명을 대상으로 모의실험한 결과, I-DAS를 숙지하기 전에 I-DAS로 비밀번호를 입력하는 시간은 키보드로 입력하는 시간보다 약 2.5배 가량 소요되었으며, I-DAS를 숙지한 후에는 약 1.5배 가량 소요되었다. 한편, 키보드로 비밀번호를 입력하는 시간은 비밀번호에 익숙해지는 정도에 따라 입력시간에 큰 차이가 없는 반면, I-DAS는 사용하면 할수록 비밀번호 입력시간이 큰 폭으로 감소하였다.

I-DAS로 비밀번호를 입력할 때, 비밀번호를 잘못 입력할 확률이 기술을 인지하지 않은 상태에서는 약 22%였으며, 기술을 인지한 후에는 약 10%였다. 또한 키보드로 비밀번호를 잘못 입력할 확률은 익숙해지는 정도에 따라 큰 차이가 없는 반면, I-DAS는 사용하면 할수록 잘못 입력할 확률이 큰 폭으로 감소하였다.

한편, 기술을 인지하지 않은 상태에서는 기술이 흥미로우나 어렵다는 의견이 대부분이었고, 기술을 인지한 후에는 높은 신뢰성을 보인 것으로 나타났다.

표 2: 비밀번호 입력 모의실험(평균±표준분산, 최소, 최대)

Password usability items		Traditional Password	I-DAS
Input times (Seconds)	After Brief learning	2.4±0.4, 1.7, 3.2	5.9±1.7, 3.7, 10.3
	After Hard learning	1.6±0.3, 0.9, 2.3	2.9±1.5, 2.0, 4.7
Error rates (%)	After Brief learning	9.4±1.2, 7, 12	21.9±9, 13, 43
	After Hard learning	5.2±1.7, 2, 8	10.1±3.6, 8, 16
User response	After Brief learning	Cumbersome	Interesting
	After Hard learning	Cumbersome	Relieved

I-DAS는 마우스로 비밀번호를 입력하는 타 기술에 비해 기술이 단순하고, 구현이 용이하다. 또한, I-DAS는 안전도와 효율성을 절묘하게 조화시킨 기술로, 향후 범용 비밀번호 입력 기술로의 자리매김이 예견된다.

5. 결론

2005년 6월 한 시중은행에서 키 스트로크를 이용해 계좌이체를 한 사건이 발생한 이후, 은행들은 인터넷뱅킹의 클라이언트측 보안강화를 위해 전력을 다하고 있다. 이러한 노력은 두 가지 방향으로 이루어지고 있는데, 하나는 이미 사용되고 있던 백신의 기능을 강화하는 것이고, 다른 하나는 OTP를 사용하도록 한다거나 마우스로 비밀번호를 입력하도록 하는 것이다.

본 논문에서는 마우스로 비밀번호를 입력하는 새로운 기술을 제안하였다. 제안한 기술은 현재 인터넷뱅킹에 바로 탑재 가능하도록 구현되어 있는 상태이다.

제안한 기술은 웹 페이지의 입력 창에 있는 내용을 가로채거나 가짜 PKI 암호 모듈로 위장한 모듈이 사용자 정보를 가로채지 못하도록 구현되었다. 또한 제안한 기술은 마우스를 이용하기 때문에 기본적으로 키 스트로크로부터 안전하며, 오프라인의 최대 보안위협인 훔쳐보기로부터 안전하다는 특징이 있다.

제안한 기술은 효율성 측면에서도 우수한 것으로 나타났다. 특히 안전도와 효율성을 절묘하게 조화시켜 그 기술의 우수성과 완성도가 매우 높아, 향후 범용 비밀번호 입력 기술로의 자리매김이 예견된다.

참고문헌

[1] SSL 3.0 Implementation Assistance, http://home.netscape.com/eng/ssl3/traces/index.html.

[2] SSL and Certificates using SSLeay, http://www.camb.opengroup.org/RI/www/prism/wwwj.

[3] X.509 Public Key Infrastructure Certificate Management Protocols, IETF. ftp://ftp.isi.deu/in-notes/rfc2510.txt.

[4] X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP, IETF. ftp://ftp.isi.deu/in-notes/frc2585.txt.

[5] X.509 Public Key Infrastructure Certificate Policy and Certificate Practice Statement Framework, IETF. ftp://ftp.isi.deu/in-notes/rfc 2527.txt.

[6] Microsoft, Microsoft Password System, http://www.domainmart.com/news/NYT_symbols-as-passwods.htm, Accessed on 30 May 2005.

[7] Realuser, Visual password system, Available at http://www. Realuser.com/cgi-bin/ru.exe/_/homepages/index.htm, Accessed on May 2005.

[8] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Applied Crypto graphy, CRC, 1997.

[9] B. Hoanca, K. Mock, "Screen oriented technique for reducing the incidence of shoulder surfing", International conference on security and management (SAM05), pp. 334-340, 2005.

[10] M. Brader, "Shoulder surfing automated", Risks Digest, April 1998.

[11] S. Lee, S. Park, "Improving Accessibility and Security for Mobile Phone Shopping", Journal of Computer Information Systems, 54, 3, pp. 124-133, Mar 2006.

[12] V. Roth, K. Richter, R. Freidinger, "A PIN-entry method resilient against shoulder surfing", Proceedings of the 11th ACM conference on Computer and communications security, Washington, DC, USA, pp. 236 – 245, October, 2004.

[13] Jablon, "Strong password-only authenticated key exchange", ACM Computer Communication Review, ACM SIGCOMM, Vol. 26, No. 5. pp. 5-20, 1996.

[14] M. Bellare, D. Pointcheaval, P. Rogaway, "Authenticated key exchange secure against dictionary attacks", Advances in Cryptology Eurocrypt'00(LNCS, 1807), pp. 139-155, 2000.

[15] V. Boyko, D.P. MacKenzie, S. Patel, "Provably secure password authenticated key exchange using Diffie-Hellman". Advances in Cryptology Eurocrypt'00(LNCS, 1807), pp. 156-171, 2000..

[16] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," Proceedings of the 2nd USENIX UNIX Security Workshop, pp. 5-14, 1990.

[17] S.J. Luck, E.K. Vogel, "The capacity of visual working memory for features and conjunctions", Nature 390, pp. 279-281, 1997.

[18] W.S. Jevons, "The power of numerical discrimination, Nature 3, pp. 281-282, 1871.

[19] G.A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information", Psychol. Rev. 63, pp. 81-97, 1956.

[20] N. Cowan, "The magical number 4 in short-term memory: A reconsideration of mental storage capacity", Behav. Brain Sci. 24, pp. 87-185, 2001.

[21] E.K. Vogel, M.G. Machizawa, "Neural activity predicts individual differences in visual working memory capacity". Nature 428, pp. 748–751, 2004.

[22] 한국은행 보도자료, "2005년 9월말 현재 국내 인터넷뱅킹 서비스 이용현황", 공보 2005-10-32 호, 2005. 10

[23] 금융감독원, "전자금융거래 보안강화 종합대책마련을 위한 은행부문 보안실무자 2차 회의자료", 2005.