DOI: 10.3745/KIPSTC.2011.18C.2.071

현금자동입출금기/현금지급기에서 개선된 비밀번호 입력 방법

김 태 희[†] · 박 승 배[††] · 강 문 설[†††]

요 약

현금자동입출금기/현금지급기에서 비밀번호를 입력할 때 신용카드나 통장의 비밀번호가 노출되어 자신도 모르게 현금이 인출되는 금융사고가 빈번하게 발생하고 있으므로 비밀번호를 입력하는 과정에서 각별한 주의가 요청되고 있다.

본 논문은 현금자동입출금기/현금지급기를 사용할 때 어깨너머로 비밀번호를 훔쳐보는 것을 방지하기 위하여 비밀번호를 안전하게 입력하는 방법을 제안하였다. 제안한 방법은 사용자가 비밀번호를 입력하는 과정을 옆이나 뒤에서 훔쳐봐도 무엇을 입력하였는지를 알 수 없도록 숫자들이 무작위 순으로 표시되었다가 사라진 상태에서 비밀번호를 입력함으로써 비밀번호 훔쳐보기를 원천적으로 차단하여 비밀번호가 유출되는 것을 방지할 수 있다. 비밀번호를 안전하게 입력하는 방법은 훔쳐보기 시험, 직관적인 관점 및 이론적인 분석으로 구분하여 안전성을 검증하였다. 또한, 현금자동입출금기/현금지급기에서 적용할 수 있도록 구현한 결과는 비밀번호 훔쳐보기 공격으로부터 비밀번호 획득 확률이 기존 방법보다 현저하게 낮은 것으로 평가되어 비밀번호가 유출되는 것을 방지할 수 있다.

키워드 : 비밀번호 훔쳐보기, 비밀번호 유출, 현금자동입출금기, 현금지급기, 금융사고

Advanced Password Input Method in Automated Teller Machines /Cash Dispenser

Kim, Tae-Hee[†] · Park, Seung-Bae[††] · Kang, Moon-Seol[†††]

ABSTRACT

Financial accidents such as password exposure of credit cards or bankbooks occur often when a password is inputted to ATM/CD(Automated Teller Machines and Cash Dispenser), so particular attention is required when inputting a password.

This study suggested a method to input a password safely to prevent stealing a glance at a password in case of the use of ATM/CD. The method is that users input a password when numbers are randomly displayed and disappear not to notice the password even though someone is next to or behind the users. As methods to input a password safely, the study verified safety by dividing the methods into a test of shoulder surfing, an intuitive perspective, and a theoretical analysis. In addition, the result of implementation to apply the method to ATM/CD shows that a percentage of acquiring a password from the attack of shoulder surfing is found to be lower than an existing method, so password exposure can be prevented.

Keywords : Shoulder Surfing, Password Exposure, ATM(Automated Teller Machines), CD(Cash Dispenser), Financial Accidents, DAS(Dynamic Authentication system)

1. 서 론

비밀번호를 포함한 개인정보를 옆이나 뒤에서 훔쳐보는 고전적인 훔쳐보기 방법부터 개인용 컴퓨터를 이용하여 금융기관 등으로부터 개인정보를 알아내어 불법적으로 이용하는 사기 수법인 피싱(Phishing) 공격 등 개인정보를 탈취하려고 하는 기술은 날로 진화하고 있지만, 이에 대한 대응이 미흡하여 사용자들의 불안감이 여전하게 높은 실정이다.

현금자동입출금기 또는 현금지급기(ATM/CD : Automated Teller Machines or Cash Dispenser)에서 현금을 인출할 때 신용카드나 통장의 계좌번호와 비밀번호가 불법으로 노출되어 자신도 모르게 현금이 인출되는 금융사고가 빈번하게 발

※ 이 연구는 2010년도 광주대학교 대학 연구비의 지원을 받아 수행되었음.
† 종신회원 : 동신대학교 디지털콘텐츠학과 부교수
†† 종신회원 : (주)신비테크 대표이사
††† 종신회원 : 광주대학교 컴퓨터공학과 교수(교신저자)
논문접수 : 2010년 10월 6일
수 정 일 : 1차 2010년 12월 15일, 2차 2011년 1월 6일
심사완료 : 2011년 1월 10일

생하고 있어 현금을 인출하는 과정에서 각별한 주의가 요구되고 있다. 범죄자들이 교묘하게 현금자동입출금기에 위장 키보드를 설치하거나 현금자동입출금기를 비추는 소형 카메라를 설치하여 현금을 인출하는 사람이 비밀번호를 입력할 때 비밀번호를 자동으로 촬영하고, 훔친 비밀번호를 이용하여 현금을 불법으로 인출해 간다.

따라서 ATM/CD에서 비밀번호를 입력할 때 절대로 옆이나 뒤에 서있는 타인이 자신의 비밀번호를 훔쳐볼 수 없도록 해야 하며, 현금자동입출금기에 의심스러운 점이 발견되면 절대로 이를 이용하지 말고 경찰이나 은행에 신고하고, 정기적으로 자신의 은행 계좌의 금액 잔고를 점검하여 이상하게 현금이 빠져나간 것이 없는가를 확인하도록 권고하고 있다.

한편, 사용자 인증은 서비스 요구자나 시스템 사용자가 인가된 사용자 인지 아닌지를 확인하는 보안 서비스를 말한다. 그리고 사용자 인증에 따른 조치를 취하는 솔루션을 인증 시스템이라 한다. 인증 시스템이 사용자 인증을 위해 이용하는 정보에는 세 가지 유형이 있다. 첫 번째는 생체 정보이고, 두 번째는 매체에 저장되어 있는 정보이며, 마지막은 사용자가 기억하고 있는 정보이다[1]. 매체 저장 정보를 이용한 사용자 인증은 매체 소유자를 인증하지 않는 경우와 매체 소유자를 추가로 인증하는 경우로 나누어진다.

매체 저장 정보를 이용하는 사용자 인증 과정에서 비밀번호로 매체 소유자를 추가적으로 인증하는 비밀번호 입력기가 개발되어 사용되고 있다[2]. 또한, 카드결제 시스템에서 비밀번호로 카드 소유자를 인증하는 기술이 개발되어 사용되고 있다. 카드 소유자 인증은 주로 사인(Signature)에 의해 이루어지다가 2000년대 들어 비밀번호 인증을 적용하는 국가가 생겨나게 되었다. 영국과 같이 카드결제시스템에서 비밀번호 인증 효과가 입증되면서 이를 도입한 국가가 날로 늘어나고 있다[3].

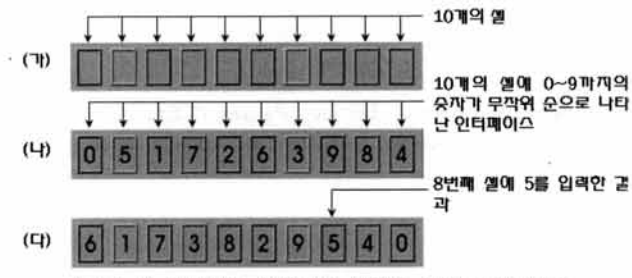
본 논문은 인지심리학에 기초한 비밀번호 훔쳐보기 공격으로부터 안전한 기술을 적용하여 ATM/CD에서 비밀번호를 안전하게 입력하는 방법(DAS : Dynamic Authentication System)을 제안하였다. 제안한 방법은 비밀번호를 입력하는 과정을 옆이나 뒤에서 봐도 무엇을 입력하였는지를 알 수 없도록 숫자들이 무작위 순으로 표시되었다가 사라진 상태에서 비밀번호를 입력할 수 있도록 구성하여 비밀번호를 누르는 과정을 옆이나 뒤에서 훔쳐봐도 알 수 없도록 하였다. 이를 입증하기 위하여 제안한 방법이 비밀번호 훔쳐보기 공격으로부터 안전함을 훔쳐보기 시험, 직관적인 관점 및 이론적인 분석으로 구분하여 검증하였으며, 훔쳐보기 공격자의 비밀번호 획득 확률이 기존 방법보다 현저하게 낮은 것으로 검증 및 평가되어 현금자동입출금기에 도입하여 활용되고 있다. 특히, 비밀번호 훔쳐보기 공격자로부터 비밀번호를 안전하게 입력하는 방법은 금융보안연구원(FSA : Financial Security Agency)으로부터 금융기관에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 평가[17]를 받아 국내 ○○은행의 현금자동입출금기/현금지급기와 인터넷 뱅킹 등에 적용되어 사용되고 있다.

논문의 구성은 다음과 같다. 2장에서는 비밀번호 입력 및 비밀번호 훔쳐보기 방지를 목적으로 진행된 관련 연구들을 살펴보고, 3장에서는 비밀번호를 안전하게 입력하는 방법을 제시하고, 비밀번호 훔쳐보기 공격으로부터 안전성을 분석한다. 4장은 현금자동입출금기에서 비밀번호를 안전하게 입력할 수 있도록 구현하여 적용한 결과 및 안정성 평가 내용을 설명하고, 5장에서 결론 및 향후 연구 방향을 기술한다.

2. 관련 연구

비밀번호 훔쳐보기는 비밀번호를 입력하는 과정을 옆이나 뒤에서 지켜보아 이를 획득하는 행위이다[4, 5]. 훔쳐보기는 비단 현금자동입출금기/현금지급기에서 뿐만 아니라 비밀번호입력기나 디지털 도어락(doorlock) 등 비밀번호를 이용하여 사용자를 인증하는 모든 곳에서 발생하는 보안 위협의 한 유형이다. 이러한 이유로 비밀번호 훔쳐보기로부터 안전한 기술을 개발하기 위한 많은 노력들이 진행되어 왔다.

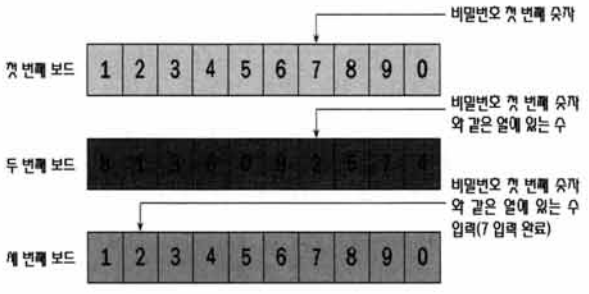
본 논문에서 비밀번호 훔쳐보기 방지를 위한 모든 기술을 열거할 수 없으므로 여기에서는 대표적 기술 몇 가지를 소개한다. 먼저 [6, 7]에서 제안한 기술을 예로서 설명하고자 한다. 비밀번호가 "5619"라 하자. 비밀번호를 입력하기 위한 인터페이스는 (그림 1(가))와 같이 10개의 셀로 이루어져 있고, (그림 1(나))와 같이 10개의 셀에는 0~9까지의 숫자가 무작위 순으로 나타나 있다. 사용자는 마음속으로 하나의 셀을 선택한다. (그림 1(나))에서 사용자가 마음속으로 8번째 셀을 선택했다고 하자. 사용자는 마음속으로 선택한 8번째 셀에 비밀번호 첫 번째 숫자인 "5"가 나타나도록 증감 버튼을 누른 후, (그림 1(다))와 같이 "5"가 나타나면 엔터키를 치면 "5"가 입력된다. 한편 사용자가 증감 버튼을 누르면 인터페이스에 나타난 모든 수가 동시에 증감하고, 증감되는 과정에서 특정 셀에는 특수문자가 나타난다. "5"를 입력한 방법과 동일한 방법으로 비밀번호 나머지 숫자인 "619"를 입력한다.



(그림 1) 비밀번호 입력기술 설명을 위한 인터페이스

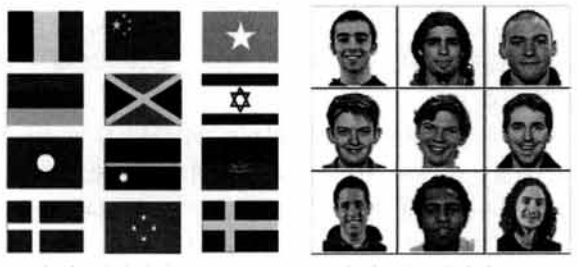
소리나무미디어(주)는 VIS(Virtual Inputting System)[8]를 제안하였다. VIS 인터페이스는 (그림 2)와 같이 세 개의 보드로 구성되어 있다. VIS는 고객이 ATM/CD를 사용할 때 어깨너머로 비밀번호를 훔쳐보는 것을 방지하기 위하여 숫자를 랜덤하게 대응시켜 줌으로써 실제 해당 비밀번호를 누르는 것이 아니라, 그 번호와 임의의 대응되는 번호를 누

름으로써 비밀번호 훔쳐보기를 원천적으로 차단하여 비밀번호가 유출되는 것을 방지할 수 있도록 개발한 시스템이다. 예를 들어, 비밀번호가 "7215"라 하면, 사용자는 숫자들이 순차적으로 나타난 첫 번째 보드에서 "7"의 위치를 확인하고, 숫자가 무작위 순으로 나타난 두 번째 보드에서 "7"과 동일한 열에 있는 숫자("2")를 확인한 후, 숫자들이 순차적으로 나타난 세 번째 보드에서 "2"를 누른다("7" 입력). 사용자가 숫자 "2"를 누름과 동시에 두 번째 보드에는 숫자들이 새롭게 무작위 순으로 나타난다. 사용자는 "7"을 입력한 방법과 동일한 방법으로 비밀번호 나머지 숫자인 "215"를 입력한다.



(그림 2) 소리나무미디어의 비밀번호 입력기술 설명을 위한 인터페이스

숫자보다는 이미지를 기억하기 어렵다는 사실에 기초하여, 이미지를 입력하는 기술들이 제안되기도 하였다. 대표적 기술로는 이미지패스워드시스템[9, 10]과 패스페이시스[11]를 들 수 있다. (그림 3(가))의 이미지패스워드시스템(IPS : Image Password System)은 인터페이스에 나타난 이미지(국기)에서 사용자가 기억하고 있는 이미지를 순차적으로 누른다. (그림 3(나))의 패스페이시스(PassFaces)는 이미지(사람 얼굴)를 입력하다는 점에서 이미지패스워드시스템과 동일하나 기억하고 있는 이미지 하나를 누르면 인터페이스에 새로운 이미지들이 나타난다는 점이 다르다.



(가) 이미지패스워드시스템 (나) 페스페이시스
(그림 3) 이미지패스워드시스템과 패스페이시스의 인터페이스

스탠포드 대학은 현금인출기 등에서 비밀번호를 눈으로 콕콕 찍어서 입력하는 기술을 개발하고 있다[12]. 눈으로 비밀번호를 입력하는 기술은 눈동자를 정확히 추적해야 함은 물론 번호를 누르기 위해 눈을 깜빡이는 것과 그냥 눈을 깜빡이는 것을 구별해야 하는 등 해결해야 할 기술적 난제들이 있다. 따라서 이 기술이 상용화되기 위해서는 비밀번호를 정확하게 입력했음에도 불구하고 틀린 번호를 입력했다고 할 확률(FRR : False Rejection Rate)과 틀린 비밀번호를 입력했음에도 불구하고 맞은 번호를 입력했다고 할 확률(FAR : False Acceptance Rate)이 제로가 되어야 할 정도로 기술적 완성도를 높여 주어야 한다.

비밀번호를 리듬에 맞추어 입력하는 기술이 제안되기도 하였다. (주)비원플러스에서 개발한 리듬패스(RhythmPass)[13]는 비밀번호를 리듬에 맞추어 입력한다. 예를 들어, 비밀번호가 "1234"이고, 리듬이 "대한민국"이면 "1234"를 "1~234"로 입력한다. 리듬패스는 키스트로크를 기반으로 한 생체인증 소프트웨어이다. 생체 인증(Keystroke Dynamics)이란 개인마다 키를 누르거나 타이핑하는 패턴 및 속도가 다르다는 사실을 기반으로 하는 기술을 말합니다. 쉽게 말하자면, 리듬패스는 윈도우에 로그인 할 때 비밀번호뿐만 아니라, 비밀번호를 입력하는 리듬까지 일치해야 로그인이 가능하도록 하는 보안 프로그램입니다. 신한은행의 현금인출기에 시험 적용한 적이 있으며, 현재는 개인용 컴퓨터 보안 제품으로 판매되고 있다. LINUX에서는 256자까지의 비밀번호를 허용하고 있으며[14], 3M사는 모니터를 옆에서 보면 모니터 내용을 알 수 없는 프라이비트 패드(Private Pad)라 불리는 물리적 제품을 개발하여 판매하고 있다.

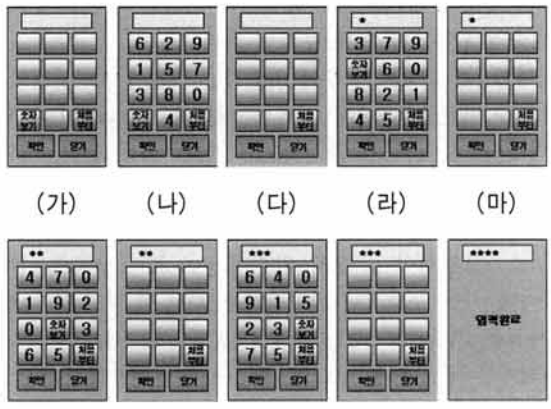
3. 안전한 비밀번호 입력 방법

이 장은 현금자동입출금기 또는 현금지급기(ATM/CD : Automated Teller Machines or Cash Dispenser)를 이용하는 과정에서 비밀번호 훔쳐보기 공격으로부터 비밀번호를 안전하게 입력하는 방법(DAS : Dynamic Authentication system)[2]을 설명하고, 제안한 비밀번호를 안전하게 입력하는 방법이 비밀번호 훔쳐보기 공격으로부터 안전함을 훔쳐보기 시험, 직관적인 관점 및 이론적 분석을 토대로 검증한 결과를 기술한다.

3.1 비밀번호를 안전하게 입력하는 과정

비밀번호를 안전하게 입력하는 과정을 비밀번호가 "1234"인 경우를 예로서 설명한다. (그림 4(가))의 인터페이스에는 숫자들이 나타나 있지 않고, "숫자보기" 버튼이 구비되어 있다. 사용자가 "숫자보기" 버튼을 누르고 있으면 (그림 4(나))와 같이 숫자들이 무작위 추출된 순으로 보이고, "숫자보기" 버튼을 누르지 않으면 (그림 4(다))와 같이 숫자들이 보이지 않게 된다. 사용자는 "숫자보기" 버튼을 누른 상태에서 "1"이 나타난 버튼의 위치를 확인하고, (그림 4(다))와 같이 "숫자보기" 버튼을 누르지 않은 상태(숫자들이 보이지 않은 상태)에서 확인한 버튼을 누르면 (그림 4(라))와 같이 "1"이 입력된다. 그러면 (그림 4(라))와 같이 "1"을 입력하기 위해 누르고 있는 버튼이 "숫자보기"가 되어 숫자들이 현재 누르고 있는 버튼을 제외한 버튼들에 무작위 순으로 나타난다. "2"가 나타난 버튼의 위치를 확인하고, (그림 4(마))와 같이 "숫자보기" 버튼을 누르지 않은 상태에서 확인한 버튼을 누

르면 (그림 4(바))와 같이 "2"가 입력된다. "2"를 입력하는 방법과 동일한 방법으로 나머지 "3"과 "4"를 입력한다[2].



(그림 4) 비밀번호를 안전하게 입력하는 과정

3.2 비밀번호 훔쳐보기에 대한 안전성 검증

(1) 훔쳐보기 시험

제안한 방법을 ATM/CD에 적용하여 비밀번호 훔쳐보기에 대한 안전성 시험을 <표 1>과 같이 2가지 방법으로 실시하였다. 첫 번째 방법은 ○○은행의 본점과 □□대학지점에 설치하여 운영하고 있는 ATM/CD에서 실제 이용자들을 대상으로 민원 발생 여부를 조사하였다. 이 시험은 제안한 방법(안전입력 모드)을 선택 사항이 아닌 기본 상태로 운영하여 진행하였으며, 시험 결과는 한 건의 민원도 발생하지 않은 것으로 확인되었다. 두 번째 방법은 162명의 대학생을 대상으로 비밀번호 훔쳐보기 시험을 실시하였다. 시험은 ① 빔 프로젝터를 이용하여 비밀번호를 안전하게 입력하는 방법을 설명하고 ② 종이에 미리 적어 놓은 비밀번호를 입력한 후 ③ 입력한 숫자에서 몇 개를 맞추었는지 조사하였다. 시험 결과는 비밀번호를 훔쳐보는 것을 포기한 학생이 118명, "모르겠다."라고 응답한 학생이 35명, 두 개 이하의 숫자를 맞춘 학생이 9명으로 나타났다.

〈표 1〉 비밀번호 훔쳐보기의 안전성 시험

시험도구	◦ ○○은행에서 운영하는 ATM/CD
시험환경	
시험목적	◦ 비밀번호 훔쳐보기 공격의 안전도 및 민원 발생 가능성 체크
시험환경	◦ ○○은행의 본점 및 대학지점의 ATM/CD
시험대상	◦ 일반인 및 대학생
시험방법	◦ 안전한 비밀번호 입력 방법의 탑재 사실을 포스터 등으로 알림 ◦ 홍보 이외에 안전한 비밀번호 입력방법이 탑재되지 않은 ATM/CD와 동일한 환경
예 상 시험결과	◦ 비밀번호 훔쳐보기에 성공한 사람이 없음 ◦ 민원 발생 가능성을 예상
실 제 시험결과	◦ 훔쳐보기 시험 : 118명은 포기했고, 35명은 '모르겠다.'라고 했으며, 9명이 2개 이하의 숫자를 맞춤. ◦ 민원이 한 건도 발생하지 않음

(2) 직관적인 관점

비밀번호를 입력하는 사람은 숫자가 무작위 순으로 나타난 상태에서 누르고자 하는 숫자 버튼을 시각적으로 확인한 후, 숫자들이 사라진 상태에서 확인한 버튼을 누른다. 반면 비밀번호 훔쳐보기 공격으로 비밀번호를 알려고 하는 사람은 숫자가 무작위 순으로 나타났다가 사라진 상태에서 번호가 입력되기 때문에 비밀번호를 입력하는 사람이 누르고자 하는 숫자 버튼을 시각적으로 확인하는 찰나에 무작위 추출된 순서로 나타난 숫자들을 순서대로 모두 기억하고 있어야 비밀번호 숫자 하나를 알게 된다.

사용자가 확인한 버튼을 누르는 순간 숫자들이 다시 무작위 추출된 순서로 나타나기 때문에 훔쳐보기 공격으로 비밀번호를 알려고 하는 사람은 이전에 입력된 번호를 알고 있다 하더라도, 이전에 알고 있던 번호와 새롭게 무작위 순으로 나타난 숫자들을 순서대로 기억하는 과정에서 번호들끼리 충돌하는 현상이 발생하게 된다.

(3) 이론적인 분석

인지 심리학에서 사람이 순간적으로 어떤 숫자를 본 후 그 숫자를 반복적으로 되뇌어 기억할 수 있는 숫자의 개수가 1.5 ~ 5라는 이론이 소개되었다. 즉, 무작위순으로 나타난 0부터 9까지의 10개의 숫자를 순간적으로 본 후 그 숫자를 반복적으로 되뇌어 기억할 수 있는 숫자의 개수가 1.5 ~ 5라는 이론이 제시되었고[15], 이 이론은 많은 논문에서 인용되고 있다.

안전한 비밀번호 입력 방법으로 비밀번호를 입력하였을 때, 비밀번호 입력 인터페이스에 무작위 순으로 나타난 10개의 숫자를 보고 임의의 숫자를 기억할 수 있는 확률을 α ($0 \le \alpha \le 1$)라 하면 α는 0.15 ~ 0.5이다[15]. 따라서 다른 모든 환경을 무시하고 안전한 비밀번호 입력 방법으로 비밀번호를 입력하였을 때 비밀번호 훔쳐보기 공격으로 비밀번호를 획득할 수 있는 확률은 [15]에 근거하여 <표 2>와 같이 0.15^4 ~ 0.5^4(0.00050625 ~ 0.0625)가 된다.

〈표 2〉 훔쳐보기 공격에 대한 안전도

α	α^2	α^3	α^4
0.15~0.5	0.0225~0.25	0.003375~0.125	0.00050625~0.0625

안전한 비밀번호 입력 방법으로 비밀번호를 입력하였을 때, 비밀번호 입력 인터페이스에 무작위 순으로 나타난 10개의 숫자를 보고 임의의 숫자를 기억할 수 있는 확률을 α라 하고($0 \le \alpha \le 1$), 입력된 번호를 기억하고 있으면서 무작위 순으로 나타난 숫자를 모두 기억하는 과정에서 일어나는 충돌 현상이 두 번째 이후의 번호를 알아내는데 미치는 정도를 β라 하자($0 \le \beta \le 1$). 그러면 안전한 비밀번호 입력 방법으로 입력된 번호 중 비밀번호 훔쳐보기로 입력된 숫자 i개를 획득할 확률은 $\alpha^i \times \beta^{(i-1)}$이다($1 \le i \le 4$).

4. 안전한 비밀번호 입력 방법의 구현 및 안정성 평가

4.1 ATM/CD에서 비밀번호 입력 모듈의 구동

사용자는 (그림 5(가))와 같이 ATM/CD의 터치스크린에 비밀번호 입력 인터페이스에 있는 "안전입력" 버튼을 클릭하여 안전한 비밀번호 입력 모듈을 구동시킨다. 안전한 비밀번호 입력 모듈이 구동되면 ATM/CD의 터치스크린에는 (그림 5(나))와 같이 "안전입력" 모드로 전환하여 비밀번호를 입력할 수 있는 인터페이스가 제공된다. 즉, 구동 결과는 ATM/CD의 터치스크린에 사용자와 안전한 비밀번호 입력 모듈이 상호작용하면서 비밀번호를 안전하게 입력할 수 있도록 인터페이스가 제공된다.

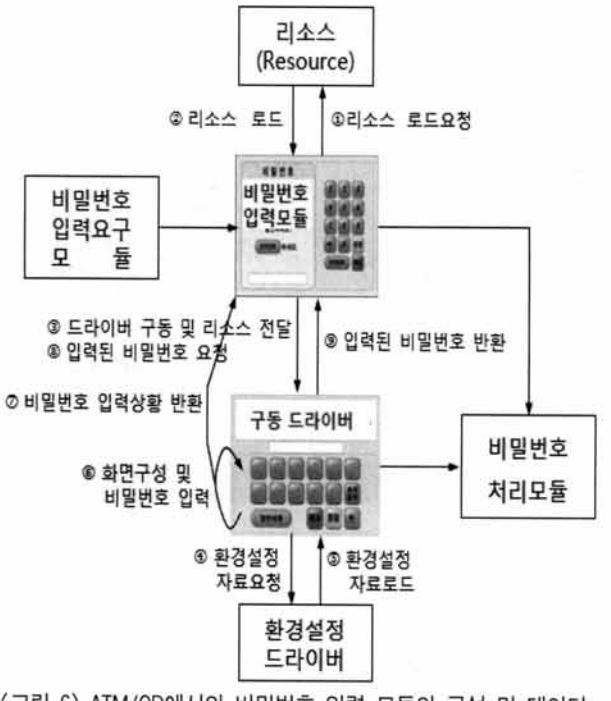
(가) "일반입력" 화면 (나) "안전입력" 화면

(그림 5) ATM/CD에서 비밀번호 입력 모듈의 구동

4.2 비밀번호 입력 모듈의 구성 및 데이터 흐름 과정

ATM/CD에서 비밀번호를 안전하게 입력하는 비밀번호 입력 모듈의 개발 환경은 윈도우즈 CE이며, TFT-LCD 터치스크린 입출력 장치에서 동작하도록 구현하였다. 구현 언어는 C와 C++이며, TSP 인터페이스 기능으로 동작을 구현하였다. 비밀번호 입력 모듈은 비밀번호 입력과 직접적인 관련이 있는 모듈과 입력된 비밀번호를 전송하는 모듈로 구성되어 있다. 비밀번호 입력과 직접적인 관련이 있는 모듈은 다시 비밀번호 입력 모듈과 구동 드라이버, 리소스, 환경설정 드라이버로 세분된다. 비밀번호 입력 모듈은 내장형 펌웨어의 중개 역할을 수행한다. 구동 드라이버는 비밀번호 입력 모듈로부터 리소스를 전달 받아 저장되어 있는 숫자를 디스플레이 순으로 재조합하여 비밀번호 입력 모듈에 넘겨주고, 비밀번호 입력 모듈과 파라미터를 주고받으며, 터치스크린 상에 GUI를 보여주고, 사용자로 하여금 비밀번호를 입력할 수 있도록 하는 등 펌웨어의 핵심기능을 수행한다. 터치스크린에 디스플레이 되는 이미지는 리소스 파일에 저장되어 있으며, 비밀번호 입력 모듈이 요청하면 리소스를 반환한다. 환경설정 드라이버는 확장성을 고려해 들어 있는 부분이다.

ATM/CD에서의 비밀번호 입력 프로세스는 (그림 6)과 같으며, 단계별 역할 및 기능은 다음과 같다[2].



(그림 6) ATM/CD에서의 비밀번호 입력 모듈의 구성 및 데이터 흐름

①~③ : 구동 드라이버는 항상 활성화되어 있는 상태에서 대기 모드 중에 있게 된다. 사용자가 "숫자보기" 버튼을 누르면 비밀번호 입력 모듈에 리소스 로드 요청을 한다. 그러면 비밀번호 입력 모듈은 리소스에서 GUI를 가져와 구동 드라이버에 전달한다.

④~⑤ : 구동 드라이버는 필요한 경우에 환경 설정 드라이버에게 동작 환경을 설정하는 자료를 요청하고, 환경 설정 드라이버는 이를 구동 드라이버에 반환한다. 이 단계가 지나면(숫자들이 보이지 않는 상태에서) 구동 드라이버가 숫자들이 보일 수 있는 준비 단계로 진입한다.

⑥ : 구동 드라이버는 숫자들의 표시된 순서 정보를 참조하고, 참조한 순서대로 터치스크린 상에 표시한다. 사용자는 숫자들이 표시된 상태에서 비밀번호를 입력한다. 구동 드라이버는 사용자가 비밀번호 입력을 완료할 때까지 숫자가 표시된 순서 정보를 참조하고, 참조한 순서대로 터치스크린 상에 표시한다. 이 단계에서 사용자가 기능 버튼을 눌렀을 때의 대응이 이루어진다.

⑦ : 한편 구동 드라이버는 비밀번호 입력 상황을 숫자 하나를 입력할 때마다 이를 비밀번호 입력 모듈에 전달한다. 사용자가 기능 버튼을 누르면 이에 대응하는 정보가 비밀번호 입력 모듈에 전달된다.

⑧~⑨ : 사용자가 비밀번호 입력을 완료하면 구동 드라이버는 이를 비밀번호 입력 모듈에 전달한다. 이 단계를 지나면 ATM/CD의 내장형 펌웨어 내부 처리 과정이 종료된다.

(그림 7) ATM/CD에서 비밀번호 입력 과정

4.3 ATM/CD에서 비밀번호 입력 과정

비밀번호를 안전하게 입력하는 방법을 내장시킨 ATM/CD에서 비밀번호가 "4910"인 경우, "안전입력" 모드를 이용하여 이 비밀번호를 입력하는 과정은 그림 7과 같다. ○○은행에서 운영하고 있는 ATM/CD에서 비밀번호를 입력하는 방법은 "일반입력"과 "안전입력"의 2가지 방법을 제공한다. "일반입력" 모드는 (그림 7(가))와 같이 숫자들이 순서적으로 표시된 상태에서 4개의 숫자를 입력하는 일반적인 비밀번호 입력 방법이고, "안전입력" 모드는 (그림 7(나))와 같이 "안전입력" 버튼을 클릭하여 (그림 7(다) ~ 그림 7(타))와 같이 비밀번호를 안전하게 입력하는 방법이다.

4.4 안정성 평가 결과 및 적용 사례 비교

비밀번호 훔쳐보기 공격으로부터 비밀번호를 안전하게 입력하는 방법을 ATM/CD에서 활용할 수 있도록 설계 및 구현하고, 이 제품을 금융보안연구원에 안전성 평가를 의뢰하여 "금융 보안 적합성 시험 결과, 비밀번호 훔쳐보기 방지를 위한 비밀번호 입력 솔루션인 안전한 비밀번호 입력 방법을 ATM/CD에서 구현한 비밀번호 입력 방식은 일반적인 비밀번호 입력 방식 보다 훔쳐보기 공격자의 비밀번호 획득 확률을 현저하게 낮출 수 있으므로 은행에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 판정되었음."이라는 평가 결과를 얻었다[17].

또한, 금융보안연구원으로부터 적합 판정을 받은 안전한 비밀번호 입력 방법은 국내 ○○은행에서 설치하여 운영하고 있는 ATM/CD의 비밀번호 입력 과정에서 (그림 7(나))와 같이 "안전입력" 모드로 활용되고 있으며, 현재까지 제품의 오류나 민원이 한 건도 발생하지 않았다. 참고로 <표 3>은 국내 금융기관의 ATM/CD에서 채택하여 활용하고 있는

〈표 3〉 ATM/CD의 비밀번호 입력 및 훔쳐보기 방지 기술 도입 현황

방 법	비밀번호 입력기술의 특징	적용사례	훔쳐보기	보안 적합성 시험
제안한 방법	○비밀번호 입력 순서가 되면 숫자가 123...순으로 나타남 ○'안전입력' 모드를 선택하면 무작위 순으로 나타남 ○비밀번호 입력할 때마다 숫자가 무작위 순으로 나타남	○○은행 △△은행	훔쳐보기를 고려하여 안전함	보안 적합 상태 시험을 통과하였고, 오류 및 민원 발생 사례가 없음
P-Protect[16]	○일부 숫자는 순차적, 나머지는 무작위 순으로 나타남 ○숫자 하나를 입력할 때 무작위 순으로 나타남	□□은행 ◇◇은행	훔쳐보기를 고려하지 않음	먼 곳에서도 훔쳐보기 가능
금융기관 자체솔루션	○비밀번호 입력 순서가 되면 숫자가 123...순으로 나타남 ○'안전입력' 모드를 선택하면 무작위 순으로 나타남 ○비밀번호 입력할 때 숫자가 123.., 789..., 순으로 나타남	☆☆은행 ▽▽은행 ◎◎은행	훔쳐보기를 고려했으나 방지효과 없음	보안 적합 상태 시험을 실시하지 않음
VIS[15]	○비밀번호 입력 순서가 되면 숫자가 123..순으로 나타남 ○'안전입력' 모드를 선택하면 세 개 모드가 나타남 ○세 번째 모드에 숫자가 무작위 순으로 나타남	♤♤은행	훔쳐보기를 고려하여 안전함	민원이 발생하여 일부 지점에서 탐재 철수
새마을금고 솔루션	○숫자들이 규칙적으로 나타남(상하좌우) ○번호 하나를 입력할 때 숫자들이 무작위 순으로 나타남	○○금고	훔쳐보기를 고려했으나 방지효과 없음	보안 적합 상태 시험을 실시하지 않음

비밀번호 입력 및 훔쳐보기 방지 기술의 도입 현황을 비교하여 요약한 것이다.

5. 결 론

ATM/CD에 신용카드 복제기를 설치하고 초소형 카메라를 설치하여 비밀번호를 알아내는 수법으로 현금을 인출해 가는 금융사고, 즉 비밀번호를 입력할 때 옆이나 뒤에 서있는 타인이 자신의 비밀번호를 훔쳐보거나 비밀번호 입력화면을 촬영할 수 있도록 초소형 카메라를 설치하여 비밀번호를 훔쳐보는 금융 사고가 꾸준하게 발생하고 있다. 이러한 금융 사고를 예방하기 위해서 금융 감독 당국에서는 ATM/CD에서 비밀번호를 안전하게 입력하는 셔플링 솔루션(Shuffling Solution), 즉 ATM/CD에서 뒷사람이나 옆사람이 비밀번호를 훔쳐보는 등 비밀번호가 유출되는 것을 방지하도록 하기 위하여 터치스크린의 비밀번호 숫자 위치를 고정하지 말고 무작위 랜덤방식으로 숫자 위치를 돌리는 방식의 도입을 권고하고 있다.

본 논문에서는 비밀번호 훔쳐보기 공격으로부터 안전하게 비밀번호를 입력하는 방법(DAS : Dynamic Authentication System)을 제안하여 안전성을 검증하였으며, 검증된 비밀번호 입력 방법을 ATM/CD에 내장하여 활용할 수 있도록 구현하였다. 먼저 인지심리학에 기초한 비밀번호 훔쳐보기로부터 안전한 기술을 적용하여 ATM/CD에서 비밀번호를 안전하게 입력하는 방법을 제안하였다. 이 방법은 비밀번호를 입력하는 과정을 옆이나 뒤에서 훔쳐봐도 무엇을 입력하였는지를 알 수 없도록 숫자들이 무작위 순으로 표시되었다가 사라진 상태에서 비밀번호를 입력할 수 있도록 구성하여 비밀번호를 누르는 과정을 옆이나 뒤에서 훔쳐봐도 알 수 없도록 하였다. 이를 입증하기 위하여 제안한 방법이 비밀번호 훔쳐보기 공격으로부터 안전함을 훔쳐보기 시험, 직관적인 관점 및 이론적인 분석으로 구분하여 검증하였으며, 제안한 비밀번호 입력 방법은 일반적인 비밀번호 입력 방법보다 비밀번호 훔쳐보기 공격자의 비밀번호 획득 확률이 현저하게 낮은 것으로 검증 및 평가되었다.

그리고 훔쳐보기 공격으로부터 안전한 비밀번호 입력 방법을 ATM/CD에 내장하여 활용할 수 있도록 안전한 비밀번호 입력 모듈을 설계 및 구현하였으며, ATM/CD에서 안전하게 비밀번호를 입력하는 방법이 비밀번호 훔쳐보기 공격으로부터 안전함을 확인하였다. 특히, 비밀번호 훔쳐보기 공격으로부터 비밀번호를 안전하게 입력하는 방법은 금융보안연구원으로부터 금융기관에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 평가[17]를 받아 국내 ○○은행의 ATM/CD와 인터넷 뱅킹 등에 적용되어 사용되고 있다.

한편, 최근에 발생하고 있는 금융사고 유형인 인증 녹화, 스크린 샷, 시스템 후킹 등을 이용한 훔쳐보기 공격을 방지할 수 있는 연구를 추가적으로 진행해야 하며, 스마트폰 열풍에 따라 스마트폰을 이용한 금융, 쇼핑, 행정 등 스마트폰을 기반으로 하는 많은 애플리케이션에서 사용자 인증이 증가할 것으로 예상되어 제안한 방법을 스마트폰에 적용할 수 있도록 구현하고자 한다.

참 고 문 헌

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Applied Cryptography", CRC Press, 1997.

[2] M.S. Kang, Y.I, Kim, Design and Implementation of Pinpad using Secure Technology from Shoulder Surfing Attack, The KIPS Transactions : Part D, Vol.17-D, No.2, pp.167~174, 2010.

[3] Financial Supervisory Service, "UK Internet banking-related fraud increased", Information of Financial Supervisory Service, No.396, pp.43~44, Nov., 2006.

[4] Li, Zhi., Sun, Qibin., Lian, Yong., Giusto, D.D., "An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack", 2005 IEEE International Conference on Multimedia and Expo(ICME-05), pp.245~248, 2005.

[5] Lei, M., Xiao, Y., Vrbsky, S.V., "Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing", Computer communications, Vol.31 No.18, pp.4367~4375, 2008.

[6] S.B. Park, M.S. Kang, Secure Password System against Imposter, The KIPS Transactions : Part C, Vol.10-C, No.2, pp.141~144, 2003.

[7] S.B. Park, M.S. Kang, and S.J. Lee, "Authenticated key exchange protocol secure against off-line dictionary attack and server compromise", Lecture Notes in Computer Science, Vol.3032, pp.924~931, 2004.

[8] Sorinamoo Solution, "Secure method for generating one time password and interpreting one time password", Korean Intellectual Property Office, 2007. 01

[9] Nebojsa Jojic and Paul Roberts, "image based password systems", http://research.microsoft.com/en-us/um/people/darkok/projectssyscli.htm.

[10] D. Kirovski, N. Jojic, and P. Roberts. "Click Passwords", 21st IFIP International Information Security Conference, pp.351~363, 2006.

[11] RealUser, "Passfaces: Two Factor Authentication, Graphical Password", http://www.realuser.com/index.htm.

[12] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry", Proceedings of the 3rd symposium on Usable Privacy and Security(SOUPS 2007), pp.13~19, 2007.

[13] BeOnePlus Co., Ltd, RhythmPass & ChamID, http://www.beone.co.kr/.

[14] Nemeth, Garth Snyder, and Trent R. Hein, "Linux Administration Handbook(2nd Edition)", Prentice Hall PTR, 2006.

[15] Edward K. Vogel & Maro G. Machizawa, "Neural activity predicts individual differences in visual working memory capacity", Nature, Vol.428, pp.748~751, 2004.
[16] INCA Internt Co., Ltd., P-Protect, http://www.inca.co.kr/include_file/pdf_down /A-P-Protect.pdf.
[17] 금융보안연구원, 'OO은행 A-DAS' 금융보안적합성 시험 검토 보고서, 금융보안연구원(FSA : Financial Security Agency, http://www.fsa.or.kr), pp.1~10, 2008.

김 태 희

e-mail : thkim@dsu.ac.kr
1991년 동신대학교 전자계산학과(공학사)
1993년 전남대학교 전산통계학과 (이학석사)
1999년 전남대학교 전산통계학과 (이학박사)
1997년~현 재 동신대학교 디지털콘텐츠학과 부교수
관심분야 : 소프트웨어공학, 객체지향 모델링, 컴퓨터 교육

박 승 배

e-mail : sbmaum@paran.com
1996년 전남대학교 전산통계학과(이학박사)
1996년~2004년 8월 초당대학교 컴퓨터과학과 조교수
2002년~2003년 (주)신비테크 연구소장
2004년~현 재 (주)신비테크 대표이사
관심분야 : 암호 알고리즘, 암호 프로토콜, 보안, 비밀번호 입력 기술

강 문 설

e-mail : mskang@gwangju.ac.kr
1986년 전남대학교 전산통계학과(이학사)
1989년 전남대학교 전산통계학과 (이학석사)
1994년 전남대학교 전산통계학과 (이학박사)
1994년~현 재 광주대학교 컴퓨터공학과 교수
관심분야 : 소프트웨어공학, 정보보호관리, 인터넷 윤리, 컴퓨터 교육