DOI: 10.3745/KIPSTD.2010.17D.2.167

비밀번호 훔쳐보기로부터 안전한 기술을 내장시킨 비밀번호 입력기의 설계 및 구현

강 문 설[†] · 김 용 일[††]

요 약

비밀번호를 입력하는 과정에서 가장 큰 보안 위협은 비밀번호를 훔쳐보는 것이다. 비밀번호 훔쳐보기는 비밀번호를 입력하는 과정을 옆에서 지켜보고 비밀번호를 획득하려고 하는 행위로서 비밀번호를 획득하는 가장 전통적인 방법이며 강력한 보안 위협이다.

본 논문에서는 인지심리학에 기초한 비밀번호 훔쳐보기로부터 안전한 기술인 역동 인증 체계(DAS)라 불리는 비밀번호 입력 기술을 제안하였다. 그리고 제안한 역동 인증 체계의 비밀번호 훔쳐보기에 대한 안전성을 직관적인 관점, 훔쳐보기 실험, 이론적인 분석으로 구분하여 검증하였다. 비밀번호 훔쳐보기로부터 안정성이 입증된 역동 인증 체계를 내장시킨 비밀번호 입력기를 설계하여 구현하였다. 구현한 비밀번호 입력기는 일반 패스워드 입력방식 보다 훔쳐보기 공격자의 비밀번호 획득 확률을 현저하게 낮출 수 있으므로 은행에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 평가를 받아 금융기관에서 도입하여 활용되고 있다.

키워드 : 비밀번호 훔쳐보기, 비밀번호 입력기, 역동 인증 체계, 보안 위협

Design and Implementation of Pinpad using Secure Technology from Shoulder Surfing Attack

Kang, Moon-Seol[†] · Kim, Young-Il[††]

ABSTRACT

When entering the PIN(personal identification number), the greatest security threat is shoulder surfing attack. Shoulder surfing attack is watching the PIN being entered from over the shoulder to obtain the number, and it is the most common and at the same time the most powerful security threat of stealing the PIN.

In this paper, a psychology based PINpad technology referred to as DAS(Dynamic Authentication System) that safeguards from shoulder surfing attack was proposed. Also, safety of the proposed DAS from shoulder surfing attack was tested and verified through intuitive viewpoint, shoulder surfing test, and theoretical analysis. Then, a PINpad with an internal DAS that was certified for its safety from shoulder surfing attack was designed and produced. Because the designed PINpad significantly decreases the chances for shoulder surfing attackers being able to steal the PIN when compared to the ordinary PINpad, it was determined to be suitable for use at ATM(automated teller machine)s operated by banks and therefore has been introduced and is being used by many financial institutions.

Keywords : Shoulder Surfing Attack, PINpad, DAS(Dynamic Authentication System), Security Threat

1. 서 론

사용자 인증은 서비스 요구자나 시스템 접근자가 인가된 사용자 인가를 확인하는 보안 서비스를 말한다. 그리고 사용자 인증에 따른 조치를 취하는 솔루션을 인증 시스템이라 한다. 인증 시스템이 사용자 인증을 위해 이용하는 정보에는 세 가지가 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. 또한, 카드결제 시스템에서 비밀번호로 카드 소유자를 인증하는 기술이 개발되어 사용되

※ 이 연구는 2009년도 광주대학교 대학 연구비의 지원을 받아 수행되었음.
† 종신회원 : 광주대학교 컴퓨터공학과 교수
†† 종신회원 : 호남대학교 인터넷소프트웨어학과 조교수
논문접수 : 2009년 12월 9일
수 정 일 : 1차 2010년 2월 17일, 2차 2010년 3월 2일
심사완료 : 2010년 3월 28일

고 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[2].

카드결제 시스템 사용자가 안전하게 비밀번호를 입력하도록 하는 기술 및 장비가 개발되어 금융기관에서 활용되고 있다. 카드결제시스템에서 카드 소유자 인증 비밀번호는 비밀번호입력기[3, 4]라 불리는 비밀번호 입력 전용단말기나 카드결제기에서 입력되며, 입력된 비밀번호는 카드결제기나 POS(Point Of Sale) 시스템[5]을 통해 VAN(Value Added Network)사로 전송된다.

한편, 보안 위협은 온라인 보안위협과 오프라인 보안위협으로 구분된다. 온라인 보안위협은 통신로를 이용한 정보보호에 반하는 행위를 말하며, 가로채기, 위변조, 위장 등이 온라인 보안위협에 해당한다. 오프라인 보안위협은 통신로를 이용하지 않는 정보보호에 반하는 행위를 말하며, 온라인 추측공격과 비밀번호 훔쳐보기가 오프라인 보안위협에 해당한다. 비밀번호 입력기는 카드결제기나 POS 시스템과 시리얼 통신을 하기 때문에 비밀번호 입력기에서는 온라인 보안위협을 고려하지 않는다. 온라인추측공격은 비밀번호를 획득할 때까지 비밀번호 후보를 반복 입력하는 행위를 말한다[6, 7]. 온라인추측공격 방지는 주로 비밀번호 오류 입력 횟수를 제한하는 방법이 이용된다[8, 9]. 이러한 경우 온라인추측공격에 대해 안전하다고 정의되지 않으며, 또한 안전하지 않다고도 정의되지 않는다. 반면 자주 눌러진 버튼들이 닳아져 시도해 보아야 하는 비밀번호 후보가 줄어든 경우는 온라인추측공격에 대해 안전하지 않다고 말한다. 비밀번호 훔쳐보기는 비밀번호 누르는 걸 옆에서 지켜보아 이를 획득하는 행위를 말한다[10, 11]. 비밀번호 훔쳐보기는 비밀번호를 획득하는 가장 오래되고 강력한 보안위협으로, 비밀번호 입력기에서 가장 많이 발생하는 보안위협이다.

본 논문에서는 비밀번호 훔쳐보기 공격자로부터 안전한 비밀번호 입력 기술인 역동 인증체계(DAS : Dynamic Authentication System)를 제안하여 안전성을 검증하였으며, 이 DAS를 내장시킨 비밀번호 입력기를 설계 및 구현하였다. 먼저 인지심리학에 기초하여 훔쳐보기로부터 안전한 기술인 역동 인증 체계(DAS)라 불리는 비밀번호 입력기술을 제안하였다. 이 기술은 비밀번호 입력을 위한 숫자가 무작위 순으로 나타났다가 사라진 상태에서 비밀번호를 입력하도록 구성하여 비밀번호를 누르는 과정을 옆에서 훔쳐봐도 알 수 없도록 하였다. 이를 입증하기 위하여 DAS가 비밀번호 훔쳐보기로부터 안전함을 직관적인 관점, 훔쳐보기 실험, 이론적인 분석으로 구분하여 안전성을 검증하였으며, 검증 결과 일반 패스워드 입력방식보다 비밀번호 훔쳐보기 공격자의 비밀번호 획득 확률이 현저하게 낮아짐을 입증하였다. 그리고 훔쳐보기로부터 안전한 기술인 DAS를 내장시킨 비밀번호 입력기를 설계 및 구현하였다. DAS를 내장시킨 비밀번호 입력기의 펌웨어 구조와 프로세스, 그리고 하드웨어 모듈을 설계 및 구현하였고, 시제품이 비밀번호 훔쳐보기로부터 안전함을 확인하였다. 특히, 비밀번호 훔쳐보기 방지를 위하여 DAS를 내장시켜 구현한 비밀번호 입력기는 금융보안연구원(FSA : Financial Security Agency)으로부터 금융기관에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 평가를 받아 금융기관의 현금인출기와 인터넷 뱅킹에 적용되어 사용되고 있다.

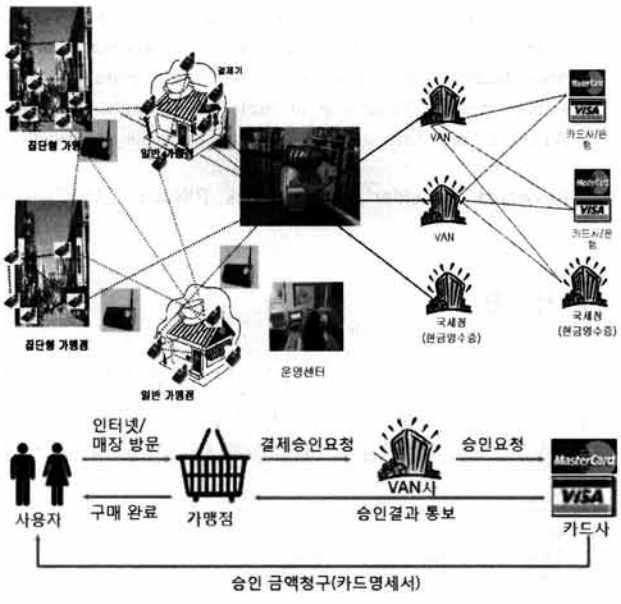
논문의 구성은 다음과 같다. 2장에서는 관련연구로 카드결재시스템과 비밀번호입력기, 비밀번호 훔쳐보기 방지를 목적으로 한 관련 기술들을 살펴본다. 3장에서는 비밀번호 입력기술인 DAS를 제시하고, DAS의 온라인 추측공격 및 훔쳐보기에 대한 안전도를 분석한다. 4장에서는 DAS를 내장시킨 비밀번호 입력기 구현 내용을 기술하고, 5장에서는 본 논문의 결론 및 향후 연구방향을 기술한다.

2. 관련연구

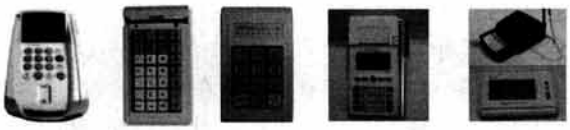
2.1 카드 결제 시스템과 비밀번호 입력기

카드결제시스템의 카드결제 과정은 (그림 1)과 같다. ① 대금결제를 위해 사용자는 가맹점주에게 카드를 건넨다. ② 가맹점주는 카드결제기에서 카드를 읽힌다. ③ 사용자는 비밀번호입력기에서 비밀번호를 입력한다. ④ 카드 정보와 비밀번호가 카드결제기나 POS 시스템을 통해 VAN사로 전송된다. ⑤ VAN사는 금융사에 결제승인요청을 한다. ⑥ 금융사는 VAN사에 결제승인 여부를 전송한다. ⑦ VAN사는 결제 승인여부를 카드결제기나 POS 시스템에 전송한다. ⑧ 결제승인이 난 경우에 한하여 가맹점주는 사용자에게 전표를 발급한다.

카드결제시스템에서 비밀번호 입력을 위한 전용 단말기를 비밀번호입력기라 한다[3, 4]. 비밀번호입력기는 카드결제기



(그림 1) 신용카드결제시스템 구성도



(가) 다양한 형태의 비밀번호입력기 (나) 카드결제기 (다) 사인패드

(그림 2) 비밀번호 입력기

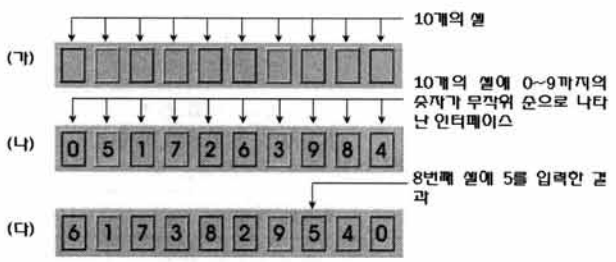
와 분리되어 있거나 카드결제기와 일체형으로 존재한다. 또한 카드 소유자 인증을 위해 사인과 비밀번호를 혼용하는 경우에 사인패드 기능이 있는 비밀번호입력기가 사용되기도 한다. 비밀번호입력기는 카드결제기나 POS 시스템과 시리얼 통신을 하므로 온라인 보안위협을 고려하지 않는다. 따라서 비밀번호입력기에서 입력된 비밀번호는 암호화되어 카드결제기나 POS 시스템에 전송되지 않는다.

2.2 훔쳐보기 방지 기술

훔쳐보기는 비밀번호를 누르는 것을 옆에서 지켜보아 이를 획득하는 행위이다[10, 11]. 훔쳐보기는 비단 비밀번호입력기에서 뿐 아니라 현금인출기나 디지털 도어락(doorlock) 등 비밀번호로 사용자를 인증하는 모든 곳에서 발생하는 보안위협이다. 이러한 이유로 훔쳐보기로부터 안전한 기술 개발을 위한 많은 노력들이 있어 왔다[12-19, 22-23].

본 논문에서 비밀번호 훔쳐보기 방지를 위한 모든 기술을 열거할 수 없으므로 여기에서는 대표적 기술 몇 가지를 소개한다. 먼저 [12-14]에서 제안한 기술을 예로서 설명하고자 한다. 비밀번호가 "5619"라 하자. 인터페이스는 10개의 셀로 이루어져 있고(그림 3)(가), 10개의 셀에는 0~9까지의 숫자가 무작위 순으로 나타나 있다(그림 3)(나). 사용자는 마음속으로 하나의 셀을 선택한다. (그림 3)(나)에서 사용자가 마음속으로 8번째 셀을 선택했다고 하자. 사용자는 마음속으로 선택한 8번째 셀에 비밀번호 첫 번째 숫자인 "5"가 나타나도록 증감 버튼을 누른 후, "5"가 나타나면 엔터키를 친다("5"입력)(그림 3)(다). 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.

소리나무미디어(주)는 VIS(Virtual Inputting System)[15]를 제안하였다. VIS 인터페이스는 세 개의 보드로 그림 4와



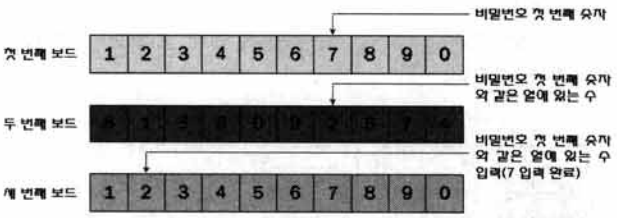
(그림 3) [12]에서 제시한 비밀번호 입력기술 설명을 위한 인터페이스

같이 구성되어 있다. 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.

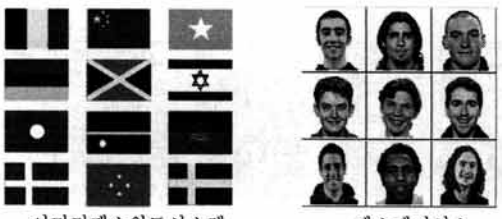
숫자보다는 이미지를 기억하기 어렵다는 사실에 기초하여, 이미지를 입력하는 기술들이 제안되기도 하였다. 대표적 기술로는 이미지패스워드시스템[16-17]과 패스페이시스[18]를 들 수 있다. 이미지패스워드시스템은 인터페이스에 나타난 이미지에서 사용자가 기억하고 있는 이미지를 순차적으로 누른다. 패스페이시스는 이미지(사람 얼굴)를 입력하다는 점에서 이미지패스워드시템과 동일하나 기억하고 있는 이미지(사람 얼굴) 하나를 누르면 인터페이스에 새로운 이미지(사람 얼굴)들이 나타난다는 점이 다르다.

스탠포드 대학은 현금인출기 등에서 비밀번호를 눈으로 콕콕 찍어서 입력하는 기술을 개발하고 있다[19]. 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[19, 24]. (주)비원플러스에서 개발한 리듬패스(RhythmPass)



(그림 4) 소리나무미디어의 비밀번호 입력기술 설명을 위한 인터페이스



이미지패스워드시스템 패스페이시스

(그림 5) 이미지패스워드시스템과 패스페이시스의 인터페이스 예

[22]는 비밀번호를 리듬에 맞추어 입력한다. 예를 들어, 비밀번호가 "1234"이고, 리듬이 "대한민국"이면 "1234"를 "1~234"로 입력한다. 신한은행의 현금인출기에 시험 적용한 적이 있으며, 현재는 개인용 컴퓨터 보안 제품으로 판매되고 있다.

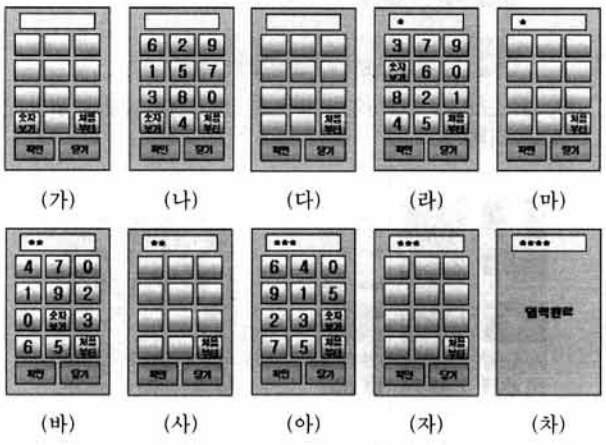
LINUX에서는 256자까지의 비밀번호를 허용하고 있으며 [20], 모니터를 옆에서 보면 모니터 내용을 알 수 없는 프라이비트 패드라 불리는 물리적 제품이 개발되기도 하였다.

3. 역동 인증 체계(DAS : Dynamic Authentication System)

본 장에서는 비밀번호 훔쳐보기 공격으로부터 안전한 기술인 DAS(Dynamic Authentication System; 역동 인증 체계)를 설명하고, 이 DAS가 비밀번호 훔쳐보기로부터 안전함을 직관적인 관점, 훔쳐보기 실험 및 이론적 분석을 토대로 입증한 결과를 기술한다.

3.1 비밀번호 입력과정

비밀번호 입력 과정을 예로서 설명한다. 비밀번호가 "1234"라 하자. 인터페이스에는 숫자들이 나타나 있지 않고, "숫자보기" 버튼이 구비되어 있다(그림 6)(가). 사용자가 "숫자보기" 버튼을 누르고 있으면 숫자들이 무작위 추출된 순으로 보이고(그림 6)(나), "숫자보기" 버튼을 누르지 않으면 숫자들이 보이지 않게 된다(그림 6(다)). 사용자는 "숫자보기" 버튼을 누른 상태에서 "1"이 나타난 버튼을 확인하고, "숫자보기" 버튼을 누르지 않은 상태(숫자들이 보이지 않은 상태) (그림 6)(다)에서 확인한 버튼을 누르고 있는다("1" 입력)(그림 6)(라). 그러면 "1"을 입력하기 위해 누르고 있는 버튼이 "숫자보기"가 되어 숫자들이 현재 누르고 있는 버튼을 제외한 버튼들에 무작위 순으로 나타난다(그림 6)(라). "2"가 나타난 버튼을 확인하고, "숫자보기" 버튼을 누르지 않은 상태(그림 6)(마)에서 확인한 버튼을 누르고 있는다(2 입력)(그림 6)(바). "2"를 입력한 방법과 동일한 방법으로 "34"를 입력한다.



(그림 6) DAS를 이용한 비밀번호 입력 과정

3.2 DAS의 비밀번호 훔쳐보기에 대한 안전도

3.2.1 직관적인 관점

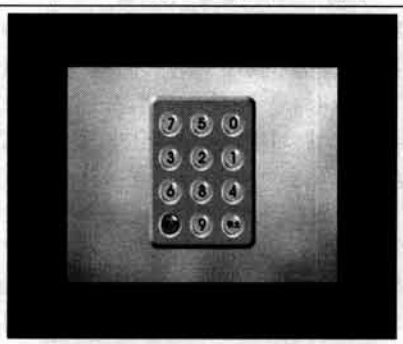
비밀번호를 입력하는 사람은 숫자가 무작위 순으로 나타난 상태에서 누르고자 하는 버튼을 시각적으로 확인한 후, 숫자들이 사라진 상태에서 확인한 버튼을 누른다. 반면 비밀번호 훔쳐보기로 비밀번호를 알려고 하는 사람은 (숫자가 무작위 순으로 나타났다가 사라진 상태에서 번호가 입력되기 때문에) 비밀번호를 입력하는 사람이 누르고자 하는 버튼을 시각적으로 확인하는 찰나에 무작위 추출된 순서로 나타난 수들을 순서대로 모두 기억하고 있어야 비밀번호 숫자 하나를 알게 된다.

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

3.2.2 훔쳐보기 실험

강의실에서 대학생을 상대로 실험이 이루어졌다. 실험은 162명을 대상으로 하였고, 162명을 세 그룹으로 나누어 실험하였다. 실험은 ① 빔 프로젝터를 통해 DAS를 설명하고 ② 종이에 미리 적어 놓은 비밀번호를 입력한 후 ③ 입력한 숫자 몇 개를 맞추었는지 조사하였다. 실험결과, 알아맞히는 것을 포기한 학생이 118명 이었고, "모르겠다."라는 유형의 답을 한 학생이 35명 이었으며, 9명의 학생이 두 개 이하를 맞추었다.

〈표 1〉 DAS의 비밀번호 훔쳐보기 안전도 실험

시험도구	데모 프로그램, 노트북, 빔 프로젝터	
시험환경		
시험목적	DAS의 비밀번호 훔쳐보기 안전도 통계 확보	
시험환경	강의실	
시험대상	학생 162명	
시험방법	① DAS에 대해 설명 ② DAS로 비밀번호 입력 ③ 입력한 숫자 중 몇 개를 맞추는지 조사	
실제 시험결과	포기한 학생	118명
	'모르겠다.'라고 표현한 학생	35명
	숫자 두 개 이하를 맞춘 학생	9명

3.2.3 이론적인 분석

인지 심리학에서 사람이 순간적으로 본 후 본 숫자를 반복적으로 되뇌어 기억할 수 있는 숫자의 개수가 1.5~5라는 이론이 [21]에 소개되었다. DAS로 비밀번호를 입력하였을 때, 인터페이스에 무작위 순으로 나타난 숫자를 보고 순간적으로 보고 기억할 수 있는 개수를 나타내는 확률을 α라 하자($0 \le \alpha \le 1$). 그러면 [21]에 기초하여 α는 0.15~0.5이다. 따라서 다른 모든 환경을 무시하고 DAS로 비밀번호를 입력하였을 때 비밀번호 훔쳐보기로 비밀번호를 획득할 수 있는 확률은 $0.15^4 \sim 0.5^4$(0.00050625~0.0625)가 된다.

DAS로 비밀번호를 입력하였을 때, 인터페이스에 무작위 순으로 나타난 숫자를 보고 순간적으로 보고 기억할 수 있는 개수를 나타내는 확률을 α라 하고($0 \le \alpha \le 1$), 입력된 번호를 기억하고 있으면서 무작위 순으로 나타난 숫자를 모두 기억하는 과정에서 일어나는 충돌현상이 두 번째 이후의 번호를 알아내는데 미치는 정도를 β라 하자($0 \le \beta \le 1$). 그러면 DAS로 입력된 번호 중 비밀번호 훔쳐보기로 입력된 숫자 i개를 획득할 확률은 $\alpha^i * \beta^{(i-1)}$이다($1 \le i \le 4$).

4. 비밀번호 입력기 구현

4.1 펌웨어

비밀번호 입력기의 임베디드 펌웨어는 서브 모듈에 변화가 있더라도 펌웨어 구조 자체는 변화가 되지 않도록 설계하였으며, 다른 적용 제품에의 확장성도 고려하여 설계하였다. 개발환경은 윈도우즈 CE이며, TFT-LCD 터치스크린 입출력 장치에서 동작하도록 구현하였다. 구현언어는 C와 C++이며, TSP 인터페이스 기능으로 동작을 구현하였다.

펌웨어는 비밀번호 입력과 직접적인 관련이 있는 모듈과 입력 비밀번호 전송 모듈로 구성되어 있다. 비밀번호 입력과 직접적인 관련이 있는 모듈은 다시 비밀번호 입력 모듈과 구동 드라이버, 리소스, 환경설정 드라이버로 세분된다.

〈표 2〉 [21]에 기초한 DAS의 훔쳐보기에 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

〈표 3〉 DAS로 입력된 번호 중 비밀번호 훔쳐보기로 i개를 획득할 확률

β	j		
	2	3	4
0.1	0.00225~0.025	0.0003375~0.0125	0.000050625~0.00625
0.2	0.00450~0.050	0.0006750~0.0250	0.000101250~0.01250
0.3	0.00675~0.075	0.0010125~0.0375	0.000151875~0.01875
0.4	0.00900~0.100	0.0013500~0.0500	0.000202500~0.02500
0.5	0.01125~0.125	0.0016875~0.0625	0.000253125~0.03125
0.6	0.01350~0.150	0.0020250~0.0750	0.000303750~0.03750
0.7	0.01575~0.175	0.0023625~0.0875	0.000354375~0.04375
0.8	0.01800~0.200	0.0027000~0.1000	0.000405000~0.05000
0.9	0.02025~0.225	0.0030375~0.1125	0.000455625~0.05625
1.0	0.02250~0.250	0.0033750~0.1250	0.000506250~0.06250

〈표 4〉 DAS 임베딩 비밀번호입력기 펌웨어 구분

구 분	세부 모듈
비밀번호 입력과 직접적인 관계가 있는 모듈	비밀번호 입력 모듈 구동 드라이버 리소스 환경설정 드라이버
비밀번호 전송 모듈	

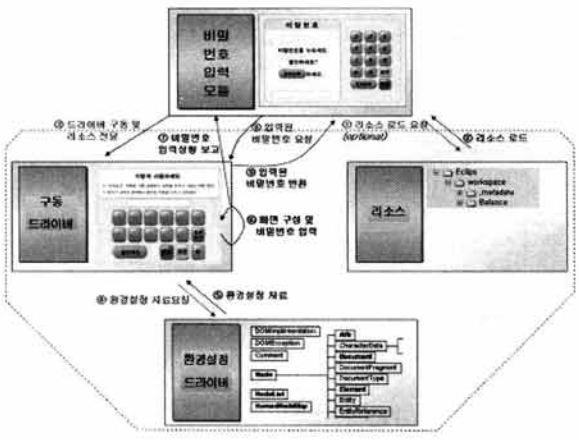
비밀번호 입력 모듈은 임베디드 펌웨어의 중개 역할을 수행한다. 구동 드라이버는 비밀번호 입력 모듈로부터 리소스를 전달 받아 저장되어 있는 숫자를 디스플레이 순으로 재조합하여 비밀번호 입력 모듈에 넘겨주고, 비밀번호 입력 모듈과 파라미터를 주고받으며, 터치스크린 상에 GUI를 보여주고, 사용자로 하여금 비밀번호를 입력할 수 있도록 하는 등 펌웨어의 핵심기능을 수행한다. 터치스크린에 디스플레이 되는 이미지는 리소스 파일에 저장되어 있으며, 비밀번호 입력 모듈이 요청하면 리소스를 반환한다. 환경설정 드라이버는 확장성을 고려해 들어 있는 부분으로, 본 논문에서의 비밀번호입력기에서는 환경설정 드라이버를 이용하지 않았다.

비밀번호 입력기의 펌웨어 프로세스는 (그림 7)과 같다.

①~③: 구동 드라이버는 항상 활성화 되어 있는 상태에

〈표 5〉 DAS 임베딩 비밀번호입력기 펌웨어 역할

모 듈	역할
구 동 드라이버	비밀번호 입력 모듈로부터 리소스 수신 리소스를 디스플레이 순으로 재조합 재조합한 리소스를 비밀번호 입력 모듈에 송신 비밀번호 입력 모듈 파라미터 수신 입출력 장치에 GUI 디스플레이 비밀번호 입력
비밀 번호 입력 모듈	펌웨어 사이의 중개 역할 프로토콜을 서브 모듈로 가지고 있음
리 소 스	이미지 저장 비밀번호 입력 모듈 요청 시 리소스 반환
환경 설정 드라이버	확장성을 고려해 구현 본 비밀번호입력기에서는 사용하지 않음



(그림 7) DAS 임베딩 비밀번호입력기에서의 비밀번호 입력 프로세스

서 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.

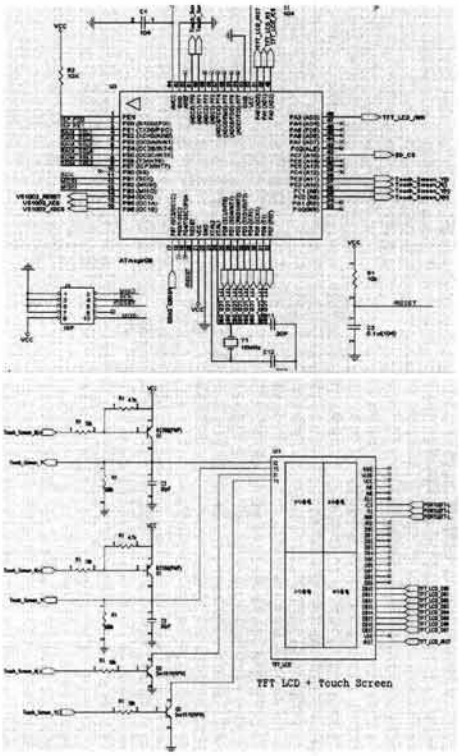
④~⑤: 구동 드라이버는 필요한 경우에 환경설정 드라이버에게 동작 환경을 설정 자료를 요청하고, 환경설정 드라이버는 이를 구동 드라이버에 반환한다. 이 단계가 지나면 (숫자들이 보이지 않는 상태에서) 구동 드라이버가 숫자들이 보일 수 있는 준비단계로 진입한다.

⑥: 구동 드라이버는 숫자들의 디스플레이 순서 정보를 참조하고, 참조한 순서대로 터치스크린 상에 디스플레이 한다. 사용자는 숫자들이 디스플레이된 상태에서 비밀번호를 입력한다. 구동 드라이버는 사용자가 비밀번호 입력을 완료할 때까지 숫자 디스플레이 순서 정보를 참조하고, 참조한 순서대로 터치스크린 상에 디스플레이 한다. 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 비밀번호 입력기 임베디드 펌웨어 내부 처리 과정이 종료된다.

입력된 비밀번호는 비밀번호 전송 모듈에 의해 카드결제기나 POS 시스템에 전송된다.



(그림 8) DAS 임베딩 비밀번호입력기 보드 설계

4.2 하드웨어

비밀번호 입력기 내장 보드를 (그림 8)과 같이 설계 및 제작하였다. 152.4mm(W)*91.44(H) 크기의 24-비트 풀 컬러 TFT-LCD 800*480 WVGA 사양의 비밀번호입력기를 제작하였다(<표 6>).

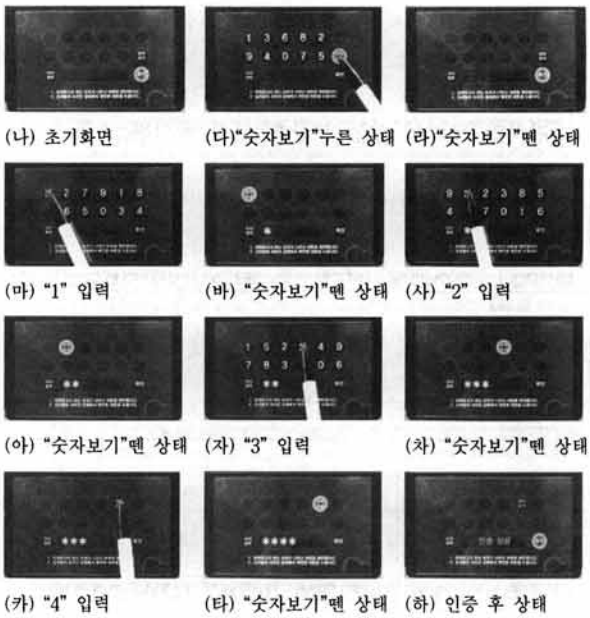
〈표 6〉 DAS 임베딩 비밀번호입력기 사양

구분	사양
해상도	TFT-LCD 800 X 480 WVGA
크기	152.4(H) X 91.44(V)
색상	24bit True Color
메모리	Nor(1MB), NAND(64MB), SDRAM(64MB)
보드율	1,200bps~115,200bps
프로세서	32bit RISC TYPE ARM Processor/ ATmega128
사용전원	5V/7mA
인터페이스	UART 2Port, JTAG 1Port, USB 1Port

4.3 비밀번호 입력기의 비밀번호 입력 과정

(그림 9)는 DAS를 내장시킨 비밀번호 입력기와 DAS를 내장시킨 비밀번호 입력기에서 비밀번호가 "1234"인 경우에 이를 입력하는 과정을 보이고 있다.

(가) DAS 임베딩 비밀번호입력기



(나) 초기화면 (다)"숫자보기"누른 상태 (라)"숫자보기"뗀 상태

(마) "1" 입력 (바) "숫자보기"뗀 상태 (사) "2" 입력

(아) "숫자보기"뗀 상태 (자) "3" 입력 (차) "숫자보기"뗀 상태

(카) "4" 입력 (타) "숫자보기"뗀 상태 (하) 인증 후 상태

(그림 9) DAS 임베딩 비밀번호입력기 및 비밀번호 입력과정

4.4 안정성 평가 및 적용 사례

비밀번호 훔쳐보기 공격으로부터 안전한 기술인 DAS를 내장시킨 비밀번호 입력기를 설계 및 구현하여, 이 시제품

을 금융보안연구원(FSA : Financial Security Agency)에 안전성 평가를 의뢰하여 "금융 보안 적합성 시험 결과, 비밀번호 훔쳐보기 방지를 위한 비밀번호 입력 솔루션인 DAS를 내장시켜 구현한 비밀번호 입력기는 일반 패스워드 입력방식 보다 훔쳐보기 공격자의 비밀번호 획득 확률을 현저하게 낮출 수 있으므로 은행에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 판정되었음"이라는 평가 결과를 얻었다.

또한, 금융보안연구원으로부터 적합 판정을 받은 DAS를 내장시킨 비밀번호 입력기술은 KJ은행에서 설치하여 운영하고 있는 모든 현금인출기, KJ은행과 JJ은행의 인터넷 뱅킹의 비밀번호 입력 과정에서 안전(보안)입력 모드로 활용되고 있으며, 현재까지 제품의 오류나 민원이 한 건도 발생하지 않았다. 그리고 DAS를 내장시킨 비밀번호 입력기는 은행이나 증권사의 창구에서 사용하는 비밀번호 입력 전용 단말기로 활용하기 위해 은행 2곳과 증권사 4곳과 서비스 시스템을 개발하고 있다. 참고로 <표 7>은 국내 금융기관에서 채택하여 활용하고 있는 비밀번호 입력 및 훔쳐보기 방지 기술의 도입 현황을 비교하여 요약한 것이다.

5. 결 론

1900년대 말까지만 해도 대부분의 나라가 카드결제 시 카드 소유자 인증 수단으로 사인을 이용하였다. 그러나 카드 도난분실에 의한 사고 등 사인으로 인한 피해가 갈수록 증대되었고, 이에 2000년대에 들어 카드결제 시 카드 소유자 인증수단으로 비밀번호를 이용하는 나라가 생기기 시작하였고 갈수록 그 국가가 늘어나고 있다.

한편, 비밀번호입력기의 가장 큰 보안위협은 비밀번호 훔쳐보기이다. 비밀번호 훔쳐보기는 비밀번호를 입력하는 과정을 옆에서 지켜보아 이를 획득하려고 하는 행위로, 이는 비밀번호를 획득하는 가장 전통적이며 강력한 보안위협이다. 또한, 카드결재 시 비밀번호로 카드 소유자를 인증하는 제도를 도입한 나라에서 비밀번호 훔쳐보기는 이미 사회문제가 된 상태이다.

본 논문에서는 비밀번호 훔쳐보기 공격자로부터 안전한 비밀번호 입력 기술인 역동 인증체계(DAS : Dynamic Authentication System)를 제안하여 안전성을 검증하였으며, 이 DAS를 내장시킨 비밀번호 입력기를 설계 및 구현하였다. 먼저 인지 심리학에 기초한 훔쳐보기로부터 안전한 기술인 역동 인증 체계(DAS)라 불리는 비밀번호 입력기술을 제안하였다. 이 기술은 비밀번호 입력을 위한 숫자가 무작위 순으로 나타났다가 사라진 상태에서 비밀번호를 입력하도록 구성하여 비밀번호를 누르는 과정을 옆에서 훔쳐봐도 알 수 없도록 하였다. 이를 입증하기 위하여 DAS가 비밀번호 훔쳐보기로부터 안전함을 직관적인 관점, 훔쳐보기 실험, 이론적인 분석으로 구분하여 안전성을 검증하였다. 검증 결과를 살펴보면, 직관점인 관점에서는 비밀번호 훔쳐보기 공격자가 무작위 순으로 나타난 숫자들을 순서대로 기억하는 과정에서 번호들끼리 충돌현상이 발생하여 비밀번호를 획득할 수 없었으며, 162명의 학생을 대상으로 훔쳐보기 실험을 실시한 결과 118명은 포기, 35명은 모르겠다, 나머지 9명만 2개 이하의 숫자를 맞추어 안전함이 입증되었고, 인지 심리학 이론에 근거하여 비밀번호 훔쳐보기로 비밀번호를 획득할 수 있는 확률이 0.15^4~0.5^4로 매우 낮게 나타났다. 세 가지 측면의 검증 결과를 종합하면, 제안한 비밀번호 입력 기술은 일반 패스워드 입력 방식보다 비밀번호 훔쳐보기 공격자의 비밀번호 획득 확률이 현저하게 떨어지는 것을 알 수 있었다.

그리고 훔쳐보기로부터 안전한 기술인 역동 인증 체계(DAS)를 내장시킨 비밀번호 입력기를 설계하여 구현하였다. 역동 인증 체계를 내장시킨 비밀번호 입력기의 펌웨어 구조와 프로세스, 그리고 하드웨어 모듈을 설계 및 구현하였고, 구현한 시제품이 비밀번호 훔쳐보기 공격자로부터 안전함을 확인하였다. 특히, 비밀번호 훔쳐보기 방지를 위하여 DAS를 내장시켜 구현한 비밀번호 입력기는 금융보안연구원(FSA : Financial Security Agency)으로부터 금융기관에서 운영하는 금융자동화기기에 적용 및 운영되기에 적합한 것으로 평가를 받아 금융기관의 현금인출기와 인터넷 뱅킹에 적용되어

〈표 7〉 국내 금융기관의 비밀번호 입력 및 훔쳐보기 방지 기술 도입 현황

솔루션	비밀번호 입력기술의 특징	적용사례	훔쳐보기	비 고
DAS	○비밀번호 입력 순서가 되면 숫자가 123...순으로 나타남 ○'안전모드'를 선택하면 무작위 순으로 나타남 ○비밀번호 입력할 때마다 숫자가 무작위 순으로 나타남	KJ은행 JJ은행	고려하여 안전함	보안적합상태 시험을 통과하였고, 오류 및 민원발생 살계가 없음
???	○일부 숫자는 순차적, 나머지는 무작위 순으로 나타남 ○숫자 하나를 입력할 때 무작위 순으로 나타남	KB은행 NH은행	고려하지 않음	먼 곳에서도 훔쳐보기 가능
Rhythm Pass[22]	○비밀번호 입력 순서가 되면 숫자가 123...순으로 나타남 ○'안전모드'를 선택하면 무작위 순으로 나타남 ○비밀번호 입력할 때 숫자가 123.., 789...., 순으로 나타남	EP은행 KE은행 SH은행	고려했으나 방지효과 없음	보안적합상태시험 통과하지 못함
VIS[15]	○비밀번호 입력 순서가 되면 숫자가 123..순으로 나타남 ○'안전모드'를 선택하면 세 개 모드가 나타남 ○세 번째 모드에 숫자가 무작위 순으로 나타남	JB은행	고려하여 안전함	민원이 발생하여 일부 지점에서 탐재 철수
Rhythm Pass[22]	○숫자들이 규칙적으로 나타남(상하좌우) ○번호 하나를 입력할 때 숫자들이 무작위 순으로 나타남	○○금고	고려했으나 방지효과 없음	보안적합상태시험 통과하지 못함

사용되고 있고, 다른 분야에서도 적용하기 위하여 관련 업체와 협의하고 있다.

한편, DAS는 비밀번호 입력기술로 사용자 인증을 하는 모든 곳에 적용 가능하다. 향후 DAS를 적용한 다른 제품을 구현하고자 한다.

참 고 문 헌

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

[2] 금융감독원, "영국의 인터넷뱅킹 관련 사기 피해 증가," 금융감독정보, 통권 396호, pp.43~44, Nov., 2006.

[3] Wikipedia, the free encyclopedia(http://en.wikipedia.org/wiki/PINpad).

[4] TTA(Telecommunications Technology Association), "Standard of Contact Type IC Card Terminal," Telecommunications Technology Association, 2003.

[5] C.Y. Han, H.W. Jang, "An Empirical Study on the Use of POS System for Inventory Efficiency," Journal of Korean Industrial Information Systems Society, Vol.10, No.1, pp.81-88, 2005.

[6] Jablon, P.D. "Strong password-only authenticated key exchange," ACM SIGCOMM Computer Communication Review, (26:5), pp.5-20, 1996.

[7] Halevi, S. and Krawczyk, H. "Public-key cryptography and password protocols," ACM Conference on Computer and Communications Security, pp.122-131, 1998.

[8] Bellovin, M.S. and Merrit, M. "Augmented encrypted key exchange: Password-based protocol secure against dictionary attack and password file compromise," Proceedings of the 1st ACM Conference on Computer and Communications Security, pp.244-250, 1993.

[9] Halevi, S. and Krawczyk, H. "Public-key cryptography and password protocols," ACM Conference on Computer and Communications Security, pp.122-131, 1998.

[10] 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.

[11] 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.

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

[13] Park, S.B., Kang, M.S. and Lee, S.J. "New authentication system," Lecture Notes in Computer Science, Vol.3032, pp.1095-1098, 2004.

[14] Park, S.B., Kang, M.S. and Lee, S.J. "User authentication protocol based on human memorable password and using ECC," Lecture Notes in Computer Science, Vol.3032, pp.1091-1094, 2004.

[15] 소리나무미디어, "일회용 비밀번호 생성 및 해석 방법," 대한민국 특허청, 2007. 01.

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

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

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

[19] 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.

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

[21] Edward K. Vogel & Maro G. Machizawa, "Neural activity predicts individual differences in visual working memory capacity," Nature, Vol.428, pp.748-151, 15 April, 2004.

[22] 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.

[23] S.B, Park, N.K. Joo, M.S. Kang, Practically Secure and Efficient Random Bit Generator Using Digital Fingerprint Image for the Source of Random, The KIPS Transactions: Part D, Vol.10-D, No.3, pp.541-146, 2003.

[24] (주)비원플러스, 리듬패스 & 참아이디, http://www.beone.co.kr/.

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, 컴포넌트기술, 정보보호관리, 인터넷 윤리

김 용 일

e-mail : yikim@honam.ac.kr

1984년 전남대학교 계산통계학과(이학사)

1986년 한국과학기술원 전산학과(공학석사)

2002년 전북대학교 전산통계학과(박사수료)

1994년~2000년 초당대학교 컴퓨터과학과 조교수

2002년~현 재 호남대학교 인터넷소프트웨어학과 조교수

관심분야 : 지능형 정보시스템, 멀티미디어 정보검색