정 보 보 호 학 회 지
제24권 제3호, 2014. 6

안전한 사용자 식별 번호 입력을 위한 사용자 인터페이스

이 문 규*

요 약

사용자 식별 번호(personal identification number: PIN)는 은행 계좌, 신용카드, 스마트폰, 도어락 등 다양한 응용에서 널리 활용되는 사용자 인증 수단이나, 전통적으로 사용되어 온 PIN 입력 방식은 PIN을 입력하는 과정을 어깨 너머로 지켜본 공격자가 이를 기억하여 그대로 입력에 사용하는 엿보기 공격 등 안전성에 많은 문제점을 가지고 있다. 본 고에서는 이러한 문제점을 해결하기 위한 그동안의 연구 결과들을 살펴보고, 향후 안전한 PIN 입력 방식의 연구에서 고려되어야 할 요소들을 도출한다.

Ⅰ. 서 론

사용자 식별 번호(personal identification number: 이하 PIN)[1]는 은행 계좌나 신용카드 승인용 비밀번호, 스마트폰 해제용 비밀번호, 도어락 개폐 비밀번호 등 다양한 용도로 사용되는 사용자 인증 수단이다. PIN이 은행 단말기에서 사용되기 시작한 것은 1967년 영국으로, 여섯 자리 10진수를 이용하는 Barclays-De La Rue 시스템과 네 자리 10진수를 이용하는 National- Chubb 시스템이 그 시초로 알려져 있다. 그러나 이후에 De La Rue 시스템 개발 팀의 리더였던 John Shepherd- Barron 이 자신의 아내가 여섯 자리 랜덤 10진수를 잘 기억하지 못하는 것을 확인한 후 PIN의 자리 수를 네 자리로 줄임으로써, 이후 대부분의 시스템에서는 10진수 네 자리로 구성된 PIN을 사용하게 되었다[1].

PIN은 사용자들에게 익숙하고 기억 및 입력이 크게 어렵지 않아 이미 위와 같은 다양한 분야에서 활용이 되고 있으나, PIN을 입력하는 과정을 어깨 너머로 지켜본 공격자가 이를 기억하여 그대로 입력에 사용하는 엿보기 공격(shoulder surfing attack)이 가능하다는 문제점이 있다. 특히 PIN이 공공장소에서 입력되는 경우가 많고, 대개의 사용자가 하나의 PIN으로 은행 계좌, 신용카드, 스마트폰 등 다수의 응용에 재활용하는 예도 많아, 실제 피해 사례가 다수 보고되고 있다. 또한 최근에는 스마트폰의 보급으로 누구나 동영상을 쉽게 촬영할 수 있으므로, 엿보기 공격의 진화된 형태인 촬영 공격(recording attack)이 가능하여 좀 더 강력한 방지 대책이 필요하게 되었다. 따라서 위와 같은 공격을 막기 위해 새로운 PIN 입력 방식을 개발하고자 하는 연구가 진행되고 있으나, 일부 방법들은 엿보기 공격의 방지에 치중한 나머지 무작위 추측 공격(random guessing attack)에 대한 저항성을 약화시키는 부작용도 존재한다. 사용자가 이러한 PIN 입력 방법을 사용할 경우, 공격자는 엿보기 또는 촬영 영상으로부터 PIN에 대한 많은 정보는 얻기 어려운 대신, 사전 정보 없이 PIN을 무작위로 추측하여 입력을 시도함으로써 1/10000보다 높은 확률로 성공할 수 있다. 따라서 엿보기 공격에 대한 방지는 무작위 추측 공격에 대한 저항성을 희생하지 않는 수준에서 실현되는 것이 바람직하다. 또한, 스마트폰과 같이 소프트웨어 설치가 가능한 상황에서는 공격자의 악성 소프트웨어에 의한 키 로깅 공격을, 사용자의 입력을 접촉식으로 받는 모든 환경에서는 사용자의 손

본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신) [과제번호 10039180], 미래창조과학부 및 정보통신산업진흥원의 대학 ICT연구센터육성지원사업 [과제번호 NIPA-2014-H0301-14-1010], 및 인하대학교의 지원으로 수행되었습니다.

* 인하대학교 컴퓨터정보공학과 (mklee@inha.ac.kr)

자국을 이용해 PIN을 재구성하는 공격을 고려하여야 한다.

본 고에서는 위와 같은 PIN에 대한 공격들을 막기 위한 다양한 방안들을 소개하고자 한다. 먼저 2장에서는 PIN에 대한 위협 상황을 좀더 정확히 정의하고, 3장에서는 이를 막기 위한 챌린지-응답(challenge- response) 기반 방법들을 소개한다. 4장에서는 소리나 진동 등 추가적인 채널들을 이용하는 방법들을 소개하고, 5장에서는 최근에 소개된 기타 방법들을 소개한다. 6장에서는 향후 안전한 PIN의 연구에서 고려되어야 할 조건들을 정리하고 결론을 맺는다.

Ⅱ. PIN에 대한 위협 분석[4]

PIN이 활용되는 상황을 일반화하면, (1) 특정 단말 또는 시스템에 로그인하기 위해 PIN의 정보를 입력하는 사용자, (2) 스마트폰이나 은행의 ATM 단말기 등 사용자로부터 인증 정보를 입력받아 사용자의 유효성을 테스트하는 인증자, (3) 정상적인 사용자가 아님에도 불구하고 시스템에 로그인하고자 하는 공격자로 구성됨을 알 수 있다. 결국, 사용자와 공격자 모두 최종 목표는 인증자의 테스트를 통과하여 시스템에 성공적으로 로그인하는 것이다. 다만, 사용자는 PIN에 대한 정보를 소유하고 있는 반면, 공격자는 PIN에 대한 전부 또는 일부의 정보를 활용, 정상적 사용자로 가장하여 테스트를 통과하는 것을 목표로 하며, 구체적인 공격의 유형은 아래와 같은 것들이 가능하다.

2.1. 무작위 추측 공격

무작위 추측 공격(random guessing attack)에서는 공격자가 사용자의 PIN을 무작위로 추측하여 인증을 시도한다. 일반적으로 PIN이나 비밀번호의 분포는 균일 분포가 아니므로[1,2,3], 공격자가 이 사실을 활용하면 추측 공격을 보다 효과적으로 수행할 수 있다. 그러나 여기에서는 문제를 단순화시키기 위해 일단 PIN의 분포가 균일하다고 가정하자. 보통 PIN 입력 실패 시 시스템이 블록되기 전 몇 번의 기회가 더 주어지는 것이 일반적이므로, PIN 입력 방법의 무작위 추측 공격에 대한 안전성을 다음과 같이 정의하자.

[정의 1][1,4]: M을 PIN 입력 방법이라 하자. M에 대한 추측 공격의 성공률 $P_{GA,n}(M)$은 공격자가 n회의 무작위 시도에 의해 M에 대한 PIN 입력 테스트를 통과할 확률이다.

[보조정리 1][4]: 모든 PIN 입력 방법 M에 대해, $P_{GA,n}(M) \le nP_{GA,1}(M)$.

예를 들어, 흔히 사용되는 regular PIN 패드(이하 REG)를 이용하여 PIN이 입력될 경우, 가능한 PIN의 종류는 10000가지이므로, 공격자가 PIN에 대한 사전 정보 없이 인증을 시도할 때에는
$P_{GA,1}(REG) = 1/10000$이고, 전형적인 은행단말기에서처럼 3회의 입력이 허용될 경우에는
$P_{GA,3}(REG) = 3/10000$이다.

2.2. 엿보기 공격 및 촬영 공격

엿보기 공격(shoulder surfing attack)에서는 공격자가 사용자의 PIN 입력 장면을 어깨너머로 관찰하여 PIN에 대한 일부 또는 전체 정보를 기억한 후 이를 인증에 활용하게 된다. 경우에 따라서는 동일한 PIN을 사용자가 입력하는 장면을 공격자가 여러 번 관찰할 수 있는 경우도 있는데, 예를 들어 은행단말기에서 1회 현금 인출 금액의 제한이 있으므로 더 많은 금액을 인출하기 위해 사용자가 인출을 여러 번 하는 경우, 스마트폰 사용자가 스마트폰의 잠김을 해제하기 위해 PIN을 입력하는 장면을 사용자와 가까운 관계인 사람이 여러 번 관찰하는 경우, 집 현관문의 비밀번호 입력 장면을 이웃에 사는 사람이 우연히 여러 번 관찰하는 경우 등이 그것이다. 공격자가 엿보기에 의해 PIN에 대한 완전한 정보를 얻은 경우, 공격자는 이 정보를 이용하여 인증에 성공할 수 있으며, 일부 정보만을 얻은 경우에는 일부 비어 있는 정보를 무작위로 추측하여 인증을 시도할 수도 있다. 따라서 PIN 입력 방법의 엿보기 공격에 대한 안전성을 다음과 같이 정의하자.

[정의 2][4]: M을 PIN 입력 방법이라 하자. M에 대한 엿보기 공격의 성공률 $P^{m}_{SSA,n}(M)$은 공격자가 m회의 사용자 인증 세션을 엿본 후 얻은 정보를 바탕으로 n회의 인증 시도로 M에 대한 PIN 입력 테스트를 통과할 확률이다.

만약 공격자가 촬영 장비를 보유한 경우, 사용자의

PIN 입력 세션을 녹화하여 이를 오프라인으로 분석함으로써 사람의 관찰 및 기억에 의존하는 것보다 PIN에 대한 더 많은 정보를 얻어낼 수도 있는데, 이와 같은 더 강력한 엿보기 공격을 촬영 공격(recording attack)이라 정의하고 이의 성공률 $P^{m}_{RA,n}(M)$을 $P^{m}_{SSA,n}(M)$와 유사하게 정의하자. 예를 들어, REG를 이용하여 PIN이 입력될 경우 공격자는 1회의 촬영만으로 완전한 PIN을 얻어낼 수 있으므로, $P^{1}_{RA,1}(REG)=1$이다.

2.3. 기타 공격

스마트폰이나 스마트패드 등 소프트웨어의 설치가 가능한 단말기에서는, 사용자가 인지하지 못한 상태에서 스파이웨어 등 공격자의 악성 소프트웨어가 설치되어 사용자의 입력을 얻어내는 것이 가능하다. 예를 들어 키 로깅에 의해 사용자의 PIN 입력 값을 직접 얻어내거나, 센서 정보의 조합으로 PIN 숫자들을 유추해내는 공격 등을 고려해볼 수 있다[5]. 또한, 스마트폰이나 스마트패드, 터치형 도어락 등 터치 인터페이스를 이용하면서 인증 시 특정 패턴만이 반복적으로 입력되는 개인 단말기에서는, 사용자의 PIN 입력 시 남는 손자국을 이미지 처리 기술을 이용하여 분석함으로써 PIN을 재구성해 내는 손자국 공격(smudge attack)[6]도 가능하다. 이러한 공격들도 현실적인 위협이 될 수 있으므로 이미 많은 연구가 진행되고 있으나[7,8], 본 고에서는 이들에 대한 구체적인 대응 방법들은 소개하지 않고 추측 공격과 엿보기 공격의 대응법을 기술하는 데 집중하기로 한다. 다만, 특히 손자국 공격에 대해서는 엿보기 공격의 대응법인 랜덤화 방안이 효과적인 방어법의 근간이 될 수 있으며, 이미 상용 도어락 제품에서 이러한 랜덤화 기술이 도입되고 있음을 언급한다[9]. 또한, 단순한 키 로깅으로 PIN을 재구성할 수 없게 하기 위해서는 역시 PIN 입력 세션마다 사용자의 입력 정보가 달라지는 랜덤화 방안이 효과적일 것이다.

Ⅲ. 챌린지-응답 기반 PIN 입력 방법

기존의 일반 PIN 패드 입력 방법이 엿보기 또는 촬영 공격에 취약한 것은 같은 PIN을 항상 같은 입력 방법으로 입력하기 때문이다. 따라서 대부분의 대응 기법들은 인증자가 무작위 챌린지(challenge)를 사용자에게 주고, 사용자가 이 챌린지에 본인이 기억하고 있는 PIN 정보를 조합하여 적절한 응답(response)을 생성하여 이를 인증자에게 전달하는 간접적인 입력 방법을 취하고 있다. 이렇게 되면 같은 PIN이라도 챌린지에 따라 올바른 응답이 달라지므로, 매번 사용자 입력을 다르게 하는 효과가 있다. 이러한 방법들은 일반적으로 사람의 단기기억(short-term memory)과 실시간 정보 처리 능력이 제한적이라는 사실을 적절히 활용하여 챌린지-응답의 생성 규칙을 설계한다. 즉, PIN을 알고 있는 사용자는 복잡한 계산 없이 간단히 응답을 만들어낼 수 있는 반면, PIN에 대한 사전 정보가 부족한 공격자는 챌린지-응답 정보를 관찰하더라도 이 정보를 실시간으로 처리하여 유용한 정보를 도출해 내기가 매우 어렵도록 PIN 입력 방법을 설계하는 것이다. 이 절에서는 이러한 설계 원칙에 입각하여 설계된 여러 PIN 입력 방법들을 소개한다. 다만, 이러한 대응 방법은 공격자가 별도의 녹화 장비를 사용하지 않고 본인의 실시간 관찰 및 단기기억에 의존할 때에만 효과적이며, 공격자가 녹화된 내용을 오프라인으로 분석할 수 있는 경우에는 안전성을 보장할 수 없다.

3.1. Binary 방법[10]

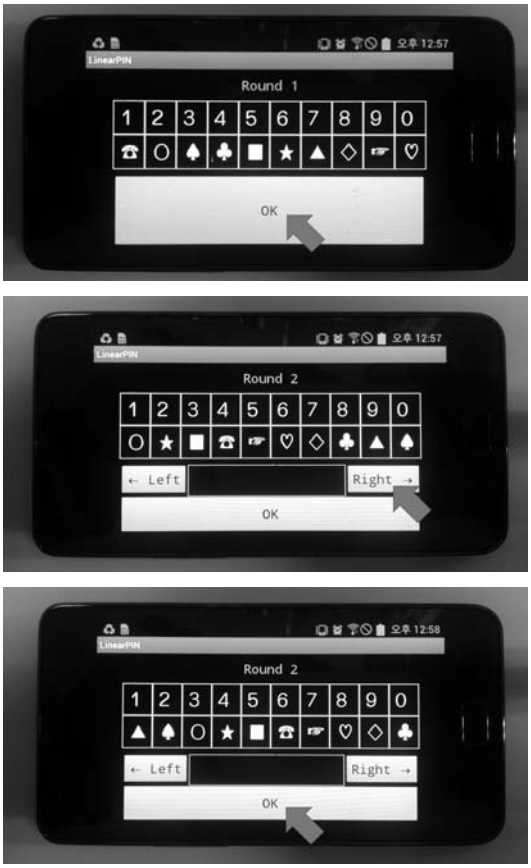
그림 1은 [10]에 소개된 binary 방법을 보여주고 있다. 인증자는 1부터 0까지 10개의 숫자들을 일반 PIN 패드와 같은 순서로 배열하되, 다섯 개는 흰색으로, 나머지 다섯 개는 검은 색으로 배경을 색칠하여 사용자에게 보여준다. 공격을 어렵게 하기 위해서 매 인증 시마다 검은 색이 칠해져야 할 숫자 다섯 개는 무작위로 결정된다. 사용자는 자신이 현재 단계에서 입력하고자 하는 숫자의 배경색을 인지한 후 아래쪽의 'Black' 또는 'White' 버튼 중 적절한 것을 입력한다. 하나의 PIN 숫자를 유일하게 결정하기 위해서는 네 단계가 필요하므로, 일반적으로 많이 쓰이는 네 자리 PIN 숫자를 입력하기 위해서는 위와 같은 작업을 16회 반복하여야 한다. 따라서 인증에 소요되는 시간이 약 20초 내외로 긴 문제가 있으며, 촬영 공격에 취약한 문제가 있다. 또한, 적절히 훈련된 공격자는 녹화 장비 없이 실시간 관찰만으로 PIN 번호의 일부 또는 전부를 복원하는 것이 가능하다[4,11]. [10]에서는 공격을 어렵게 하기 위해 네 단

계의 챌린지를 보여준 후 네 개의 응답을 한꺼번에 입력하게 하는 방법도 제시하고 있는데, 이는 [12]에서 제안된 챌린지와 응답에 시차를 두는 방법을 응용한 것이다. 다만 이 방법은 인증 시간이 더 증가되어 편의성을 감소시키는 문제가 있다. 한편, [11]에서는 흰색과 검은색 이외에도 다양한 색을 부여하는 등, [10]의 버튼 배치를 유지하면서 안전성을 개선하는 몇 가지 방법을 제시하였다.

〔그림 1〕 Binary 방법: '3'을 입력하기 위해 'White' 버튼을 누르는 모습〔10〕

3.2. LIN 방법[4]

[10]의 방법은 특히 공격자가 여러 번 엿보기를 반복할수록 안전성이 현저히 떨어지는 문제점이 존재하는데 [4], 그 이유는 PIN 입력의 각 단계가 이전 또는 이후 단계들과는 독립적으로 구성됨으로 인해 여러 번의 엿보기에서 관찰된 부분적인 정보들을 재조합하면 완전한 정보를 구성할 수 있기 때문이다. 이를 방지하기 위해서는 PIN 입력의 각 단계가 독립적으로 구성되지 않고 인접 단계들과 연관되도록 구성하는 것이 바람직하다. 그림 2는 이와 같은 관찰을 기반으로 설계된 LIN 방법[4]을 보여주고 있다. LIN 방법의 첫 라운드는 임시 세션키의 전달 단계로, 인증자는 먼저 1~0의 10개 숫자들 아래에 'O'나 '★' 등 익숙한 기호들을 무작위로 배치하는데, 사용자는 자신의 PIN 번호 첫 번째 숫자(그림의 경우에는 '2') 아래에 있는 기호를 세션키로 기억한 후 'OK' 버튼을 누른다. 2단계부터 4단계는 PIN의 두 번째부터 네 번째 자리 수를 이 세션키에 맞추어 입력하는 단계로서, 그림 2의 두 번째 그림과 같이 챌린지가 주어질 경우 'Left' 또는 'Right' 버튼을 적절히 눌러 세션키가 해당 단계의 PIN 숫자와 맞도록 이동시킨 후 'OK'를 눌러 입력하게 된다. 5단계는 선택사항으로, 다시 PIN의 첫 번째 자리 숫자를 세션키에 맞추어 같은 방법으로 입력하게 할 수 있다. [4]에서는 5단계를 배제한 방법을 LIN_4, 5단계까지 수행하는 방법을 LIN_5로 명명하고 있다. [4]에서는 비교 실험을 통해 Binary 방법보다 LIN 방법이 녹화 장비 없는 엿보기 공격에 대해 더 안전하며, 인증 시간도 절약되는 것을 확인하였다.

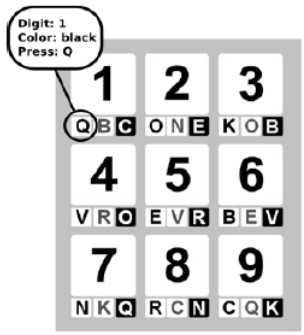


〔그림 2〕 LIN 방법: PIN이 '2371'일 때 PIN의 첫 자리 '2'로부터 랜덤 세션키 'O'을 인식하고 두 번째 라운드에서 PIN의 두 번째 자리 '3'에 세션키를 맞추어 입력하는 모습〔4〕

3.3. PIN 패드의 랜덤 재배치 방법[13]

[13]에서는 PIN 숫자를 직접 터치하여 입력하는 기본 PIN 패드의 입력 방법은 그대로 유지하되, PIN 패드 상의 1~0 숫자들의 배치는 인증 시마다 무작위로 재배치하는 방법을 제안하였다. 또한, 안전성을 강화하기 위해, 재배치된 숫자들은 사용자가 위치를 확인한 후 사라지게 하고 사용자는 본인이 입력하고자 하는 숫자가 있던 자리의 빈 버튼을 터치함으로써 간접적으로 숫자를 입력할 수 있게 하였다. 사용자는 입력하고자 하는 숫자 하나의 위치만을 기억하면 되지만, 공격자는 모든 10개 숫자의 무작위 위치들을 매번 기억해야 하므로 공격이 어려워질 것으로 기대할 수 있다. 다만, 촬영 공격에 대해서는 PIN 번호가 유일하게 결정되므로 취약하며, 녹화 장비 없는 엿보기 공격에 대한 안전성은 정량적으로 분석된 바는 없다.

3.4. ColorPIN[14]



〔그림 3〕 ColorPIN: '1(검정)'을 입력하기 위해 '1' 아래에 있는 검은색 글자 Q를 선택하는 모습〔14〕

경우에 따라서는 PIN의 정의를 바꾸면 안전성 또는 효율성을 향상시킬 수 있다. 예를 들어 [14]에서 제안된 ColorPIN은, PIN의 각 자리가 1~9 중 하나의 숫자와 검정, 빨강, 흰색 중 하나의 색깔의 순서쌍으로 구성되도록 PIN을 새로 정의하였다. 예를 들어 PIN은 '1(검정), 2(빨강), 3(흰색), 4(검정)'와 같이 정의되는데, 그림 3과 같은 챌린지가 주어질 경우 사용자는 자신의 첫 번째 PIN 숫자인 1의 아래쪽에 무작위로 주어진 세 글자들 중 자신의 첫 번째 PIN 색깔인 검정으로 칠해진 'Q'를 확인하여 이를 키패드 상에 입력하면 된다. 결국 PIN의 가능성은 10000개가 아닌 $(9\times 3)^4 = 531441$ 개로 늘어나게 되며, PIN 패드 상의 총 27개 글자들은 9개의 서로 다른 글자가 총 3회씩 나오도록 설계되었으므로, 무작위 추측 공격의 성공률은 $P_{GA,1}(ColorPIN) = 1/6561$이다. 또한, 촬영 공격을 1회 수행하더라도 공격자의 공격 성공률은 1이 아닌 $P^1_{RA,1}(ColorPIN) = 1/81$이다. 다만, 사용자가 인증을 위해 기억해야 할 정보가 더 많아지므로, 이 방법은 본질적으로 일반 PIN의 자리수를 늘리는 방법의 일종으로 간주할 수 있다.

또한, PIN의 정의를 바꿀 경우 기존 PIN과의 호환성 문제도 고려하여야 하는데[4], 안드로이드의 Pattern Lock과 같이 스마트폰의 잠금 해제를 위해 사용하는 경우 등은 새로운 형태의 PIN을 정의하는 것이 문제가 없으나, 은행 단말기에서의 인증과 같이 좀더 일반적인 응용에 적용하기에는 무리가 있다. 은행 계좌의 PIN의 형태를 바꾸게 되면 모든 은행 단말기와 PIN 패드의 물리적인 형태가 바뀌어야 하고, 여기에 연관된 소프트웨어들도 모두 업데이트가 되어야 한다. 더욱이, 기술적 변화에 익숙하지 않은 사용자들은 이러한 변화에 적응하기 어려워할 수도 있으므로, 보다 넓은 활용도를 갖기 위해서는 PIN 입력 방법은 PIN 정의 자체를 바꾸는 것보다는 PIN은 그대로 두되 입력 인터페이스만을 변경하는 것이 바람직하다. 이 경우, 예를 들어 은행단말기는 사용자로 하여금 전통적인 입력 방법을 쓸 것인지, 혹은 최근에 개발된 좀 더 안전한 입력 방법을 쓸 것인지를 선택하게 할 수 있을 것이다.

Ⅳ. 안전한 추가 채널을 이용한 PIN 입력 방법

4.1. 무작위 추측 공격과 촬영 공격의 관계

이 장에서는 먼저 2장에서 정의된 무작위 추측 공격과 엿보기 공격(촬영 공격)의 반비례 관계에 대해 알아보고자 한다. 이 장에서 제시하는 정리 및 증명은 [4]의 것을 그대로 가져온 것이다.

[정리 1][4]: PIN 입력 방법 M에 대한 모든 가능한 PIN의 집합을 S_M 이라 정의하고, 그 원소의 개수를 $|S_M|$이라 하자. 사용자의 PIN이 S_M 으로부터 균일하게 무작위로 선택된다고 가정하고, 공격자가 인증 세션의 모든 챌린지-응답을 관찰 및 기록 가능하다고 가정하면,

어떠한 PIN 입력 방법 M에 대해서도 $P_{GA,1}(M) \times P^1_{RA,1}(M) \geq 1/|S_M|$ 이 성립한다.

[증명] : 정상 사용자에 의해 수행된 PIN 입력 장면(챌린지 및 응답)을 공격자가 기록하였다고 가정하자. 공격자는 $|S_M|$ 가지의 가능성 중에서 올바른 PIN을 유추하려고 노력할 것이며, 이를 위한 가장 간단하면서도 강력한 방법은 시뮬레이션을 수행하는 것이다. 즉, S_M 내의 각 원소 s에 대해, s가 올바른 PIN이라 가정하고, 공격자는 자신이 획득했던 챌린지 및 응답이 s와 양립할 수 있는지를 확인한다. 즉, 공격자는 PIN이 s라고 가정하고, 본인이 인증자 입장이 되어 위의 챌린지를 제공한 후 사용자로부터 위의 응답이 돌아왔을 경우 이를 올바른 응답으로 받아들일 것인지를 결정하면 된다. 만약 받아들일 수 있다면, 이 s는 올바른 PIN의 후보가 될 수 있다. 이러한 시뮬레이션을 모든 가능한 s에 대해 반복하면, PIN의 후보 집합 C를 구성할 수 있다. 이 때 $P^1_{RA,1}(M) = 1/|C|$이다. 만약 촬영 공격을 방지하기 위해 하나의 챌린지-응답 쌍에 의해 PIN이 유일하게 결정되지 않도록 PIN 입력 방법을 설계하였다면 $|C| > 1$ 일 수 있음에 유의하자.

다음에는 무작위 추측 공격을 고려해 보자. 실제로는 C 내의 원소들 중 하나만이 올바른 PIN임에도 불구하고, C 내의 모든 원소들은 위에서 관찰된 챌린지들에 대해 위에서 관찰된 응답을 제시한 경우 인증에 성공했을 것이다. 따라서 이 세션에 대해 공격자가 촬영 공격이 아닌 무작위 추측 공격을 수행하였다면, 적어도 $|C|/|S_M|$의 확률로 성공할 것이다. 따라서 위 정리가 성립한다.

위의 정리는 추측 공격에 대한 안전성과 촬영 공격에 대한 안전성이 반비례 관계에 있음을 보여준다. 예를 들어 촬영 공격에 대한 안전성이 높아지도록 $|C|$의 값이 크게 PIN 입력 방법을 설계할 경우 추측 공격의 성공률은 높아지게 된다. 이에 대한 가능한 개선책 중 하나는 [15]에서 이미 제안된 대로 $|S_M|$을 크게 하는 것이지만, 앞에서 설명한 대로 사용자의 기억력의 한계나 호환성 문제 때문에 적용에 한계가 있다.

또 다른 해결 방법으로 고려할 수 있는 것은 위 정리의 가정을 피해가는 방법이다. 즉, '공격자가 인증 세션의 모든 챌린지-응답을 관찰 및 기록 가능하다'는 가정이 성립하지 않도록, 챌린지 또는 응답의 일부를 공격자가 관찰 불가능한 채널을 통해 전달하는 것이다. 이러한 방법은 이미 오래전부터 제안된 바 있는데, 예를 들어 사용자의 응시 지점을 카메라가 인식하여 간접적으로 응답을 입력받는 eye-gaze 방법[16], 심지어는 뇌파 기반의 BCI (brain-computer interface)를 이용하는 방법[17]도 실험되었다. 그러나 좀 더 현실적인 대안으로, 최근에는 대부분의 휴대용 단말에 탑재되어 있는 소리나 진동 채널을 활용하는 다양한 방법이 제안되었는데, [18], [19], [20], [21], [22], [23] 등이 그것이다. 본 고에서는 이러한 방법들 중 비교적 가장 최근에 제안되고 가장 실용적인 것으로 평가되는 두 가지 방법을 소개한다.

4.2. Phone Lock[24]

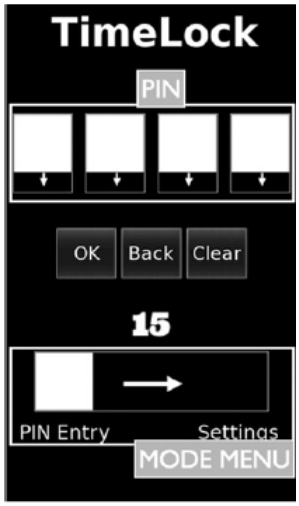
〔그림 4〕 Phone Lock〔24〕

Phone Lock[24]은 진동과 소리를 모두 활용할 수 있으나, 진동을 이용하는 버전은 소리 버전에 비해 편의성이 떨어지는 것으로 확인되었으므로, 소리를 이용하는 버전만 설명하기로 한다. Phone Lock의 화면 구성은 그림 4에서 보이는 것처럼 가운데의 작은 원 주변을 10개의 같은 크기의 영역들이 둘러싸는 모양으로 되어 있다. 사용자가 이 10개의 영역 중 임의의 영역을 터치하면, 인증자는 0부터 9 사이의 임의의 숫자, 즉 챌린지를

음성으로 들려준다. 예를 들어 화면에 보이는 반전된 영역을 터치하였을 때 '3'이라는 음성이 들렸다면, 원 주변의 인접 영역을 차례로 터치할 경우 '4', '5', '6' 등이 순차적으로 들리게 된다. 단, 반드시 인접 영역을 순차적으로 터치하여야 하는 것은 아니며 몇 개 영역을 건너뛰어 사용자가 원하는 영역의 소리를 듣는 것도 가능하다. 이동 중 목표가 되는, 즉 본인의 PIN 번호 숫자를 소리내는 영역에 도달하면, 사용자는 그 영역을 끌어 중앙의 원으로 옮긴 후 손가락을 뗌으로써 원하는 숫자의 입력을 수행하게 된다. 매 인증 시마다 숫자의 배치는 무작위로 바뀌게 되나, 숫자가 인접 영역을 지나면서 순차적으로 1씩 증가한다는 성질은 유지된다. 음성 챌린지가 안전하게 전달되기 위해서는, 사용자가 이어폰이나 헤드폰 등을 착용함으로써 공격자가 소리를 들을 수 없도록 하여야 한다. 이렇게 되면 공격자가 관찰하는 정보는 모양이 모두 같은 10개의 영역 중 하나를 사용자가 끌어다 중앙으로 옮겨놓는 것이 전부이므로, 인증을 여러 번 반복하여도 PIN의 정보가 유출되지 않는다. 진동을 이용할 경우에는, 진동의 강도를 적절히 조절함으로써 사용자는 진동을 느끼되 공격자는 진동 정보를 알 수 없게 함으로써 안전한 채널을 구성하게 된다. 따라서, 만약 네 자리 표준 PIN을 이용할 경우, 임의의 m에 대해 $P_{GA,1}(Phone\ \ Lock) = P^{m}_{RA,1}(Phone\ \ Lock) = 1/10000$ 임을 쉽게 알 수 있다.

4.3. Timelock[25]

그림 5에 보이는 Timelock[25]은 또 다른 방식으로 소리나 진동을 활용하는 방법으로, PIN 숫자를 직접 전달하는 것이 아닌, 일정 패턴의 소리나 진동을 여러 개 발생시킴으로써 이들을 일종의 카운터로 쓰는 방법이다. 이러한 신호들은 사용자가 버튼을 누르고 있는 동안 랜덤한 간격을 두고 안전한 채널을 통해 사용자에게 전달되며, 사용자가 버튼을 놓는 순간 그때까지 전달되었던 신호의 개수가 누적되어 PIN 숫자로 입력된다. 다만, 최악의 경우 10개의 신호가 전달되어야 하므로, 시간을 절약하기 위해 Timelock에서는 PIN 숫자들을 1, 2, ..., 5로 한정하고, 대신 네 개의 버튼을 누르는 순서를 PIN의 일부로 정의하였다. Phone Lock과 달리 진동이나 소리로 단순한 신호들만을 전달하므로, Timelock은 진동 버전과 소리 버전의 성능 차이는 크지 않은 것으로 확인되었다[25].



〔그림 5〕 Timelock〔25〕

Ⅴ. 기타 PIN 입력 방법

앞의 3장 및 4장에서 소개된 것 이외에도, 독특한 아이디어를 활용한 다양한 PIN 또는 패스워드 입력 방법이 존재하는데, 이 장에서는 그 중 몇 가지만을 소개하고자 한다. 먼저, [26]은 단말기의 뒷면에 있는 터치 패널을 이용함으로써, 사용자 쪽에서 엿보기 공격을 하는 공격자를 무력화시키는 방법이다. 또한 [27]은 사용자가 인증을 수행하는 손 이외의 또 다른 손으로 단말기의 화면을 효과적으로 가리게 하여 챌린지 및 응답을 공격자가 관찰하기 어렵게 하는 방법이다. 또한, 가짜 커서를 활용하는 [28]의 방법은, 터치 인터페이스가 아닌 마우스 등 포인터 인터페이스를 사용할 때, 실제 포인터 커서 이외에 가짜 커서들을 화면에 다수 배치함으로써 공격자가 사용자 입력을 추적하기 어렵게 만드는 방법이다.

Ⅵ. 향후 연구를 위한 제안

이 장에서는 앞에서 소개된 몇 가지 PIN 입력 방법들의 특성을 비교하고, 안전하고 효율적인 PIN 입력 방법이 가져야 할 바람직한 특성을 정리하고자 한다. 먼저, 앞서 살펴본 PIN 입력 방법들로부터, 다음과 같이 PIN 입력 방법에 대한 일반적인 요구사항을 도출할 수 있다.

(1) 안전성: 엿보기(촬영) 공격, 무작위 추측 공격 등에 안전하여야 하며, 기타 키 로깅이나 손자국 공격에 대한 저항성을 가지는 것이 바람직하다.
(2) 편의성: PIN 입력 방식은 가능하면 직관적이고 간단하게 설계되어 인증 소요 시간은 가능하면 짧게, 정상 사용자의 인증 오류율은 가능하면 낮게 유지되어야 한다.
(3) 호환성: PIN 입력 방식이 범용으로 활용되기 위해서는 기존의 PIN 정의를 바꾸지 않고 입력 인터페이스만을 변경하여 호환성을 유지하는 것이 바람직하다. 다만, 도어락이나 스마트폰 등 한정된 응용에서만 사용한다면 PIN을 재정의하는 것도 무방하다.
(4) 경제성: eye-gaze, BCI 등 고가의 장비를 이용하는 것은 바람직하지 않으며, 대부분의 시스템 또는 단말에 구비된 인터페이스만으로 구현되는 것이 바람직하다.

〔표 1〕 PIN 입력 방법 비교

방법	별도 채널	호환성	편의성	안전성	
				$P_{GA,1}$	$P^1_{RA,1}$
REG	×	○	상	1/10000	1
Binary[10]	×	○	하	1/10000	1
LIN_4[4]	×	○	중	1/1000	1/10
LIN_5[4]	×	○	중	1/10000	1
ColorPIN[14]	×	×	중	1/6561	1/81
Phone Lock[24]	○	○	중/하	1/10000	1/10000
Timelock[25]	○	×	중/하	1/15000	1/625

표 1은 위의 기준에 입각하여 각 PIN 입력 방법들의 특성을 비교한 것이다. 표에 의하면, Phone Lock과 Timelock은 진동, 소리 등 별도 채널을 이용하여 두 가지 안전성 요소를 모두 높은 수준으로 유지할 수 있는 반면, 별도 채널을 활용하지 않는 나머지 방법들은 $P_{GA,1} \times P^1_{RA,1} = 1/|S_M|$ 이 성립함을 확인할 수 있다. 다만, 현재까지 개발된 별도 채널 이용 방법들은 편의성이 다소 떨어지는 것이 문제점으로 지적되고 있다. 표에서 보이듯, 현재의 방법들은 위의 기준들을 모두 만족하고 있지 못하므로, 이를 개선하기 위한 지속적인 연구가 필요하다.

참 고 문 헌

[1] J. Bonneau, S. Preibusch, and R. Anderson, “A birthday present every eleven wallets? The security of customer-chosen banking PINs,” in Financial Cryptography (LNCS),New York, NY, USA: Springer-Verlag, 2012, pp. 25-40.

[2] M. G. Kuhn. (1997). Probability Theory for Pickpockets, ee-PIN Guessing [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/

[3] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes,” in Proc. 13th Conf. USENIX Security Symp., 2004, pp. 151-164.

[4] M-K. Lee, “Security notions and advanced method for human shoulder-surfing resistant PIN-entry,“ IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp.695-708, April 2014.

[5] L. Cai, H. Chen, “TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion,” HotSec 2011, 6th USENIX Workshop on Hot Topics in Security, 2011.

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens,” in Proc. 4th USENIX Conf. Offensive Technol. WOOT, 2010, article 1-7, pp.1-10.

[7] E. von Zezschwitz, A. Koslow, A. D. Luca, and H. Hussmann, “Making graphic-based authentication secure against smudge attacks,” in Proc. IUI, 2013, pp. 277-286

[8] T. Kwon, S. Na, "TinyLock: Affordable Defense Against Smudge Attacks on Smartphone Pattern Lock Systems," Computers & Security, 42, pp. 137-150, May 2014.

[9] 삼성 SDS 스마트 도어락, http://www.samsungkey.co.kr/

[10] V. Roth, K. Richter, and R. Freidinger, “A PIN-entry method resilient against shoulder surfing,” in Proc. CCS, 2004, pp. 236-245.

[11] T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Trans. Syst.,

Man, Cybern., Syst., 44(6), pp. 716-727, June 2014.

[12] D. S. Tan, P. Keyani, and M. Czerwinski, “Spy-resistant keyboard: More secure password entry on public touch screen displays,” in Proc. 17th Austral. Conf. Comput. Human Interaction OZCHI, 2005, pp. 1-10.

[13] 박승배, 관찰자에게 입력정보가 노출되는 것을 방지할 수 있는 정보입력방법, 대한민국 특허 제 10-0743854호, 2007.

[14] A. D. Luca, K. Hertzschuch, and H. Hussmann, “ColorPIN: Securing PIN entry through indirect input,” in Proc. CHI, 2010, pp. 1103-1106.

[15] Q. Yan, J. Han, Y. Li, and R. H. Deng, “On limitations of designing leakage-resilient password systems: Attacks, principles and usability,” in Proc. NDSS, 2012, pp. 50-58.

[16] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, “Reducing shoulder- surfing by using gaze-based password entry,” in Proc. SOUPS, 2007, pp. 13-19.

[17] J. Thorpe, P. van Oorschot, and A. Somayaji, “Pass-thoughts: Authentication with our minds,” in Proc. NSPW, 2005, pp.45-56.

[18] H. Sasamoto, N. Christin, and E. Hyashi, “Undercover: Authentication usable in front of prying eyes,” in Proc. CHI, 2008, pp. 183-192.

[19] A. D. Luca, E. von Zezschwitz, and H. HuBmann, “Vibrapass: Secure authentication based on shared lies,” in Proc. CHI, 2009, pp.913-916.

[20] T. Perković, M. Čagalj, and N. Rakić, “SSSL: Shoulder surfing safe login,” in Proc Int. Conf. Softw., Telecommun. Comput. Netw., 2009, pp. 270-275.

[21] A. Bianchi, I. Oakley, J. K. Lee, and D.-S. Kwon, “The haptic wheel: Design & evaluation of a tactile password system,” in Proc. CHI, 2010, pp.3625-3630.

[22] A. Bianchi, I. Oakley, and D.-S.Kwon, “The secure haptic keypad: A tactile password system,” in Proc. CHI, 2010, pp. 1089-1092.

[23] A. Bianchi, I. Oakley, and D.-S. Kwon, “Spinlock: A single-cue haptic and audio PIN input technique for authentication, ” in HAID (LNCS). New York, NY, USA: Springer-Verlag, 2011, pp. 81-90.

[24] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, “The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices,” in Proc. TEI, 2011, pp. 197–200.

[25] A. Bianchi, I. Oakley, and D.-S. Kwon, “Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry, Interact. Comput., vol. 24, no. 5, pp. 409-422, 2012.

[26] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, et al., “Back-of-device authentication on smartphones,” in Proc. CHI, 2013, pp. 2389-2398.

[27] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, “Designing leakage resilient password entry on touchscreen mobile devices,” in Proc. ASIACCS, 2013, pp. 37-48.

[28] A. D. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, “Using fake cursors to secure on-screen passwordentry,” in Proc. CHI, 2013, pp.2399-2402.

〈저자소개〉

이 문 규 (Mun-Kyu Lee)
종신회원

1996년 2월 : 서울대학교 컴퓨터공학과 졸업
1998년 2월 : 서울대학교 컴퓨터공학과 석사
2003년 8월: 서울대학교 전기,컴퓨터공학부 박사
2003년 8월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재 : 인하대학교 컴퓨터정보공학과 부교수
관심분야 : 정보보호, 암호, 계산이론