어깨너머 공격에 강한 PIN과 패턴 이미지 기반의 사용자 인증 방법

김영삼[*,**], 김수형[**], 진승헌[*,**]
[*]과학기술연합대학원대학교 정보보호공학과
[**]한국전자통신연구원 인증기술연구팀
e-mail:kim03, lifewsky, jinsh@etri.re.kr

Shoulder-Surfing Resistant User Authentication Method Based on PIN and Pattern Image

Young-Sam Kim[*,**], Soo-Hyung Kim[**], Seung-Hun Jin[*,**]
[*]Dept of Information Security Engineering, University of Science and Technology
[**]Authentication Research Team, ETRI

요 약

모바일 기기나 ATM에서의 사용자 인증에는 PIN(Personal Identification Number)이 주로 사용된다. 그 이유는, PIN은 사용자가 외우기 쉽고 단순한 UI(User Interface)로 구현이 가능하다는 장점이 있기 때문이다. 하지만 PIN은 어깨너머 공격에 취약하다는 단점이 있다. 기존의 연구들은 이미지 기반, 인식 기반, PIN과 이미지의 혼합방식을 이용한 다양한 사용자 인증 방법들을 제안하였다. 하지만 이들 연구는 모바일의 작은 화면을 고려하지 않아 구현이 어렵거나, 어깨너머 공격에 취약하거나, 사용자에게 기억에 대한 부담을 증가시키는 등의 문제점이 있다. 본 논문에서는 PIN과 패턴 이미지를 결합하여 모바일 기기에 적합하면서, 어깨너머 공격에 대해 기존의 방법들에 비해 안전하고 사용자가 외워야 하는 기호(숫자, 이미지 등)가 적은 사용자 인증 방법을 제안한다.

1. 서론

PIN을 이용한 사용자 인증은 단순한 프로토로로 인하여 구현이 용이하고, 사용자가 기억해야할 기호(숫자, 문자, 이미지 등)의 길이가 짧아서 현재 휴대폰이나 ATM 등의 기기에서 널리 사용되고 있다.

하지만 PIN을 이용한 사용자 인증은 어깨너머 공격에 취약하다. 어깨너머 공격이란 육안을 이용하거나, 카메라, 비디오 카메라 등을 이용하여 사용자 기기를 훔쳐보는 것을 말하는데, 이 공격을 통해 공격자는 사용자의 PIN을 알아낼 수 있고 사용자 인증을 통과할 수 있다.

어깨너머 공격을 막기 위해서는 사용자가 어떤 PIN을 입력하는지 공격자가 알 수 없도록 만들어야 한다. 어깨너머 공격은 단순히 기기를 가리거나 PIN 길이를 늘리는 것으로 어느 정도 해결할 수는 있지만, 사용자의 부주의나 기억력의 한계로 인해 실용적인 해결책은 아니라고 할 수 있다.

본 논문에서는 PIN길이를 늘리지 않고 하나의 기호만을 추가적으로 사용하여 어깨너머 공격을 효과적으로 막을 수 있는 사용자 인증 방법을 제안한다. 그리고 제안하는 방법이 어깨너머 공격에 대해 어느 정도의 안전성을 가지는지 분석한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 어깨너머 공격의 정의를 내리고 공격 능력에 따라 공격자를 분류하였다. 그리고 3장에서는 어깨너머 공격에 안전한 기존의 사용자 인증 방법들을 조사하고 분석하였다. 4장에서는 제안하는 사용자 인증방법을 설명하였고, 5장에서 제안한 방법의 안전성을 검증하였다. 그리고 6장에서는 제안하는 사용자 인증방법에 대한 사용성 및 안전성 측면에서의 결론을 내렸다.

2. 어깨너머 공격의 정의 및 공격자 분류

어깨너머 공격은 사용자의 기기를 훔쳐봄으로써 사용자의 PIN을 알아내는 공격방법이다.[3] 어깨너머 공격을 하는 공격자는 시각적 능력과 기억 능력에 따라 표 1과 같이 나눌 수 있다.

일반인은 본의와 상관없이 또는 단순한 호기심에 어깨너머 공격을 하는 사람이다. 이들은 공격범위가 좁고 공격을 통해 얻은 정보를 가공하는 속도가 느리며, 정보의 저장 시간도 짧아 공격능력이 가장 적다.

초보공격자부터 고급공격자까지는 공격의 의도를 명확하게 드러내는 사람들이다. 먼저, 초보공격자는 종이와 펜을 사용하여 기억능력을 향상시킨 사람이다. 하지만 이들은 처리시간이 길기 때문에 복잡한 계산(본 논문에서는 확률을 이용한 공격을 말한다.)을 하기는 어렵다. 다음으로, 중급공격자는 비디오 카메라를 이용하여 초급공격자에 비해 시각적 능력을 향상시킴으로써 공격범위를 넓혔으며, 컴퓨터를 이용하여 획득한 정보를 빠르고 정확하게 처리할 수 있다. 마지막으로 고급공격자는 스파이웨어를 이용

<표 1> 공격능력에 따른 공격자의 분류

공격자	시각적 능력	기억 능력	처리 능력
일반인	육안	뇌	뇌
초보공격자	육안	종이와 펜	뇌
중급공격자	비디오 카메라	컴퓨터	컴퓨터
고급공격자	스파이웨어	컴퓨터	컴퓨터

하여 중급공격자에 비해 시각적 능력을 향상시킨 사람이다. 고급공격자는 시간과 장소에 구애받지 않고 원하는 기기의 정보를 여러 번에 걸쳐 정확하게 획득할 수 있다.

3. 관련 연구

가장 단순한 사용자 인증 방식은 키패드를 이용하여 PIN을 직접 입력하는 것이다. 이는 표 1의 일반인조차도 쉽게 PIN을 획득할 수 있어 매우 취약한 방법이다.

이러한 어깨너머 공격을 막을 수 있는 방법을 제안한 연구들은 S3PAS(Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentiation Scheme)[5], CHC(Convex Hull Click)[3], Cognitive Authentication[2], PIN-Entry[1], fakePointer[6]가 있다.

먼저 S3PAS는 패스워드 기반의 사용자 인증 방법으로서 패스워드를 직접 입력하지 않고 패스워드를 통해 생성될 수 있는 삼각형을 이용하여 세션 패스워드를 입력하도록 한다. 패스워드를 알고 있는 사용자만이 마음속으로 삼각형을 그릴 수 있으며, 삼각형 내의 문자를 클릭할 수 있다. S3PAS는 화면에 한 번에 표시할 수 있는 문자가 많아질수록 공격자가 패스워드를 유추해내는 것이 어려워진다. 하지만 이를 PIN에 적용하는 경우는 문제가 발생하게 된다. 숫자패드에서 그릴 수 있는 삼각형의 종류는 120가지이지만 삼각형의 내부에 최소한 하나의 숫자가 있어야만 세션 PIN값을 선택할 수 있게 된다. 또한 PIN에 중복된 숫자가 있을 경우도 삼각형을 그릴 수 없다. 이를 해결하기 위해서는 해당 PIN값을 사용하지 못하도록 해야 하는데 이는 PIN의 공간(전체집합)을 줄이는 결과를 가져와 안전성에 문제가 발생하게 된다.

두 번째로, CHC는 S3PAS와 비슷한 형식을 취하고 있으나 패스워드 대신 이미지를 기억하도록 하며 삼각형 대신 볼록 다각형(Convex Hull)을 사용한다. 하지만 CHC도 PIN에 적용하면 S3PAS와 같은 문제가 발생한다.

세 번째로, Cognitive Authentication(COA)은 이미지에 대한 인식(Cognition)을 바탕으로 인증을 한다. COA는 사용자에게 N개의 이미지 중에 M개를 선택하도록 하고, N+M개 중 임의의 이미지를 선택하여 배열한 화면을 보여준다. 사용자는 화면의 왼쪽 상단의 이미지부터 시작하여 자신이 선택했던 이미지이면 아래로, 선택했던 이미지가 아니면 오른쪽으로 이동한다. 화면의 가장 오른쪽 열과 가장 아래쪽 행에는 0 ~ P-1까지의 숫자가 랜덤하게 배열되어 있으며 사용자는 도착한 곳의 숫자를 세션 패스워드로 선택하게 된다. COA는 이 과정을 k번 반복함으로써 $1 - (1/P)^k$의 확률로 사용자를 인증하게 된다. 그러나 M의 크기가 화면에 표현할 수 있는 이미지의 수보다 작을 경우 k번의 세션패스워드 선택과정을 통해, M개의 선택된 이미지를 알아낼 수 있다. 이는 중급공격자 능력 수준에서 가능하다.

하지만 N과 M의 크기를 늘려서 화면에 보여지는 이미지를 지속적으로 바꿀 수 있다면 고급공격자라도 공격에 성공할 수 없다. 왜냐하면, 공격자가 임의의 $B \subset M$ 를 알아내더라도 다음번 인증에서는 새로운 $B' \subset M$이 화면에 나타날 것이기 때문이다. 그러나 N과 M의 크기를 늘린다는 것은 사용자의 인식 능력을 훈련하는 시간도 증가한다는 것을 의미하므로 현실적인 한계를 가진다.

네 번째로 PIN-Entry는 COA와 같이 인식기반이며, 이때의 인식은 PIN이 특정 집합에 속하는지 아닌지에 대한 것이다. 기기는 PIN과 색깔을 이용하여 화면을 구성한다(그림1). 그리고 사용자에게 검은색과 흰색 중에 어느 집합에 PIN이 속하는지를 물어보게 된다. 이는 베르누이 확률분포를 따르기 때문에 한 번의 질문에 1/2의 확률로 사용자가 PIN을 알고 있음을 인증할 수 있으며 이는 $\log_2|A|$(|A|는 PIN의 알파벳 종류)번 반복된다.

하지만 PIN-Entry는 중급공격자에게 어깨너머 공격을 쉽게 허용한다. 이는 하나의 집합의 크기가 PIN의 알파벳 집합 크기보다 작기 때문에 가능하다. 예를 들면, PIN이 숫자이고 첫 번째 알파벳이 6인 경우 네 번의 질문이 실행된다. 중급공격자가 각각의 질문과 답변을 수집하였고, 이 때 집합의 원소들이 각각 S_1 = (4,5,6,7,8), S_2 = (2,3,6,8,9), S_3 = (1,2,6,7,9), S_4 = (1,2,3,4,6)이라고 하자. 이 네 개의 집합에서 PIN의 첫 번째 알파벳인 6이 모두 발견될 확률은 1며, 그 이외의 알파벳들은 $(4/10)^4$의 확률로 나타나게 된다(집합의 원소들은 랜덤하게 선택된다). 따라서 공격자는 PIN을 구별해낼 수 있게 된다.

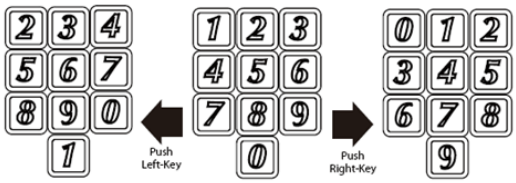
마지막으로, fakePointer는 PIN과 PIN의 길이에 맞는 이미지를 이용하여 사용자를 인증한다. 예를 들어, 네 자리 PIN일 경우 사용자는 네 개의 이미지를 외워야 한다. fakePointer의 PIN입력 방식은 PIN값의 각 자리를 이미지와 겹치도록 위치시킴으로써 이루어지며, PIN값의 위치 이동은 그림 2와 같이 이루어진다.

fakePointer는 중급공격자로부터의 공격에 대해 1/5040의 안전성을 가지며, 고급공격자로부터는 어깨너머 공격이 반복됨에 따라 안전성이 감소하게 된다. 이에 대해서는 5장에서 자세히 알아보도록 한다.

4. PIN-패턴이미지 기반의 사용자 인증 방법

본 논문에서 제안하는 사용자 인증 방법은 PIN과 하나의 패턴이미지를 조합하여 fakePointer와 같은 안전성을 가지며 사용자의 기억부담을 줄일 수 있다.

(그림 1)
PIN-Entry의
사용자 인증 화면



(그림 2) fakePointer의 숫자 이동

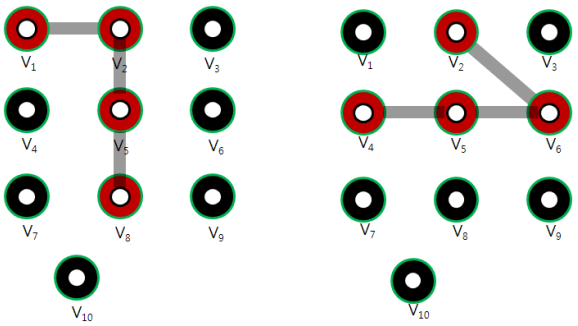
4.1. PIN-패턴이미지-패턴방향을 이용한 사용자 인증

제안하는 방법은 다음과 같다. 먼저 사용자는 하나의 PIN P와 패턴 V(그림 3)를 기기에 안전하게 등록하였다고 가정한다. 그리고 P의 길이는 k이며 각각의 자리를 P_i, i = 1,...,k라고 하고 V의 정점의 개수는 k와 같으며 각각의 정점을 V_i, i = 1,...,k라고 하자.

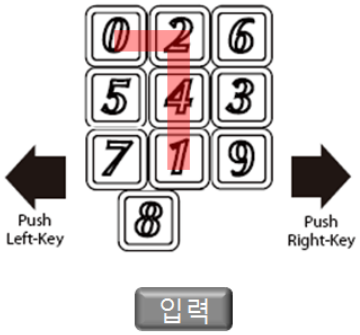
사용자 인증과정은 Challenge-Response방식을 따르며 UI는 그림 4와 같다.(그림 4의 패턴은 사용자에게 보이지 않는다.) 이제 사용자는 인증을 위해 P_i를 k번에 걸쳐 입력한다. 각각의 입력은 P_i를 V_i에 위치시킴으로써 이루어진다. 예를 들어 P가 2956이고 패턴이 그림 3의 왼쪽과 같고 그림 4와 같은 숫자배열이 화면에 나타났다고 하자. 그러면 사용자는 먼저 패턴을 떠올려 숫자패드에 겹쳐놓는다. P_1인 2를 입력하기 위해, 사용자는 왼쪽 화살표를 한번 누름으로써 2를 V_1에 위치시킬 수 있으며 "입력" 버튼을 눌러서 입력한다. "입력" 버튼을 누르면 숫자패드는 임의로 재배열 되며 같은 방식으로 P_2를 V_2, P_3를 V_3, P_4를 V_4에 위치시키고 "입력" 버튼을 눌러 PIN입력을 완료한다. 기기는 이를 바탕으로 PIN을 올바르게 검증할 수 있다.

4.2. PIN-패턴이미지 기반의 사용자 인증

4.1.에서 제안한 방법은 패턴이 그림 3의 오른쪽과 같을 경우 모호해질 수 있다. 만약 사용자가 자신이 입력한 패턴의 방향을 기억하지 못하고 이미지만을 기억할 경우 패턴의 시작점을 알 수 없게 되기 때문이다. 만약 제안하는 사용자 인증에서 패턴의 방향을 고려하지 않는다면 시작점과 끝점의 위치는 기억할 필요가 없으며, 따라서 사용성이 증가한다. 하지만, 이는 시작점과 끝점이 다른 두 패턴을 같다고 인정하는 것이기 때문에 안전성은 1/2로 감소하게 된다. 이러한 상충관계(trade-off)는 응용의 요구사항에 따라 조절될 수 있다.



(그림 3) k=4인 패턴의 예



(그림 4) 제안하는 PIN 입력 방법

5. 안전성

이번 장에서는 4.1.절에서 제안한 사용자 인증방법의 안전성을 2장에서 분류한 공격자유형에 따라 분석하도록 한다.

5.1. 일반인

제안하는 사용자 인증 방법은 일반인에게 임의의 난수 화면만을 제공한다. 일반인은 난수배열을 기억하기 어려우며, "입력" 버튼을 누르는 시점에 어느 숫자가 입력되었는지도 알 수 없다.

따라서 일반인이 제안하는 인증을 통과하기 위해서는 랜덤하게 입력을 할 수밖에 없다. 이를 "랜덤입력"이라고 하자. 일반인이 임의로 입력한 숫자는 패턴의 각 정점과 일치해야 하며 각각의 확률은 1/10이며, 모든 PIN을 입력하는 경우 인증을 통과할 확률은 $(1/10)^k$이다. 이는 k자리 PIN의 안전성과 같다.

5.2. 초보공격자

제안하는 사용자 인증 방법은 초보공격자에게 임의의 난수 화면만을 제공한다. 초보공격자가 얻을 수 있는 정보

는 일반인과 크게 다르지 않다. 단 초보공격자는 보조기억매체인 종이와 펜이 있기 때문에 사용자가 입력하는 시점의 숫자배열을 얻을 확률이 있다. 하지만 입력시의 숫자배열은 랜덤하기 때문에 이로부터 얻을 수 있는 정보는 거의 없다. 따라서 초보공격자도 랜덤입력을 통한 인증통과가 최선의 공격방법이다.

5.3. 중급공격자

중급공격자는 사용자의 인증화면을 명확하게 기록하여 분석할 수 있다. 또한 컴퓨터를 이용하여 여러 가지 확률공격이 가능하다. 중급공격자는 먼저 길이가 k인 모든 정점 $\{V_n|0<n<{}_{10}P_k\}$를 조사한다. 그리고 사용자의 입력화면과 비교하여 각 패턴별로 PIN의 후보를 생성한다. 예를 들어 k가 4일 경우 PIN의 후보는 5040가지가 나오게 된다. 공격자는 이 중 하나를 랜덤하게 선택하여 인증을 통과할 수 있다.

3장에서 살펴본 fakePointer의 경우도 이와 같은 공격이 가능하며, 따라서 제안하는 방안과 같은 안전성을 갖는다. 이는 사용자 인증 횟수의 제한으로 간단히 제어할만한 수준이기 때문에 안전하다고 할 수 있다.

5.4. 고급공격자

고급공격자는 사용자의 인증화면을 명확하게 그리고 여러 번 획득하여 분석할 수 있다. 그리고 고급공격자는 각각의 사용자 인증에 대해 중급공격자와 같은 분석을 시도할 수 있다. 만약 고급공격자가 중급공격자와 같은 패턴별 PIN 후보 집합을 m개 가지고 있다면, 실제 PIN이 m개의 PIN 후보 집합에 모두 나타날 확률은 1 인 반면, PIN이 아닌 나머지 숫자가 m개의 PIN 후보 리스트에 모두 나타날 확률은 $({}_{10}P_k/10^k)^m$,m>1 이다.(기존의 fakePointer 역시 같은 안전성을 갖는다.)

결론적으로, 제안하는 방안은 다수의 어깨너머 공격이 가능한 고급공격자로부터 안전하지 못하다. 제안하는 방안이 고급공격자로부터 안전하기 위해서는 일정 횟수마다 사용자의 PIN을 변경하도록 해야 한다.

<표 2> 어깨너머 공격에 대한 fakePointer와 제안 방안의 안전성 비교(k는 PIN의 길이, m은 공격 횟수)

	fakePointer	제안방안
일반인	10^{-k}	10^{-k}
초급공격자	10^{-k}	10^{-k}
중급공격자	$({}_{10}P_k)^{-1}$	$({}_{10}P_k)^{-1}$
고급공격자	$({}_{10}P_k/10^k)^{-m}$	$({}_{10}P_k/10^k)^{-m}$

<표 3> fakePointer와 제안 방안에서 사용자가 기억해야할 기호(symbol) 비교

	fakePointer	제안방안
기호	k자리의 PIN + k개의 이미지	k자리의 PIN + k 길이의 패턴

6. 결론

본 논문에서는 PIN과 패턴이미지를 기반으로 하여 사용자를 인증하는 방법을 제안하였다. 제안하는 방법은 현재 널리 사용되고 있는 PIN기반 인증 시스템의 변경을 최소화하면서 어깨너머 공격에 대응할 수 있다. 또한 제안한 사용자 인증 방법은 PIN과 하나의 패턴이미지만을 사용함으로써 기존에 어깨너머 공격을 막기 위해 제안된 방법들에 비해 사용자의 기억부담을 줄였다.

하지만 제안하는 사용자 인증 방법은 다수의 어깨너머 공격에는 취약하다. 이에 대한 해결방법은 PIN을 자주 변경해주는 것인데 이는 현실적이지 못하다. 향후에는 고급공격자의 공격에도 안전하고 사용성도 고려한 사용자 인증 방법에 대해 연구할 필요가 있다.

참고문헌

[1] Volker Roth, Kai Richter, and Rene Freidinger, “A PIN-Entry Method Resilient Against Shoulder Surfing", Proceedings of the 11th ACM conference on Computer and communications security, Washington DC, USA, 2004, pp. 236-245.

[2] Daphna Weinshall, "Cognitive Authentication Schemes Safe Against Spyware", Proceedings of the 2006 IEEE Symposium on Security and Privacy, 2006, pp. 295-300.

[3] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Briget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme“, Proceedings of the working conference on Advanced visual interfaces, Venezia, Italy, 2006, pp. 177-184.

[4] M. N. Doja, and Naveen Kumar, "User Authentication Schemes for Mobile and Handheld Devices", 2007.

[5] Huanyu Zhao, and Xiaolin Li, "S3PAS: Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st International Conference on Advanced Information Networking and Applications Workshops, Ontario, Canada, pp. 467-472.

[6] Tetsuji Takada, "fakePointer: A User Authentication Scheme that Makes Peeping Attack with a Video Camera Hard", Proceedings of the 2008 The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008, pp. 395-400.