훔쳐보기 공격에 강인한 비밀번호 방식

성진택*

목포대학교

A Password Method Resistant to Shoulder Surfing Attacks

Jin-Taek Seong*

Mokpo National University

E-mail : jtseong@mnu.ac.kr

요 약

기존에 주로 사용된 잠금장치는 PIN 방식으로서 악의적인 사용자에 의해 비밀번호가 노출되는 문제를 갖고 있다. 쉽게 말하면, 누군가가 옆에서 잠금장치 암호를 훔쳐보기만 하더라도 정확한 비밀번호를 바로 알게 된다. 본 논문에서는 이러한 보안 문제를 해결하고자 한다. 제안하는 암호 방식은 암호 공격자가 잠금장치 비밀번호를 쉽게 알 수 없도록 설계된다. 이를 위해 우리는 PIN 방식의 비밀번호를 직접 입력하는 것 대신 숨겨진 비밀번호 방식을 이용하여 누군가가 잠금장치 비밀번호를 훔쳐보더라도 정확한 비밀번호가 공격자에게 노출되는 것을 막는다.

ABSTRACT

The previously used locking device is a PIN method and has a problem in that the password is exposed by malicious users. In other words, if attackers looks at lock passwords from the side, correct passwords are known. In this paper, we aim to solve these security problems in lock devices resistant to shoulder surfing attacks. The proposed encryption approach is designed so that attackers cannot know lock passwords. To this end, we use a hidden password method instead of directly entering a PIN-type password to prevent the correct password from being exposed to an attacker even if someone steals the lock password.

키워드

Locking Device, Shoulder Surfing Attack, Password

Ⅰ. 서 론

최근 들어 잠금장치는 보안 시장에서 꾸준히 성장하고 있으며 스마트 도어락이 개발되면서 편리성을 더하고 있다. 하지만 국내에서는 도어락 시스템을 이용한 범죄가 끊임없이 매년 증가하고 있다. 경찰청 경찰범죄통계에 따르면 일반 가정집을 대상으로 한 범죄율이 매년 증가하고 있고 그 중에서 현관문을 이용한 범죄가 50%로 비중을 차지한다[1]. 현관 출입문 보안을 강화하기 위한 방안으로써 NFC(근거리 무선통신), Wi-Fi, 블루투스, RFID, 생체인식 등을 이용한 잠금장치들이 등장하였다. 그러나 이러한 첨단 기술을 사용하고 있음에도 불구하고 각종 범죄가 끊이지 않고 있다. 현관 출입문 패스워드를 동영상으로 촬영하거나, 드라이버와 전기 충격기 등을 이용하여 잠금장치를 강제로 열 수 있다[2].

본 논문에서는 잠금장치의 활용 가능성과 보안성을 높이기 위해 새로운 비밀번호 방식을 제안한다. 기존 PIN 방식을 이용할 경우 누군가가 옆에서 도어락 비밀번호를 훔쳐보기만 하더라도 정확한 비밀번호를 바로 알아낼 수 있다[3]. 그러나 본 논문에서 제안하는 비밀번호 방식은 이러한 단점을 미연에 막을 수 있다. 즉, 악의적인 사용자가 어깨너머 비밀번호를 훔쳐보더라도 정확한 비밀번호를 알 수 없게끔 설계하여 훔쳐보기 보안성을 높인다.

* corresponding author

II. 제안하는 잠금장치 비밀번호 방식

본 장에서는 제안하는 비밀번호 방식을 소개한다. 먼저 그림 1은 잠금장치에 사용할 비밀번호 화면을 보여준다. 암호 방법의 기본적인 동작 원리는 비밀번호 화면의 각 자리별 숫자를 화면 내의 각 열의 지정된 영역에 각각 위치시킨다. 이때 정확한 비밀번호는 각 열에 놓인 위치에 상관없이 무작위로 배열된다. 같은 방법으로 화면의 두 번째 열은 비밀번호의 두 번째 수를 위, 중간, 아래 위치에 상관없이 빨강색 점선 범위 내에 무작위로 위치시킨다. 마지막으로 세 번째 비밀번호 숫자도 세 번째 열의 빨강색 점선 범위 내에 위치에 상관없이 위치시키면 된다. 그리고 비밀번호를 해제한다.

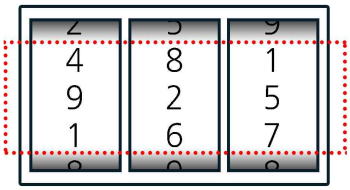

그림 1. 잠금장치 비밀번호 화면

그림 2를 예로 비밀번호 해제가 성공하거나 실패한 경우를 설명한다. 제안된 방식에 대해 비밀번호의 각 자리는 숫자 0부터 9로 구성된 3자리 비밀번호라고 가정한다. 물론 4자리 비밀번호를 사용한다면 비밀번호의 열은 하나가 더 늘어나서 4개가 된다. 비밀번호를 입력시키는 방법은 화면의 각 열을 위아래로 움직인다. 이때 화면의 지정된 영역 내에 비밀번호 숫자를 모두 위치시키면 인증을 해제할 수 있다. 그림 2는 비밀번호가 (7 5 7) 이라고 했을 때의 인증과정을 보여준다. 비밀번호 인증이 성공한 경우는 (7 5 7) 숫자가 지정된 영역 내에 모두 위치한 경우에 해당된다. 그러나 (7 5 7) 숫자가 지정된 영역 내에 모두 놓이지 않는다면 비밀번호 인증은 실패하게 된다.

기존의 PIN번호를 눌러 패스워드를 해제하는 방식은 누군가가 옆에서 비밀번호를 훔쳐보게 되면 비밀번호가 바로 노출되는 문제점을 갖고 있다. 그러나 제안하는 비밀번호 방식은 비밀번호를 화면의 지정된 영역에 위치시키기만 하면 되기 때문에 훔쳐보기로 인한 비밀번호가 타인에게 노출되더라도 정확한 비밀번호를 알아내기는 어렵다. 그렇기 때문에 제안하는 비밀번호 방식은 기존 PIN번호 입력 방식과 비교하여 훔쳐보기 상황에서 비밀번호 노출에 대한 보안성이 개선된 이점을 제공한다.

그림 2. 암호 해제 성공과 실패 예시

누군가가 훔쳐보기를 하여 비밀번호를 유추하는 경우라고 가정하자. 이때 훔쳐보기로부터 유추하여 정확한 비밀번호를 알아맞힐 확률은 다음과 같다. 기존 PIN번호 입력 방식의 경우, 훔쳐보기를 하여 그 패스워드를 정확히 기억하거나 저장한다면 비밀번호를 알아맞힐 확률은 1이다. 즉, 한 번의 훔쳐보기만으로 패스워드가 알려지게 된다. 그러나 제안하는 비밀번호 방식의 경우, 앞선 그림 1과 같이 10개의 숫자를 이용하고 비밀번호 자릿수가 3이고 각 열의 지정된 영역을 3이라고 가정하여 훔쳐보기로 비밀번호를 알아맞힐 확률을 생각해 보자. 이 경우에 패스워드를 알아맞힐 확률은 3^{-3} 이다. 즉, 평균적으로 27번 패스워드 인증과정을 해서 한 번 성공하는 정도에 지나지 않는다.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the korean government (NRF-2020R1I1A3071739).

References

[1] National Police Agency. Crime Statistics [Internet]. Available : http://www.police.go.kr/.

[2] S.-W. Lee, S.-M. Park, K.-B. Sim, “Smart Door Lock Systems using encryption technology”, *Journal of korean Institute of Intelligent Systems*, vol. 27, no. 1, pp. 65-71, Feb. 2017.

[3] K. Renaud, and A. De Angeli, “Visual passwords: cure-all or snake-oil?,” *Communications of the ACM*, vol. 52, no. 12, pp. 135-140, Dec. 2009.