Secure User Authentication: Survey

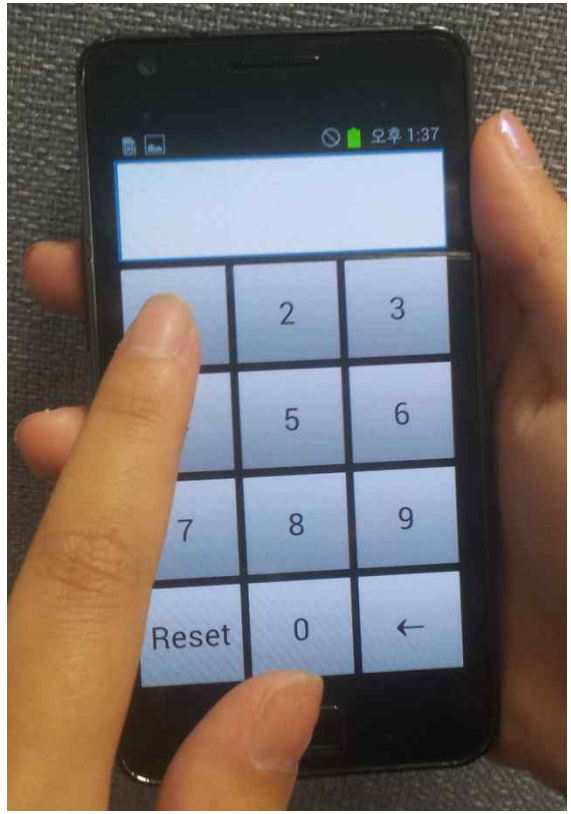
Mun-Kyu Lee
Inha University, Korea

User authentication

- The act of establishing or confirming something (or someone) as authentic.
  - Especially in computer security, authentication is the process of attempting to verify the digital identity of a user as a request to log in.
- Classification of authentication mechanisms
  - Using what you know
    - a password and a PIN (personal identification number)
  - Using what you are. (biometric verification)
    - physiology: fingerprint, face recognition, hand geometry, iris
    - behavior: signature, keystroke dynamics, voice
  - Using what you have, such as
    - ID card, hardware token

Personal Identification Number

- well-known user authentication method used in smartphone, ATM, doorlock, etc.
- In Regular PIN-entry method
  - Layout is fixed.
  - User always inputs the same information.
  - Involves no randomness.
- There are concerns about the security of PINs.
  - Anyone who observes the authentication procedure over the user's shoulder can easily memorize the user's PIN and impersonate the user.



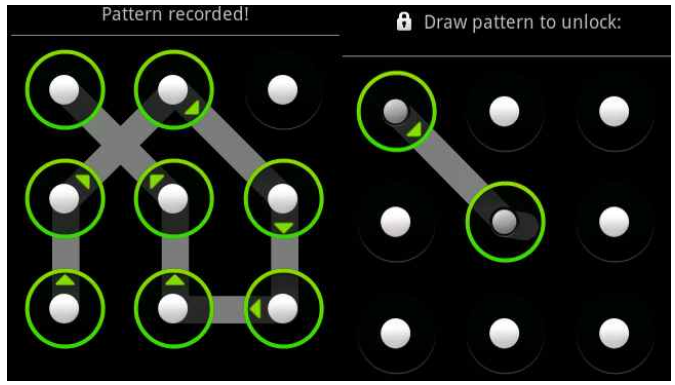
Shoulder Surfing Attack (SSA)

- This kind of attack is called a Shoulder Surfing Attack (SSA).
- This is an actual threat because
  - In many cases, PINs are used in public places.
  - Moreover, PINs are used for financial transactions.
- Also, random guessing attack is another issue.

source: http://blogs.elon.edu/technology/

Some Previous Proposals

- There are many proposals to solve this issue in the literature.
  - Complicated mathematical calculations and cryptographic protocols
    - Increased authentication time and erroneous input
  - Dedicated hardware
    - Eye-gaze based scheme
    - Brain-computer interface
  - New PIN set
    - Not sure if it is actually secure
    - Only applicable to limited usage, e.g., pattern lock in android
    - Not for general purpose, e.g., ATM



source: http://www.florian-alt.org/academic/wp-content/uploads/2012/10/gazeauthentication_defining-pins.jpg
source: http://4.bp.blogspot.com/-MkxbwHN37xw/UC7w1MnR10I/AAAAAAAAFJw/HEkynWIBLKM/s1600/interface_By_scientific_american.jpg
source: http://phandroid.s3.amazonaws.com/wp-content/uploads/2012/03/android-unlock-pattern.jpg

General Approach to SSA Resistance (1): Randomization

- Challenge-response based PIN-entry

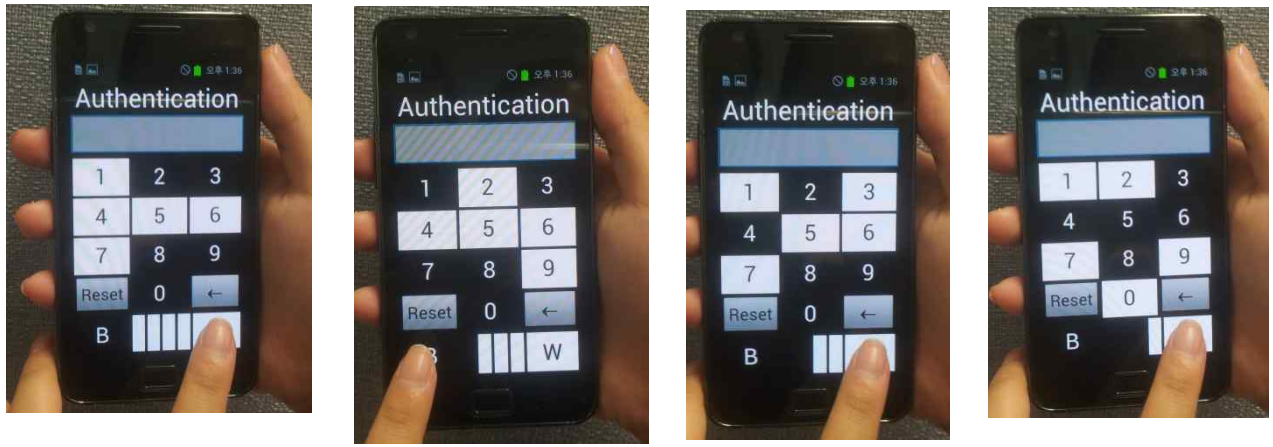
Random challange

User's response

  - A user enters a response to a random challenge given by the system, instead of entering the PIN directly.

Previous Solution

- Binary method (IOC)
  - V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp. 236-245, Oct. 2004.
  - Digits are displayed as two distinct sets by randomly coloring half of the keys black and the other half white.
  - The user recognizes the color assigned to the current PIN digit.

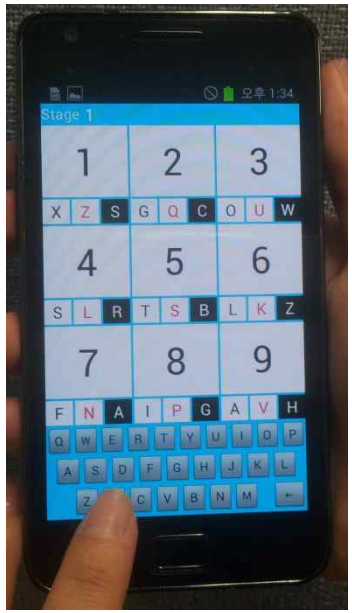


To enter a digit '1', the user touches W, B, W, and W.

The pictures have been taken from our app reproduced according to the description in the above paper.

Previous Solution

- ColorPIN
  - A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN – securing PIN entry through indirect input," CHI 2010, pp.1103-1106, April, 2010
  - A PIN is redefined as a combination of digits such as 1(black)-2(red)-3(white)-4(black). (Not compatible with the regular PIN)



To enter the first PIN digit, 1(black), the user recognizes the black letter right below '1', which is 'X' in this case. Then the user inputs 'X'.

The pictures have been taken from our app reproduced according to the description in the above paper.

General Approach to SSA Resistance (2): Invisible Channel

- Secondary channel other than visual one
  - Challenges or responses are transmitted through the secondary channel.

(Hidden challenge)

User's response

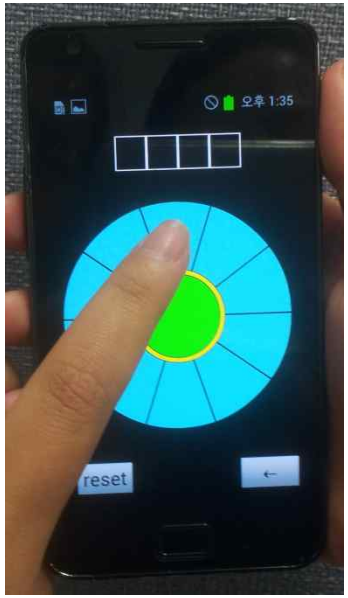
OR

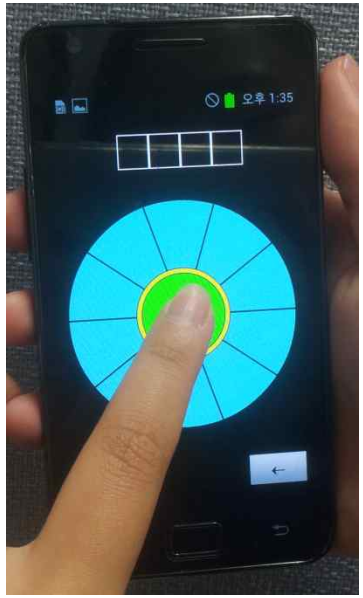
Random challange

(Hidden response)

Previous Solution

- Phonelock
  - 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," TEI 2011, pp. 197-200, January, 2011
  - Two modes: audio and vibration





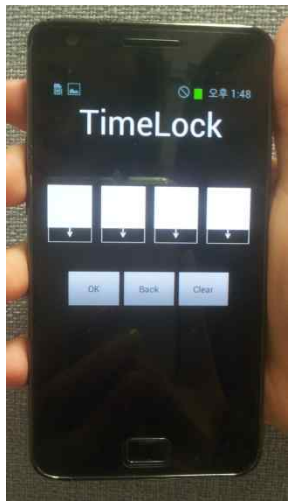
Audio mode example

When user touches any sector
among ten sectors,
the phone tells the user a random
number between 0 to 9, say 3.
Then the user moves the finger
along the circle, touching adjacent sectors.
Then, the phone tells 4, 5, 6, … in turn.
When the user encounters a sector
corresponding to the PIN digit,
s/he slides the finger to the center circle,
confirming the choice.
For security, the audio signals should be
transmitted through an isolated channel,
e.g., an earphone.

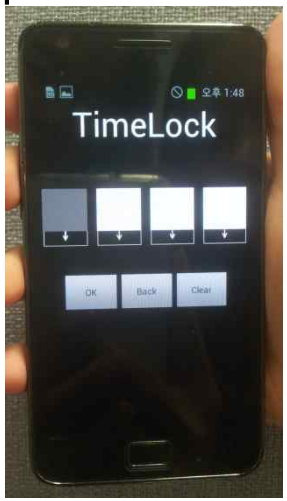
The pictures have been taken from our app reproduced according to the description in the above paper.

Previous Solution

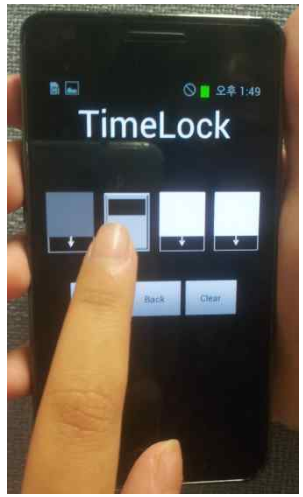
- Timelock
  - A. Bianchi, I. Oakley, D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry," Ineracting with Computers, 24(5), 409-422 (2012)
  - A PIN is the sequence of digits between 1 to 5.
    But the order in which buttons are touched matters.
    (Not compatible with the regular PIN)



Initial state



First digit entered.



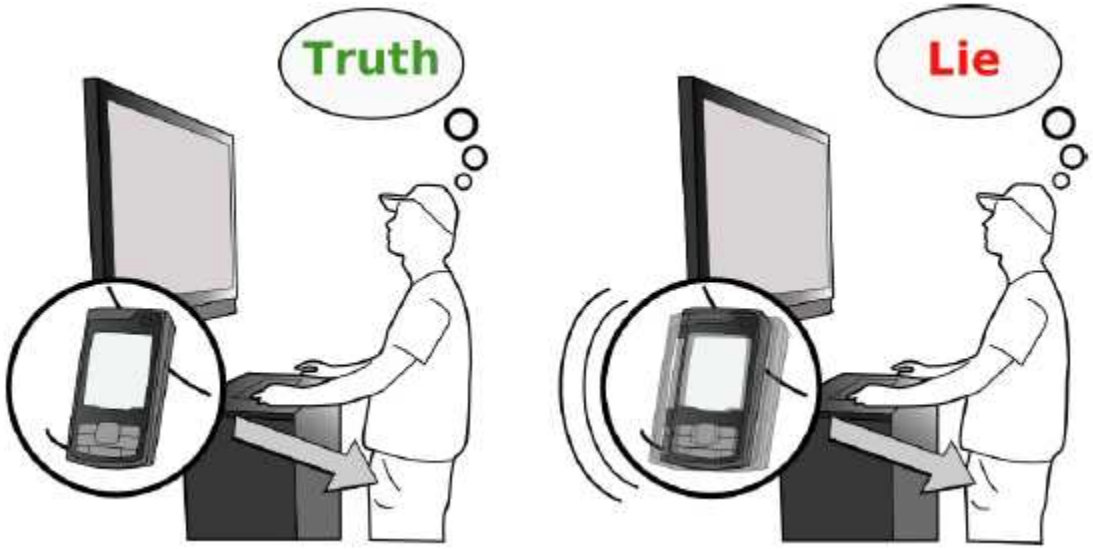
The user is entering the second digit
by touching the appropriate button
and counting the beeps or vibrations.

4 digits entered.

The pictures have been taken from our app reproduced according to the description in the above paper.

Previous Solution

- Vibrapass
  - A. D. Luca, E. V. Zezschwitz and H. Hußmann, "VibraPass-Secure Authentication Based on Shared Lies," CHI 2009, pp. 913-916, April, 2009
  - Use a mobile phone as a second-channel.
  - When the mobile phone vibrates, the user enters a false number, if not, a correct one.



The figures are from the above paper.

Issues of Previous Methods

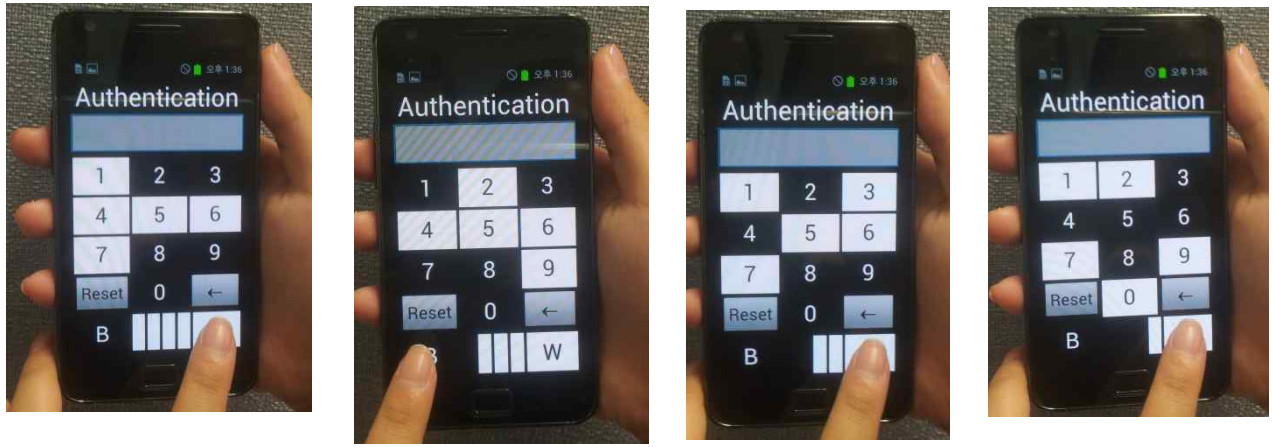
- Some methods do not provide the claimed security.
  - Binary (IOC) method: vulnerable to recording and even to human
- Some are not compatible. (Cannot be used for ATM)
  - ColorPIN, Timelock
- Some are very expensive.
  - Eye-gaze, Brain-computer interface
- Some require too long time to enter a PIN or their error rates are too high.
  - Because the procedure where the user computes an appropriate response from the given challenge is very complex due to security requirement.
  - Binary method, Vibrapass
- The use of secondary channels are cumbersome.
  - For an audio channel: It is a very annoying (and time-consuming) task to prepare an earphone or to stop the current job such as listening to music whenever an authentication is needed.
  - For a haptic channel: The amount of information transmitted through vibration is very limited.
  - Phonelock, Timelock

Trade-off Between Attacks

- Definitions
  - For a PIN-entry method M, the success probability of a guessing attack against M, denoted by $P_{GA}(M)$, is the probability that the attacker passes a PIN-entry test by guessing a correct PIN in one trial.
  - The success probability of recording attack against M, denoted by $P_{RA}(M)$, is the probability that the attacker passes the PIN-entry test in one trial using the information obtained during a recording attack.
  - Let S_M be the set of possible PINs for a PIN-entry method M and $|S_M|$ be its cardinality.
- Theorem
  - Assume that a user's PIN is selected uniformly at random from S_M and that an attacker can observe all challenge-response pairs for authentication.
  - Then, $P_{GA}(M) \times P_{RA}(M) \geq 1/|S_M|$ for any method M.

Trade-off Between Attacks

- Example: Binary method
  - Case 1: Four rounds for a digit
    - $P_{RA}(IOC) = 1$, $P_{GA}(IOC) = (1/10)^4$
    - $P_{RA}(IOC)$ X $P_{GA}(IOC) = 1/10000$
  - Case 2: One round for a digit
    - $P_{RA}(IOC) = (1/5)^4$, $P_{GA}(IOC) = (1/2)^4$
    - $P_{RA}(IOC)$ X $P_{GA}(IOC) = 1/10000$

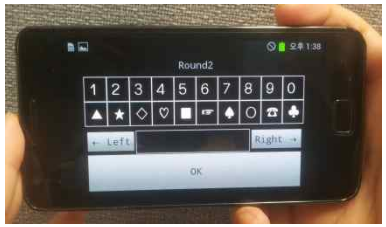


The pictures have been taken from our app reproduced according to the description in the above paper.

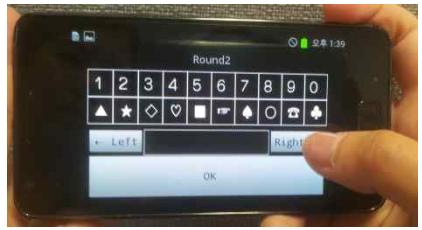
Human SSA-Resistant Methods

- Linear PIN (LIN_4 and LIN_5)
  - First stage: the user recognizes the session key below the first PIN digit.
  - Next stages: the user aligns the session key to the corresponding digit.

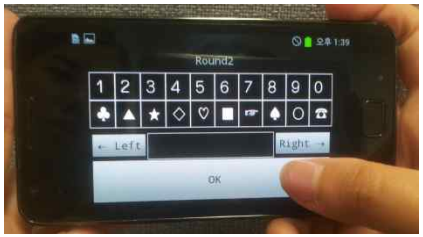
When the PIN is 13…, the user recognizes a star right below 1, the first digit of PIN, and touches OK.



In the second stage, the user verifies that the star is below 2.



Using the 'Right' button, the user aligns the star with 3, the second PIN digit.



By touching 'OK', the user confirms the choice.