Cognitive Authentication Schemes
Safe Against Spyware

Daphna Weinshall

Presenter: Chi-Tsong Su
Do you know ....

➢ How many things do you have to remember immediately or permanently?

- Telephone Number
- Social Security Number
- Vocabulary
- Name
- Card Number
- .......

• Let us test how well you can remember things
Contract Bridge

- Playing Contract Bridge requires moderate memory capacity on text
  - Played Cards, Play Process, Bidding Process
  - Basic Play Rule in a No-Trump Game
    - 13 Tricks in a play with 4 players
    - The first card played in a trick by a player is called the lead, and the remaining players play a card clockwise around the table by following the same suite
    - The hand that plays the highest card in the suit of the lead wins the trick
      - A>K>Q>J>10>........
    - Any card can win a trick if with the same suite, no other card is higher than it. This also holds when no other card with the same suite appears.
- A Complete Play
- Test1  Test2  Test 3
What if we ask you to recognize pictures, rather than text?

● How do you recognize a person?
  ● Usually, we recognize his face first, and remember his name
  ● Outline, hair, eyes, nose, mouth, voice and other features
  ● There exists an association between a face and a name

● How do you recognize a picture?
  ● The story *hides* underneath the picture
  ● Only people who have seen it can construct a pattern for recognition

● Geared in Security
  ● It is not easy to present all associations within a short time
  ● Even though these associations are randomly ordered in a sequence, the complexity of the sequence is less complicated to users than to attackers
What is the difference between recall and recognition in authentication?

- **Recall:**
  - Involves digging into memory and bringing back information on a response basis
  - Example:
    - What is the capital of England?
    - Who is the first human that walked on the Moon?

- **Authentication: Knowledge-based systems**
  - Need precise recall with passwords
  - If passwords are simple to remember, they are also vulnerable to attack
  - If passwords are complex and arbitrary, they are difficult to remember
What is the difference between recall and recognition in authentication? (Cont.)

- **Recognition:**
  - A process that occurs in thinking when some event, process, pattern, or object recurs.
  - People are much better in *imprecise recall*, and its capacity is limitless.
  - Example:
    - Facial Recognition
    - Pattern Recognition
    - Handwriting Recognition
  - Flawed if it is implemented alone in authentication.
    - Weak under attacks of cumulative observations with powerful resource.
    - If recognition-based authentication combine with interaction in a proper way, this protocol is difficult to break.
Problem

What are the issues of the current authentication protocols?

- Token-Based Protocol
  - Forgeable
  - Missing Token
  - Guessing Attack?

- Knowledge-Based Protocol
  - Simple knowledge means vulnerability
  - Complex knowledge is considered as impractical

- Biometrics
  - Devices can be unpleasant to users

- Graphic Password Schemes
  - Easier to remember, but not safer than regular password against eavesdropping
How should we customize this system?

- This system itself should generate a set of randomly selected pictures proposed for authentication.
- Other than graphic passwords, we need to add some questions in the pictures to ensure that the passwords are not guessable.
- We have to trade-off login time and training time.
- This system can decide whether to authenticate users or reject them by the accuracy rate at which they respond to a challenge protocol.
Methodology

**Challenge Response Protocol**

- A set of $B$ of $N$ common pictures *generated by the system*, rather than by the discretion of the user
- A set of randomly selected $F$ $B$ of $M < N$ pictures
- Unlike some other protocols, e.g. Deja vu, the user is asked a complex or simple multiple-choice question with $P$ possible answers about the random set in addition to a set of picture challenge.
  - High Complexity Query: $N=80$, $M=30$, $P=4$
  - Low Complexity Query: $N=240$, $M=60$, $P=2$
- With accuracy higher than pre-fixed threshold as to exclude random guessing, the system authenticates the user.

**How about the price?**

- It takes a lot of time to train users for recognizing a bunch of pictures and know the story underneath the pictures
Results

<table>
<thead>
<tr>
<th>N</th>
<th>M</th>
<th>P</th>
<th>Query Size</th>
<th>$H^*$</th>
<th># bits $H^*$</th>
<th># bits $H^\wedge$</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>30</td>
<td>4</td>
<td>8*10</td>
<td>8.87141E+21</td>
<td>72.90965</td>
<td>47</td>
</tr>
<tr>
<td>120</td>
<td>50</td>
<td>2</td>
<td>8*10</td>
<td>1.83617E+34</td>
<td>113.8223</td>
<td>84</td>
</tr>
<tr>
<td>95</td>
<td>40</td>
<td>8</td>
<td>8*10</td>
<td>9.9718E+26</td>
<td>89.68798</td>
<td>47</td>
</tr>
<tr>
<td>145</td>
<td>55</td>
<td>4</td>
<td>4*5</td>
<td>4.26646E+40</td>
<td>134.9702</td>
<td>47</td>
</tr>
</tbody>
</table>

Security
- Resistance to various attacks
  - Eavesdropping
  - Brute-force Attacks, unless attackers have powerful resources
  - Enumeration Attacks

Success Rate
- After undergoing three training sessions on three consecutive days, all participants had the success rate over 95% per query
- Many participants had perfect memory retention in last trail

Time needed in authentication
- 3 minutes in high complexity protocol
- 1.5 minutes in low complexity protocol
Take-Away

- We can combine recognition-based and recall-based protocol for authentication
- Even though this protocol is Human-friendly, it is not practical in emergency
But ........

- Is it worth training a user for 3 days?
- Is there any other scheme able to reduce training time?
- How about the overhead of this system?
- How far can we go with imprecise recall for authentication?
- Is memory of recognition influenced by re-store memory with subtle difference?