A Graphical PIN Authentication Mechanism for Smart Cards and Low-Cost Devices

Luigi Catuogno
Dip. di Informatica ed Applicazioni
Università degli Studi di Salerno

Clemente Galdi
Dip. di Scienze Fisiche
Università degli Studi di Napoli “Federico II”
The problem
The problem
One time password

*Authentication through insecure channels*

• In order to be authenticated, the user has to prove that she knows the secret x
  – The system issues a random challenge C
  – The user computes the proof $P = F(x, C)$
    • Often the user computes $F()$ by means a personal crypto-device
  – The user sends $P$ to the system
  – The system verifies the proof…etc.
Graphical password

• A one-time password mechanism where:
  – The system issues a random graphical challenge
    • Often called “scene”
  – The user computes the proof by means a cognitive function of what she sees on the screen
    • without the need of any external device
Cognitive functions

• Image recognition
• Image position recognition
• Answering simple queries about the scene
• Repeating a sequence of actions in a scene
PassFaces

http://www.realusers.com

• The system choses three passfaces for the user
PassFaces/2

- During the logon, the system shows to the user three scenes each one containing one of user’s passfaces
- The user has to recognize her passfaces in each scene
- The user select the passfaces by
  - Mouse clicks,
  - Tapping by the stylus
A useful application…

• Everybody uses ATM and POS terminals everyday.
  – PINs and passwords are frequently subject to attacks and frauds
  – PINs are not user-friendly

• Graphical PINs could be a good improvement
But...
But..

- Many G.P. schemes require non-trivial visualization and pointing devices
- ATM machines, POS terminals, Cellular phones….
  - Small sized and low resolution displays
  - No pointing devices (mouse, touchscreen…)
  - Poor computational resources (slow processors, small memory…)
GRAPE
http://www.dia.unisa.it/GRAPE

- Handles authentication by means of a numerical one-time PIN
- Uses both sophisticated pointing devices and numerical key-pad.
- The graphical challenge is composed of low-resolution objects
- Challenge generation and proof validation require poor computational resources
GRAPE/2

- The user’s secret is a sequence of queries formed like:
  - “On which row is the object x?”
- Where the object x is a geometrical shape like:
  - Purple full rectangle
  - Red empty rectangle
  - White empty exagon
  - ...
The user types the PIN. Each digit represents the row number of the corresponding object.
Threats

• Shoulder surfing attack:
  – A human adversary observes an authentication session
    • What can he remember of the session?
    • What can he learn about the secret?

• Human adversary:
  – Poor computational capabilities
  – Small memory
  – Errors
Threats

• Camera based attack
  – The adversary can:
    • record, by means of a camera, a complete session
    • memorize some number of sessions
    • automatically analyze sequences of sessions
  – How many session are needed to discover the secret?
GRAPPE/4

If the secret is composed of $m$ queries.

• **Naive protocol**
  – The user answers correctly to $m$ queries

• **Randomized protocol 1**
  – The user answers correctly to *at least* $r<m$ queries and *randomly* to the rest

• **Randomized protocol 2**
  – The user answers correctly to $c<m$ queries and *wrongly* to the rest
Security evaluation

Chances of guessing the secret after analyzing $n$ sessions

<table>
<thead>
<tr>
<th>Protocol</th>
<th>P=0.95</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive</td>
<td>5</td>
</tr>
<tr>
<td>Rand 1  $(\text{correct}=11,\text{random}=4)$</td>
<td>11</td>
</tr>
<tr>
<td>Rand 2  $(\text{correct}=11,\text{wrong}=4)$</td>
<td>16</td>
</tr>
</tbody>
</table>

Challenge: 80 objects, 8 rows; Queries: $m=15$
Usability evaluation

- Average login time
- Error rate
- Can the user easily remember the secret?
  - Geometrical shapes can be replaced by different objects (pictures, letters...
Conclusion

• Our scheme
  – Improves the security of ATM transactions
  – Prototype (web applications, smart card)
• Usability
  – a study is currently in progress
  – can be improved using more familiar objects
    (where display makes it possible)
• To be done:
  – Analisys of probabilty of being authenticated
    without knowing the secret
Thank you!