New Directions in Social Authentication

Sakshi Jain, LinkedIn
Neil Gong, UC Berkeley
Sreya Basu Roy, Princeton
Juan Lang, Google
Prof. Dawn Song, UC Berkeley
Prateek Mittal, Princeton

USEC 2015
Shortcomings in commonly used authentication systems

**Passwords:**
- Same across websites
- Prone to dictionary attacks
- Do not tend to change with time

**Secret Questions:**
- Users forget the answers to difficult questions
- Answers do not tend to change with time
Shortcomings in commonly used authentication systems

Two Factor Authentication

- Security better than previous two but very inconvenient
Using information from a user’s social network to authenticate him/her

- Prone to attacks that employ face recognition attacks
  [ACSAC ’12] I. Polalkis, et al. "All your face are belong to us: breaking Facebook's social authentication"
- Attacks by user’s friends
  [FC ’12] H. Kim, et. al. “Social authentication: Harder than it looks"
Contributions

Information in a user’s social network is ever changing! Can we use this to get rid of static nature of secrets?

- Rethink the space of social authentication challenges beyond photographs and provide a systematic way to explore the same
- Proof-of-concept implementation on Facebook users
- Pilot user study and usability evaluation of the Facebook prototype
Challenge Format:

Given some criteria, identify the connection that matches it
Desirable properties of a challenge

Usability:
  Reliability:  \( \text{Pr} \) [true user can correctly solve the challenge]
  Applicability:  \( \text{Pr} \) [at least one connection matches the challenge criteria]

Security:
  \( \text{Pr} \) [attacker is able to correctly solve the challenge]
Edge
  e.g., message
c  comment
  poke

Pseudo-edge
  e.g., group
  school

Node
  e.g., photo
  hometown

You

message/
comment/
poke

photo

group/
school
Facebook Prototype

Message Test
One of the following five pictures is of a friend with whom you exchanged a message with recently. Type in the complete name of that friend (Please wait for the images to load)

.name

Kindly note that the options for this question is independent of the answer to the previous question

Submit
# Facebook Prototype

<table>
<thead>
<tr>
<th>Question</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name the friend tagged in the photo</td>
<td>Node</td>
</tr>
<tr>
<td>Name the friend you went to same school with</td>
<td>Pseudo-edge</td>
</tr>
<tr>
<td>Name the friend you recently poked</td>
<td>Edge</td>
</tr>
<tr>
<td>Name the friend you recently sent a message</td>
<td>Edge</td>
</tr>
</tbody>
</table>

**Answer Format:** Type in the name of a matching connection  
*(edit distance used to accommodate for spelling errors)*
Number of participants: 90
Recruitment:
   Amazon Mechanical Turk
   $5 on completing the survey

Age distribution:

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>42%</td>
</tr>
<tr>
<td>25-34</td>
<td>39%</td>
</tr>
<tr>
<td>35+</td>
<td>19%</td>
</tr>
</tbody>
</table>
## Usability Results of Prototype

<table>
<thead>
<tr>
<th>Type</th>
<th>Question</th>
<th>Reliability</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Friend tagged in the photo</td>
<td>28% ±9%</td>
<td>77% ± 8%</td>
</tr>
<tr>
<td>Pseudo-edge</td>
<td>Friend you went to same school with</td>
<td>54% ± 10%</td>
<td>51% ± 10%</td>
</tr>
<tr>
<td>Edge</td>
<td>Friend you recently poked</td>
<td>71% ± 9%</td>
<td>48% ± 10%</td>
</tr>
<tr>
<td>Edge</td>
<td>Friend you recently sent a message</td>
<td>66% ± 10%</td>
<td>98% ± 2%</td>
</tr>
</tbody>
</table>
Future Work

- Results are skewed by selection of question criteria. Design a broader set of questions within each category.
- Compare our prototype with Facebook’s existing social authentication system.
- Compare usability and security of various answer types:
  - Text box without options
  - Radio buttons
Discussion

- **Replacing passwords?**
  - Proposed model is intended to be an auxiliary authentication mode, not a primary one

- **Privacy Implications:**
  - Leakage of information like message exchanges
  - Note that user is confirmed via primary authentication

- **Security:**
  - Depends on user’s privacy
  - Edge > Pseudo-edge > Node
Questions?