Social Networking Sites Security

Social networks contain plethora of personal information:
- Real name, profile picture, email address
- Friends, social surrounding, locations
- Events, “Likes”, hobbies
- Possibly much, much more

All networks have only weak security on the network layer:
- No encryption (HTTPS)
- Weak session management
- Only “reactive” security

Social Networking Site

<table>
<thead>
<tr>
<th>Name</th>
<th>Claimed users</th>
<th>HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>500 x 10^8</td>
<td>Login only</td>
</tr>
<tr>
<td>Friendster</td>
<td>110 x 10^6</td>
<td>No</td>
</tr>
<tr>
<td>Orkut</td>
<td>100 x 10^6</td>
<td>Login only</td>
</tr>
<tr>
<td>hi5</td>
<td>6 x 10^6</td>
<td>No</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>60 x 10^4</td>
<td>Login only</td>
</tr>
</tbody>
</table>

Table: Top five social networking sites and their support for HTTPS.

Our FITM Attack

FITM - Friend in the Middle Attack
- Traditional session hijacking for social network communications
- Either actively (Botnet, ...) or passively (unencrypted Wifi, ...)
- Undetectable to the
  - client
  - social network operator
- Can be used to retrieve or publish social network data
- Foundation for further attacks on the users

Attack Cycle

1. Sniff network for social network connection
2. Clone HTTP header and authentication cookies
3. Acquire all available data, either by
   - installing custom third-party application, or
   - adding malicious account with full data access
4. Generate tailored spam & phishing messages
   - publicly to all friends e.g., comments or wall posts
   - social network private messages
   - “offline”, e.g., email or IM
5. For every successfully phished friend: start from 1

Countermeasures:
- Secure social network architecture
- User education

Consequences

Social Phishing
- “Social” information increases effectiveness, 16% to 72% according to [Jagatic et al., 2009]
- Based on the social graph
- Improves with “friendship metadata”, like recent communications or shared events
- Basically automated social engineering

Context-Aware Spam
- Relationship-based attack
- Unshared-attribute attack
- Shared-attribute attack
- according to [Brown et al., 2005] e.g., electronic birthday card, picture gallery, ...

Modelling propagation strategies
- Simulating social graph with a configuration model
- Graph properties:
  - no loops
  - degree of nodes according to power law distribution
  - number of nodes: 10^4

Conclusion

Problems in Research
- Impossible to do “in the wild”
- Social networking sites have no incentives to release social graph
- Legal questions
- Ethical questions:
  - How to obtain "attack seeds"
  - How to get consent from users?
- Simulation can only solve parts of the problems

Conclusion
- Powerful attack method
- Hard to defend against
- All deployed social networks vulnerable

Future research:
- Are future generation social networks (Peerson, Diaspora, ...) secure by design?
- Are people really falling for social phishing?