“Elderly, with location data, while shopping?”

Spotting Privacy Threats Beyond Software: A Quasi-Experimental Study

Authors: Tuisku Sarrala and Tommi Mikkonen
Presenter: Tuisku Sarrala, University of Jyväskylä tuisku.rad.sarrala@jyu.fi
Tuisku Sarrala

• Academic
  – Doctoral student (DBA), Information Technology, Jyväskylä University, Finland
  – Master’s Degree in Cyber Security, JAMK University of Applied Sciences, Finland, 2021
  – BSc(Hons) Computing & Systems Practice (Open), The Open University, UK, 2014

• Professional
  – Privacy professional with 10+ years of experience, currently Cyber Security & Privacy Manager at Nokia Technologies
  – CIPP/E, CIPT
Broadening developers’ view of privacy
Motivation

**Problem situation**
- Privacy legislation
- Developers’ understanding

**Approach**
- Engineering activity
  - Privacy threat modeling
- Approach
  - Systems thinking
- Implementation
  - Personas technique
  - Scenarios technique
  - Ideation cards

**Research Question**
- RQ: *How does a method with systems thinking features compare to a method with traditional features in privacy threat discovery in terms of identified threats?*
Experiment setting

Course
- 5-week remote course
- 65 participants
- Varied programming confidence 0-10
- Varied relevant work experience 0-10+ yrs

For the experiment
- 8 + 8 teams (3-5 participants each)
- Based on programming confidence, then work experience
Results

Similarities
- 43 threats
- Timings
- Threats per group

Experimental
- Broader scope
- Social scope
- Context-based
- Personal harmed party

Control
- In line with existing research
- Security-focused
- Software artifact and malicious actors
- Non-personal harmed party

TYPE OF THREATS

<table>
<thead>
<tr>
<th></th>
<th>EXP</th>
<th>CTRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Security</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Other</td>
<td>31</td>
<td>21</td>
</tr>
</tbody>
</table>

SCOPE OF THREATS

<table>
<thead>
<tr>
<th></th>
<th>EXP</th>
<th>CTRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Society</td>
<td>15</td>
<td>21</td>
</tr>
<tr>
<td>Social</td>
<td>5</td>
<td>14</td>
</tr>
<tr>
<td>Malicious</td>
<td>26</td>
<td>3</td>
</tr>
<tr>
<td>Software</td>
<td>29</td>
<td>19</td>
</tr>
</tbody>
</table>

CONTEXT-BASED?

<table>
<thead>
<tr>
<th></th>
<th>EXP</th>
<th>CTRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-definable</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td>Context-based</td>
<td>29</td>
<td>19</td>
</tr>
</tbody>
</table>

HARMED PARTY

<table>
<thead>
<tr>
<th></th>
<th>EXP</th>
<th>CTRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persona</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Neutral</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>None</td>
<td>26</td>
<td>25</td>
</tr>
</tbody>
</table>
Same cards, but different results?

• Mixing and matching → wider scope, contextuality
• More material to consider → wider scope, contextuality but same quantity
• Scenarios before privacy principles → threats not pre-defined
• Personas → person’s story, rather than privacy concepts
Validity

- Time and available threats
- Persona use challenges
- Participants and participation
- Presence of complexity and systems thinking?
- Control method realistic?
- Plausible threats?
- Generalised to industry?
Conclusion

• Attributing the results to a shift of focus
  – Artifact and privacy principles → human interaction scenarios with software
• Systems thinking features may improve the situation; a promising direction of research
• Applications: Inform the design of privacy threat modeling and privacy impact assessment methods for developers as well as privacy education
Future work

- Analysis of recordings
- Refining cards
- Refining user guidance
- Validation in the industry
Thank you

Privacy, security and ethics in software development

Tuisku Sarrala, University of Jyväskylä
tuisku.rad.sarrala@jyu.fi