Top 10 Privacy Risks Project

Results presentation @ German OWASP Day 2014
9 December 2014, Hamburg

Florian Stahl (Project Lead, msg systems, Munich)
Privacy

• Definitions:
  – A state in which one is not observed or disturbed by other people
  – The right to be let alone (Edward Warren, 1890)

• Different approaches (Europe vs. US)

• IT Security enables Privacy in most cases

Picture source: thedailydose.com
Problem

• Many web applications contain privacy risks
• Anyway, they are compliant to privacy and data protection laws because
  – They are hosted in countries with poor privacy laws
  – Lawyers focus on compliance, not on real-life risks for personal data
• No existing guidelines or statistical data about privacy risks
• Foundation of the OWASP Top 10 Privacy Risks Project in early 2014
• Member of Internet Privacy Engineering Network (IPEN)
• Nearly 100 privacy and security experts participated
Goal

• Identify the most important technical and organizational privacy risks for web applications
• Independent from local laws based on OECD Privacy Principles
• Focus on real-life risks for
  – User (data subject)
  – Provider (data owner)
• Help developers, business architects and others to understand and improve web application privacy
• Provide transparency about privacy risks
Method (1/2)

- Model Creation
- Defining Protection Requirement
- Identifying Violations
- Rating of Violation Impact
- Investigation of Frequency of Occurence
- Rated List of Privacy Risks
  - Evolve Counter-Measures
  - Evolve Best Practices
Method (2/2)

Survey to evaluate frequency of occurrence

- 62 privacy and security experts participated
- Rated 20 privacy violations for their frequency in web sites

Impact rating

<table>
<thead>
<tr>
<th>Protection demand</th>
<th>Criteria for the assessment of protection demand</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Application operator perspective</td>
</tr>
<tr>
<td></td>
<td>Impact on reputation and brand value</td>
</tr>
<tr>
<td>Low – 1</td>
<td>The impact of any loss or damage is limited and calculable.</td>
</tr>
<tr>
<td>Medium – 2</td>
<td>The impact of any loss or damage is considerable.</td>
</tr>
<tr>
<td>High – 3</td>
<td>The impact of any loss or damage is devastating.</td>
</tr>
</tbody>
</table>
Result: Top 10 Privacy Risks

P1  Web Application Vulnerabilities
P2  Operator-sided Data Leakage
P3  Insufficient Data Breach Response
P4  Insufficient Deletion of personal data
P5  Non-transparent Policies, Terms and Conditions
P6  Collection of data not required for the primary purpose
P7  Sharing of data with third party
P8  Outdated personal data
P9  Missing or Insufficient Session Expiration
P10 Insecure Data Transfer
P5: Non-transparent Policies, Terms & Conditions

• Privacy Policies, Terms & Conditions are not up-to-date, inaccurate, incomplete or hard to find
• Data processing is not explained sufficiently
• Conditions are too long and users do not read them
• Hard to standardize
• Possible Solutions:
  – Text analyzer: readability-score.com
  – HTTPA: http with accountability
P7: Sharing of Data with 3rd Party

Third Parties:
- Advertisers
- Subcontractors
- Video integration
- Maps
- Social networks

Problems:
- Data is transferred or sold to third parties without user’s knowledge and consent
- Complete loss of control

Picture sources: Ghostery, heise.de
P9: Missing or Insufficient Session Expiration

Automatic session timeout and a highly visible logout button is security state-of-the-art, not for:

- Google
- Facebook
- Amazon

Solution:

- Configure to automatically logout after X hours / days
- Obvious logout button
- Educate users

WEB.DE Sicherheitshinweis
Bitte loggen Sie sich immer aus!

Nur durch einen Klick auf "Logout" beenden
Sie Ihre aktuelle Sitzung in Ihrem Postfach und verhindern,
dass Unbefugte in Ihre Privatsphäre eindringen können:

Der Logout schließt Ihr Postfach ab und dient zu Ihrer eigenen Sicherheit!

Picture sources: facebook.com, web.de
Outlook

• Aiming to receive Lab Project Status
• Currently collection of countermeasures
• Master student wanted (preferred location Munich)
• Spread the Word
  • 22 January 2015: CPDP, Brussels (IPEN panel discussion)
  • 4-6 March 2015: IAPP Global Privacy Summit, Washington
• Regular review of Top 10 Privacy list
Top 10 Privacy Risks Project

Results presentation @ German OWASP Day 2014
9 December 2014, Hamburg

Florian Stahl (Project Lead, msg systems, Munich)
## Backup

### Top 10 Privacy Risks Project

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Frequency</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Web Application Vulnerabilities</td>
<td>High</td>
<td>Very high</td>
<td>5.32</td>
</tr>
<tr>
<td>P2</td>
<td>Operator-sided Data Leakage</td>
<td>High</td>
<td>Very high</td>
<td>4.76</td>
</tr>
<tr>
<td>P3</td>
<td>Insufficient Data Breach Response</td>
<td>High</td>
<td>Very high</td>
<td>4.16</td>
</tr>
<tr>
<td>P4</td>
<td>Insufficient Deletion of personal data</td>
<td>Very high</td>
<td>High</td>
<td>4.14</td>
</tr>
<tr>
<td>P5</td>
<td>Non-transparent Policies, Terms and Conditions</td>
<td>Very high</td>
<td>High</td>
<td>3.96</td>
</tr>
<tr>
<td>P6</td>
<td>Collection of data not required for the user-consented purpose</td>
<td>2.1</td>
<td>1.8</td>
<td>3.78</td>
</tr>
<tr>
<td>P7</td>
<td>Sharing of data with third party</td>
<td>1.8</td>
<td>2</td>
<td>3.6</td>
</tr>
<tr>
<td>P8</td>
<td>Outdated personal data</td>
<td>1.6</td>
<td>2.2</td>
<td>3.52</td>
</tr>
<tr>
<td>P9</td>
<td>Missing or insufficient Session Expiration</td>
<td>1.4</td>
<td>2.4</td>
<td>3.36</td>
</tr>
<tr>
<td>P10</td>
<td>Insecure Data Transfer</td>
<td>1.3</td>
<td>2.4</td>
<td>3.12</td>
</tr>
<tr>
<td>P11</td>
<td>Inappropriate Policies, Terms and Conditions</td>
<td>1.7</td>
<td>1.8</td>
<td>3.06</td>
</tr>
<tr>
<td>P12</td>
<td>Transfer or processing through third party</td>
<td>1.6</td>
<td>1.8</td>
<td>2.88</td>
</tr>
<tr>
<td>P13</td>
<td>Inability of users to modify data</td>
<td>1.3</td>
<td>2.2</td>
<td>2.86</td>
</tr>
<tr>
<td>P14</td>
<td>Collection without consent</td>
<td>2</td>
<td>1.4</td>
<td>2.8</td>
</tr>
<tr>
<td>P15</td>
<td>Collection of incorrect data</td>
<td>1</td>
<td>2.4</td>
<td>2.4</td>
</tr>
<tr>
<td>P16</td>
<td>Misleading content</td>
<td>1.3</td>
<td>1.8</td>
<td>2.34</td>
</tr>
<tr>
<td>P17</td>
<td>Problems with getting consent</td>
<td>1.6</td>
<td>1.4</td>
<td>2.24</td>
</tr>
<tr>
<td>P18</td>
<td>Unrelated use</td>
<td>1.7</td>
<td>1.2</td>
<td>2.04</td>
</tr>
<tr>
<td>P19</td>
<td>Data Aggregation and Profiling</td>
<td>1.4</td>
<td>1.4</td>
<td>1.96</td>
</tr>
<tr>
<td>P20</td>
<td>Form field design issues</td>
<td>1.2</td>
<td>0.6</td>
<td>0.72</td>
</tr>
</tbody>
</table>