Top 10 Privacy Risks in Web Applications

IAPP Global Privacy Summit 2015
5 March 2015, Washington DC

Florian Stahl (Project Lead, msg systems, Germany)
About me

Florian Stahl

- Master’s degree in Information System Science with Honors (University of Regensburg, Germany)
- Master’s degree in Computer Science (Växjö University, Sweden)
- CIPT, CISSP, CCSK

Working with information security & privacy for more than 8 years:
- Security & Privacy Consultant at Ernst & Young
- Lead Consultant Information Security, msg systems in Munich
- Project Lead OWASP Top 10 Privacy Risks Project

Goal: Interdisciplinary and holistic understanding of information security and privacy in organizations

Hobbies:
- Wife and son
- Travelling, mountain biking, snowboarding
Agenda

1. Situation
2. Top 10 Privacy Risks Project
   a. Background
   b. Goal
   c. Method
   d. How would you rate?
   e. Results
3. Countermeasures
4. Summary
Laws do not address real-life privacy risks anymore

Technical solutions do not provide sufficient privacy and transparency

Secret services undermine privacy without justification and real control

Safe Harbor not trusted by EU anymore

Globalization requires global privacy standards

Privacy laws

Real Life

Global Use

NSA & Co.

Technology

Situation
Forget about laws...

... we want REAL PRIVACY in web applications

• Currently 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
  – Main focus on compliance, not on real-life risks for personal information
• No existing guidelines or statistical data about privacy risks in web applications
• Foundation of the OWASP Top 10 Privacy Risks Project in early 2014
• Nearly 100 privacy and security experts participated

Sponsored by
Project 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 legal to reach a common understanding of web application privacy

• Provide transparency about privacy risks

• Not in scope: Self-protection for users
Open Web Application Security Project

- Community dedicated for web application security
- Open source and non-profit organization
- Creates freely-available articles, methodologies, documentation, tools, and technologies
- Known for its Top 10 Security risk list (established standard) and other projects
- Provides platform for the Top 10 Privacy Risks project
Member of IPEN

Internet Privacy Engineering Network

- Founded in 2014 by EU Data Protection Supervisor's Head of Policy
- Goal to bring together privacy experts with developers
Project Method (1/3)

Model Creation → Identifying Violations → Rating of Violation Impact
OECD Privacy Principles → Identifying Violations → Investigation of Frequency of Occurrence

Rated List of Privacy Risks

Evolve Counter-Measures → Rated List of Privacy Risks → Evolve Best Practices
Survey to evaluate frequency of occurrence:
- 63 privacy and security experts participated
- Rated 20 privacy violations for their frequency in web sites
- Example: Sharing of data with third party (average 1.8)
Project Method (3/3)

Impact rating

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

Example

<table>
<thead>
<tr>
<th>V14</th>
<th>Impact on operator’s reputation and brand value</th>
<th>Financial loss for operator</th>
<th>Social standing and reputation of data subject</th>
<th>Financial wellbeing of data subject</th>
<th>Personal freedom of data subject</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing of data with 3rd party</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Privacy Risks: How would you rate?

a. Non-transparent Policies, Terms and Conditions
b. Insufficient Data Breach Response
c. Outdated personal data
d. Sharing of data with third party
e. Operator-sided Data Leakage
f. Missing or Insufficient Session Expiration
g. Insufficient Deletion of personal data
h. Insecure Data Transfer
i. Collection of data not required for the primary purpose
j. Web Application Vulnerabilities
Results: 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
# Results in detail

## Top 10 Privacy Risks Project

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Frequency</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Web Application Vulnerabilities</td>
<td>High</td>
<td>Very high</td>
</tr>
<tr>
<td>P2</td>
<td>Operator-sided Data Leakage</td>
<td>High</td>
<td>Very high</td>
</tr>
<tr>
<td>P3</td>
<td>Insufficient Data Breach Response</td>
<td>High</td>
<td>Very high</td>
</tr>
<tr>
<td>P4</td>
<td>Insufficient Deletion of Personal Data</td>
<td>Very high</td>
<td>High</td>
</tr>
<tr>
<td>P5</td>
<td>Non-transparent Policies, Terms and Conditions</td>
<td>Very high</td>
<td>High</td>
</tr>
<tr>
<td>P6</td>
<td>Collection of data not required for the primary purpose</td>
<td>Very high</td>
<td>High</td>
</tr>
<tr>
<td>P7</td>
<td>Sharing of Data with Third Party</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>P8</td>
<td>Outdated personal data</td>
<td>High</td>
<td>Very high</td>
</tr>
<tr>
<td>P9</td>
<td>Missing or insufficient Session Expiration</td>
<td>Medium</td>
<td>Very high</td>
</tr>
<tr>
<td>P10</td>
<td>Insecure Data Transfer</td>
<td>Medium</td>
<td>Very high</td>
</tr>
<tr>
<td>P11</td>
<td>Inappropriate Policies, Terms and Conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P12</td>
<td>Transfer or processing through third party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P13</td>
<td>Inability of users to modify data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P14</td>
<td>Collection without consent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P15</td>
<td>Collection of incorrect data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P16</td>
<td>Misleading content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P17</td>
<td>Problems with getting consent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P18</td>
<td>Unrelated use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P19</td>
<td>Data Aggregation and Profiling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P20</td>
<td>Form field design issues</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Frequency**

- High: 3.0
- Very high: 4.0
- Medium: 2.0

**Impact**

- High: 3.0
- Very high: 4.0
- Medium: 2.0
P2: Operator-sided Data Leakage

Internal procedures or staff are often a reason for data leakage

• Poor access management
• Lack of awareness
• Unnecessary copies of personal data
• Weak anonymization of personal data:
  – For publishing or using inside the company: e.g. “We are using anonymized data for marketing purposes.”
  – Anonymization can go wrong: e.g. AOL search data leak
  – Location data, browsing behavior or device configuration can be used to identify people
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
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 source: Ghostery
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

Picture sources: facebook.com, web.de
Countermeasures (1/4)

Raise **Awareness** among:

- **Product / Application Designers (business)**
  - They decide about functionality that affects privacy
- **Developers / IT**
  - Sometimes have the choice to implement privacy friendly applications
- **Data Protection / Legal**
  - Personal information is mainly processed in IT systems
  - IT has to be considered when implementing privacy programs
- **Questions:**
  - How many of you have a legal background?
  - How many of you consider web applications in their privacy programs?
Countermeasures (2/4)

Implement **processes**

- That consider privacy in all development stages from requirements analysis to implementation (preventive)
- To audit privacy measures in web applications (detective)

**Ask simple questions**

- Did you consider privacy when designing the application?
- Did you address the OWASP Top 10 Privacy Risks?
  - How are privacy incidents handled?
  - How is data deleted?
  - How do you avoid vulnerabilities in the application?
  - ...

Sponsored by OWASP
Countermeasures (3/4)

Technology examples

• Avoid Data Leakage
  – Restrictive Access Management
  – Awareness campaigns
  – Strong anonymization techniques
  – Data Leakage Prevention (DLP) solutions

• Improve session timeout
  – Configure to automatically logout after X hours / days
  – Obvious logout button
  – Educate users
Countermeasures (4/4)

Technology examples

• Ideas for better transparency in terms & conditions
  – Text analyzer: readability-score.com
  – HTTPA: http with accountability developed by MIT

• Share data with third party on click only
  – Youtube embedded video: Enhanced privacy mode
  – Facebook buttons: heise Shariff

Picture source: heise.de
Summary

• Currently there are many privacy risks in web applications
• Compliance-based approach does not cover all of them
• Lack of awareness regarding real-life privacy risks
• OWASP Top 10 Privacy Risks project created to address this issue and educate developers and lawyers
• The project identifies technical and organizational risks independent from local laws
• Try to consider these risks when implementing or auditing web applications and apply countermeasures!
Further information

• OWASP Top 10 Privacy Risks Project: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

→ Feel free to contribute

• Internet Privacy Engineering Network (IPEN): https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN

• Project sponsor: http://www.msg-systems.com

• My personal blog: http://securitybydesign.de/