OWASP Top 10 Privacy Risks

Version 2.0 presented by Florian Stahl at the OWASP Stammtisch Hamburg

https://owasp.org/www-project-top-10-privacy-risks/
About me

Florian Stahl

• Principal Security Consultant @ msg Security Advisors (Munich / Regensburg)
• Dipl.-Winf., MSc, CISSP, CISM, CIPT
• 15 years of experience in information security & privacy (from pentester to team manager)
• Founder and Leader of the OWASP Top 10 Privacy Risks Project
• Hobbies: Family, tennis, snowboarding, travelling
• florian.stahl@owasp.org
Situation

- Schrems II
- Lack of enforcement and insufficient control by authorities
- Strong lobbyism
- Lack of implementation and expert knowledge
- NSA & Co.
  - Surveillance because of excessive fear of terror – despite doubtful effectiveness
- Global Use
  - Globalization requires global privacy standards
- Internet Technologies
  - Surveillance as business model – Feudal internet
- Privacy
  - Violation of fundamental rights by surveillance
Top 10 Privacy Risks Project – Facts & Figures

• 2014 Foundation & Publication of version 1.0
• 2015 Member of IPEN (Internet Privacy Engineering Network)
• 2016 Publication of countermeasures
• 2021 Publication of version 2.0
• Currently working on countermeasures v2.0
• Available in 5 languages (soon in 7)
• OWASP Lab Project
Project Goal

- Identify the 10 most important **technical and organizational** privacy risks for web applications
- Provide transparency about privacy risks
- Independent from “local” laws based on OECD Privacy Principles
- Show countermeasures
- Educate developers, business architects and legal
- Not in scope: Self-protection for users

1. Limitation of Collection
2. Data Quality
3. Specification of the Purpose
4. Use Limitation
5. Security
6. Transparency
7. Individual Participation
8. Accountability
Method (1/2)

- Model Creation
- OECD Privacy Principles
- Identifying Violations
- Rating of Violation Impact
- Investigation of Frequency of Occurrence
- Rated List of Privacy Risks
- Evolve Counter-Measures
- Evolve Best Practices
Method (2/2)

Survey to evaluate frequency of occurrence

- 60 privacy and security experts participated (62 in 2014)
- Rated 20 privacy violations for their frequency in web sites
- Slider instead of 4 radio buttons unexpectedly caused less differences

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>
## Results Overview

### 2021 OWASP Top 10 Privacy Risks

<table>
<thead>
<tr>
<th>2021</th>
<th>2014</th>
<th>Privacy Risks</th>
<th>Frequency</th>
<th>Impact</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>⇒ Web application vulnerabilities</td>
<td>High</td>
<td>Very high</td>
<td>O</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>⇒ Operator-sided data leakage</td>
<td>High</td>
<td>Very high</td>
<td>O+T</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>⇒ Insufficient data breach response</td>
<td>High</td>
<td>Very high</td>
<td>O+T</td>
</tr>
<tr>
<td>4</td>
<td>New</td>
<td>✠ Consent on everything</td>
<td>Very high</td>
<td>High</td>
<td>O+T</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>⇒ Non-transparent Policies, Terms and Conditions</td>
<td>Very high</td>
<td>High</td>
<td>O</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>⇒ Insufficient deletion of personal data</td>
<td>High</td>
<td>High</td>
<td>O+T</td>
</tr>
<tr>
<td>7</td>
<td>New</td>
<td>✠ Insufficient data quality</td>
<td>Medium</td>
<td>High</td>
<td>O+T</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>⇒ Missing or insufficient session expiration</td>
<td>Medium</td>
<td>Very high</td>
<td>T</td>
</tr>
<tr>
<td>9</td>
<td>13</td>
<td>⇒ Inability of users to access and modify data</td>
<td>High</td>
<td>Very high</td>
<td>O+T</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>⇒ Collection of data not required for the user-consented purpose</td>
<td>High</td>
<td>High</td>
<td>O</td>
</tr>
</tbody>
</table>

Type O: Organizational, T: Technical
P1: Web Application Vulnerabilities

How to check?
• Are regular penetration tests performed (OWASP Top 10)?
• Are developers trained regarding web application security?
• Are secure coding guidelines applied?
• Is any of the used software out of date (server, DB, libs)?

How to boost?
• Apply procedures like the Security Development Lifecycle
• Perform regular penetration tests by independent experts
• Install updates, patches and hotfixes on a regular basis
P2: Operator-sided Data Leakage

How to check?
• Research the reputation and reliability of the operator
• Audit the operator (before signing the contract or using it):
  • Paper-based audit (fair)
  • Interview-based audit (good)
  • On-site audit and system-checks (best)

How to boost?
• Implement Awareness Campaigns
• Encrypt personal data
• Appropriate Identity & Access Management
• Strong Anonymization or Pseudonymization
• Further measures to prevent leakage of personal data (ISO 2700x)
P3: Insufficient Data Breach Response

How to check?
• Incident response plan in place?
• Plan tested regularly (request evidence like a test protocol)?
• Computer Emergency Response Team (CERT) / Privacy Team in place?
• Monitoring for incidents (e.g. SIEM) in place?

How to boost?
• Create, maintain & test an incident response plan
• Continuously monitor for personal data leakage and loss
• Respond appropriately to a breach
  • Assign incident manager and incident response team
  • Notify data owners
  • ...
P4: Consent on Everything *New*

How to check?
• Is consent aggregated or inappropriately used to legitimate processing?
• Data flow restrictions rather than consent

How to boost?
• Collect consent separately for each purpose (e.g. use of website and profiling for advertising).
• Consent should be voluntarily
• Helen Nissenbaum on Post-Consent Privacy - YouTube

“Stop Thinking About Consent: It Isn’t Possible and It Isn’t Right”

Dateneinstellungen verwalten
Alle akzeptieren

Picture sources: Why Data Privacy Based on Consent Is Impossible (hbr.org) & www.facebook.com
P5: Non-transparent Policies, Terms & Conditions

How to check?
Check if policies, terms and conditions:
• Are easy to find and understandable for non-lawyers
• Fully describe data processing
  • Which data are collected, for what purpose, ...
  • In your language
• Complete, but KISS (Keep it short and simple)

How to boost?
• Use a text analyzer, e.g.: [https://readable.com/](https://readable.com/)
• A short version of the T&Cs and pictograms can be used for easier understanding
• Use release notes to identify change history of T&Cs and policies/notices over time
• Deploy Do Not Track (W3C standard) and provide Opt-out
P6: Insufficient Deletion of Personal Data

How to check?
• Inspect the data retention or deletion policies / agreements.
• Evaluate their appropriateness
• Request deletion protocols
• Test processes for deletion requests

How to boost?
• Delete personal data after termination of specified purpose
• Delete data on rightful user request
• Consider copies, backups and third parties
• Delete user profiles after longer period of inactivity
P7: Insufficient Data Quality *New*

How to check?
• Is it ensured that personal data is up-to-date and correct
• Check for possibilities to update personal data in the application
• Regular checks for validation, e.g. “Please verify your shipping address”
• Question how long it is likely that data is up to date and how often it usually changes

How to boost?
• Provide an update form
• Ask user if his/her data is still correct
• Forward updated data to third parties / subsystems that received the user’s data before
P8: Missing or Insufficient Session Expiration

How to check?
• Is there an automatic session timeout < 1 week (for critical applications < 1 day).
• Is the logout button easy to find and promoted?

How to boost?
• Configure to automatically logout after X hours / days or user-defined
• Obvious logout button
• Educate users
P9: Inability of users to access and modify data

How to check?
• Do users have the ability to access, change or delete data related to them
• Are access, change or deletion requests processed timely and completely

How to boost?
• Provide easy-to-use ways to access, change or delete data
• Appropriate Data Structure Model to handle user rights
P10: Collection of data not required for the user-consented purpose

How to check?
• Request description of purpose
• Check if collected data is required to fulfill the purpose
• If data is collected that is not required for the primary purpose(s), check if consent to collect and process this data was given and is documented
• Are individuals notified and asked if purpose or processing is changed?

How to boost?
• Define purpose of the collection at the time of collection and only collect personal data required to fulfill this purpose
• Data minimization
• Option to provide additional data voluntarily to improve service (e.g. product recommendation, personal advertisement)
Challenges in creating version 2.0

• Time, time, time ...
  • Work on version 2.0 began in the beginning of 2020 and was done more than one year later

• Coordinate a (new) virtual team of people with different background from all over the world
  • Few conference calls
  • Work in Google Docs
  • You need someone with the big picture and the goal in mind

• It was harder to find volunteers than in 2014 – privacy experts seem to be busier

• Overlaps between risks (e.g. P7 and P9) and abstraction level
Next steps

• Translations (Chinese)
• Countermeasures v2.0
• Spread the word e.g. at:
• Apply in practice ;-)