Top 10 Privacy Risks Project

Update & countermeasures
9 September 2016, IPEN Workshop, Frankfurt

Florian Stahl (Project Leader, msg systems, Munich)
A Look back

- Open source project founded in 2014
- Goal: Educate developers, business architects and legal in web application privacy by showing (technical and organizational) risks
- Best practices, but not always 100% bullet-proof privacy
- Initial presentation of results at IPEN workshop 2014 in Berlin
Project Method

Model Creation → Identifying Violations → Rating of Violation Impact → Rated List of Privacy Risks → Evolve Counter-Measures

OECD Privacy Principles → Identifying Violations → Investigation of Frequency of Occurrence → Rated List of Privacy Risks → Evolve Best Practices
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P8  Outdated personal data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
Recent developments

• German translation available
• Recommended by DPAs (Bavarian, Hessian?)
• Countermeasures document published in April 2016
  - Contains sections on how to check risks and improve
P1: Web Application Vulnerabilities

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• Is any of the used software out of date (server, DB, libraries)?

How to improve?
• Apply procedures like the Security Development Lifecycle (SDL)
• Perform regular penetration tests by independent experts
• Install updates, patches and hotfixes on a regular basis
P7: Sharing of Data with 3rd Party

How to check?
• Are third party solutions in use (plugins, buttons, maps, videos, advertising, etc.), which ones and what personal data is transferred?
• Is third party tracking disclosed (which third parties and what data)?
• Are third parties rated and checked regarding privacy?
• Is privacy and handling of personal data part of the contract and if yes, what restrictions are in place?

How to improve?
• Use third party content only where required, not by default
• Develop a Third Party Monitoring Strategy
• Use privacy friendly solutions like
  – Social networks buttons that only send data on click (heise Shariff)
  – Youtube enhanced privacy mode
  – ...

heise Shariff: https://github.com/heiseonline/shariff
P9: 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 improve?

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

Picture sources: facebook.com, web.de
Further information

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

• Project sponsor: [http://www.msg-systems.com](http://www.msg-systems.com)

• My personal blog: [http://securitybydesign.de/](http://securitybydesign.de/)