OWASP
Open Web Application Security Project

Your most valuable asset: your users' data

Dr Konstantinos Papapanagiotou

Innovating for Privacy,
Athens, 3/4/2015

.about

- 10+ years of experience in InfoSec as a consultant and researcher
- Currently: InfoSec Solutions Sales Manager at OTE S.A.
- Involved with OWASP since 2005 as the Greek Chapter Leader
  - Co-Started the Hackademic Challenges Project in 2011.
  - Organized the OWASP AppSec Research 2012 conference.
- Research
  - PhD in Trust in MANETs – Univ. of Athens, GR
  - 10+ publications and 50+ citations
  - Teaching InfoSec and AppSec at Greek universities

r@ndol.ph @rabryst · Mar 29

I'd love to know why @Airbnb needs to know my Google Drive file names, and what it has to do with their business. pic.twitter.com/gbvcnaVifl

Airbnb Help

@AirbnbHelp

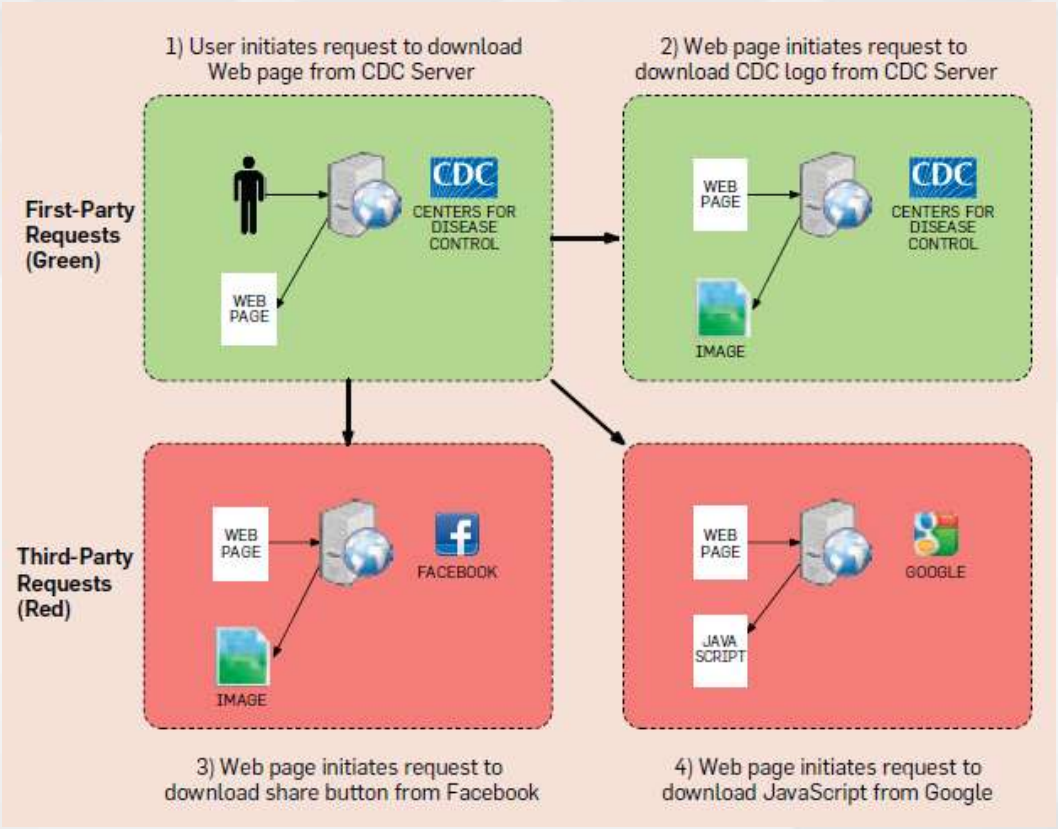
Follow

@rabryst "View metadata for files & documents in your Google Drive" gives us history & provides proof that it isn't a newly-created account

FAVORITE 1

10:09 PM - 29 Mar 2015

The “referrer” header leak



Timothy Libert, **“Privacy Implications of Health Information Seeking on the Web”, CACM, March 2015.**

About OWASP

Non-profit, open source organization

"Drive visibility and evolution in the safety and security of the world's software."

OWASP Core Values

OPEN: Everything at OWASP is radically transparent from our finances to our code.

INNOVATION: OWASP encourages and supports innovation and experiments for solutions to software security challenges.

GLOBAL: Anyone around the world is encouraged to participate in the OWASP community.

INTEGRITY: OWASP is an honest and truthful, vendor neutral, global community.

OWASP 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- P8 Outdated personal data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

OWASP

Top 10 Privacy Risks

Alpha Version 1.0

Website Application Vulnerabilities

#1

Frequency: High
Impact: Very High

Vulnerability is a key problem in any system that guards or operates on sensitive user data. Failure to suitably design and implement an application, detect a problem or promptly apply a fix (patch) is likely to result in a privacy breach. This risk also encompasses the OWASP Top 10 List of web application vulnerabilities and the risks resulting from them.

Operator-sided Data Leakage

#2

Frequency: High
Impact: Very High

Failure to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. Introduced either due to intentional malicious breach or unintentional mistake e.g. caused by insufficient access management controls, insecure storage, duplication of data or a lack of awareness.

Insufficient Data Breach Response

#3

Not informing the affected persons (data subjects) about a possible breach or data leak, resulting either from intentional or unintentional events; failure to remedy the situation by fixing the cause; not attempting to limit the leaks.

Frequency: High
Impact: Very High

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.”
  - Location data, browsing behavior or device configuration can be used to identify people

P5. Non-transparent, Policies, Terms and 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 data with 3rd parties

- 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

User Privacy Protection Cheat Sheet

- Panic Modes
  - For distressed users or users under threat.
  - Allows them to delete their data upon threat, log into fake inboxes/accounts/systems, or invoke triggers to backup/upload/hide sensitive data.
- Remote Session Invalidation
  - Allow users to view and invalidate current online sessions
- Allow Connections from Anonymity Networks

User Privacy Protection Cheat Sheet

- Prevent IP Address Leakage
  - Allow users to block 3rd party content
- Honesty & Transparency
  - Inform users on how their information is or might be used.
  - Allow users to remove sensitive information.
  - Cultivate a culture of trust.

Logging Cheat Sheet

- Sensitive information can be leaked through log entries
- Secure management of log data
  - Avoid logging personal or sensitive attributes in log entries.
  - Control access to log files.
  - Secure disposal of logs.

OWASP Mobile Top 10

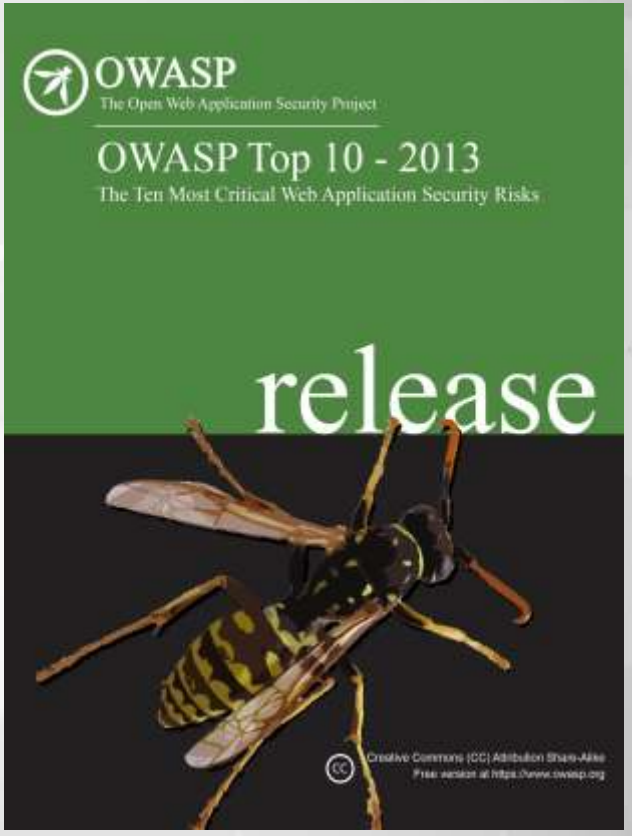
- M2. Inecure Data Storage
- M3. Insufficient Transport Layer Protection
- M4. Unintended Data Leakage
- M6. Broken Cryptography
- M10. Lack of Binary Protections

OWASP Top 10

- A6. Sensitive Data Exposure
- A5. Security Misconfiguration

Indirectly:

- A1. Injection
- A2. Cross-Site Scripting



To Do

- Raise Awareness/educate
  - Product/Project Managers, Solution Architects
  - Developers/IT
  - Data Protection/Legal
- Implement design, implementation and audit processes for privacy protection.
- Deploy privacy protection technology.

Resources

- OWASP Top 10 Privacy Risks
  - https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- OWASP User Privacy Protection Cheat Sheet
  - https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet
- OWASP Logging Cheat Sheet
  - https://www.owasp.org/index.php/Logging_Cheat_Sheet
- OWASP Top 10
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- OWASP Top 10 Mobile Risks
  - https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

THANK YOU

Dr Konstantinos Papapanagiotou
konstantinos@owasp.org