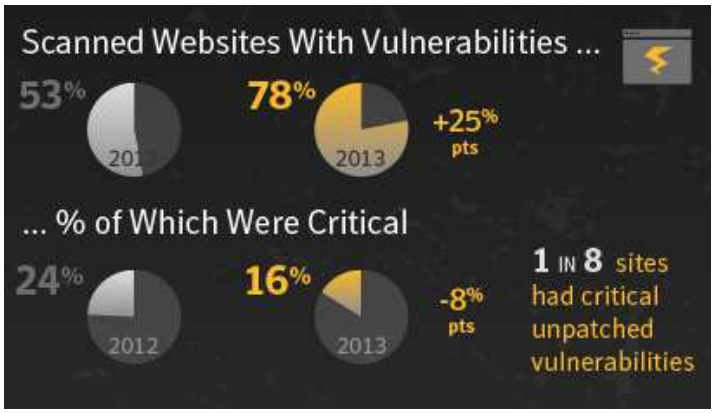
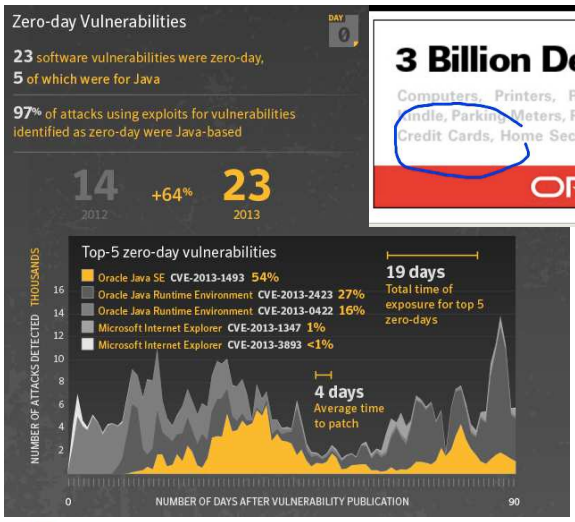
Application Security: To the future and beyond
OWASP LATAM TOUR 2014

Fabio Cerullo
OWASP Global Board
CEO @ Cycubix Limited
fcerullo@cycubix.com

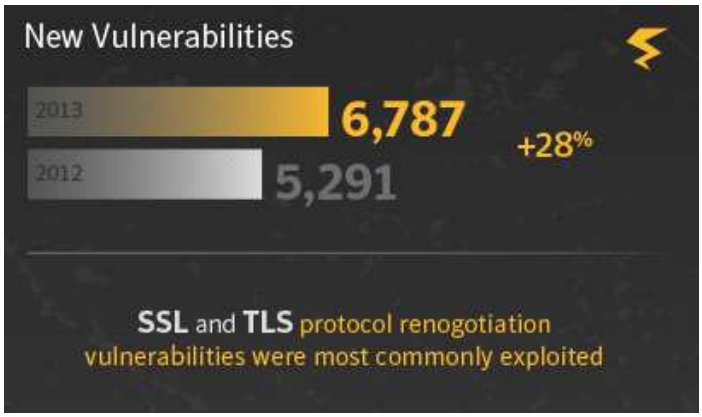
Software Threats



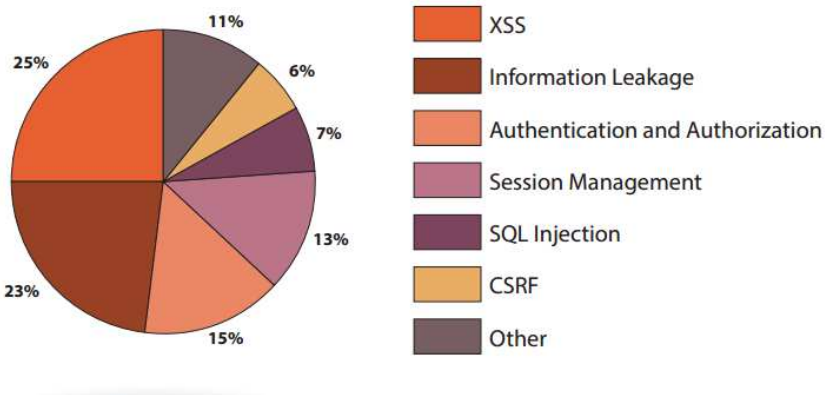
Software Threats



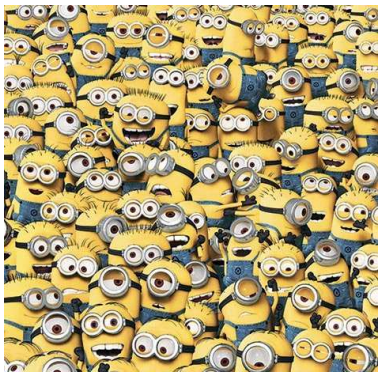
Software Threats



Web Application Threats



Web Application Threats

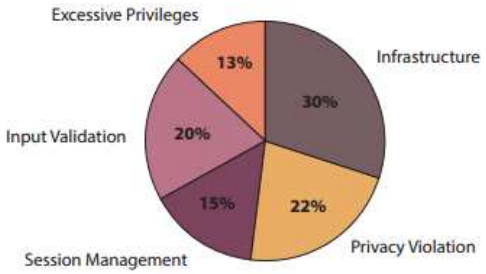


OWASP Top 10 2013

A9 – Using Components with known vulnerabilities

Proliferation of APIs
Code Reuse
COTS

Mobile Application Threats



& 2+ Million Apps combined

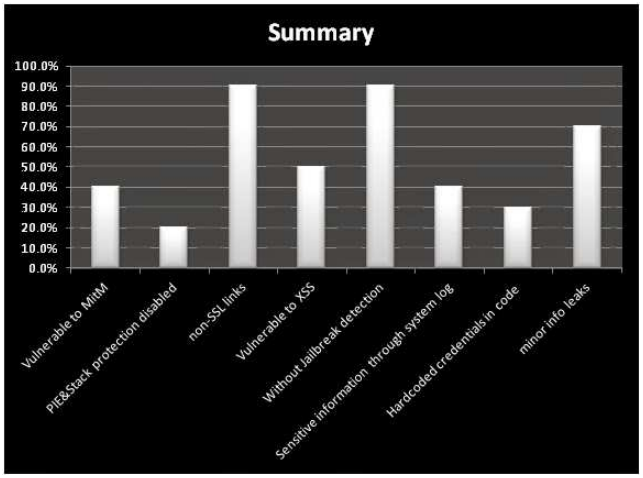
Mobile Application Threats

Android WebView Exploit, 70% Devices Vulnerable (Feb 2014)

- Android 4.0-4.2
- Javascript vulnerability
- Discovered 2012
- Google Glass
- Metasploit

https://docs.google.com/file/d/0B3_TQgTE2uPcMkdBOExKNjh0N28/edit

Mobile Application Threats



iOS Mobile Banking Apps

- 40 apps sampled from major financial institutions. 90% contain vulnerabilities.
- New vectors of attack.

Mobile Application Threats

Tesla Model S API Authentication Flaws via Mobile App

6 chars password
Token valid for 3 months
No track of valid tokens
Caching of token
Storage of credentials

Embedded systems

Toyota Prius "Intelligent" park hack

Hacked Smart Refrigerators sending spam

Nissan Recalls Over 1M Cars for Air Bag Glitch

Recommendations

Developer Awareness

Risk Based approach

Security Testing & Code Review

Web Application Firewall/SIEM

Stringent Review of 3rd Party Apps/APIs

Mobile App Reverse-Engineering Protection

Thank you

Questions?

Sources:

Symantec Internet Security Threat Report 2014

Cenzic Vulnerability Trends Report 2014

OWASP Mobile Security Project

About Cycubix Limited:

Founded in 2011, Cycubix provides information security goods and services including:

- **Risk Management:** Identification, assessment and mitigation of information security risks. Implementation of risk metrics and supporting management information (e.g. risk dashboards).
- **Application Security:** Technical consultancy in the areas of penetration testing, secure code review and secure application development; assuring that IT application software and infrastructure are designed, implemented, and operated in accordance with applicable security standards and best practices (OWASP, SANS).
- **Security Assurance & Compliance:** Implementation and management of information security policies, processes and projects that adhere to industry standards such as ISO27001, PCI.
- **Security Training:** Delivery of trainings in various information security topics for technical and business audiences.

cycubix Information Security