OWASP Mobile 2016 & Self-healing Apps

By Milan Singh Thakur

OWASP
The Open Web Application Security Project

Bits of My Profession

OWASP
The Open Web Application Security Project

- Tech Enthusiast and Speaker
- Security Consultant @ Aujas Networks
- Global Project Leader @ OWASP Mobile
- AppSec INDIA Leader @ OWASP
- Security Blogger @ Data Security Council of India (DSCI)

Proposed Mobile Top Ten for 2016

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Client Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality

What is to be done..?

- We stick to OWASP Mobile Top Ten 2016 as standard control
- SSL Pinning (just a recommendation, nightmare for developers)
- Strict Input validation
- Recursive Appsec activity

Majority of Vulnerabilities

- Injection attacks
- Parameter tampering
- Hooking of Malicious apps with genuine app
- And of course MITM plus many more
- Launching of unwanted events/activities

Few questions in mind..?

- Why we need Self-Healing apps, when we are already doing Appsec?
- Which domains will benefit from this concept?
- How will we ensure integrity of request/response?

The Self-Healing Concept..

- Signing HTTP headers and agent (Securing our Req/Resp Model)
- Use Time stamps to detect delays
- Timestamp + Hash .... Much safe ☺
- Example: JSON web signatures is already implemented
- https://tools.ietf.org/html/rfc7515

Contd..

- Learning at server side can be used
- Google Volley
  - Automatic scheduling of network requests
  - Request prioritization – checking time
  - Cancellation request API
  - Retry and Backoff customization
  - Concentrate on App specific logic

Thank you OWASP CHINA…!! Happy Security ☺

OWASP

Mobile Security Project