Becoming a Pro

IN Mobile Applications Testing

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

Workshop : ANSWER THESE QUESTIONS

1. *What do you consider to be the biggest security issues with mobile phones?*
2. *How seriously are consumers and companies taking these threats?*
3. *What can be done about these threats?*

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

- Attacks on mobile devices range in volume and severity, but all have the potential to cause chaos at both a device and network level.

Just like in the conventional fixed Internet world, attacks come in all shapes and sizes – such as:

- Phishing (criminals attempt to trick users into sharing passwords etc)
- Spyware (tracks user's activity, perhaps selling data to advertisers)
- Worms (a program that copies itself onto multiple devices via network connections)
- Trojans (a program that looks genuine but hides malicious intent)
- Man-In-The-Middle Attacks (where a criminal intercepts and manipulates messages between two devices or device and computer).

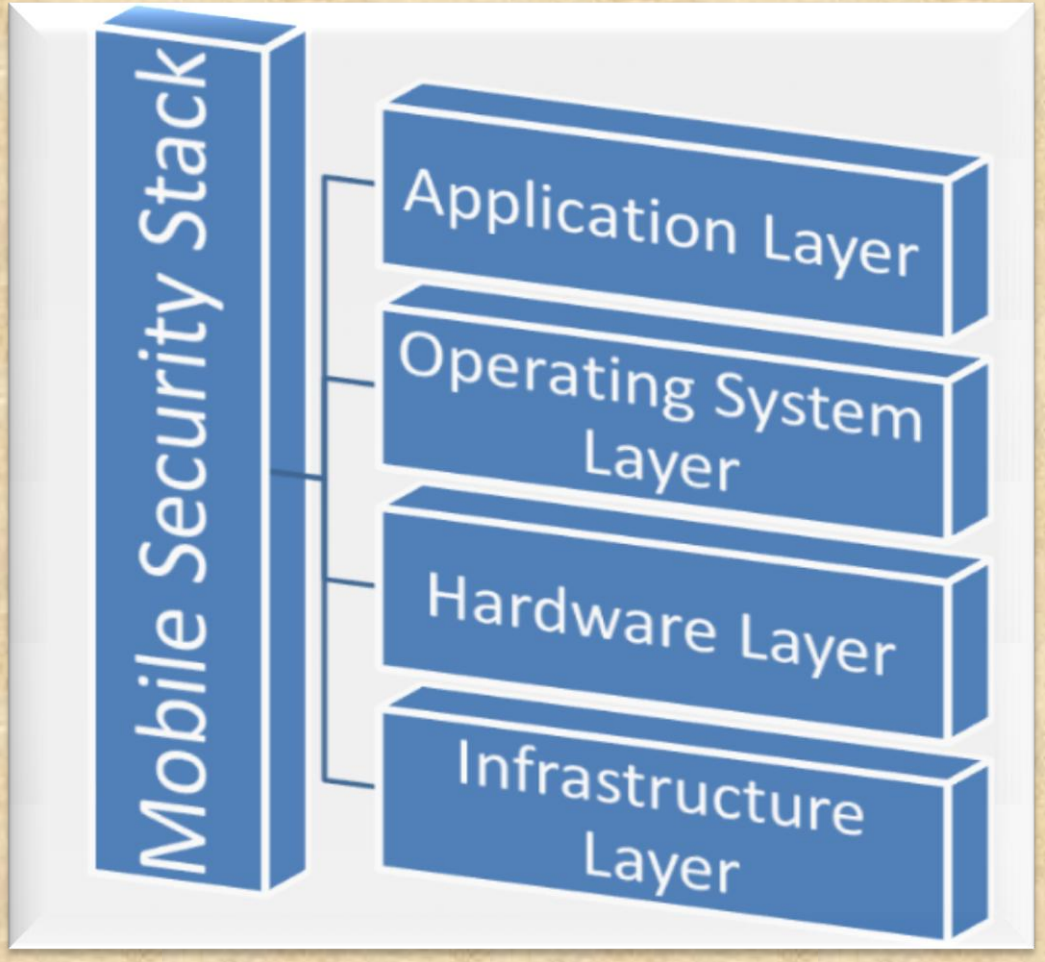
Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

The Mobile Code Security Stack

- The mobile code security stack can be broken up into four distinct layers.
- Each layer of the mobile code security model is responsible for the security of its defined components and nothing more.
- The upper layers of the stack rely on all lower layers to ensure that their components are appropriately safe



Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

Mobile Device Risks at Every Layer

- NETWORK
- HARDWARE
- OS
- APPLICATION

Example :

Your device isn't rooted but all your email and pictures are stolen, your location is tracked, and your phone bill is much higher than usual.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA

What is OWASP ?

- The Open Web Application Security project is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of Web App Security

OWASP Top Ten:

- The Top Ten was first published in 2003 and is regularly updated.
- Its goal is to raise awareness about application security by identifying some of the most critical risks facing organizations.
- The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, Defense Information Systems Agency, FTC, and many more.

CWE – COMMON WEAKNESS ENUMERATION :
https://cwe.mitre.org/about/

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

There are two main categories of mobile code security risks:

MALICIOUS FUNCTIONALITY

- The category of malicious functionality is a list of unwanted and dangerous mobile code behaviors that are stealthily placed in a Trojan app that the user is tricked into installing.
- Users think they are installing a game or utility and instead get hidden spyware, phishing UI or unauthorized premium dialing.

VULNERABILITIES.

- The category of Mobily Security vulnerabilities are errors in design or implementation that expose the mobile device data to interception and retrieval by attackers.
- Mobile code security vulnerabilities can also expose the mobile device or the cloud applications used from the device to unauthorized access.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN 2017

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Sensitive Data Exposure
- A4-XML External Entities (XXE)
- A5-Broken Access Control
- A6-Security Misconfiguration
- A7-Cross-Site Scripting (XSS)
- A8-Insecure Deserialization
- A9-Using Components with Known Vulnerabilities
- A10-Insufficient Logging&Monitoring

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

A1-Injection

Injection flaws, such as SQL, OS, XXE, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query.

Example:

- The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

2. A2-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly,

Attackers can compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

3. A3-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII.

Example:

Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

4. A4-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents.

External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

5. A5-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced.

Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

6. A6-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

7. A7-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript.

XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

8. A8-Insecure Deserialization

Insecure deserialization often leads to remote code execution.

Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

9. A9-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

10. A10-Insufficient_Logging &Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test

CREATE CHECK LIST BEFORE

- Phone identifiers such as (IMSI or IMEI)
- Address Book
- Account Details
- E-maiL
- Stock application data
- Banking Data
- GPS Location(s)
- Web History
- User's Dictionary
- Images
- Notes
- Calendar Appointments
- Call Logs
- Encryption Keys

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps EXTRA

SUMMARY

Functional
- Validation of Functionality
- Smoke / Regressions Testing
- Offline access testing
- Negative Testing

Non Functional
- Network Strength / Outage / Recovery
- Different NW Types
- Peripheral Testing

Interoperability (IOP)
- Voice / SMS interrupts
- Notifications
- Battery /Cable Removal

Memory Leak
- Memory Usage
- Memory Leaks
- Garbage Collection

Performance Testing
- CPU Usage testing
- Network Usage
- Page Render time or activity Render time

Usability Testing
- User Experience
- Competitive Analysis
- Expert Review

Installation Testing
- New App Install
- Uninstall and **Reinstall**
- Upgrade testing

Security Testing
- OWASP Vulnerabilities
- Dynamic Testing
- Static Code Analysis
- Data Encryption

Language Testing
- Validation for Locales
- Images and Text
- Currencies, time zones etc.
- Context