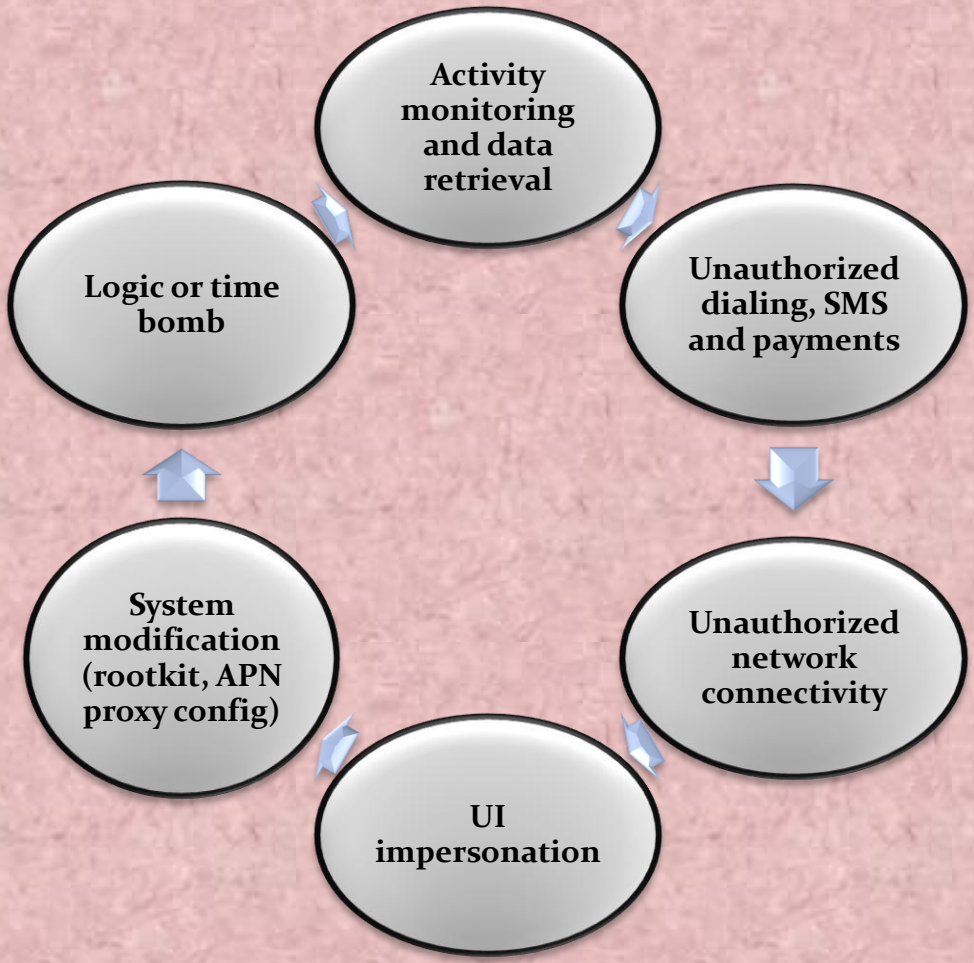
Becoming a Pro

IN Mobile Applications Testing

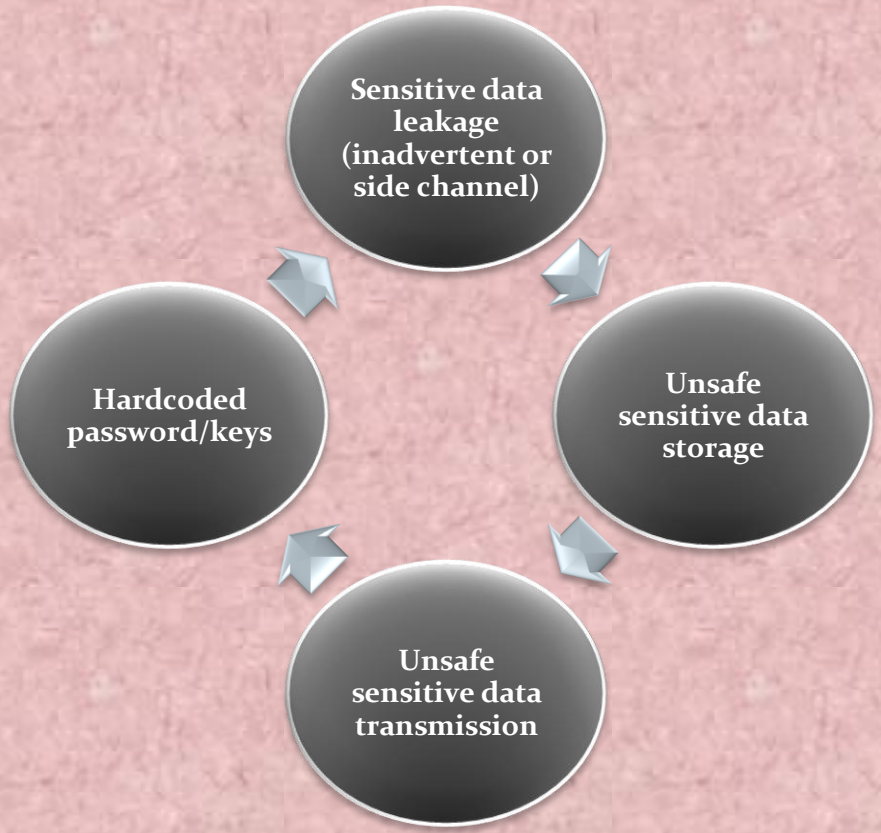
Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN



Malicious Functionality



Vulnerabilities

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

1. Activity monitoring and data retrieval RISKS

EMAIL SPAM sent to 3rd Party addresses

Monitoring phone calls/MIC recording

Stored data, contact list or saved email messages retrieved.

Examples

attackers can monitor and intercept:

- Messaging (SMS and Email)
- Audio (calls and open microphone
- recording)
- Video (still and full-motion)
- Location – Contact list
- Call history
- Browsing history
- Input
- Data files

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

2. Unauthorized Dialing, SMS, and Payments RISKS

Directly monetize from a compromised device

Premium rate phone calls, premium rate SMS texts mobile payments

SMS text message as a spreading vector for worms.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

3. Unauthorized network connectivity RISKS

Mobile devices are designed for communication

Therefore Spyware or other malicious functionality typically requires exfiltration to be of benefit to the attacker.

Examples

examples of communication channels attackers can use for distribution of a malicious SW:

- Email
- SMS
- HTTP (Hypertext Transfer Protocol) get/post
- TCP (Transmission Control Protocol) socket
- UDP (User Datagram Protocol) socket
- DNS (Domain Name Server) exfiltration
- Bluetooth
- Blackberry Messenger

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

4. UI impersonation RISKS

Similar to phishing - attacks that impersonating website of their bank or online service.

Web view applications on the mobile device can proxy to legitimate website.

Malicious app creates UI that impersonates phone's native UI or the UI of a legitimate application.

Victim is asked to authenticate and ends up sending their credentials to an attacker.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

5.System modification RISKS

Malicious applications will often attempt to modify the system configuration to hide their presence.

This is often called rootkit behavior.

System Configuration changes also make certain attacks possible.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

6. Logic or Time Bomb RISKS

Logic or time bombs are classic backdoor techniques that trigger malicious activity based on a specific event, device usage or time.

When a logic bomb is programmed to execute when a specific date is reached, it is referred to as a time bomb. Time bombs are usually programmed to set off when important dates are reached

A logic bomb is a piece of malicious code that executes when specific trigger conditions are met. A typical example would be a program that monitors a company's payroll system, and attacks the company if a specific employee is terminated.

ALL SECURITY DATABASE : https://www.security-database.com/cwe.php?page=26&action=list

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

7. Sensitive Data Leakage RISKS

Sensitive data leakage can be either inadvertent or side channel.

A legitimate apps usage of device information and authentication credentials can be poorly implemented thereby exposing this sensitive data to 3rd parties.

Location

Owner ID info: name, number, device ID

Authentication credentials

Authorization tokens

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

8. Unsafe Sensitive Data Storage RISKS

Mobile apps often store sensitive data:

Banking and payment system PIN numbers, credit card numbers, or online service passwords.

Sensitive data should always be stored encrypted.

– Make use of strong cryptography to prevent data being stored in a manner that allows retrieval.

– Storing sensitive data without encryption on removable media such as a micro SD card is especially risky.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

9. Unsafe Sensitive Data Transmission RISKS

It is important that sensitive data is encrypted in transmission lest it be eavesdropped by attackers.

Mobile devices are especially susceptible because they use wireless communications exclusively and often public WiFi, which is known to be insecure.

SSL is one of the best ways to secure sensitive data in transit

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test EXTRA- OWASP TOP TEN

10. Hardcoded password/keys RISKS

The use of hardcoded passwords or keys is sometimes used as a shortcut by developers to make the application easier to implement, support, or debug.

Once this hardcoded password is discovered through reverse engineering it renders the security of the application or the systems it authenticates to with this password ineffective.

Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

Security Test

2016 OWASP Release Candidate (not yet official)

- 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

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

Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE

Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE

How to Start Testing a Mobile Page

Find and divide page into components/modules

Create a list/table of modules/testing types/ testing

Create a variety of variables and conditions within each module

Specify the Expected and leave place for Actual Results

FOR TROUBLESHOUTING Create a list/table to view ANY problem from different angels

Create a Check List for Testing Categories:

Functionality Testing

Usability testing

Interruption testing

Connectivity testing

Compatibility testing

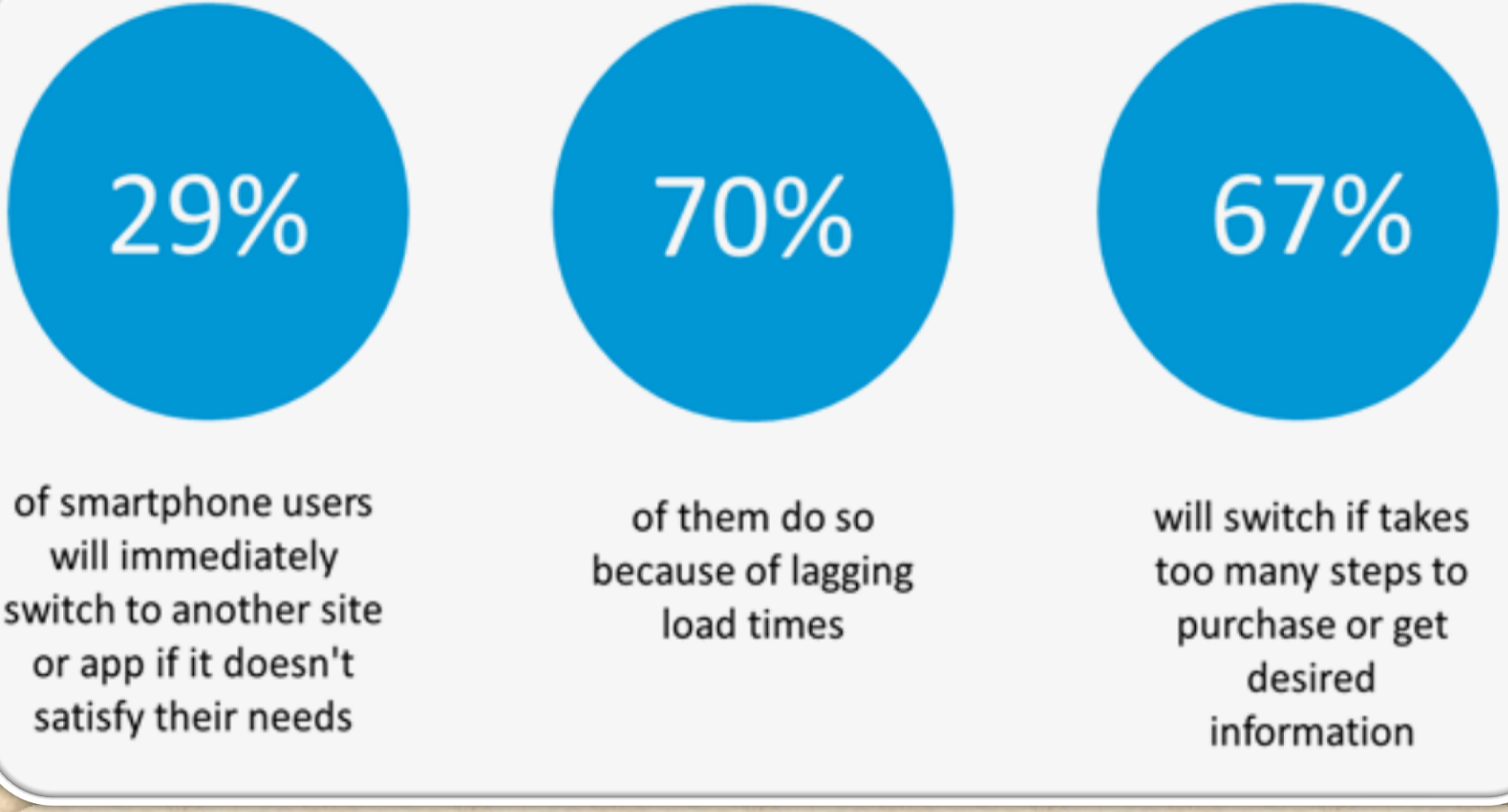
Performance testing

Security testing

Mobile Test Industry Standards

Testing Strategies for Mobile Apps : LETS PRACTICE

Consumers behaviour only on the basis of experience delivered by app



Mobile Test Industry Standards :

Testing Strategies for Mobile Apps

GUI TEST Checklist

- Navigation
- Formatting
- Color and fonts
- Scrolls
- Controls and alignments
- Spelling and grammar
- Justification
- Look and feel
- Default and shortcut keys
- Tab
- Opening input
- Alternatives
- Behavior
- Modality and multiple windows
- Contrast
- Images