Mobile Device Security

OPTIMAL RISK
Be Prepared, For Anything

The Problem

1. Mobile platforms are the most used platform in the corporate environment, and this proliferation has created the most widespread vulnerability.
2. Employees are issued with smartphones to improve productivity and responsiveness, but without any threat or risk implications taken into account.
3. Mobile devices are constantly introduced into corporate network (either by design, or inadvertently) – without any clear policy, or testing for the exposure that such devices introduce to the corporate security landscape.
4. Applications are built in-house, commissioned, or simply bought off the shelf. None of which are going through any assurance process, and are prevalent at every level of the organization.
5. Mobile platforms carry an implicit trust with them since they seem like limited devices with well-designed user interfaces and use-cases. They are actually built on fairly open platforms, fully featured computing platforms (equivalent of PCs), and a fully featured network stack.
6. Malicious software is easy to introduce into EVERY platform in the market (iOS, Android, BlackBerry OS, Windows Phone 7).

Breaching the Network Perimeter

‼ Mobile devices have essentially de-perimiterized even the more vigilant organizations.

‼ WiFi connectivity to the corporate network, combined with 3G access to the public internet, and occasional connectivity to unknown networks (coffee shops) have rendered these devices into a highly sought after attack vector for criminals.

‼ Conclusion: Companies need to assess their current situation internally in terms of mobile platform threats, as well as create a development and testing framework for the applications they build for their customers and users.

Mobile Application Security Review & Design

Testing existing applications for security flaws including:

- ✓ Data leakage through mobile platforms
- ✓ Creating network breaches/bridges into the corporate LAN
- ✓ Compromising applications and devices for spying and exploiting additional corporate resources

Comparing risk postures of mobile application use vs. standard online (web) or client-server models used, by analyzing the threat and risk models of both channels, and creating a roadmap that assures security on both.

Mobile Application Security Testing

Mobile platform exposure risk analysis provides an accurate risk analysis for the organisation, with actionable recommendations for policies & controls by:

- ➢ Review & test of mobile usage in a corporation.
- ➢ Test currently deployed applications, platforms, and topology.
- ➢ Check newly introduced devices

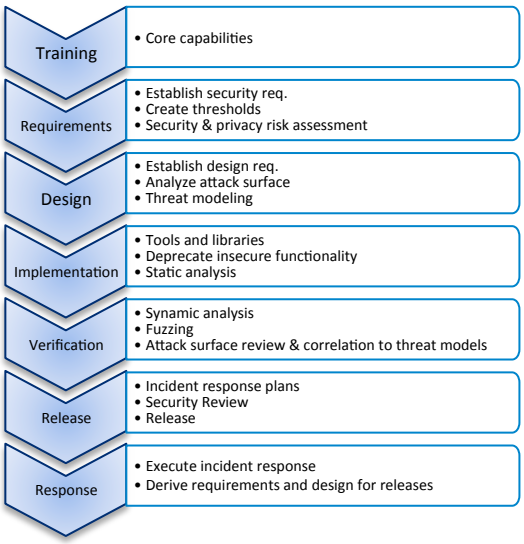
Our testing methodology for mobile devices includes, but not limited to:

- ✓ Local Vulnerabilities
- ✓ Remote Vulnerabilities
- ✓ Network Vulnerabilities
- ✓ Fraud-Proof/Phishing/Usability
- ✓ Theoretical Attacks

Secure Development LifeCycle for Mobile Application R&D

We offer several services that can be obtained as a full package or on a staged basis for application security testing.

- ✓ Design review and modifications
- ✓ Architecture review
- ✓ Threat Modelling
- ✓ Code review
- ✓ Black/Grey/White box testing of an application
- ✓ Testing of Mobile applications



For more information contact Dan Solomon at: dan.solomon@optimalrisk.com