Mphasis
Unleash the Next

Mobile Application Security Testing

Focusing on identifying and fixing security issues

A White Paper

by Giridhara Chitrapadi (Giri)
Architect, Advanced Security Testing

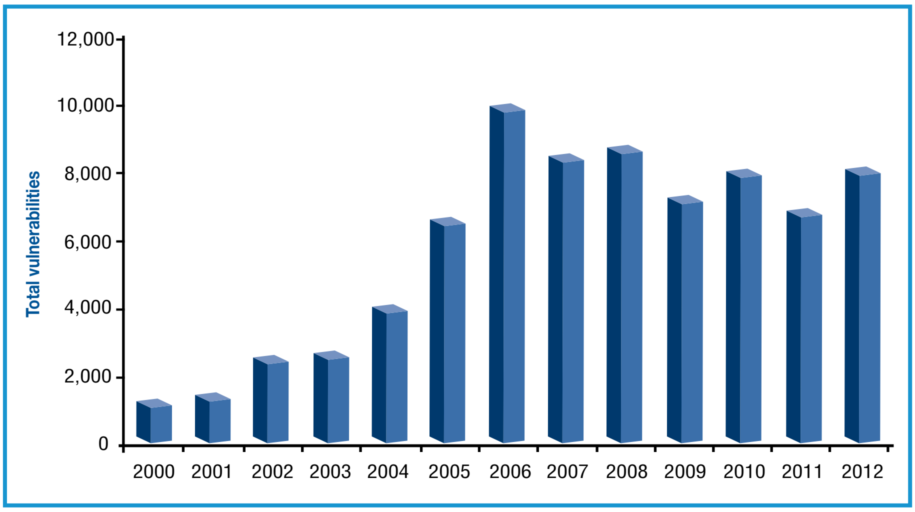
Contents

Introduction

The world is becoming smarter everyday with smarter mobile technology. There is an increased demand for smart applications especially in the area of Banking and Retail sector. The increasing reliance on these applications has given rise to major security issues. While most enterprises focus on releasing mobile applications in a short span of time to keep up with the competition, security considerations are often overlooked. Compared to desktop or web applications, mobile applications are difficult to test for security since they run on devices that are not managed by the enterprise which stores tremendous amount of personal, commercial and financial data that attracts both targeted and mass-scale attacks.

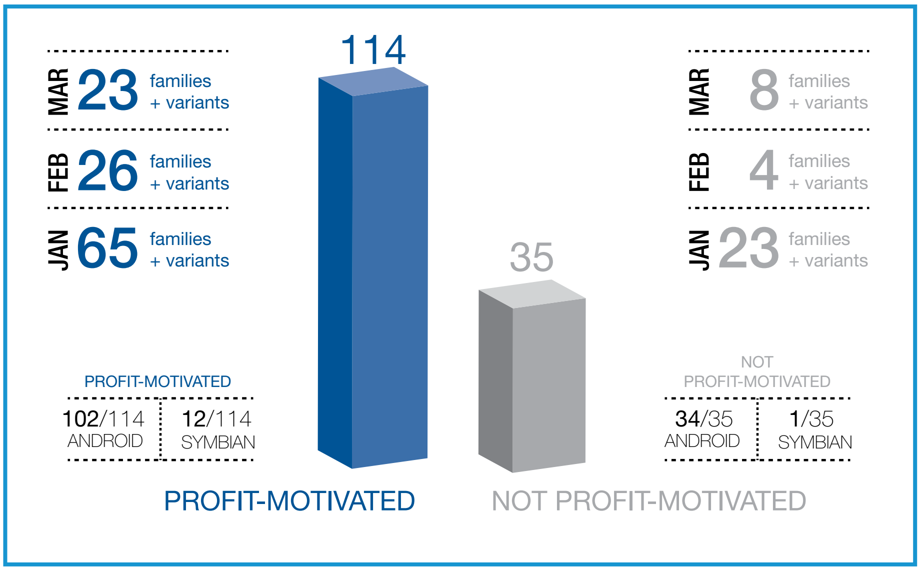
Mobile Application Security Facts and Challenges

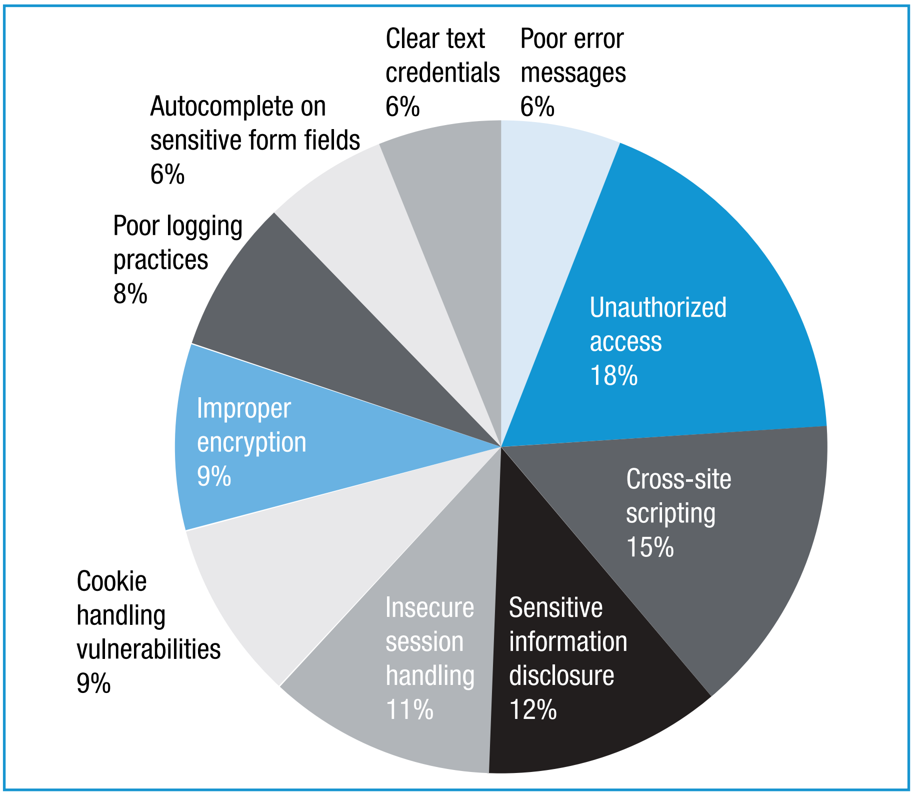
Below are some of the Mobile Application Security facts from recent studies.



800% increase in Vulnerability disclosures had been sighted in the HP Cyber Risk Report of 2012.

In a quarterly study, F-secure found out that there were about 149 families + variants of threats which was 50% higher than the last quarter. Out of these threats an alarming 76.5% was profit motivated.





Static and Dynamic analysis revealed Top-10 mobile vulnerabilities, published in HP Cyber Risk Report 2012.

These facts and figures clearly state that mobile application should be subjected to periodic scan to identify vulnerabilities and subsequent fixing methods, in order to ensure that there are no security risks for consumers.

The Mobile Application Threat Landscape

Mobile devices and apps are becoming ubiquitous to both personal and professional lives, allowing for near anytime access to critical information. As a result, mobile device operating systems and applications are immensely vulnerable to security risks. It is crucial to identify and fix these risks at regular intervals.

A variety of mobile application threats have been identified and categorized. Some of the key categories are:

Application-based threats

Mobile devices have the ability to host myriad of third-party applications and a user may unwittingly install a malicious application which may gain access to code and data. Independent studies have found that Google's android OS is at most risk of malware since the malware volumes reached 63% in year 2012. Another avenue is when an adversary may willingly hack the phone or reverse engineer the application to steal secrets used by the application.

Some of the examples of Application-based threats are: Vulnerable Applications, Privacy Threats, Malwares, Spywares etc.

Web-based or data-stealing threats

Sensitive information such as Contacts, User Data and Geographical locations could be lost due to malicious mobile applications. Though the threat probabilities may wary from mobile platform to platform, multiple platforms were exploited by an app called "Find and Call". The app claimed to help users sort and manage their contacts, instead shared the location and contacts with spammers.

Examples of web-based threats are: browser exploits, phishing scams and drive-by-downloads

Network-based threats

Cellular networks adopt new technologies to provide faster, more flexible access to cellular-based services. Devices have different software that operates on these local or cellular networks. Network exploits can take advantages of such software. Often, certain flaws in the mobile operating system can also lead to network sniffing. Under such circumstances, sensitive data get exposed while being sent from one device to the another with the help of improper security measures.

Some examples of network-based threats are: Wi-Fi sniffing, network exploits etc.

Physical threats

Fueled by insatiable demand for smarter mobile devices their physical security is an important consideration. There are innumerable lost and stolen devices and this is one of the most prevalent threats. The mobile device is valuable not only because the hardware itself can be re-sold but more importantly because it may contain information that are sensitive to a certain person or organization. It was reported that the Citibank iPhone app had customer-sensitive information stored in it. Storing of such data on mobile devices can prove risky, and if stolen can damage reputation of the enterprise and may also result in legal action against the enterprise.

The Mobile Application Vulnerabilities and Remediation

This section entails few of the key vulnerabilities that have been identified along with a possible remediation plan.

Scenario 1. Data-Stealing Threats: An adversary can steal sensitive information from the screenshots cached due to the iPhone's default screen capture feature.

Pressing the Home button while using a particular application can be risky. iOS inevitably takes a screen shot each time an application is used on an iPhone. The screenshot is taken in order to simulate the zoom-out and zoom-in animation. Certain devices, that do not have a user passcode for such situations, are at risk as the critical data that are displayed during this process are eventually lost or stolen.

The best solution to protect critical data from appearing in the screenshot cache is to:

- set "window.hidden" to "YES" in the applicationDidEnterBackground: delegate

- "window.hidden" to "NO" in the applicationWillEnterForeground:delegate.

This suspends the UI in the background before the screenshot is taken and restores it when the application is relaunched. Alternatively, you can choose to hide certain UI elements instead of the entire window.

```
- (void) applicationDidEnterBackground:(UIApplication *)application

{window.hidden = true;}
```

Scenario 2. Network-based threat: HTTP parameter manipulation attack can be used to transfer funds from another user's account.

Mobile applications often communicate with backend web application APIs to perform operations or receive data. A mobile-banking application talks to a mobile-banking API that performs operations that the mobile banking client requests. In this attack, the resilience of the backend application and web services are tested by manipulating HTTP request parameters to transfer funds. By changing the account number in the HTTP Request sent to the backend API it induces the API to transfer funds from another user's account.

Solution

1. Implement server-side mapping of the user to the respective accessibility. The features applicable to different privilege levels should be accessible strictly to those level users only.

2. Implement strong session management and log the user out if parameters are tampered with at any time.

Scenario 3. Application-based threat: Attackers may gain useful knowledge from sensitive information logged into Shared preferences folder.

Improper local storage can be another crucial reason for loosing sensitive data through mobile application. Android apps create a shared preferences folder for each application. This folder, if accessible by an adversary or malicious application can give away sensitive data and information. In the present scenario, the application log contains user's "credentials" into an xml file under shared preferences folder.

Solution

1. Implement server-side mapping of the user to the respective accessibility. The features applicable to different privilege levels should be accessible strictly to those level users only.

2. Implement strong session management and log the user out if parameters are tampered with at any time.

Mphasis Mobile Application Security Testing Overview

Mphasis Mobile Application Security testing services enables developers to focus on identifying and fixing security issues. We help enterprises gain security assurance for every mobile application that is being developed. Our security testing services are focused at identifying security risks under the four broad security threat areas. Our Mobile application security consultants conduct a comprehensive security test on mobile applications, using an established and proven testing methodology that leverages off-the-shelf tools, automation scripts for various platforms that are capable of identifying threats specific to the application – even those related to its business logic, rules and processes.

A detailed actionable report(s) will be delivered with in-depth explanations on vulnerabilities, specifically indicating vulnerabilities in application feature and code along with a possible remediation (where possible). Our "Post-remediation" security test can quickly confirm or report if all the security issues reported have been taken care of.

Mphasis mobile application security testing solution ensures apps are secure before they go live and every new version undergoes rigorous security testing against a 12-point stringent certification criteria that maps to OWASP Mobile Top 10, SANS Top 25, and other regulatory standards like PCI-DSS.

Achieving compliance to security standards like OWASP mobile top 10 is a key factor to gaining your customer trust for your mobile applications.

Assessment types

Mphasis offers 2 types of security assessments for mobile applications, both of these lead to security certification. Depending on the availability of application, app user credentials and source code a particular type of assessment can be chosen.

Mobile gray box security assessment

This methodology aims at identifying vulnerabilities that can be exploited using applications on mobile phones. The assessments attempts at hacking into the application both as a registered user and an anonymous user. This also tests the application's resilience against reverse engineer attacks, and leverages both open source and commercial tools. Testers build custom threat profiles to discover contextual security vulnerabilities that are specific to the application.

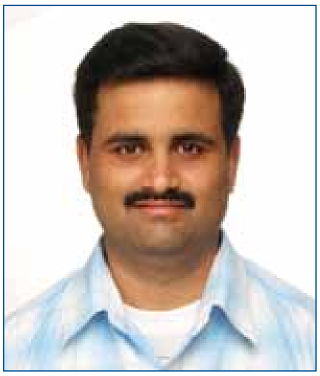
Mobile white box security assessment

Mobile White Box Security Assessment for IOS/Android aims at identifying vulnerabilities at the source code level. The assessments attempts at finding vulnerabilities from the coding or design flaws and the exploits the identified vulnerabilities as a registered user and an anonymous user. This type of security assessment leverages automated scripts and tools to analyze source code. This type of assessment aims at identifying backdoor and suspicious code, weak algorithm and cryptographic usage. Testers build custom threat profiles to discover contextual security vulnerabilities that are specific to the application.

Conclusion

Enterprises focus on developing mobile application to address their business needs, however in order to gain a competitive edge; security issues concerning mobile applications must be addressed. It is extremely important to examine these issues throughout development lifecycle, and ensure that any such risks are adequately mitigated. OWASP and other known security forums periodically release guidelines for securing mobile applications. All these guidelines should be diligently followed by developers and a structured mobile application security testing program should be implemented.

About Author



Giridhara Chitrapadi (Giri)

Architect, Advanced Security Testing

Giri has more than 11 years of exclusive experience in Consulting, Architecting and Deploying various security solutions such as Identity and Access Management, Application Security and Data Security. Extensive experience in a pre-sales role for security solutions and also has deep understanding of Architectural concepts, issues, trends, industry-specific requirements and regulations driving security solutions. Involved in programs with Fortune-500 companies worldwide and has managed teams located across geographies.

About Mphasis

Mphasis (an HP Company) enables chosen customers to meet the demands of an evolving market place. Mphasis fuels this by combining superior human capital with cutting edge solutions in hyper-specialized areas. Contact us on www.Mphasis.com

For more information, contact: marketinginfo@Mphasis.com

USA
460 Park Avenue South
Suite #1101
New York, NY 10016, USA
Tel.: +1 212 686 6655
Fax: +1 212 683 1690

UK
88 Wood Street
London EC2V 7RS, UK
Tel.: +44 20 8528 1000
Fax: +44 20 8528 1001

INDIA
Bagmane World Technology Center
Marathahalli Ring Road
Doddanakundhi Village
Mahadevapura
Bangalore 560 048, India
Tel.: +91 80 3352 5000
Fax: +91 80 6695 9942

Copyright © Mphasis Corporation. All rights reserved.

VAL 6/3/14 A4 BASIL 2487