International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 1 (January '2017)

MOBILE APPLICATION SECURITY

S.Danusree,
Sri Krishna Adithya College of Arts and Science,
Coimbatore, India.

D.Aldrine Douglas,
B.Sc (CS).,
Sri Krishna Adithya College of Arts and Science
Coimbatore, India.

N.Anurag,
B.Sc (CS).,
Sri Krishna Adithya College of Arts and Science
Coimbatore, India.

Abstract: This mobile application over security is about the essential mobile app security ecosystem security decisions on authentication and authorization one based on the values of these inputs. The World where communication traffic between mobile Apps will be completely secure. Nowadays in Android Smartphone many apps are developed some of them are causing virus hanging to their mobile phones because these phones are not protected by the security it appears to be impervious to decryption efforts. The trend to encrypt communication is a consequence of this reach for privacy secure communication is peer to peer architecture with end to end encryption. Data storage is protected data stored on the device whether in volatile memory persistent memory or removable storage. Security uses to secure access and deployment of approval enterprise is in they give security any thought they figure developers too late of all that for them 360 security apps IV manager are the Some of the apps to secure the mobile phones through security.

Keywords: Mobile Application Security, Data Storage, Android, Smartphone

I.INTRODUCTION

Mobile Application Security testing contains a small part of the Mobile Security testing process. Mobile Security testing consists of two steps. They are 1.Mobile Device Security Testing 2.Mobile Application Security Testing. Mobile Security Testing is a process of testing that the device as well as applications protects the data while maintaining the required functionality as planned. Mobile Device Security Testing involves protection of the devices such as phones, tablets, notebook computer and the network they are connected to, against threats and vulnerabilities linked with wireless networks. Mobile Application Security Testing means checking of mobile applications to stick fast to the highest grade security standard. And, also testing the application for security issues [1]. Most legacy applications used in the operation were not designed with a mobile interface in brain. Once business introduces mobile devices into the workplace, they have to reorganize how business application will be accessed from the devices, and smoothing over architectural problems just won't do it. As with most things, a one-size-fits-all approach to mobile app security testing is not satisfactory, because every mobile application is unique and requires a different level of mobile security. Doing it right requires that you can understand the challenges mobile application security testing brings.

Mobile app security testing is critical to meet today's security threats. In 2013 SANS survey found that organization are most concerned about:

- Device security
- VPN access controls for protection of company application
- Achieving unified access that supports security policies [2].

Mobile Security threats include both physical and software based threats that can cooperate the data on smart phones, tablets and similar mobile device. Mobile security threats include everything from mobile forms of malware and spyware to the potential for unlawful access to a device's data, particularly in the case of unplanned loss or stealing of the device. Mobile malware and spyware security threats can access a device's private data without a us knowledge of the users or permission and can also perform hateful actions without the user knowing, including transferring control of the device to a hacker, sending unwanted messages to the device contacts, making classy phone calls on smart phones, and more[3].

II.THE ESSENTIAL MOBILE APP SECURITY ECOSYSTEM

Mobile application must be treated as fundamental parts of an enterprise security ecosystem, extending from the device to the cloud or data center. A mobile software initiative (MSI) that starts and stops with mobile device management (MDM) has not done enough. Simply controlling the mobile device itself doesn't protect the data that the device access, transmits and stores. Nor it is enough to just apply mobile application management (MAM) without considering the security of wireless communications, the data center and cloud services. A complete approach to mobile application security is required -- where the mobile app is viewed as an integral part of a security ecosystem, reaching from the mobile device to the core of the cloud and/or data center. Although an end to end security approach is the goal, this column focuses on those security capabilities that center on the mobile endpoint, its apps and data. These essential EMM security features include:

A. Environmental and Biometric Sensors

Environmental and Biometric Sensor in a device (such as video, image capture, sound, motion, fingerprint, point of reference, proximity, acceleration, ambient temperature, wetness, etc.) should fulfill with the organization's data capture policy, and their use should be selectively controlled by MDM.

B. Device Access Control

Device Access Control that protects physical access to the device by requiring successful credit of a policy defined password, pattern swipe, biometric scan, voice or facial recognition.

C. Content Management / Data Loss Prevention

Content Management/Data Loss Prevention software uses encrypted on-device data storage ("containerization"), policy-defined cut-and-paste controls and website access control via URL filtering to restrict the intentional or inadvertent non-compliant sharing of protected content.

D. Encrypted Data Storage

Encrypted Data Storage is cipher-encoded protected data stored on the device, whether in volatile memory, persistent memory or removable storage.

E. Application Management and Security

Application Management and Security uses MAM to secure access and use of accepted enterprise mobile application, including the ability to approve (white list) compliant apps, and quarantine (blacklist) non-compliant apps. MAM services, such as those from Air Watch, Mobile Iron, typically incorporate an enterprise application store, which provide a central online location for downloading and tracking policy-compliant mobile apps for use by employees.

F. Device Management and Security

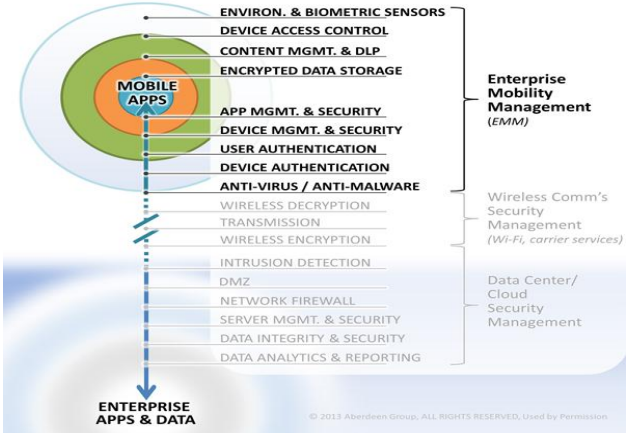
Device Management and Security uses MDM to describe and implement policy regarding control of the mobile device remotely, over the air. Typical services, available from Box Tone, SAP Afaria and Fiberlink, include over-the-air device wipe means erase all applications and data on the device, device lock means block device access and remote device configuration.

G. User Authentication

User Authentication requires confirmation of the user's distinctiveness as described in a corporate directory service before giving access to protected data or software. Two factor authentications is usually recommended for private data, such as a user name or password combination plus a effectively answered challenge question or positive fingerprint identification.

H. Device Authentication

Device validation confirms the uniqueness of the physical device. It must meet security and arrangement requirements, independent of any of its users.[4]



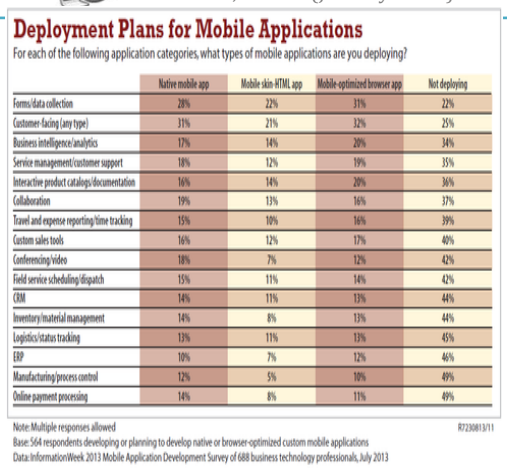
III. SECURITY DANGERS

Most people are not thinking about security and data privacy when buying a scone at Starbucks with their phones, playing Angry Birds while commuting, or using whatever clever application is the keystone of your digital business strategy. If they give security any thought, they figure the developers took care of all that for them. The app is from a reputable company, and they got it from the application store or even directly from their employer. What could go wrong? A lot. The global mobile infrastructure is a complex, interconnected, and desirable target. While security particulars vary widely, depending on the type of app being deployed, it's up to Information Technology leaders to ensure that user convenience never trumps protection of valuable enterprise or consumer information.

A. Insecure data storage

The Starbucks mobile app is one of the most widely used mobile payment application in the United States. Consumers simply enter their passwords once when activating the payment portion of the app and use it again and again to make unlimited purchases without having to reinput their password or user name. While that might be suitable for a caffeine-starved public, Starbucks recently confirmed that its app was storing usernames, email address, and password in clear text.

That allowed anyone with access to the phone to see passwords and usernames just by connecting the phone to a PC. Clear text also displayed user's geo location tracking points. With this information in hand, unauthorized individuals would have the credentials to log in to the Starbucks website as well. It's common for users to employ the same username and the password across systems, so if someone compromise that particular password, the potential also exists for them to compromise additional user accounts. Design application in such a way that serious information such as passwords and credit card numbers do not reside directly on a device. If they do, they must be stored securely. For iOS, passwords should be stored within an encrypted data section in the iOS keychain. For Android, they should live within encrypted storage in the internal app data directory, and the application should be marked to disallow backup.



Deployment Plans for Mobile Applications

For each of the following application categories, what types of mobile applications are you deploying?

	Native mobile app	Mobile skin-HTML app	Mobile-optimized browser app	Not deploying
Forms/data collection	28%	22%	31%	22%
Customer-facing (any type)	31%	21%	32%	25%
Business intelligence/analytics	17%	14%	20%	34%
Service management/customer support	18%	12%	19%	35%
Interactive product catalogs/documentation	16%	14%	20%	36%
Collaboration	19%	13%	16%	37%
Travel and expense reporting/time tracking	15%	10%	16%	39%
Custom sales tools	16%	12%	17%	40%
Conferencing/video	18%	7%	12%	42%
Field service scheduling/dispatch	15%	11%	14%	42%
CRM	14%	11%	13%	44%
Inventory/material management	14%	8%	13%	44%
Logistics/status tracking	13%	11%	13%	45%
ERP	10%	7%	12%	46%
Manufacturing/process control	12%	5%	10%	49%
Online payment processing	14%	8%	11%	49%

Note: Multiple responses allowed R7230813/11
Base: 564 respondents developing or planning to develop native or browser-optimized custom mobile applications
Data: InformationWeek 2013 Mobile Application Development Survey of 688 business technology professionals, July 2013

Data collection is a accepted function in both platform specific and browser based application, according to a recent Information Week mobile application development survey.

***B.* Weak server-side controls**

When creating their first mobile applications, businesses often expose systems that had not previously been accessible from outside of their networks. Often, these formerly protected systems are not fully vetted against security flaws. A number of back-end APIs assume (quite wrongly) that an app will be only thing that will access it. However, the server that an application is accessing should have security measures in place to prevent illegal users from accessing data. It's serious that backend services be hardened against malicious attackers. This means all APIs should be verified and proper security methods be employed to ensure only official personnel have access.

C. Unintended data leakage

Brands covet the kind of personal information some mobile apps glean. Being able to personalize promoting offers to consumers is a key digital business goal. But it's important that this desire to gather personal data doesn't compromise a consumer's privacy. For instance, media informed recently contended that the NSA had tapped popular smart phone application like Angry Birds to gather the huge amounts of personal data including age, location, gender, and more that they collect. This is what's meant by a "leaky" application. It's not just consumer application that are at risk. Consider a healthcare app this is used to track how often a patient experiences a particular indication of a disease.

If the application also contained analytics that reported how often that same section of the application was viewed, it would be possible for someone with analytics access to determine the medical condition of a specific user and place the provider in destruction of HIPAA compliance .Every employee in the world has been there, unhappy in their current job. They begin the search for a new job using their private accounts and job websites. For most employees, they felt safe in the haven of their personal devices, personal email, and personal social media accounts. Use caution when choosing analytics providers and implementing advertising. Watching what, how, when, and where data moves can give an attacker a gold mine of information. Do this tracking before the bad guys and obfuscate where necessary.

D. Broken cryptography

Many widely used cryptographic algorithms and protocols, like MD5 and SHA1, have proven to be not enough for current security requirements. But there's no easier way to mishandle mobile encryption than for an organization to create and use its own encryption algorithms or protocols. Always use modern algorithms that are received as strong by the security community, and whenever possible use state-of-the art encryption APIs within mobile platforms -- think AES with a 256-bit key for encryption and SHA-256 for hash. If you're not sure about your cryptography, invest in manual analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. Poor key management is another issue that warrants close consideration. Many organizations make the mistake of using strong encryption algorithms, but implement their own keys and certificates in areas that are vulnerable to attackers. An example is when an app ships with keys stored in the byte code. Since the keys are common across all app installs, the security is negated because anyone who gains access to someone's encrypted data can decrypt it.

E. Security decisions via untrusted inputs

A mobile app can accept data from all kinds of sources. In the absence of sufficient encryption, attackers could modify inputs such as cookies and environment variables. When security decisions on authentication and authorization are made based on the values of these inputs, attackers can bypass your security.For example, in 2012 a flaw in Skype security allowed hackers to open the Skype app and dial arbitrary phone numbers using a simple link in the contents of an email. Similarly, a bug in the iPhone 1 OS enabled hackers to listen in on phone conversations when those phones were connected to insecure wireless networks. Any app that has openings to accept data from external sources must include checks to all inputs used to build the app.If all this sounds complicated, that's because it is. Before embarking on a DIY mobile strategy, make sure your mobile developers can think through unintended consequences of app design. If they can't, get help. Delivering an easy-to-use app won't win you any points if you put customer or enterprise data at risk[5].

IV. REFERENCE

[1] Toshedra Sharma, "Introduction to mobile application security", Jan.5.2016.

[2] Adam Shearin, "The importance of mobile app security testing", May.26.2014.

[3] Forrest Stroud, "Mobile Security threats"

[4] Andrew Borg "How to keep Enterprise mobile appa secure ", Oct.1.2013.

[5] Charlie Fairchild, "Mobile app development: five security dangers", April.18.2014.