Mobile Apps Security Key Consideration

TECHNICAL PAPER

Introduction

As the rate of mobile device adoption continues to spike and the sophistication of these devices advance, users are becoming more efficient with the power they have in their hand anywhere and anytime. Unfortunately, they're also introducing a lot of risk into the IT equation. The more capable these devices are of helping users access and manipulate data, the more likely they are of being used by hackers for the same purpose. Mobile devices are a consumer's dream — and an IT security and management nightmare, for exactly the same reasons.

Mobile users are increasingly using applications, instead of the in-built web browser on the mobile device to access information, collaborate with other users and perform transactions online. When it comes to mobile security, all smartphones and tablets share a common set of challenges like — they carry a lot of data; they are often moving around in someone's pocket where they can be easily misplaced; they transfer data over a network that can be intercepted; and they run applications that may or may not be well written.

It is imperative for an organization to have their mobile security policies clearly defined and should be followed across the entire app lifecycle of conceptualization to deployment. This paper explains the key security considerations which should not be ignored while developing mobile apps.

Key Considerations - Mobile AppSecurity

App Data Security

Apps are as good as the data they display or generate. It is very important to secure the data that is stored on the device, based on its sensitivity identified by stakeholders. Data should be classified into Public, Private, Sensitive and accordingly different levels of security measures should be applied.

Password Storage on Device

As far as possible avoid storing passwords on the device, unless, it is the need of the application functionality. Passwords should not be in plain alphabetic String or text. It must be an alphanumeric word containing special characters also and the length should be 8 characters.

Passwords should not be stored locally on device, in worst case even if it is required to be stored, it should be tokenized or its Hash value should be generated using slow Hash algorithms like bcrypt, PBKDF2. This data then should be stored in a secure place for ex: iOS Keychain.

App Sensitive Data Storage

Special care should be taken of the sensitive data stored on the device by using a strong algorithm for encryption of all the sensitive data.

Use Encryption Algorithms like 256bit-AES

AES encryption algorithm has never been successfully cracked yet. 256 bit-AES is considered to be the World's safest encryption algorithm. It has 1.1*10^77 possible key combinations.

Encryption Key

Ensure the key used for data encryption is properly secured and not stored in the app or in the application code; it should be dynamically generated using a key derivation function such as PBKDF2 and user passphrase.

Ensure Security of Data - In Transit

Use SSL

SSL should be implemented on server for securing the data transfer over https. For implementing SSL, a valid SSL certificate must be installed on server. Applications should also use the APIs provided to make secure connections while connecting to the server.

Server Certificate Pinning

To avoid 'Man in the Middle Attack', certificate pinning should be done in the app. It is advisable to pin the public key (SPKI) rather than the certificate, to avoid any issues if the certificate is rotated by the site. It is a good practice to pin all the certificates in the SSL chain. I.e. Root CA, Sub CA and the leaf SSL. The Public key should not be stored as plain text in app; it should be hashed and stored. Only certificates from trusted CAs should be accepted by the app.

Client Digital Certificate Validation

Client certificates should be installed on mobile devices and stored on secure locations like keychain, these certificates n every

web-service call, the certificate which is validated by the server, should be sent. These certificates should be unique for each server and should be generated by an enterprise that issues Certificate Authority. Only a valid certificate will be accepted by the web-services. This will certainly avoid 'Man in the Middle' attack and is a better way of authentication.

Maintain Session

As per the need of application, sessions should be maintained both with the client and server. The longer the sessions stay active, the more they are vulnerable for attacks. Requests made after session expiry should be rejected by server and session timeouts should occur.

Authentication, Secure Devices and Code

User Authentication

Stateless tokens based authentication model should be used for communication between Mobile apps and the backend servers. No user state should be ever stored on the server and each individual request made by the client should be authenticated. This can be achieved by sending an authentication token in the header of every request where authentication is required.

Jail Broken Devices

Rooted or jailbroken devices are more prone to malware infection, and it's easier for a jailbroken device's operating system to be compromised. Mobile apps at launch should check if the device is rooted, if found the app should have a mechanism to terminate itself.

Uglify Code files

App builds like .ipa, .apk especially for hybrid apps can be easily expanded to view the HTML/JS/CSS source files. Use tools like Grunt to minimize and uglify the source code files.

Push notifications

Avoid sending sensitive or secure data over Push Notifications. It is recommended not to include sensitive/critical information in push titles, or body texts, as these will be visible when the message arrives in the notification console of the device.

Caching Data

HTTP Data should not be cached on device as it can compromise security. Storing and caching any part of response data should be avoided. All cookies should be deleted on app termination.

Logging

Debug logs should be removed from distribution and production builds as they can be easily viewed by configuration tools.

Streaming Media

Securing streaming media is more complex than other web service requests. There is no session in place, other alternative mechanisms are required. One of the better practices is to create Temporary random URLs and send them back to app on request. Rules set should be such that after a fixed time period these temporary URLs expire.

Create Strong Policies and enforce them using MDM

As per the type of organization, appropriate controls should be established that are aligned to your corporate policies.

Policies like setting up of complex pass-codes, ensuring full device encryption, remote wipe incase of the device being lost or stolen, limiting end users ability for access to a particular device feature or an app (Black listing/ White listing of apps) are some of the critical ones that need to be enforced.

These policies can be set through a Mobile Device Management solution. The mobile devices should be enrolled using the appropriate MDM solution that will help in managing these devices and ensure correct security profiles are installed on the device.

Hence, investing in a good MDM solution should be at high priority before allowing corporate data on mobile devices. There is always a debate that in case of BYOD the users may not like to have such strict policies on their personal devices, like changing of pass-code after every few days, etc. In such cases, the organizations need to divide the devices into categories like trusted devices-provided by organizations, tolerated devices of employees and non-supported devices.

Organizations can then create a set of policies for each category that should clearly define the kind of data or app to be accessed from each category. This will help the company in defining the different access levels without sacrificing security or control while providing flexibility to workers at the same time.

Mobile Risk Management

Organizations need to assess their risk profile, determine their own acceptable level of risk, and deploy the tools they need to protect their assets and stay within their compliance.

The risks associated with mobile deployments go far beyond the devices themselves and can be exposed through both physical threats (i.e. unauthorized access to lost or stolen devices) and digital threats (i.e. cyber-attacks, malware, malicious apps, etc.). Organizations need to take a holistic approach to risk management that will enable them to minimize the impact of potential breaches and non-compliance.

These threats can expose the organization to potentially expensive risks like:

- Financial Risk due to non-compliance of regulatory norms
- Security breaches and violations leading to reputation risk
- Intellectual property or data leakage leading to competitive risk

The first and last line of defence for mobile devices is its user. Users are running at admin level with the ability to install and delete apps, reconfigure settings, back up data or not. How well are the organizations informing them about risks? They need to know what action is to be taken when they see something suspicious going on with their mobile devices. Comprehensive mobile security awareness training is very effective at reducing risk. It is one of the strongest security control measures organizations can invest in outside of MDM technology.

Hence, every organization should identify their risks related to access of sensitive data, mobile device usage and theft, non-compliance of regulatory norms. Suitable MDM tools need to be introduced with the right MDM tools and increase employee awareness in order to mitigate the risks at the earliest.

Conclusion

Mobile security concern is a reality. If we are serious about a paradigm shift to mobility, our attitudes towards mobile data security, viruses, malware, should reflect that seriousness as well. We should not approach security on a mobile platform any differently than we would on a corporate desktop/laptop.

Enterprises should take special care while designing security solutions specifically for the mobile devices. These solutions should have the capability to communicate through multiple network topologies, cellular technologies and deliver security-related features in an efficient manner.

A comprehensive solution includes training people to use mobile devices securely, enforcing security policies to mobile devices and following the best security practices while developing mobile applications. The benefit of mobility outweighs the risks, but we need to be prepared to handle these situations with minimum risk.

Ultimately, one needs to find the right balance between what level of app security works for an organization and what the users of the app are ready to accept so that the app is easy to use and adopted well.

Author:
Navneet Cheema
Principal Solution Architect
Zensar Technologies

Zensar Technologies

Zensar is a leading digital solutions and technology services company that specializes in partnering with global organizations across industries on their Digital Transformation journey. A technology partner of choice, backed by a strong track-record of innovation; credible investment in Digital solutions; assertion of commitment to client's success, Zensar's comprehensive range of digital and technology services and solutions enable its customers to achieve new thresholds of business performance. Zensar, with its experience in delivering excellence and superior client satisfaction through myriad technology solutions, is uniquely positioned to help them surpass challenges around running their existing business most efficiently, helping in their legacy transformation, and planning for business expansion and growth through innovative and digital ways.

Corporate Headquarters: Pune, India
Global Offices: USA | UK | Europe | South Africa

For more information please contact: marketing@zensar.com | www.zensar.com