Security Considerations for mobilizing Enterprise applications

Mike Stauffer

Advanced mobile data networks and the promise of accessing mission critical apps anytime from anywhere are two reasons behind the increase in mobilizing enterprise applications. Palindrome recommends that any organization document all the security implications of mobilizing an Enterprise Application with a comprehensive security architecture. Additionally, Palindrome recommends thorough end-to-end testing of the mobile application…from backend servers to the mobile app itself.

Palindrome Technologies
100 Village Court
Suite 102
Hazlet, NJ 07730
Tel: +1 (571) 344-2960
www.palindrometech.com

Security Considerations for Mobilizing Enterprise Applications

Michael Stauffer

Introduction

The recent trend in enterprise applications is to leverage the BYOD momentum made possible by smartphones and tablet architectures built on Android and iOS to enable anytime and anywhere access to mission critical resources. The catalysts behind this trend include but are not limited to: more capable devices, a younger generation of users, Fortune 500 acceptance, and faster and more widespread data coverage. Application suites such as Remedy have tools that enable an organization to enable mobile access in addition to canned mobile applications that can be deployed. The result of this trend toward mobility is two-fold. First, the ability of users to access applications anytime from anywhere has provide demonstrable increases in productivity, increased ability to meet SLAs, and faster response times. Second, the ability to access sensitive corporate data from a new class of devices running Operating Systems derived from Desktop Operating Systems over various 802.11 or 3G/4G data networks places that information at increased risk of compromise. In this paper, Palindrome will outline two key principles for mobilizing enterprise applications: the proper development of a security architecture for mobile enterprise applications, and the proper and thorough testing of the applications and platforms that will enable this key functionality for our customers.

Remedy Mobile App

Security Architecture

Analysis of the types of data to be gathered, stored, and transmitted, the threats against that information, security requirements to mitigate the threats, and mechanisms to realize the requirements are properly identified and documented in a security architecture for the application to be mobile-enabled.

Android Application Permissions

The first element to be documented in the security architecture is the type of data that is to be gathered, stored, and moved between backend services and mobile platforms. The mobile application landscape is characterized by high-value information and low-value applications. When determining the criticality of the data being handled, regulatory considerations may apply. Does the data being accessed qualify as Personally Identifiable Information (PII)? Card Holder Data (CHD)?, Health-Related? GPS (Geo-Location) information? Information about the device (such as IMEI, MEID, CDN, ICCID)? In any situation, there are regulatory or industry-specific security requirements that must be considered. Keep in mind that well over 85% of incidents involved targeted PII and CHD, while roughly 1% of known incidents have user credentials as the target of attack. Once the exact nature of the data being manipulated is documented, then a threat analysis should be performed, taking into account the scenarios that are unique to mobile applications….lost

phones in particular. Remember that in the mobile environment, physical security is practically non-existent. Threats unique to the mobile environment might range from malicious apps in an app store to the reduced functionality that accompanies mobile browsers displayed on small screens. Threats might come from user devices with older versions of operating systems, or the general anti-patching mentality of most carriers in addition to the lag time for mobile OS patches generally. These threats might include the choices users have to make when installing app store applications, as shown for android in figure 2. Most importantly, these threats must include the backend servers, where most of the processing takes place, and not just on the mobile device. Attacks against the backend processing will be the most costly.

After the threats to the mobile data are documented and understood, security requirements are listed that will serve to mitigate the threats that have been listed to a level that is acceptable to the system owner. As mentioned previously, these requirements may well originate in regulatory or industry standards such as SOX, HIPAA-HITECH, PCI, or ISO 27001/27002. At the highest level, these requirements will look similar to the Confidentiality-Integrity-Availability triad most IA professionals are familiar with.

The final component of the mobile application security architecture is the documentation of the security mechanisms that will be deployed and utilized to realize the security requirements. If confidentiality of data in transit is a requirement, then non-proxied SSLv3/TLS with NIST-validated encryption algorithm may be the mechanism used to satisfy the requirement. The final product of the security architecture process is a complete picture of how security has been addressed throughout the deployment, with mechanisms that range from the type of allowed cryptographic transforms for data at rest and in transit to the policies for blacklisting old versions of mobile browsers and denying access to random devices. Included in the final comprehensive security architecture are the steps to be taken to educate the users about the security implications of having mobile access to critical data. Among these user-specific aspects might be the use of a corporate standard for SLD (such as m.corp.com vs. www.corp.com/mobile) and the user base should be advised to only use the corporate standard when accessing the mobile app. Users should be trained to know when SSL or TLS is being utilized, and not to click on links embedded in e-mails.

The next important area for mobilizing enterprise applications is validating the implementation to ensure that the security controls are enforced properly. This verification entails of executing specific test cases that aim in identifying inconsistencies in the implementation and potential weaknesses.

Security Testing / Assessment

The importance of performing end-to-end testing of the final mobile application architecture cannot be understated. As mentioned before, it is imperative to test not just the end device and its operating system, and the strength and integrity of any secure transport method, but also the security posture of the backend servers, operating systems, databases, etc. The goal of a committed attacker will rarely be the end device, but rather the backend services where the bulk of the critical data is stored.

Palindrome uses an end-to-end holistic approach to security testing for mobile applications. Listed here are a few considerations for testing mobile applications:

- Mobile portals are tested using full desktop testing platforms. Mobile portals may not be as robust as full web servers and should be tested thoroughly.

- Reversing and Debugging techniques (such as Java reversing) should be utilized while testing and measures to counteract reversing and debugging should be included in mobile application development.
- XSS, CSRF, HTTP redirects, etc. should be thoroughly tested. For Android applications, the Android emulator should be utilized for testing and development.
- Mobile Web portals utilize fields such as user-agent and accept request headers to determine which mobile browsers are being used and the implications of this usage should be thoroughly tested.
- The implications of utilizing proxied SSL/TLS (often the case in mobile applications) must be tested and documented.
- Backend testing must be particularly thorough as this is where most of the processing takes place for mobile applications.

- Depending on the criticality of the information being handled, the use of NIST-validated crypto modules may be recommended.
- Test mobile application on rooted / jail broken end devices. Be sure to see what the attacker sees.

Conclusion

As more and more organizations discover the benefits of having mission critical applications available to personnel anytime and anywhere, the growth of mobile enterprise applications will continue at a rapid pace. In order to ensure that due diligence has been performed prior to exposing proprietary data to the potential hazards of mobile device operating systems and their shortcomings, it is recommended that a thorough understanding of the threats, requirements, and mechanisms be obtained through documentation of the security architecture as well as security testing of the mobile application environment. Palindrome Technologies stands ready to leverage deep expertise to assist in deploying a mobile enterprise application in the most secure manner possible.

For further reading:

Juniper Networks. 2011 Mobile Threats Report. http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

Payment Card Industry Security Standards Council. PCI Mobile Payment Acceptance Security Guidelines. V1.0. September 2012

Foundstone Professional Services. Mobile Application Security Testing. http://www.mcafee.com/us/resources/white-papers/foundstone/wp-mobile-app-security-testing.pdf