SECURITY IN THE MOBILE ENTERPRISE

RHOMOBILE WHITE PAPER

This white paper was written by Adam Blum, Founder & CEO of Rhomobile.

12/18/2010

SECURITY IN THE MOBILE ENTERPRISE

Smartphone usage has exploded over the last couple of years, and its usage requires a different architecture than that which has been used over the past 15 years of information technology. Specifically, smartphone app usage is dominated by NATIVE apps not web apps. This pushes computing back to the edge as opposed to centralized processing done by web apps. With this new paradigm there are a new set of security issues and best practices that are not simply a rehash of web app best practices.

In order to reach the edge, enterprise smartphone apps require true, synchronized data for effective use in the enterprise. However, while synchronized data is the only way to get true app usage, it does introduce new security issues that need to be addressed. This document describes the five most important native smartphone app security issues:

- ✓ Transmission security
- ✓ Storage security
- ✓ App management
- ✓ Enterprise authentication
- ✓ Backend app authorization

In addition, this paper describes how Rhomobile products effectively handle each of these issues. These security concerns apply to any enterprise smartphone app, so we hope you will benefit from this outline whether or not you use Rhodes or RhoSync.

TRANSMISSION SECURITY

If you are sending sensitive information over the public internet, (which is generally the case with most smartphone apps) then you will need to secure the information in some way. This should be done with SSL, and via an https connection.

With Rhodes, just as with an Objective C or Android Java app, you will transmit the data over SSL (https). Both Rhodes and RhoSync support the use of https as a transport. In fact, it is easier with Rhodes than with Objective C. This is because with the Rhodes AsyncHttp.get call, you just list an https URL and Rhodes will connect to the backend appropriately. In contrast, when writing to underlying SDKs, significantly different code must be written in order to connect to an https URL.

STORAGE SECURITY

With native smartphone apps, unlike web apps or mobile web apps, generally you want to have data available on your device, and of course if you are using synchronized data that will always be the

case. If you are concerned about the availability of data on your device in the clear, then you can encrypt that data. As a best practice we recommend encrypting only the attributes that are truly sensitive information.

In Rhodes you can encrypt data with your Rhodes app using the Ruby crypt library calls. Block cyphers currently available include Blowfish, GOST, IDEA, and Rijndael (AES). Cypher Block Chaining (CBC) has been implemented, and Twofish, Serpent, and CAST256 are planned for release soon.

You can also use SQLCipher for transparent encryption. Finally, to ease some of the burden of integrating SQLCipher into your app, we will be adding transparent encryption as a model option in Rhodes 2.3.

APP MANAGEMENT

Native smartphone apps present new issues of managing access and updates to these apps. We recommend that enterprises consider some product to manage their apps and the data for those apps. It is important that the chosen software:

- ✓ update users with new apps that they should have
- ✓ provide updates to those apps
- ✓ remove apps, and the associated data, that those users should no longer have
- ✓ remove the app management portal when appropriate

Note that in these "Bring Your Own Device" days we do not recommend full mobile device management. MDM creates additional maintenance burden for IT administrators and is not likely to be accepted by users on their own devices.

Rhomobile's solution for this problem is called RhoGallery. RhoGallery is the first hosted app management solution, providing ease of deployment and use not seen before. Whether or not you use RhoGallery, we recommend choosing some mobile app management solution, but steering clear of full device management due to the complexity, cost and conflict with the BYOD future.

ENTERPRISE AUTHENTICATION

In order to achieve optimal sync server security, there must be delegated authentication to some form of enterprise directory. Ideally this should be the company's well-maintained LDAP directory. It is important that any sync solution support "delegated authentication" to tie into a company's overall directory system for authentication.

RhoSync makes it very easy to perform delegated authentication by simply providing an "authenticate" method that can call to any directory authority. A typical authenticate method is less than five lines of code.

BACKEND APP AUTHORIZATION

All sync source adapters should always login to the backend with the appropriate user ID. This ensures that users are only getting the information that they have rights to. It is important to avoid use of some form of global "app ID" to perform this data synchronization because overall information authorization schemes would be compromised.

Rhomobile's RhoSync follows this best practice, and authenticates simply with your backend app via the "login" method in each source adapter itself.

CONCLUSION

Mobile security in the enterprise is an issue of vital importance and concern to many companies that are expanding their mobile strategy. As sensitive information is pushed farther and farther to the edge by ever expanding mobile technology, it is necessary to follow the best practices outlined in this paper. Only send sensitive information via SSL and an https connection. Use encrypting to securely store data on the device. Employ the use of a mobile app management solution, like RhoGallery, but avoid the use of full mobile device management. Achieve optimal sync by requiring delegated authentication to the enterprise directory, and by requiring login to the backend database to ensure that only appropriate data is released to the user.

Rhomobile understands the risks associated with enterprise mobility and is constantly working to mitigate these risks. To learn more about how Rhomobile is the safest way to mobilize your enterprise, please see the **Rhodes Page** or contact **sales@rhomobile.com**.

rhomobile