



GoodDynamics

Key Considerations: **Developing and Deploying Secure Mobile Applications**



■ Contents

Executive Summary	3
The Realities of Developing Secure Enterprise Applications	3
How Data Leaves Mobile Devices	3
Developing and Deploying Secure Mobile Applications	4
Mobile Security in the Real World	5
A Platform for Speedy Deployment of Secure Apps	6
Speeding through Security Issues	7

Executive Summary

Mobility has become synonymous with productivity in the modern enterprise. Everyday business routines have been transformed by the ability to remotely access mission-critical corporate information from the road. Because mobile workers are always connected, highly pragmatic, independent, and demanding, enterprise application developers are constantly challenged with having to deliver secure mobile applications quickly enough to satisfy the needs of their end users. This is a daunting task, especially given the migration from company owned devices to personal devices, driven by the growth of personal smartphones and tablets flooding the enterprise.

The Realities of Developing Secure Enterprise Applications

The pace and pressure that developers are under to develop mobile applications as quickly as possible has made security an afterthought in most organizations. In some cases, developers' ability to deploy the same applications on multiple OS-based devices quickly may be the company's only hope of staying competitive and meeting business demands. This presents a real quandary for the typical mobile developer, who has neither the additional time, nor the technical skillset required to write security code for operating systems as diverse and eclectic as iOS, Android, and the myriad of web apps now widely available.

Businesses simply won't wait. Today, the most productive companies are the ones who have found a progressive approach to mobile device management—one that allows employees to have freedom of choice in the phones and tablets they find most comfortable using. Plus, in a standard enterprise deployment, several hundred, if not thousands of employees will need daily access to enterprise applications from a mobile device.

But businesses also can't afford the risks associated with unsecured, unmanaged devices. To balance a respect for the privacy and freedoms of their employees without compromising the security of their corporate data, managers are looking for a security, deployment, and management strategy that creates a strong separation between private information and the critical data employees need to get their jobs done.

How Data Leaves Mobile Devices

The common perception is that by securing the mobile device itself (for example, requiring an employee to enter a strong password to use their phone), one secures the data, as well. Unfortunately, securing the device alone does not prevent data loss. For example, critical data can be lost when an employee downloads sensitive enterprise information from the company CRM system onto their mobile device, as some devices are not able to encrypt application data – either on device or over the air. Another example of data loss occurs when an employee inadvertently (or intentionally) copies information from a corporate application to a consumer application.

Developing and Deploying Secure Mobile Applications

To address these challenges, mobile application developers and corporate IT should consider adopting the following best security practices:

Encrypt the Data at All Levels. While device-level security is important, it is generally a best practice not to rely solely on device-level security. For optimal protection, mobile enterprise data should be encrypted at all levels, including at the file system, application, database access, and device levels.

Use Strong Encryption. All application data should be encrypted with strong encryption—whether data is at rest on the device, or in transit between the device and servers behind your firewall. All information should be secured from end-to-end.

Isolate Corporate Application Information. All corporate application information accessed via mobile devices should be completely isolated from a user's personal data. This is particularly important for "BYOD" environments, although it holds true for corporate-liable devices, as well. Isolating mobile application data requires wrapping a layer of protection around enterprise-deployed apps, which securely separates corporate data from an employee's private information and consumer applications. Within an isolated or "contained" application, employees are free to be as productive as they are mobile — without behaving in an unsafe manner. Employees can exit the container housing the corporate applications to use their own consumer applications — without compromising company information. The overall effect of isolating corporate applications and data is a solution that increases employee satisfaction and productivity, while ensuring compliance. More importantly, the container-based method ensures that security is uncompromised at every level of transmission, reducing the risk of corporate data loss.

Enforce User-Level Application Security Policies. Mobile application developers should ensure that user-level application policies can be defined and enforced by IT security administrators. For example, strong application authentication would ensure that users are required to enter a strong password before they can launch the given application. Likewise, enabling remote-wipe of application data after a failed number of incorrect passwords, disabling sequential numbers in passwords, and requiring special characters in passwords helps to ensure that access to corporate applications and data is protected.

Ensure Secure Network Access. Enterprises should minimize the need to open inbound ports and expose the network. The secure mobile application solution should only serve encrypted packets, authenticating applications and granting access solely to those provisioned to specific servers and services—thus preventing rogue attacks.

Secure the Platform. Strong controls for securing the platform include detection of jailbroken phones, and prevention of access to other services, if necessary.

Partner with a Proven Player. Mobile application developers should partner with a proven mobile security provider. This will allow them to secure their applications without having to acquire myriad development tools, learn security best practices, or ask their IT infrastructure team to invest in and build out their own security infrastructure. It can also significantly reduce the time required to develop a secure mobile application, while enabling developers to focus on addressing the functional requirements of the mobile applications themselves.

Mobile Security in the Real World

SCENARIO ONE: If a new employee has recently joined the company and needs mobile access to corporate resources or data when she is out of the office, she may wish to use her personal smartphone to perform business tasks, such as checking customer information on a CRM system. To enable this access, her IT administrator must first make sure that appropriate entitlement and security policies are in place for the new employee. Subsequent steps would include the following:

1. The administrator provisions the mobile CRM app to the employee; this action would automatically generate an access key for the employee, and send it to her email address.
2. The employee then follows instructions in the email to download and activate the application. To ensure a high degree of security, each access code should only be used for a single activation.
3. Once the user has downloaded and installed the application, the application should follow its set-up instructions and performing the following tasks:
 - a. Create a unique profile for the mobile device in the system and authenticate the user's access key. The entitlement of the user to the application in use should also be checked at this stage.
 - b. Create a secure repository for organization data on the mobile device, and populate it with whatever data the user is allowed to see and use.
 - c. Download the appropriate policies for the user (e.g. password expiration).
 - d. Once the user is authenticated and authorized, a secure connection should be established to the system behind the enterprise firewall; this will allow the user to receive profile and policy updates via a push channel.
 - e. If there is a policy update that requires a security password to be set, then the user should be prompted to set this password before using the application.

SCENARIO TWO: An employee in the field loses his mobile device and needs to re-establish communication with the enterprise. There are three goals in such a situation: to preserve network and data security, to reconnect the employee quickly and securely, and to de-authorize and purge the lost device of sensitive data.

- Once the organization is aware of a lost device, a corporate IT administrator must be able to initiate a wipe, deleting corporate application data from the employee's device. **This preserves data security.**
- The association between the disabled application and the employee must also be deleted; this way, the employee is still entitled to run the application, but this particular instance of the application is no longer granted access to the corporate network. **This ensures network security.**
- The employee must then activate the application once again on a new device. In activating an application on a new device, the employee should still be recognized by the system as an authorized user, although there is no longer a registered device associated with this person. The organization's IT administrator must prompt the system to issue a new access code so the employee can begin the registration process for the device and a new application instance. The user can subsequently follow the process described in Scenario One, above, to register the device and new application instance, and initialize the secure mobile application.

SCENARIO THREE: Invariably, there will be times when an organization needs to implement a policy change or update an application client. Any deployed solution must accommodate changes to application entitlement or password and compliance policies, ideally through a centralized management console, leveraging a “push” notification system. The IT administrator should be able to apply such changes to either an individual employee or groups of employees.

■ A Platform for Speedy Deployment of Secure Apps

Leveraging the same technology used in Good Technology’s market-leading Good for Enterprise secure mobile device management and collaboration application, the Good Dynamics development platform enables corporations, independent software vendors, systems integrators, and in-house mobile application developers to build and deploy secure containerized applications – cost-effectively, across multiple device platforms. Good Dynamics is a ready-to-use security architecture that developers can put to work immediately to add dynamic security enhancements to their applications, without slowing development time.

Developers can quickly add Good Dynamics’ existing security libraries to their application builds—without having to learn about security or buy new tools. To get started, developers simply download the Good Dynamics SDK and server installers, initiate the SDK and server installation process, and rapidly integrate GD libraries into their applications.

A developer or administrator may then register the company’s new custom application with the Good Control (GC) web-based console, which includes features for providing a name, description, application ID and version. Once an application is registered, a user may be given entitlement to use the application. The enterprise IT administrator assigns the employee to the appropriate policy set, which may require the user to enter a strong password to access the company’s application on their mobile device. The employee is either assigned to an application group or given specific access to the required custom application. The administrator triggers the sending of a single-use access key to the user; the system sends the employee an email that includes the key, with instructions on how to activate the application.



Speeding through Security Issues

Good Dynamics is a comprehensive solution for enterprises tasked with quickly delivering secure mobile applications. It enables developers to get their applications out the door fast—but with a layer of security unmatched in the industry. Good Dynamics addresses the challenges of collaboration, connectivity, and choice, while giving IT the means to streamline the security and management of their mobile fleet. Leveraging an end-to-end encryption infrastructure that already serves the world's largest corporations, as well as defense and intelligence agencies, Good Dynamics is a ready-to-use security architecture that developers can put to work immediately to add dynamic security enhancements to their apps without slowing development time.

IT professionals can get started with a Good Dynamics SDK by joining the Good Dynamics Network at begood.good.com/community/gdn-welcome!input.jspsa. Or by calling 866-7-BE-GOOD.

© 2012 VISTO Corporation and Good Technology, Inc. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for Government, Good for You, Good Mobile Messaging, Good Mobile Intranet, Good Dynamics, and Powered by Good are trademarks of Good Technology, Inc. ConstantSync, Constant Synchronization, Good Mobile Client, Good Mobile Portal, Good Mobile Exchange Access, Good Mobile Platform, Good Easy Setup, Good Social Networking and Good Smarticon are either trademarks or registered trademarks of VISTO Corporation. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners. Good and Visto technology are protected by U.S. patents and various other foreign patents. Other patents pending.