Mobile applications and data security

Sean Szarkowicz
LANSA North America

The rate and speed at which mobile apps are being pushed into the marketplace is phenomenal and is not expected to slow down in the near future. Businesses are quick to capitalize on mobile technology in innovative and creative ways, both to please their customers and stay competitive in the marketplace, as well as to improve efficiency by providing employees with effective and productive access to data. As organizations rush to deliver mobile apps, they are at risk of overlooking critical security considerations.

To put mobile applications and data security in perspective, here are some statistics* that highlight the need to be mindful of security:

1. 85% of companies surveyed by AT&T have experienced one or more data breaches.
2. Malware increased by 97% from 2012 to 2013.
3. 36% of people do not have a password for their mobile device. 30% of those who do, save their password in notes on the device.
4. 3.1 million people were victims of smart phone theft in America in 2013, an increase of 194% on the reported thefts in 2012.
5. The number of mobile devices used for business purposes is expected to exceed 1 billion by 2018, of which almost 35% will be consumer owned (BYOD).

Luckily most of these security risks can be avoided, or at least their effect minimized, with some simple proactive steps.

Mobile application security can be broken down into three main categories.

- Securing data at rest on the mobile device
- Securing communication between the mobile device and the server
- Securing application access to the data

This article explores the challenges and solutions to developing and deploying secure mobile applications that ensure adequate protection of business information, while still allowing for user privacy and rapid rollout.

Securing Data at Rest

The first and most simple step is to secure access to the device itself by configuring password, PIN and gesture recognition that limit unauthorized access.

As native mobile apps have the ability to read from and write data to the device, it is extremely important to secure locally stored information. Only the authorized applications should be able to access the data.

Most mobile devices offer the ability to install business applications in a secure sandbox environment. Each sandbox provides a tightly controlled set of resources for its guest program(s), such as isolated disk space and memory. This allows for separation of corporate and personal data and applications. The corporate sandbox, controlled by the IT department, should be without any access to or from the personal sandbox. This approach protects the security of corporate business data, as well as the privacy of personal data.

When data is stored on the mobile device, the following are important considerations:

- Is the data properly encrypted, using an industry standard encryption algorithm?
- How sensitive is the information? If it is very sensitive, should it be stored at all?
- Has application access to the data been secured, for example with user ID/password?
- If the device is lost or stolen, can application access be immediately revoked and its data wiped remotely?
- What is the lifespan of the data? Will it be erased by an app and, if so, when?

Securing Communication

Most mobile apps access the corporate server using HTTP (HyperText Transfer Protocol), which is the most common Internet protocol. Unfortunately hackers can intercept data that is transferred over the Internet, including data transmitted to and from mobile apps, with sniffing tools and man-in-the-middle attacks.

The easiest ways to make communications more secure is to use HTTPS (S=Secure) instead of HTTP. Technically HTTPS is not a protocol in itself, rather it is the result of layering HTTP on top of the SSL/TLS protocol. Transport Layer Security (TLS), and its predecessor Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over the Internet. By using a HTTPS connection, data is automatically encrypted with a digital certificate that is configured on the server. Digital certificates and encryption keys, ranging from 128 to 4096 bits,

ensure that the data being transmitted is secure and is not available to hackers.

With the latest advancements in cryptography and digital certificates built into the IBM i OS and the Apache Web server, the IBM i stays on top of the list of the most reliably secure platforms.

Securing Application Access to Data

To ensure that mobile device users are only given access to information that they are authorized to view, some common best practices should be implemented:

- Setup role-based security on the server. This allows you to quickly revoke access to data and applications for an entire group of users.
- Perform security checks on the server.
- Never store passwords/PINs on the device.
- Log all application activity from all devices, on the server. Restrict access based on the unique device identifier and revoke access when a device is lost or stolen.
- Prompt for an additional PIN when access to critical data is requested.
- Revalidate login credentials after a period of user inactivity.
- Implement a firewall and a DeMilitarized Zone (DMZ) on the servers that are exposed to the outside world.
- Provide VPN access that can be easily enabled or disabled on the server side.
- Use remote monitoring capabilities and remotely wipe a device if it is lost or stolen.
- Encrypt sensitive information on the server and only send information that's strictly required to the mobile app.
- Update employees regularly about your security policies.

Conclusion

Application and data security will continue to be a cat and mouse game, as new vulnerabilities are found and exploited by the bad guys, while the good guys try to fix them. The good news (for the good guys) is that device manufacturers and operating system vendors are constantly improving their security features, for example, to detect malicious activity or viruses.

Organizations that aim to deliver secure mobile applications on a realistic budget should consider a cost effective and productive mobile application framework, using the following evaluation criteria:

- Does the vendor have a proven track record?
- Does the framework include ready to use building blocks?
- Does the framework support your choice of mobile devices (e.g. Apple and Android) and corporate servers (e.g. IBM i and Windows)?
- Does the framework leverage existing developer skill sets?

LANSA's LongRange mobile app development framework comes with building blocks for application navigation, user interface, security and also with example code for a variety of applications. IT departments can use their existing skill set (RPG, COBOL or LANSA) coupled with their business knowledge, to build and support secure mobile applications that deliver real business value.

LongRange's ability to run while connected and store data securely offline, provides a ready-made secure mobile infrastructure.

LongRange lets you combine authentication and login mechanisms that integrate mobile apps with existing business assets. It supports GUID (Globally Unique IDentifier), a method for identifying and authorizing mobile devices. LongRange can create a GUID at installation, or you can assign a GUID to each device. Another option is to issue a onetime access code to the device user.

Data transmissions between the LongRange app and server are compressed and encrypted with cryptographic nonce (a number or bit string used only once) to ensure that the data cannot be tampered with. Communications using HTTPS and VPN are supported.

LongRange supports multiple levels of authentication using the built-in user profiles and security tools that are part of the operating system on the server (e.g. level 50 on IBM i servers). Application level security further restricts access to applications and data. LongRange's authentication mechanism can be customized using the built-in exit points that are part of the LongRange mobile platform.

Data stored on the device by LongRange resides in a sandbox and is not accessible by other mobile apps. Last but not least, data can be encrypted and access restricted.

Often referred to as 'the most secure computing platform on the planet', the IBM i platform has a proven built-in object-based and user-profile management system. Even so, it is not a question of 'if' but 'when' attacks will occur. Therefore you should also consider security in a wider context. The checklist below will help you to ensure that multiple layers of security exist to keep the bad guys out.

***Sources for statistics:**

http://bit.ly/mob_sec_stats ■

12-Point Mobile Application and Data Security Checklist

1	Update your mobile device whenever application patches or operating system upgrades are released.
2	Always use a passcode to lock/unlock your device.
3	Do not jail-break, root or modify the operating system files.
4	Regularly backup or synchronize data to avoid loss of information due to theft. For additional security, install device-tracking apps to locate your device if it gets lost.
5	Only install apps from reputable vendors and check the app's review and ratings before downloading.
6	Never click on unknown URLs or respond to requests for personal information.
7	Make protecting your mobile device a priority, install a firewall and regularly scan for viruses and spyware.
8	Be careful when using public WiFi hot spots. Do not make purchases or other financial transactions and do not provide personal Information.
9	Access to business applications and data should always use a secure HTTPS connection or a VPN. Do not store sensitive data locally on the device unless it is encrypted and secured.
10	Work with your IT department to implement a security policy regarding what information is allowed to be accessed from mobile devices and how the organization will handle lost or stolen devices.
11	Make sure your development team incorporates security into the entire application development lifecycle by identifying and prioritizing critical applications and testing for security vulnerabilities. Retest when an application or infrastructure has changed.
12	Be prepared to adapt to the changing mobile landscape and regularly review your security policies and risk assessments.