Integrated Solutions For RETAILERS

10 Tips for Mobile Application Security

By Rick Hayes, Sr. Principal Consultant and Karthik Rangarajan, Principal Consultant, Dell SecureWorks

Mobile phones, tablets and applications enable you to access information anytime and anywhere you like. In the retail environment, mobile solutions help consumers make more informed purchase decisions, and provide new ways for retailers to engage with customers, employees, and partners.

Not surprisingly, smartphones and tablets represent the majority of net new growth in device adoption forecasts for the next four years. According to industry reports, smartphone sales now represent more than half of all mobile phone sales. And retailers are eagerly looking for ways to take advantage of this technology to help their bottom line. As mobile access and applications grow, however, so do the security challenges. So, how do you keep the bad guys out while still being innovative and keeping up with the latest technologies?

Why Is Mobile Application Security Important?

Mobility has spawned an unprecedented growth in application development. There are more than 1 million applications available across platforms such as Apple's IOS, Google's Android, and Microsoft's Windows. Retailers have seen the potential benefits of using these mobile platforms and applications for all aspects of their business. Mobility can drive higher customer satisfaction and sales, stronger dialogue with customers, reduced costs, increased operational efficiencies, stronger partner collaborations, and greater employee productivity.

Retailers everywhere are developing applications to interact socially, send coupons, disburse advertisements, and create sales. Companies like Nordstrom, JC Penney, Kohl's, Kmart, Sears, Macy's, Target, Starbucks, and Neiman Marcus are just a few of the retailers that have developed consumer-facing applications to engage consumers in new and innovative ways and in turn, increase revenue and brand loyalty.

With more retailers and customers using these applications, ensuring adequate security across multiple platforms is critical to mitigate risks and avoid devastating data breaches. A data breach can have a deep impact to not only the immediate bottom line; it can also undermine customer confidence and loyalty, and damage your brand reputation.

Must-know Tips for Deploying Secure Mobile Applications

Dell SecureWorks has more than 12 years of experience in managed security services, and has a world-class counter threat unit team of GIAC GCIA certified security analysts and multiple 24/7 security operations centers around the world. This enables us to provide customers with global visibility and threat intelligence, delivered through our Security and Risk Consulting services (SRC). Using this expertise, we have developed our top 10 must-know tips for deploying secure mobile applications.

Dell, the Dell logo, and Dell SecureWorks are either registered trademarks or service marks of Dell, Inc. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. Integrated Solutions For Retailers is a registered trademark of Jameson Publishing, Inc. © 2012 by Peterson Partnership. All rights reserved.

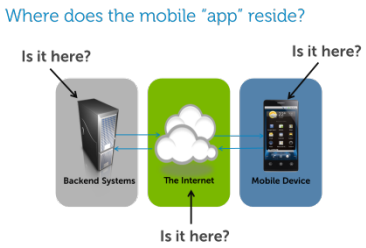
For more information, visit www.dell.com/retail or www.retailsolutionsonline.com.

Integrated Solutions For RETAILERS

1 Take into consideration the different use cases, limitations, and additional capabilities that mobile applications offer. Understand the differences and limitations of each platform from device to device and operating system to operating system. Encryption data, passwords, and even geo-location data must be controlled and sent only to authorized recipients.

2 Understand how to enable high security features and disable insecure ones. All high security features must be monitored and controlled so your channel remains secure. Remember, an attacker doesn't care what your system was intended to be used for; they only care if they can breach it.

3 Take into consideration platform-specific differences. Different operating system revisions have different features. For example, Android 2.1 is vastly different from Android 3 or 4. You need to account for any changes in security introduced by these multiple versions.



4 Consider backend systems for security and risk assessments. Backend systems are just as vulnerable to attacks as frontend systems. If an attacker can gain a foothold in your network using a backend system, they will do it. Best practices are to include backend systems in any risk or security evaluations.

5 Know the differences between the mobile app's backend infrastructure and those of traditional applications. Transport mechanisms and authentication can be completely different on the mobile platform.

6 Don't forget to test! Have someone knowledgeable in web application security help with the testing. Thinking that an application is just a mobile version of a web page can result in poorly coded mobile apps and vulnerabilities.

7 Understand how and where the app will be connecting to the network. The mobile device has to be connected to the Internet in some way, normally via cellular networks or Wi-Fi. Using a VPN instead of a public, non-encrypted Wi-Fi network will offer additional security.

8 Protect sensitive information in transit. Make sure you know what data you are going to be transmitting on the network and how it will be protected. Best practices recommend encrypting communications like initial login data is just one example to follow.

9 Be very careful how you store and use data. Do not store any sensitive data if it can be avoided. Storing unnecessary data adds to your risk level. Use encrypted data containers, key chain, or secure areas. Use cookies instead of stored passwords and minimize logs.

10 Be aware of what data you are using, gathering, storing, and transmitting. Consider any regulations that may impact data security. Privacy and information security regulations are frequently updated, particularly Payment Card Industry (PCI) requirements. GPS, IMEI, device numbers, and customer personal information all have privacy implications that must be noted. If the data is stored on the phone, is it encrypted? If the data is stored on the backend, who has access to it?

Dell, the Dell logo, and Dell SecureWorks are either registered trademarks or service marks of Dell, Inc. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. Integrated Solutions For Retailers is a registered trademark of Jameson Publishing, Inc. © 2012 by Peterson Partnership. All rights reserved.

For more information, visit www.dell.com/retail or www.retailsolutionsonline.com.