



REAL LABS. REAL PRODUCTS. REAL RESULTS.

ELECTRONICALLY REPRINTED FROM NOVEMBER 5, 2010

IT Security & Network Security News

# Mobile Application Developers Face Security Challenges

By: Brian Prince

Reports of security issues in mobile banking applications for PayPal, Chase bank and others highlights some of the security challenges facing mobile app developers.

**M**obile banking has been on the rise. In July, IDC reported mobile banking use doubled in between its annual surveys on the topic.

But the growth in popularity may not be matched by a growth in security, something underscored by problems recently reported in mobile applications from a variety of high-profile companies, including Wells Fargo and PayPal. The problems – reported here by viaForensics – include a failure to securely store passwords and usernames, and according to some, paint a

not so rosy state of mobile application security.

“The mobile device itself cannot be considered to be trusted, devices are lost and stolen all the time,” opined Richard Wang, manager of SophosLabs, the research arm of security firm Sophos. “I think these incidents show that the comparative lack of experience of mobile developers when it comes to security considerations. Threats against the PC existed long before online banking became commonplace so developers had to build in security from the start...storing usernames and passwords in plain text on

the device is a rookie mistake.”

A huge difference between mobile applications and Web applications is that Web apps store their data and programming code mostly on the server side, whereas mobile applications have most of their code and a lot of the data on the device, said Dan Cornell, CTO of Denim Group.

“For mobile applications most of the application code and a lot of the data resides on the device and these devices are under the control of the attackers,” Cornell said. “When you deploy a mobile application for your organization you have to assume that an attacker will

install the device on their phone, root or jailbreak the phone and then be able to inspect the application. I have a whole presentation online along with some code that demonstrates how to perform some of this. This allows attackers to actually retrieve the code that runs the application in many cases.”

Rutul Dave, technical marketing manager at Coverity and himself a former software developer, said that many app developers and phone software providers have used software designed to run on traditional computing systems and customized for mobile to get to market faster. It has been an effective strategy, he said, but has created security concerns.

“Security needs to be addressed in development, in software code,” he said. “On top of(a) shortage of developers who are experienced in app development for mobile, it’s hard to find developers who understand security on this

new computing platform.”

“The common thread as far as security concerns go for Web apps and mobile apps is that they are connected to the network, and in-turn accessible to hackers,” he added. “However, mobile apps add a new dimension to the security threat because the applications (that) are running on mobile devices are a new breed of software designed to specifically run on platforms that are very different from your traditional computing platforms.”

The situation is further complicated because mobile applications don’t have the additional security buffers of firewalls and security software that are available on the fully-fledged computing systems, Dave noted. Then there is the number of platforms involved - each with its own security capabilities.

Fortunately, there are best practices mobile application developers can follow. One,

Cornell said, is to keep sensitive data on the server side whenever possible and to write all server-side portions of the applications in such a way that they validate any information sent from the smartphone software.

Beyond that, general best practices, such as performing threat modeling early in the development process and testing software for security, are the rule of the day, Cornell added.

“All (developers) certainly aren’t going to be experts but everyone ought to have at least some base-level knowledge and most teams should probably have a “go to” security person with more advanced knowledge and training,” he said. “For teams building mobile applications they should be instructed on the security features of their chosen mobile development platform(s) as well as any specific concerns for security in the environment(s).”



www.denimgroup.com  
210.570.4400