



Old school flaws still haunt mobile Web apps

SECTOR 2010: Two security researchers say the same mistakes that were being made 10 years ago in the PC world are being repeated in the mobile market. Find out more from this year's SecTor security conference in Toronto

By: bill brenner

CSO (US) (28 Oct 2010)

When using a [BlackBerry, Android, iPhone or other smart phone](#), we tend to assume all the nifty Web apps on these devices are relatively secure. At the least, we expect that a lot of the painful security lessons we received on PCs a decade ago have been applied to today's phone apps.

But when Intrepidus Group researchers Zach Lanier and Mike Zusman started taking mobile phone apps apart to see what makes them tick, they discovered that our assumptions have been wrong. At the SecTor 2010 conference Wednesday, they walked their audience through some of the more glaring examples of old-school flaws they uncovered in many Web apps for mobile phones.

The problems that need fixing are on the developer side, Lanier said. In the rush to satisfy smart phone users hungry for new apps, the same mistakes that were made around 1999-2000 in the PC world are being repeated. After looking at the more popular phones like Android and BlackBerry, the two discovered, among other things, that:

- Intercepting one's credentials on an app like Foursquare is pretty easy.
- Storage apps -- popular among those who like to store and easily retrieve music and video on their phones -- contain security holes an attacker could exploit to cause a denial of service or bypass digital rights management controls.
- Carrier-based apps tend to trust you just because you happen to be on the carrier network.
- Third-party apps are sometimes better than carrier-based apps in this regard, but there's still incomplete support for open standards.
- Man-in-the-middle attacks are fairly trivial across the board.
- It's trivial for a bad guy to replay a [BlackBerry user's picture upload requests](#) and send their own, potentially malicious files to random accounts. Zusman said injection flaws in RIM's picture upload feature abound and that it was fairly simple to inject their own XML attribute.

Lanier and Zusman concluded that in the mobile phone Web app world there's a lack of guidance, standards and best practices for developers. "We learned about many of these weaknesses 10 years ago," Lanier said. "We're forgetting the lessons we already learned."

By exposing these old-school problems, the researchers hope to shake the developer community into a state of vigilance.

Over the course of their research, the duo relied on such techniques as white box source code review, black box code review that included acquiring the Web app binaries, and lots of reverse engineering, disassembly and decompilation, and network-protocol analysis.

Copyright © 2010
ITworldcanada.com

[web analytics](#)