



Climate Tips for the Planet

fightglobalwarming.com

Data Protection

Google Custom Search

Thursday, October 28, 2010

[Data Protection](#) | [Identity & Access](#) | [Business Continuity](#) | [Physical Security](#) | [Security Leadership](#) | [Basics](#) | [Tools & Templates](#) | [Security Jobs](#) | [Blogs](#)

[Home](#) » [Data Protection](#) » [Wireless/Mobile Security](#)

NEWS

SecTor 2010: Touring (and surviving) the mobile app minefield

Our smart phone apps are full of old-school, exploitable vulnerabilities. A look at how the past has come back to haunt us and what to do about it (from the SecTor 2010 conference).

» [Comments](#)

You like SecTor 2010: Touring (and surviving) the mobile app

By **Bill Brenner, Senior Editor**

October 27, 2010 — CSO —

TORONTO -- 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.

See also: [Mobile Malware: What happens next?](#)

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 [user's picture upload requests via a third-party upload app for BlackBerry](#) and send their own, potentially malicious files to random accounts. Zusman said injection flaws in the 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.

WIRELESS/MOBILE SECURITY ESSENTIAL READING

- [Wireless security basics](#)
- [Wireless intrusion detection systems](#)
- [Stupid things people do with mobile devices](#)
- [Protecting the mobile workforce](#)
- [Mobile security: 6 classic gadgets](#)

WIRELESS/MOBILE SECURITY WEBCASTS

- [60 Minutes: The Future of the Perimeter](#)
- [Smart Techniques for Application Security](#)
- [The Business Case for Data Protection](#)
- [Utility Mandate: Software Security for the Smart Grid](#)
- [CyberAttacks ... Are you protected or prepared to pay?](#)
- » [View All Wireless/Mobile Security Webcasts](#)

WIRELESS/MOBILE SECURITY WHITE PAPERS

- [Pilot House Awards recognizes Google Message Security for excellence](#)
- [Enterprise Strategy Group Report on SaaS Archiving](#)
- [The Critical Need for Email Archiving](#)
- [Google Messaging Discovery Datasheet](#)
- [Why Cloud-Based Security and Archiving Make](#)

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.

1 2 3 4 5 »

Sign up for the [CSO Tech Watch](#) newsletter. »

Print Comments

Like You like SecTor 2010: Touring (and surviving) the mobile app

The screenshot shows a Twitter search interface with the following content:

- Search bar: "Search Tweets"
- Search results for "http://onlywire.com/r/13857371 Ways to make money | increase experts warn of mobile phone malware Article by at 2010-10-27 04:25:59 Catego":
 - Result 1: User [lambertalma](#) (0 retweets, 0 replies)
 - Result 2: RT @FSecure: Is your cell phone secure? F-Secure's Mikko Hypponen explains the latest in mobile malware threats. <http://fb.me/LmcoGnwg> (User: [vickyr](#), 2 retweets, 0 replies)
 - Result 3: #Freeware: Lookout Mobile Security: [pcworld.com] Protect your mobile phone against malware and thieves with this... <http://dlvr.it/7JR8p> (User: [winappz](#), 0 retweets, 0 replies)
- Input field: "What are you thinking?"
- Search results powered by **TOPSY**
- Buttons: "Insert this article url", "Follow CSOOnline", "Tweet" (140 characters)

RELATED ARTICLES

- [iPhones, iPads in the enterprise: 5 security perspectives](#)
- [The mobile security survival guide](#)
- [Study: Users OK with mobile devices for sensitive transactions](#)

POST A COMMENT

Your name: *

E-mail: *

The content of this field is kept private and will not be shown publicly.

Sense

The Business Case for a Next-Generation SIEM: Delivering operational efficiency and lower costs through an integrated approach to network security management

» [View All Wireless/Mobile Security White Papers](#)

LATEST POSTS

» [more blogs](#)



Lohrmann On GovSpace

by Dan Lohrmann

- [Technology Priorities Are Still Consolidation and Security](#)
- [Cybersecurity Governance: State CISO Roles - Past, Present and Future](#)
- [Security Career Problem 7: Perspective Stuck in a Box](#)



Security In the (Apple) Core

by Chad McDonald

- [Shiny New Security Shoes](#)
- [Insecure but Safe - The Mayberry Paradox](#)
- [Peeling Apples - Reconsidering Mac Security](#)

Advertisement for CSO newsletters with the following text:

- > Newest security technologies
- > Strategies that work
- > Career advice
- Stay ahead with **CSO newsletters**
- CSO** SECURITY AND RISK
- SUBSCRIBE NOW!**

Advertisement for CSO newsletters with the following text:

- Get the latest news and analysis on data protection, leadership & business continuity with CSO newsletters.
- CSO** SECURITY AND RISK
- SIGN-UP**

Comment: *

- Allowed HTML tags: <a> <cite> <code> <dl> <dt> <dd>
- Lines and paragraphs break automatically.

WHITE PAPERS

- ▶ Pilot House Awards recognizes Google Message Security for excellence
 - ▶ Enterprise Strategy Group Report on SaaS Archiving
 - ▶ The Critical Need for Email Archiving
 - ▶ Google Messaging Discovery Datasheet
 - ▶ Why Cloud-Based Security and Archiving Make Sense
 - ▶ The Business Case for a Next-Generation SIEM: Delivering operational efficiency and lower costs through an integrated approach to network security management
 - ▶ IDC Technology Spotlight: Leveraging the Benefits of Cloud Computing with Specialized Security
 - ▶ Strong Authentication for the Here and Now
 - ▶ Addressing the Grand Challenge of Cloud Security
 - ▶ Securing Virtualization In Real World Environments
 - ▶ How Mature is your IT Risk Management?
 - ▶ Laptop Theft – The Internal and External Threats
 - ▶ Higher Education Data Center 101: Using Flexible Architecture
 - ▶ Virtualizing Network Connections and Capacity with HP FlexFabric
 - ▶ Achieving Improved Network Security with IP and DNS Reputation
 - ▶ A Comprehensive Framework for Securing Virtualized Data Centers
 - ▶ ROI of a Complete Networking Portfolio: Delivering Value from the Network Edge to the Core
 - ▶ Establishing Trust in Remote Access Transactions
 - ▶ Hassle-free Compliance
 - ▶ Five Challenges to Continuous PCI DSS Compliance
- More White Papers »**

SPONSORED LINKS

- ▶ Best practices in email security and security software as a service. Read more >>
- ▶ Download the Forrester Study to learn how 305 IT decision makers are protecting their corporate secrets
- ▶ RSA Archer gives you one smart choice for security, risk & compliance

Junos[®] Pulse Mobile Security Suite  [Learn more](#) 

RESOURCE CENTER

Securing the Enterprise, new white paper

New approaches to enterprise cyber security using the Consensus Audit Guidelines

100% Online MBA's

Earn a Masters in Business Administration 100% Online. No GMAT Required!

Mail Security for Windows and Linux

Proprietary SRL reputation, In-content URL reputation, heuristic analysis, more.

[buy a link »](#)

ADS BY **techwords**

THE IDG NETWORK

[CIO](#) | [Computerworld](#) | [CSO](#) | [DEMO](#) | [GamePro](#) | [Games.net](#) | [IDC](#) | [IDG](#) | [IDG Connect](#) | [IDG Knowledge Hub](#) | [IDG TechNetwork](#) | [IDG Ventures](#) | [InfoWorld](#) | [ITwhitepapers](#) | [ITworld](#) | [JavaWorld](#) | [LinuxWorld](#) | [Macworld](#) | [Network World](#) | [PC World](#)



© 1994 - 2010 CXO Media Inc. a subsidiary of [IDG Enterprise](#)