

---

[EMAIL THIS](#)

Mobile Computing News:



# iPhone hacking: Lessons from the front line

By Lisa Phifer, contributing writer  
02 Mar 2009 | [SearchMobileComputing.com](#)

 [Mobile advice](#)

 [Digg This!](#)

 [StumbleUpon](#)

 [Del.icio.us](#)

 [Google](#)

At last month's Gartner [Wireless and Mobile Summit](#), the iPhone was the elephant in the room - an enormous IT challenge that's here to stay, no matter how hard enterprises try to ignore it.

In his annual update on mobile devices, Gartner analyst Ken Dulaney described the iPhone as a consumer-class mobile device with increasingly universal enterprise impact. Apple Mac OS X smartphone sales overtook Windows Mobile in 3Q08. At 13% and climbing, the iPhone is now rapidly approaching RIM's BlackBerry marketshare.

Nonetheless, Dulaney expects Apple to continue putting the consumer first, enterprise second. Apple isn't particularly accustomed to working with (or catering to) enterprises, he said. Moreover, the iPhone's SDK goes only so far when it comes to supporting complex business applications -- especially those that require background processing. "We expect the iPhone OS to become slightly more open," he said. "But it will never be truly enterprise-oriented."

Dulaney graded the iPhone A+ for its "pheromone rating," but a last-place C in security. Ultimately, breadth of business applications will determine which mobile device(s) win or lose the enterprise market. For now, plentiful consumer applications are pushing the iPhone into the enterprise through the backdoor, creating a security gap. Many IT departments see this runaway train barreling toward them but feel powerless to stop it.

## ***Batten down the hatches***

In his presentation *iPhone Forensics: How a Thief Can Bypass Security to Steal Personal Information and Corporate Secrets*, McAfee research scientist Jonathan Zdziarski instructed a packed house how to jump out of that train's way.

"I'm not here to tell you not to develop enterprise applications for the iPhone," he said. "I'm telling you to develop your applications in a smarter way."

When the iPhone was released, love for the device led Zdziarski (aka "NerveGas") to join its

nascent hacking community, working to jailbreak (unlock) the platform to enable new applications. "You used to be able to go to our website and install patches and software for your iPhone," he said. "We had ported over SSH and some other great applications."

After Apple released its SDK and launched the iTunes AppStore, that hacker culture shifted. "You saw iPhone hackers break into malicious subgroups -- for example, one group got together to focus on DRM cracking and piracy," Zdziarski said. "On one side, you had Apple trying to lock the phone; on the other, you had hackers trying to pick those locks. This led to the unhealthy situation we have today."

As a result, Zdziarski refocused his iPhone expertise on forensics. Today, he helps law enforcement prosecute criminals who use iPhones, leveraging that mobile device's stored data as evidence.

"We've been working on the iPhone 3G and crimes that are committed with them," he said. From sexual assault, narcotics and murder to terrorism, identify theft and financial fraud, Zdziarski has assisted in numerous investigations. He even wrote an [\*iPhone Forensics\*](#) manual now used by more than 250 law enforcement agencies.

### ***Know your weaknesses***

At the Gartner summit, Zdziarski leveraged his iPhone savvy to help enterprises protect their business data. "The bad guys are going to do these things," he said. "They'll spy on coworkers; they'll commit identity theft; they'll steal business contacts, corporate data, photos and trade secrets. If someone steals [an employee's iPhone], they have a lot of this information."

Enterprises interested in writing applications for the iPhone need to know how to design more secure applications, according to Zdziarski. "A lot of developers are writing applications that could potentially expose business data on the iPhone," he said. To reduce exposure, enterprises must understand the platform's vulnerabilities.

"The iPhone has a read-only partition that stays in a factory state when you boot the phone; it also has a user data partition that holds all of your information," he explained. The iPhone updates its firmware by booting from RAM disk, overwriting the system partition without destroying the user data partition. Hackers can easily develop their own RAM disks to install custom payloads. At that point, anything recorded on the user data partition becomes fair game for recovery and analysis.

How can iPhone thieves exploit this? "The biggest problem right now is that the iPhone's passcode is easily bypassed," Zdziarski said. "Anyone with the right know-how can delete a file and your passcode goes away. There's no real [file vault] encryption on the device, so all of your data is now sitting right there, unprotected." Because this can be accomplished in under a minute, "someone can easily take your iPhone, remove your passcode, and give it back to you before you even realize it was stolen."

That unlocked iPhone can now fall victim to another major vulnerability: unencrypted data synchronization. "If I spend another two or three minutes [synchronizing iTunes with a stolen

iPhone], all of your data gets copied onto my desktop," Zdziarski explained. "It's very simple to gain access to user data contained in that backup file."

Zdziarski performed a live demo during his Gartner session, illustrating how quickly a synchronized backup file could be unzipped, converted to XML, and decoded to produce a desktop folder containing a stolen iPhone's entire file system. "If you're an enterprise application developer, all of your information is going to end up here, right on the hacker's desktop -- and that's not good," he warned.

The iPhone's raw disk further increases data exposure. "People who are already familiar with OS X raw disks know how to access deleted information, like email, images, voicemail and application data," Zdziarski said. "The raw disk gives [hackers] access to the iPhone's entire file system, not just user data, including stuff that's not normally synchronized."

Unfortunately, the iPhone's raw disk is impervious to restore. "If you're going to sell your iPhone on eBay, you might think you've removed your data, but that's not true," he said. "I know of [someone] who bought a factory refurbished iPhone and found all of the previous owner's data, including his contacts, pictures of his girlfriend. We called [that owner's] parents and found out that he'd returned the iPhone to Apple before it turned up on that refurb list."

Apple created a disk utility to wipe an entire iPhone clean, including its raw disk. Unfortunately, Apple's secure erase takes several hours to run. "You still have users that don't know about secure erase," Zdziarski said. "And you have a first generation of iPhones that lack this capability." To fix this, Zdziarski developed his own utility to overwrite free space quickly without destroying active user data. Dubbed [iErase](#), this utility is still awaiting iTunes App Store approval.

Another major vulnerability is the iPhone's unprotected keychain, according to Zdziarski. "You're basically giving the person who steals your iPhone both the lock and the key," he said. "The keychain's key is stored right on the iPhone; they don't need your passcode to [decrypt sensitive values stored on] your keychain."

### ***Understand your exposure***

Combine these vulnerabilities with the way that iPhone applications operate, and you have quite a bit of valuable data. But this goes well beyond the obvious user data like contacts and email messages. "The iPhone operating system stores a lot of information that's good for law enforcement but bad for privacy," Zdziarski warned.

"In my forensics work, one of the most useful pieces of evidence has been the hundreds of screenshots that the iPhone uses to produce its 3D transition effect whenever you press the home button," he said. "Even if you clear your cache and delete your email, you have hundreds of screenshots -- including browser pages and email -- that are still on your iPhone. Whenever you hit home out of Google maps, whatever you were looking at is stored."

When applications exit, those screenshots are deleted -- but as previously noted, deleted data still lives on the raw disk. During his demo, Zdziarski stepped through transition snapshots

extracted from an iPhone backup, including call histories, text messages, contact details, Web searches, map tiles, and waypoints. Using a perl script, he assembled a series of GPS maps to reconstruct the route a criminal had driven. "When you're developing applications for the iPhone, think about this," he said. "Everything you display to the user could get stored in this way."

### ***Proceed with caution***

Nonetheless, Zdziarski said that enterprises can use the iPhone safely if they take steps to mitigate risk. "People just need to understand that the iPhone isn't a secure device -- it's not even as secure as PCs are today," he said. "But if you're willing to write an application that compensates for that, you can still write a pretty secure application for the iPhone today."

For starters, he recommends that application developers securely delete all data by writing over it again at least once. Because employers can't control what native iPhone applications do, they should bar employees from using iPhones to access corporate data. "Don't let iPhones have access to your enterprise email," he said. "And tell your employees to use the iPhone's *Erase contacts and settings* tool frequently."

In addition, developers should encrypt their own application files. "There's nothing stopping you from doing this; most hackers aren't going to bother cracking a proprietary application that uses proprietary encryption," he said. Never rely on the iPhone's passcode for providing application or physical security, however, and never store enterprise application keys on the iPhone's keychain. "Prompt the user for your application key, or use two-factor authentication instead."

To circumvent those iPhone transition snapshots on raw disk, Zdziarski advises against displaying private data. "Don't display account numbers, credit card numbers, or any other information that you don't really have to show the user," he said. "Also clear out the iPhone's keyboard cache using the *Reset keyboard dictionary* utility -- if you do this often enough, it'll probably get overwritten."

To eliminate any old/deleted and potentially illegal content stored on used iPhones, Zdziarski recommends initiating a secure wipe before (re)issue. "If you make this part of your policy, then you can say without a doubt that all of those bits were clean when you gave the iPhone to your employee," he said. "That protects you as a company as well as your employee -- if you give the employee a phone with malicious content, you could be held liable."

Those developing iPhone applications should always avoid caching data. "Take advantage of that 3G connection to go get data every time you need it. As soon as you're done with data, overwrite it," he said. In addition, overwrite and then wipe temp files upon application exit or suspension. Employers can require iPhones to be auto-locked after one minute of inactivity, triggering those applications to exit and thereby causing temp files to be deleted at regular intervals.

Finally, Zdziarski advocates creating a safety seal to check kernel integrity. "The secure kernel prevents unauthorized applications from running," he said. "If a self-signed application can run, then the secure kernel is broken, and you could have spyware or other malicious programs on

the iPhone." By running a self-signed application, employers can detect and avoid using jailbroken iPhones for business activities.

To learn more about these and other secure application development techniques for the iPhone, visit Zdziarski's website (<http://www.zdziarski.com>) or check out his new book, *iPhone SDK Application Development: Building Applications for the AppStore* [ISBN 0596154054].



**About the author:** Lisa Phifer is president and co-owner of Core Competence, a consulting firm focused on business use of emerging network and security technologies. At Core Competence, Lisa draws upon her 27 years of network design, implementation and testing experience to provide a range of services, from vulnerability assessment and product evaluation to user education and white paper development. She has advised companies large and small regarding the use of network technologies and security best practices to manage risk and meet business needs. Lisa teaches and writes extensively about a wide range of technologies, from wireless/mobile security and intrusion prevention to virtual private networking and network access control. She is also a site expert to SearchMobileComputing.com and SearchNetworking.com.