

## Why Lawyers Shouldn't Use The iPhone: A Security Nightmare

By Sharon D. Nelson, Esq. and John W. Simek

© 2010 Sensei Enterprises, Inc.

As Joan Rivers might say, "let's talk."

First, we want you to know that we don't hate Apple. In fact, we admire the company, which consistently produces excellent products that are user-friendly. Unlike Microsoft, which tends to give you products that it thinks you should want, Apple studies what consumers want and then gives it to them. It's been a good business model and Apple clearly has its finger on the pulse of the consumer market.

However . . . business is (or should be) different. Lawyers, blinded by the glitzy advertising and sex appeal of the iPhone, have been demanding iPhones from their IT departments or purchasing them on their own. Every law firm seems to have its share of Apple "fanboys" who evangelize over every new product unveiled by Apple. But it's time to slow down and study the mass migration to the iPhone.

First, we acknowledge that our initial complaint about the iPhone has vanished. It now has the requisite software applications that most lawyers use. Of course, you're still stuck with the lousy and pricey AT&T network. However, the phone itself works well and lawyers tend to love it – great web browsing, excellent audio for conference calls, a wonderful e-mail interface, integration with Microsoft Exchange servers, etc. So why forego a phone that attorneys seem pre-disposed to love?

As lawyers, we are ethically compelled to keep our confidential data secure – and we have a lot of it, these days, on our smartphones. So whatever smartphone we implement in our law practices, we sure as shootin' better know something about its security. So let us part the curtains and describe the iPhone's security from the vantage point of legal technology and computer forensics.

The words iPhone and security do not belong in the same sentence, although you would never know it from the Apple marketing blitz. Some of the advertised features of the iPhone 3GS are the inclusion of hardware encryption and remote wipe functions. As most folks know, encryption is a killer for computer forensic examiners and a fine way to protect your data. So what does encryption do for the 3GS? Not a heck of a lot. From our foxhole, it appears that encryption was an afterthought and not inherent in the iPhone design. The iPhone is feature rich and has lots of consumer appeal – but secure? Nope.

So if the 3GS is encrypted, how can we get to the user's data? Jonathan Zdziarski has demonstrated (<http://www.youtube.com/watch?v=kHdNoKIZUCw>) how easy it is to gain access to a supposedly secure iPhone 3GS. Should we believe him? We certainly do,

especially since we own his book on iPhone forensics and have personally seen the mountains and mountains of electronic evidence that is stored on an iPhone. The key to gaining access to the data is to extract a disk image from the device. First off you “jailbreak” the phone by placing it into recovery mode and installing a custom RAM disk to the iPhone. Jonathan mentions that the tools are only available to law enforcement (nice thought, but not so), but also acknowledges that it is fairly simple to develop your own. Several products like Red Sn0w and Purple Ra1n are freely available to “jailbreak” the phone. You then install a Secure Shell (SSH) client to port the raw disk image onto your computer.

Those of us in the forensic community know that sucking a disk image from an encrypted drive to a destination drive just gets you another encrypted image which is no earthly good to you. What makes the iPhone 3GS any different? This is the part where Apple is so very, very helpful. Even though the data on the iPhone disk is stored in an encrypted form, the iPhone actually decrypts the data as it feeds the zeros and ones through the SSH connection. You call that security? What genius at Apple came up with that one?

Just as Billy Mays would say, “But wait...it gets even better.” In order to secure your iPhone, make sure you configure an unlock code. Then again, tsk, tsk, tsk, perhaps you shouldn’t waste your time. Jonathan has another demo (<http://www.youtube.com/watch?v=5wS3AMbXRLs>) where he replaces the passcode file with one that contains a blank password, effectively removing the unlock code. How is this possible? Just like the previous explanation, putting the iPhone into recovery mode doesn’t require the passcode PIN. What a great design. As we said before, security appears to have been a complete afterthought to the phone’s developers. Don’t they test these things? Geez.

Some have commented that bypassing the PIN is sophisticated hacker action. Really? We don't see this same flaw on a BlackBerry, Windows Mobile, Symbian or other cell phone and there are many available free tools to unlock the iPhone PIN depending on the installed firmware version. We acknowledge that you can configure the iPhone to automatically wipe the device after a number of invalid PIN attempts. So what? If you can bypass the PIN by immediately putting it into recovery mode, you haven't even made a single invalid PIN attempt. Game over.

Others have pointed out that you can remotely wipe the phone via the MobileMe service. Don't get us going about AT&T's ability to know where the iPhone is at all times. You call that privacy? The bottom line is that you have to be connected to the network for the remote wipe to work and as we note below, disconnecting from the network is a breeze.

So let's summarize. The iPhone encryption is a non-starter and accessing the device is child's play even if it is password protected. Now, granted, in both cases you have to have physical access to the device. And no one ever loses their phone, right?

Apple says losing your phone is not a problem. If you leave your iPhone in the back seat of a taxi (the ditzzy one of this writing partnership has done just that), you just use the remote wipe feature to "kill" all of the personal data. Alas and alack, there's a problem with that too. As we've already mentioned, the remote wipe feature requires that the iPhone be connected to the cellular network. Oh, my. The last we checked, removing the SIM card or placing the phone in a Faraday box would solve the network connection problem. Take the phone off the cellular network and you can take all day to retrieve the disk image (in an unencrypted form) from the iPhone 3GS. Again, what a crud design. Seriously, Apple (like Ricky Ricardo) has a lot of 'splaining to do. Even Microsoft (and yes, it hurts to say something nice about Microsoft) has a secure remote wipe function with Windows Mobile that actually works. When you establish a security policy for Windows Mobile or BlackBerry, the device does not have to be on the network to destroy the data. Define the number of invalid PIN attempts before the wiping begins and the personal data is gone, network or no network. You can't access the data on a Windows Mobile or BlackBerry without the proper PIN, which can't be bypassed like the 3GS. What a novel concept.

Also, most users are not aware that the iPhone conveniently creates a screenshot and saves it as a temporary file on the phone. *Wired* has an article that explains the how and why and is available at <http://www.wired.com/gadgetlab/2008/09/hacker-says-sec/>. The end result is that there is a nearly complete "audit trail" of activity that is done on an iPhone, even if the user doesn't save any data. As an example, you can open a message that contains personally identifiable information and then immediately delete it. Guess what? All of that private data is on the phone until it is overwritten, which could be some time. These recoverable screenshots are another reason why we are concerned with iPhone usage in a law firm. We've never seen this type of activity on any other phone.

Does all of this mean that the iPhone is the ONLY insecure cellular phone on the market? Obviously not, but it is at the top of our list, especially considering the hundreds of phones we get each year for evidence analysis. Any smartphone with a browser is subject to the same attacks and infection as any Internet user. We know many iPhone users are saying that security is the issue and is not unique to the iPhone. Perhaps the truth hurts. Security is a major issue for any law firm, but using a device that does not enforce PIN integrity is a little crazy in our book. We wouldn't want to make that argument to a malpractice carrier.

Bottom line...we love the iPhone. Not because of its technical superiority, but because its design gives us access to more electronic evidence than any other phone we've ever seen. Keep up the good work Apple. We now believe you when you say the 'S' in 3GS is

for speed and not security. If you've implemented the iPhone (which is clearly a consumer phone and NOT an enterprise phone as currently designed), you've hung yourself out to dry if a phone "goes missing" with confidential data.

So, in a world where lost or stolen laptops and phones scream at us from newspaper headlines and data breaches invite multi-million dollar government fines and lawsuits, do we want a smartphone whose insecurity is well documented? In our judgment, no.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) [www.senseient.com](http://www.senseient.com)*