Herding Cats:
Pocket Storage for All

December 2012

BrandenWilliams
SECURE BUSINESS GROWTH

I can hear the friendly ribbing now.

“Oh GEE Brando, an issue dedicated to storage? I am sure you will have fun towing the company line on that one! After all, you joke about how storage is cheaper for you than others when you talk about collection without limitations.”
Sure, generic security guy, I do joke about that. But I wanted to take this month’s column in a different direction. It does deal a little bit with storage, but it’s the storage we carry with us every day. Yep, the old smartphone problem, and what the heck is that thing doing?

I’m presently writing this column about three weeks before you will read it. It’s the week following BSidesDFW, which was a great success thanks to the fantastic organizers and community surrounding them. One session in particular that I really enjoyed was with Francisco Artes live, and hilarity from Gal Shpantzer via Skype, where they discussed how smartphone storage worked and the security features of both the Android and iPhone platforms. I’ve written and blogged about the super forensic-friendly nature of these devices, but it wasn’t until this session that I really began to understand the nature of what is left around on these devices.

I’ve been very interested in doing forensic analyses of the phones in my house, but I’ve not had the time or networking abilities to get into the right crowds to both gain the knowledge and equipment required. Here’s the good news. If you have an iPhone, you probably have pretty seamless upgrades into newer versions of iOS and the adoption rate is insane (over 61% at the end of October). If you have an Android, you may be frustrated with your ability to upgrade depending on the carrier or handset. So let’s talk bad news for iPhone users now, because I was certainly enlightened to learn how the underlying storage and the security models work.

Everything on your iPhone is essentially stored in a database. Great for quick access and organization, and it allows for some containerization such that application data doesn’t commingle. Sounds great so far, right? But what happens if you delete a text message or something from an application? Since you deleted it, it must be gone, right?

Nope.

The database entry is marked in a way that allows it to eventually be overwritten, but it still is on the phone. So a forensic analysis will show all those texts that you thought you deleted. But wait, because it gets SO much worse.

Every time you back up your iPhone, all of those entries that you have marked as deleted are backed up right with all the good stuff that you want to see. This means that it becomes insanely hard to remove them from your device because they now are in your backups. If you grab the newest iPhone and restore from your old backup, all of those deleted texts now make their way onto your new phone! According to Francisco and Gal, the only way to prevent this is to set up your iPhone as a NEW device, not restoring from backup. That is, start all over.

Now let’s put on our tin foil hats and get really suspicious of everything with a battery. Maybe you are one of the many iPhone users who don’t have a (working) home computer. Or maybe you want to take advantage of Apple’s generous offer to back up your phone for you via iCloud so that no matter where you are, you can restore your phone if you have a problem. Do you see where I am going? All of those deleted texts are now up in the cloud and out of your control. If you were thinking of doing something illegal and coordinating it from your iPhone, your backups could be subpoenaed without your knowledge and all of those deleted texts might be in the hands of the Feds. Yikes!

The point of Francisco and Gal’s presentation wasn’t necessarily to make everyone run from the room screaming in fear, but to uncover some of the good security-related things that mobile devices can do while highlighting the snakes in the grass that we all need to be aware of—especially corporate security folks who are charged with keeping information secure on those devices. It might be time to re-think about how information moves throughout your company and see how bad a lost cell phone might actually be.

Contact information for requests for permission to reproduce or distribute materials available are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school junior. Now, a graduate of the University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004. Williams is sought after as both an speaker and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.