Stored-Data Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Yet another chapter bites the dust: this week I have some additions to a chapter on stored-data security.

* * *

Addition and footnote to a section on "Volume Encryption and Encrypting File Systems:"

I/O to and from the mounted volume can be significantly slower than from an unencrypted disk drive. For example, observations in June 2013 showed that mounting an entire 7 GB partition encrypted by Symantec PGP Desktop v10.20.0 took ~7 seconds. In comparison, the same 7 GB of data encrypted using WinZip and 256-bit AES encryption took about an hour to decrypt in toto on a 7200 rpm two-disk performance RAID 0 set running under 64-bit Windows 7 Professional SP 1 on a 3.2 GHz AMD Phenom™ II X4 955 quad-core processor with 12 GB of RAM. Copying a 1.23 GB file took 85 seconds (~15 MB/sec) on the PGP encrypted volume (located on the RAID 0 hard drive) but only 20 seconds (~63 MB/sec) on the RAID 0 itself .

* * *

New section on "Smart-Phone Encryption:"

Users may store confidential information on mobile phones and tablets; typical entries include contact entries with phone numbers and sometimes with ancillary sensitive data such as passwords, personally identifiable information (e.g., government-issued identification numbers), and call records. Such devices may also be used as if they were flash drives, with potentially gigabytes of sensitive data downloaded from other sources and carried in a pocket, briefcase or handbag – and therefore easy to steal or to lose.

Another factor that can be significant for some users is that under US law at the time of writing in June 2013, a suspect who is questioned, interrogated or arrested cannot normally be forced to divulge the decryption code.[1]

Phones using Android 2.3.4 or later usually come with integrated total encryption; the process typically takes about an hour, ideally starts with a fully charged battery and connection to a power supply, and must not be interrupted. Interruption of this encryption process can damage or delete the data stored on the phone and requires a factory reset that wipes all current data and personal settings from the device.[2]

Apple iOS and Microsoft Windows Phone 7 also include encryption functions with varying coverage. Third-party software is available for all the operating systems discussed above.[3]

In March 2013, researchers at the Friedrich-Alexander University discovered how to access data encrypted on a version of the Android operating system:

> The team froze phones for an hour as a way to get around the encryption system that protects the data on a phone by scrambling it…. The attack allowed the researchers to get at contact lists, browsing histories and photos…. [They] put Android phones in a freezer for an hour until the device had cooled to below -10C. …[Q]uickly connecting and disconnecting the battery of a frozen phone forced the handset into a vulnerable mode. This loophole let them start it up with some custom-built software rather than its onboard Android operating system. The researchers dubbed their custom code Frost - Forensic Recovery of Scrambled Telephones.[15]

REFERENCES:

[1] Radia, R., "Why you should always encrypt your smartphone." ArsTechnica (2011-01-16). http://arstechnica.com/gadgets/2011/01/why-you-should-always-encrypt-your-smartphone/

[2] How-To Geek, "How to Encrypt Your Android Phone and Why You Might Want To." (2013). http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/

[3] UNC-Chapel Hill, "Encrypting Cell Phones." University of North Carolina at Chapel Hill | Help & Support (2013-03-19). http://help.unc.edu/help/encrypting-cell-phones/

[4] BBC, "Frozen Android phones give up data secrets: Freezing an Android phone can help reveal its confidential contents, German security researchers have found." BBC News | Technology (2013-03-07). http://www.bbc.co.uk/news/technology-21697704

* * *

Some additions to the list of suggested readings:

Griffin, D. *The Four Pillars of Endpoint Security: Safeguarding Your Network in the Age of Cloud Computing and the Bring-Your-Own-Device Trend.* CreateSpace Independent Publishing Platform, 2013.

EMC Education Services. *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments* 2nd edition. Wiley, 2012.

Hitachi Data Systems. *Storage Concepts: Storing And Managing Digital Data*, Volume 1. HDS Academy, 2012.

Loshin, P. *Simple Steps to Data Encryption: A Practical Guide to Secure Computing.* Syngress, 2013.

Souppaya, M. and K. Scarfone. *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication SP800-124 Revision 1. 2013-06. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *