http://www.oxygen-forensic.com
+1 877 9 OXYGEN
+44 20 8133 8450
+7 495 222 9278

PRESS-RELEASE
For Immediate Release

Oxygen Software Performs Forensic Study of Password and Pattern Lock Protection in Android OS Devices

Revealing or bypassing passwords protecting suspects' mobile devices is one of the most important goals in today's mobile forensics. Oxygen Software performs a forensic study of device password and pattern lock protection of Android devices, discovers ways to reveal or bypass such protection, and analyzes forensic feasibility of doing so.

In this study, Oxygen Software enhances forensic feasibility of recovering or bypassing password lock and pattern lock protection of mobile devices running the Android OS.

In Android security model, pattern lock and password lock are two different methods used to unlock the device, wake it up from power off or sleep mode, or gain access to device's desktop after a period of inactivity. The two methods use different input methods to achieve the task. With password lock, the user enters a plain passcode by typing on the virtual keyboard. Pattern lock works with gestures, allowing the user to enter a password by using a specific touch pattern or sequence, e.g. swiping a finger in different directions.

Researchers from Oxygen Software, the manufacturer of Oxygen Forensic Suite 2011, analyzed this security mechanism and discovered how password lock and pattern lock work and how password and gesture information is stored.

The plain-text password information is stored in the /data/system/pc.key file. The data is represented as a one-way SHA1 hash or the actual password. In order to recover the password, a common brute-force or dictionary attack can be used.

Apparently, pattern lock data is kept in a file named gesture.key and stored in the /data/system folder. The data is encrypted with a SHA1 algorithm. In case of pattern lock, gesture information is being stored instead of the actual password it represents. For example, a finger swipe from the top-left point of the input screen and to the bottom-right, the pattern will be recorded as the following byte sequence: 0x00, 0x01, 0x02, 0x05, 0x08, representing the number sequence 1, 2, 3, 6, 9. Dictionary attack is not applicable when recovering gesture information, so brute-force is the only way. Apparently, in this case, some byte combinations would not make sense and cannot appear close to each other. By knowing this, researchers were able to eliminate the impossible combinations, making the recovery of pattern-lock gestures significantly faster than by using plain brute-force.

Performing further analysis, Oxygen researchers found the need of recovering either the plain-text password or a pattern-lock combination questionable. Indeed, in order to recover the password or pattern lock combination, the researcher needs access to pc.key or gesture.key files stored in the device. In order to gain access to these files the device must be rooted (Oxygen Forensic Suite 2011 with Android Rooting Add-On is a perfect tool to do that) and the USB debugging mode setting must be switched on. Alternatively, the device can be booted in recovery mode with a special boot loader. However, if the phone is rooted and has a USB debugging mode already enabled, then neither pattern lock nor password lock can prevent accessing information from the device.

Moreover - if an Android device is rooted, investigators can simply delete two files containing the password and pattern locks, or replace these files with ones containing known passwords or patterns. Either way, investigators will be able to access device's desktop without knowing the original gesture or password, or even bothering to recover one.

There are commercially available tools offering the recovery of Android passwords or pattern lock sequences. The features are typically marketed as product highlights. Oxygen researchers found that, in the case of Android OS, the recovery is not needed in order to perform a forensic analysis of the device. Granted, Apple and BlackBerry employ a different security model, tying many more essential things to user passcodes. In the case of Android, user-selectable device unlock keys are not being used to encrypt either user or system data, and can be ignored entirely by investigators.

About Oxygen Software

Founded in 2000, Oxygen Software offers the most advanced forensic data examination tools for smartphones and mobile devices. The company is dedicated in delivering the most universal forensic solution covering the widest range of mobile devices running Symbian, Windows Mobile, Blackberry, iOS, and Android operating systems. As a result, Oxygen Forensic Suite consistently wins the highest awards in media, and occupies a spot in the top of the list in relevant tests for extracting more data than competition.

More information about the company and its forensic solutions is available at www.oxygen-forensic.com

# # #

Press Contact:
Nickolay Golubev
Marketing Communications Manager
+1 (877) 9-OXYGEN (USA)
+44 (0) 20 8133 8450 (UK)
press@oxygen-forensic.com
www.oxygen-forensic.com