C16 Breaking User Passwords in Android™ Devices Through Recovery Partition Substitution

Pedro M.S. Eleuterio, MSc, Brazilian Federal Police, Campo Grande 79040010, BRAZIL*

Learning Overview: After attending this presentation, attendees will learn how to put the Android™ device in other boot methods to: (1) replace the original recovery partition of the Android™ device; (2) make a full internal memory backup without rooting the device; and (3) discover the smart phone user password, if it is a pattern, Personal Identification Number (PIN), or password. Attendees will also be able to understand where Android™ stores the password files and how to gain access to some password-protected Android™ devices to make a forensic analysis.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by revealing an additional method for experts to break user-defined passwords in some Android™ smart phones, allowing access to the data stored on the internal memory of a protected device. The presentation includes computer mobile forensics knowledge about Android™, including boot methods, password files, and security artifacts.

One of the main challenges in computer forensics is the analysis of smart phones, especially the device's internal memory. In the most cases, smart phone users protect their devices with Android™ native available patterns, PINs, or passwords. Thus, the computer forensics experts need to discover or bypass the lock to gain access to internal smart phone data. This study presents a new method to discover the user password in some Samsung™ smart phones with Android™ (up to version 6 (Marshmallow)) and with an external memory card slot.

Android™ has three types of initialization modes: Normal, Download (Fastboot) and Recovery, depending the keys pressed to power on the device. The strategy is to replace the original Recovery partition of the smart phone, using a custom recovery, known in some cases as Clock Work Mode (CWM) or TeamWin (TWRP). In some Samsung™ models, it is possible to replace the original Recovery Partition using Odin Software, initializing the smart phone in Download mode, and flashing the custom recovery. After replacing the recovery partition, the expert must initialize the smart phone in Recovery mode. The new custom Recovery often offers the option to backup the entire data of the internal memory of the smart phone to an external memory SDcard. Therefore, the forensic expert must use a blank memory card in the smart phone slot, which will store the full internal backup. In most cases, this backup also includes the protected user data, even without rooting the device. With the internal data of the smart phone, the forensic expert can discover the defined password, using forensic techniques, including a directed brute-force attack in the case of PIN/password protection.

If the user key is a pattern, the experts need to get the hexadecimal value stored in the "data/system/gesture.key" file, comparing it with a full pattern dictionary, which contains all pattern combinations, easily discovering the defined pattern. On the other hand, if the user key is a PIN or password, the expert needs to analyze some files, such as "data/system/password.key" (which stores the password hash), "data/system/device_polices.xml" (which stores the password mask and size), and also find the password salt, which can be stored in "/data/data/com.android.providers.settings/databases/settings.db" or "data/system/locksettings.db-wal" files, depending on the Android™ version. With all that information, the forensic expert needs to brute-force attack the PIN/password, using a program such as Hashcat, directing the attack with a known mask observed within "device_polices.xml" file. Hashcat is a free brute-force password attack program, which supports hundreds of password types, including MD5 and SHA-1, typically employed in Android™. In most cases, only a few minutes attack is necessary for Hashcat to discover the PIN/password, allowing the forensic expert to gain access to the smart phone and finally begin the forensic analysis of the device.

If recovering deleted files with data carving is not essential in the case, the experts do not need to obtain the user password since the full internal memory backup has all active data of the smart phone and, in some cases, this information is enough to discover the digital evidence contained on the smart phone.

Otherwise, there are known limitations of this strategy. For example, newer Android™ versions changed the way it stores the user password; some Samsung™ devices have Factory Reset Protection (FRP) or Secure Download Enabled, which prevent the partition from being overwritten; some Samsung™ models do not have a specific custom recovery; and the device will lose its warranty.

Mobile Forensics, Password Breaking, Android™