Android Security Internals

An In-Depth Guide to Android's Security Architecture

by Nikolay Elenkov

Errata updated to print 7

Page	Error	Correction	Print corrected
297	Most mobile devices today have some kind of **UICC**.	Most mobile devices today have some kind of **IC card (either UICC, which can host multiple applications; or a single application SIM card, in the case of older devices) to identify to the mobile network**.	Print 2
298	**SWP is used to connect the UICC to a NFC controller, allowing** the NFC controller to expose the UICC to external readers when in card emulation mode.	**When the NFC controller is physically connected to the UICC, SWP allows** the NFC controller to expose the UICC to external readers when in card emulation mode.	Print 2
299	Insertion	**Note that switching modes resets the eSE, and thus the target applet needs to be selected again. The next section shows how to use the wired mode to communicate with the eSE from an Android app.**	Print 2
330	The `neverallow` rule **says that the declared operation should never be allowed, even if an explicit allow rule that allows it exists. For example, the rule shown in Listing 12-15 forbids all domains but the init domain to load the SELinux policy**.	The `neverallow` rule **ensures that an `allow` rule for the declared operation will never be generated, even if such a rule were explicitly specified in the policy source. Because `neverallow` is a compiler-enforced rule, any policy source that conflicts with `neverallow` rules will generate a compile error. For example, adding an `allow` rule that tries to permit any domain different from init to load the SELinux policy will result in a compiler error because the `neverallow` rule shown in Listing 12-15 forbids that**.	Print 2
351	This flag allows the bootloader to detect if it has ever been **locked** and disallow some operations or show a warning even if it is in a locked state.	This flag allows the bootloader to detect if it has ever been **unlocked** and disallow some operations or show a warning even if it is in a locked state.	Print 2
369	However, several security enhancements in Android 4.37 and later versions disallow apps from executing SUID programs by dropping all capabilities from the bounding set of Zygote-spawned processes, and mounting the system partition with the **`nosetuid`** flag.	However, several security enhancements in Android 4.37 and later versions disallow apps from executing SUID programs by dropping all capabilities from the bounding set of Zygote-spawned processes, and mounting the system partition with the **`nosuid`** flag.	Print 2