Securing private key operations on mobile phones: SELinux vs. ARM Trustzone

Christopher Jämthagen

Abstract

More and more mobile payment solutions emerge as Smartphones become more common to every man. With these new technologies people have the freedom to choose from a wide range of payment options. However, as with most new technologies, security is often a low priority for the developers, who rather focus on functionality and usability. This is especially true for Smartphone OS developers who have to take performance and battery life into account, mainly due to the competitive market and the fact that end-users care more about that kind of features than security. If Smartphones are to become a substitute for wallets, ID documents and other important functionality, security must be the single most important feature to focus on.

We will be looking at how we can implement security features in the Android operating system to make sure that private key operations, which are common in most, if not all, mobile payment solutions, are secured from potential malware locally on the smartphone, as well as from remote attackers. We will take a look at two different technologies and see how well they can confine applications and provide trusted UIs to make sure the end-user is secure.

The first solution is SELinux, which provides Mandatory Access Control at the kernel level and allows the system administrator to confine applications in their own sandboxes such that even the superuser is prohibited to access the application and its files. The second solution is ARM TrustZone, which is a hardware security extension to several ARM architectures. TrustZone provides two virtual CPUs, one of which runs in the normal, or unsecure, world and the other one runs in the secure world. Applications running in the secure world are completely isolated from those running in the normal world. We will be looking at the strengths and weaknesses of each solution to find the best fit for Android.

The payment solution we will be focusing on securing is the decentralized cryptocurrency called Bitcoin. The reason for choosing this technology is because of its open nature and the plethora of solutions on multiple systems. Of course the techniques that will be researched may be applied to any solution utilizing private key operations and thus isn’t limited to bitcoin.