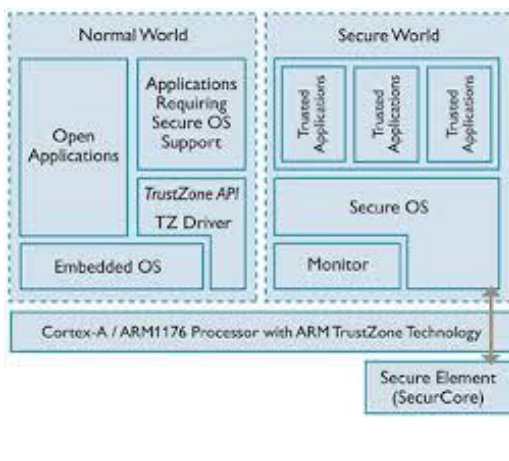


Title of internship : **DPL_2015_SP_012** Implementation of a secure video player application for Android making use of the Trusted Execution Environment available on a common Android device.

Summary of the internship (for Technicolor internship offer web page).

 <p>The diagram illustrates the ARM TrustZone architecture. It is divided into two main worlds: the Normal World and the Secure World. The Normal World contains Open Applications, Applications Requiring Secure OS Support, TrustZone API, and TZ Driver. The Secure World contains Trusted Applications, Secure OS, and a Monitor. Both worlds are supported by the Embedded OS. At the bottom, the Cortex-A / ARM1176 Processor with ARM TrustZone Technology is shown, which includes a Secure Element (SecurCore).</p>	<p>The goal of this internship is to design an Android video player that processes video buffers in a secure CPU context.</p> <p>Skills: Linux enthusiast, Linux drivers, embedded system developments, security awareness</p> <p>Keywords: Software protection, TEE, Trustzone, Android</p>
--	---

Detailed description

Context
<p>As of today, Android is not suitable to run an application that deals with highly sensitive data for the following reasons:</p> <ul style="list-style-type: none"> - Devices openness: On most Android devices, the bootloader can be unlocked, making it possible to install and launch customized ROM. In addition, the original ROM will let you install applications from “untrusted sources” (i.e not from the play store). Furthermore, a study by RiskIQ reports in 2013 that more than 42 000 apps in Google’s store (the “trusted sources” according to Google) contained malware/spyware/fake applications. Finally, on most devices, there is no root of trust, no integrity check on the system partition and finally no encrypted system partition - Source code openness and platform popularity: Nearly all the software embedded in an Android device is open source. There are many hackers and security researchers looking for peer recognition or trying to sell a security product/service. They are all exploring the source code in the hope of finding the next exploitable vulnerability. - Bad and non-homogenous long term support: Security flaws are found every single day. However, stock ROM updates with recent security patches are parsimoniously released, and the frequency depends on the manufacturer. At best, Google guarantees that Nexus devices gets recent updates 18 months after the product launch time. Many vulnerable devices are left behind. - Android let the user decides... <ul style="list-style-type: none"> o about trusted sources 7 users in 10 explicitly enable untrusted sources - Forristal Blackhat-US2013 o about application permissions. Sadly, the user usually does not care and is not a security expert. <p>By chance, ARM Trustzone and Global Platform Trusted Execution Environment specifications provide a (more)</p>

Apply at: stage.rennes@technicolor.com



Technicolor R&D France Snc
975 av des Champs Blancs – CS 17616
35576 Cesson-Sévigné Cedex - France

tél. + 33 (0)2 99 27 30 00
fax + 33 (0)2 99 27 30 01

Internship proposal for 2015
Proposal ref:
DPL_2015_SP_012

secure CPU execution context enabled on more and more devices. This technology is widely marketed as the silver bullet for protecting user data, inputs, payments and privacy as well as premium video contents, particularly because the protection is still effective on rooted/infected devices.

Objective

Starting from an Android video player application playing protected video content on an Android device, the intern will move the content protection code to a standalone service running in the Secure Execution Environment (SEE).

The main difficulty is to achieve this on a common (on the shelf) Android device without changing the stock Android firmware. The secure service running in the SEE will be launched from the Android application using the appropriate API.

The video chunks that reach the SEE will be computed and stored in an unprotected form in the SEE. At this point, the intern will make some propositions to secure the video data path to the sink (display, HDMI).

The software will be written mainly in C and C++.

Task description

The intern will study the Global platform TEE specifications and the Secure Execution Environment API.

He will design the interface between an Android video player application and a secure service that processes the video buffers in a secure CPU context.

He will use an Android SDK and the Secure Execution Environment SDK to implement this application.

Working environment

Linux / Android
C, C++
ARM DS-5