Joakim Harbitz

Studentid: 120924 / 12HBISA

Obligatory exercise #1

2014-09-03

Task

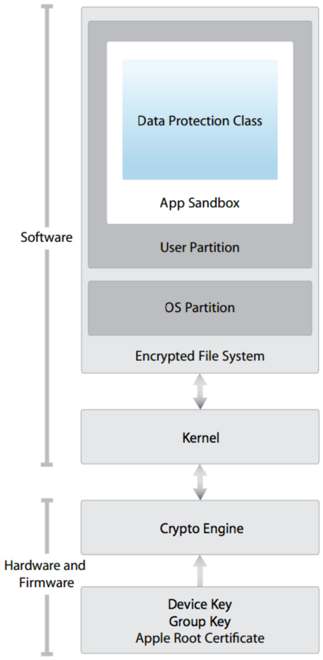
- Choose an operating system that does not have "Microsoft Windows" in its name, e.g. Mac OS, Linux, iOS, Android, Multics, Plan 9, Turaya, Solaris.
- Find out and describe how the OS implements the concept of a trusted path (if it does).
- Include references to the sources that support your findings (scientific articles, developer documentation).

iPhone Touch ID & sandboxing

A trusted path is defined as a mechanism that provides confidence that the user is communicating with what the user intended to communicate with, ensuring that attackers can’t intercept or modify whatever information is being communicated.

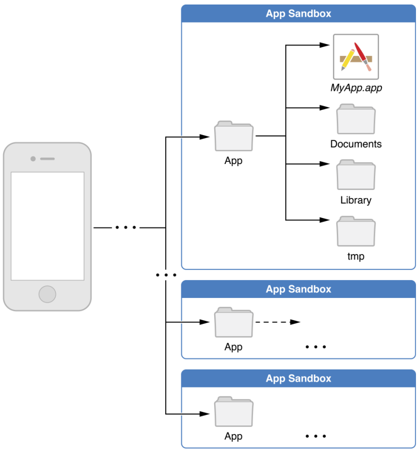
There are different ways to authenticate a user to a system. The most common way is the password, where the user provides a password, and the system checks if the password is correct according to it’s records. Another way of authenticating is, biometry. Apple has released a phone, called iPhone 5s where the user can get authenticated to the system by scanning one of their fingers on a «Touch ID sensor».

Trusted path



Software can only be installed and run if Apple has signed the binaries. As a part of the «secure boot chain», a read-only Boot ROM containing Apple’s root certificate checks that the boot loader and kernel is not modified by checking that every step in the secure boot chain is signed by Apple. This ensures that only code accepted by Apple, is allowed to run on the device. The same applies to the processor controlling the Touch ID sensor, which is called «The Secure Enclave» and is a coprocessor located beside main A7 processor. TSE uses encrypted memory so that other processes cannot read its data. Communication between it and the A7 processor is isolated in shared memory data buffers. As no app on the device has access to the encrypted finger print data stored by TSE, or the sensor input, the sensor is considered safe.

It’s not just the Touch ID sensor that has a trusted path, but also every app. As long as the iPhone is not «jailbroken» and app signing is still enforced, users have a trusted path when entering any type of input into an app, since no app can take control over another app because of sandboxing. This means that every app is separated from each other and cannot «see» or communicate



with each other without the operating system allowing it.

Sources:

http://en.wikipedia.org/wiki/Trusted_path

http://techcrunch.com/2014/02/26/how-touch-id-and-secure-enclave-work/

http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf