Web Cryptography & utilizing ARM TrustZone based TEE (Trusted Execution environment) for authentication, cryptography and beyond

ARM TrustZone is a technology which is being utilized on ARM based Cortex A series SoCs to achieve a trusted execution environment, which can totally isolates rich OS such as Android, iOS, Windows Phone and Firefox OS from a trusted execution environment by using various enablers in memory management, interrupt management, bus architecture, CPU modes, etc.

ARM TrustZone technology and TEE solutions utilizing it are already available on millions of mobile devices and the usage is being spread to desktops and laptops with the adaption of ARM based SoCs.

ARM TrustZone technology can be used for the following uses cases to achieve a high level of security:

- DRM (Digital Rights Management). The DRM technologies that utilize ARM TrustZone include but not limited to Microsoft PlayReady and Widevine DRM technologies. Secure video path DRM functionality can easily be achieved by utilizing ARM TrustZone technology. Meaning that encrypted content can be decrypted and processed without revealing any content to rich OS.

- Authentication: Multifactor authentication including OTP (One Time Password), certificate based authentication, biometric authentication (e.g. fingerprint readers) can be achieved securely by utilizing ARM TrustZone technology

- Integrity measurement: ARM TrustZone technology can be utilized for achieving rich OS kernel run time integrity measurement (e.g. Linux kernel runtime integrity), remote attestation. It can also be used by various integrity measurement architectures such as IMA/EVM.

- Secure display and touch: Allows retrieving and displaying data on touch displays without revealing any information to rich OS

- Cryptography & key management: Allows cryptographic key material generation, key derivation and encapsulation in an isolated trusted execution environment, handling crypto operations without revealing key material, confidential data to rich OS, accessing crypto HW accelerators securely. ARM TrustZone based TEE is currently being utilized by HW assisted Android KitKat keymaster for various crypto operations such as RSA, DSA, ECDSA key data generation, sign, verify, import key data, get public key, etc..

- Secure random data generation (e.g. secure access to TRNG, generating pseudo random data, etc..)

ARM TrustZone based TEE solutions can provide all required functionality to achieve the cryptographic operations mentioned in [1]. This includes, secure key generation, key derivation, symmetric and asymmetric cryptographic operations (e.g. RSA operations with various padding such as PKCS# v1.5, PSS and OAEP, DSA operations, ECDH and ECDSA operations, AES with various

modes). ARM TrustZone based TEE solutions can also allow achieving high level of security to handle authentication peripherals as well as processing authentication data securely. Optional crypto extensions can also be used to speed up SHA and AES operations as well as AES GCM operations on ARMv8 based SoCs.

There is considerable interest in the mobile market in using TEE for cryptography and identity functions but adoption has been hampered somewhat by fragmentation and lack of accessibility through standardized APIs. Those problems are now being solved at the mobile OS/apps programming layer. It can only make sense to also bring this accessibility to the Web programming layer.

[1] http://www.w3.org/TR/WebCryptoAPI/

Ilhan Gurel is a security engineer working for Security & Crypto team at Trustonic and has been in various security engineering roles at Nokia and Giesecke & Devrient. He has been involved in various projects related to chipset security, OS and application security during his employment at Nokia, Giesecke & Devrient and Trustonic.