

Solutions to Assignment 4

Xinxin Fan

Solutions

1. (a) A certificate update protocol for a newly generated pk_A is as follows:
 - The platform uses its private key sk_C to sign the new pk_A and sends $pk_A, Sig_{sk_C}(pk_A)$ and pk_C that is certified by the root public key to a certificate authority (CA).
 - CA first verifies the authenticity of pk_C using the root public key and then verifies the validity of the platform's signature on pk_A using the platform specific public key pk_C . If both verifications succeed, CA will issue a certificate for pk_A .

(b) The advantage of the combined method is that the remote party only needs to verify the CA's signature on pk_A instead of a certificate chain from the root public key on the platform. However, the disadvantage of this combined method is that CA should be always online and support a certificate update protocol and another interface is needed for the platform to communicate with CA.
2. (a) Since only the first 50 bits of the hash value of the root public key is protected, the attacker can perform an exhaustive search which will find a collision on the root public key pk_{root} (i.e., the attacker can find another string pk' such that $\text{Truc-SHA-1}(pk') = \text{Truc-SHA-1}(pk_{root})$, where $\text{Truc-SHA-1}(\cdot)$ means truncating the output of $\text{SHA-1}(\cdot)$ to 50 bits) in around 2^{50} trials. Note that the root public key, which is used to verify the signature on the very first software entity in the boot string, is stored in the regular storage area. Hence, if the attacker replaces the real root public key pk_{root} by pk' , he will break the secure boot string in millions of device because the signature on the first software entity can be verified successfully with pk' and the platform will install the attacker's software.

(b) If a platform specific key K_p is available on the platform and protected, then a manufacture can store the first 50 bits of $\text{SHA-1}(pk_{root}||K_p)$ in the OTP memory. In this way, the attacker only can break the secure root string for one device each time. Therefore, the effect is limited, i.e., only one device is a victim.
3. (a) Note that the KEK is used to protect other storage keys and is only accessible by the cryptographic coprocessor. Therefore, all encryption/decryption operations are performed within the cryptographic coprocessor and symmetric key algorithms are appropriate in this application scenario. Moreover, it is not necessary to replace KEK by a public/private key pair because the storage keys are only encrypted by and stored in the cryptographic coprocessor (i.e., the sender and the receiver of the message is the same entity) and the symmetric key algorithms are more efficient in this scenario.

(b) If an authentication key and the application code are stored, a user needs to present the message authentication code (MAC) each time when the application is executed. Once an adversary intercepts the MAC in some communication session, he/she can use the application code in other sessions.