FROST & SULLIVAN

Wisecure Technologies

END-TO-END SECURE COMMUNICATION USING WISECURE'S μSD/X

WiSECURE's public sector client was in need of a secure communication on top of its existing communication encryption application. WiSECURE's μSD/X was able to integrate into Signal's cross platform application, bulking up the client's SCA prevention strategy through cryptographic algorithms.

A Frost & Sullivan whitepaper commissioned by ITRI.

SUMMARY

WiSECURE is a subsidiary of InfokeyVault Technology Co. (IKV-Tech), a Hardware design service provider with several years of experience in hardware security risk assessment, threat analysis, hardware design service and production.

The company has strong capabilities in providing advanced and standardized products, supported by Taiwan's mature semiconductor ecosystem. At present, WiSECURE has steadily penetrated the hardware side of the bitcoin storage world, with several cold wallet applications using security hardware modules designed by WiSECURE.

CASE STUDY

The Client: A public sector institution that handles large volumes of classified information, requiring high levels of privacy and security in their communication channels.

Challenge:

The client used WiSECURE's μSD/X to facilitate a secure communication environment on Signal, the communication application they used to provide end-to-end encryption for messages and calls.

Even though Signal provided end-to-end encryption for this client, the databases they stored on personal devices were still a critical pain point. These were open vulnerabilities, at risk of being attacked by hackers who could easily use Side Channel Attacks (SCAs) to analyze communication content through backdoors and spyware within mobile applications.

Solution:

The WiSECURE μSD/X platform supports a wide range of cryptographic algorithms and is able to accelerate storage encryption to 10 MB per seconds, surpassing all similar competitive products. It provided the client with a range of security functions, from one-way and bilateral voice and data communication to bilateral key exchange, decryption and encryption services, and modified elliptic curve key protocols. After WiSECURE deployed their platform within the client's communication networks, users were able to initiate their encryption service, set up PIN codes and then create a set of unique authorization identities before registering into Signal: a personal Identity Key (IK), a Signed Prekey (SPK), One-time Prekeys (OPKs), and perform the application secure communication (such as X3DH) within μSD/X.

Results:

WiSECURE's μSD/X was able to easily integrate into Signal's cross platform applications. With its secure hardware, it bulked up the client's SCA countermeasure strategy through cryptographic algorithms, managing the process of key storage and enhancing the security efficiency out of the application.