USE CASE - SECURE MESSAGING PLATFORM

Securer Than The Securest

Optimization Of Signal

Designed for device-side security in the form of micro SD, µSD/X is a hardware security module ensuring users' privacy in end-to-end communications.

Features of signal

Signal[1] is a secure messaging application gaining widespread popularity with its measures in code auditing and sophistication in cryptographic functions. It offers an open source platform for the client and server sides, allowing experts and advanced users to produce a collective reflection and make improvement. As to cryptographic functions, the X3DH (Extended Triple Diffie-Hellman)[2] key agreement protocol establishes a shared secret key between two parties who mutually authenticate each other through the server. Two parties' private keys are kept in user environments during the establishment, which considerably mitigates the risk of private key leakage. Then the Double Ratchet algorithm is used by two parties to exchange encrypted messages based on the shared secret key already agreed on. While two parties communicate, new keys are derived for every Double Ratchet message so that earlier keys cannot be calculated from later ones and vice versa. The property ensures the confidentiality of earlier, later and another party's messages in case a party's keys are compromised.

Security risks on personal devices

Fast, simple and secure as Signal appears, in its pursuit of simplicity and user-friendliness lie inconspicuous vulnerabilities. On the one hand, users' private keys reside in internal storage, likely to be compromised by backdoors and Trojans in other applications. They are also prone to be extracted by side-channel attack (SCA) through analysis of power consumption, and accessed due to security breaches in the operating system. On the other hand, the method to recover cryptographic keys encrypting the app database has been discovered by Kamil KACZYŃSKI[4]. It has been implemented by WiSECURE Technologies and proved effective in acquiring key data in KeyStore service and deciphering conversation histories.

µSD/X - protecting keys and database

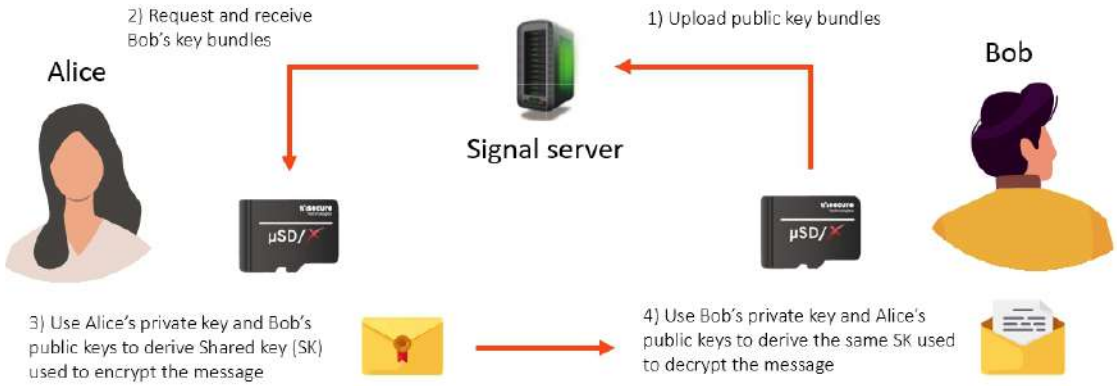
Designed for device-side security in the form of micro SD, µSD/X can integrate with Signal and address aforementioned security concerns. With storage, agreement, generation and other cryptographic functions performed in the module, there is no way for attackers to acquire key materials. In the module, there is a high-end secure element, Infineon SLE 97[5], which can render latest cryptographic protocols adopted in Signal resistant to side-channel attack (SCA). The protocols included Edwards-curve Digital Signature Algorithm (EdDSA) [6] and the Double Ratchet algorithm. In addition to security, a cryptographic accelerator is embedded to address security-performance trade-off that may affect user experience, making heightened security and uncompromised performance go hand in hand.

Use case – How does µSD/X ensure the security of keys?

Upon registration, µSD/X generates an identity key (IK) for account binding and a signed prekey (SPK). Then every time communication occurs, one-time prekeys (OPK) are computed to encrypt messages. Without authorization, none of these keys are allowed for extraction or revealed, even during cryptographic operations.

If Alice sends an encrypted message to Bob via Signal, the encrypted communication flow involving µSD/X is as follows.

1. To perform X3DH and then compute a shared key for secure communication, Bob exports the key bundle containing the paired public keys of IK, SPK and OPK(s) from µSD/X to the Signal server.
2. Acquiring the key bundle from Bob, Alice performs X3DH using Bob's key bundle and her private key, after which a shared key is computed in µSD/X.
3. Alice sends to Bob her identity key, a random-generated one-time public key and confidential message encrypted with the shared key. Then Bob can compute a shared key accordingly and decrypt the confidential message from Alice.



Successful use case application

µSD/X has been applied to our customer's secure communication, providing key exchange and encryption services for voice and data communication. The latest elliptic curve digital signature scheme, Edwards-curve Digital Signature Algorithm (EdDSA), is performed in compliance with National Institute of Standards and Technology (NIST). µSD/X also features high-speed encryption and data transport, which means the shorter it takes to compute keys, the lower the likelihood is to induce key leakage. Lastly, our capability of customizing algorithms, including the one specified for hardware attack, such as side-channel attack countermeasures, allows WiSECURE Technologies to become the option considered first among other security solutions.

Reference

[1] https://signal.org/#page-top
[2] https://signal.org/docs/specifications/x3dh/
[3] https://signal.org/docs/specifications/doubleratchet/
[4] Kamil KACZYŃSKI, "Security Analysis of Signal Arduino Database Protection Mechanisms,"International Journal on Information Technologies & Security, № 4 (vol. 11), 2019.
[5] https://www.infineon.com/cms/en/product/security-smart-card-solutions/security-controllers/sle-97/
[6] https://en.wikipedia.org/wiki/EdDSA

Wisecure Technologies