Signal & The Double Ratchet

Robert (Bobby) Picciotti

Notable Features of The Double Ratchet

- Forward Secrecy
- Future Secrecy
- Asynchronicity
- Message Unlinkability

The Primitives

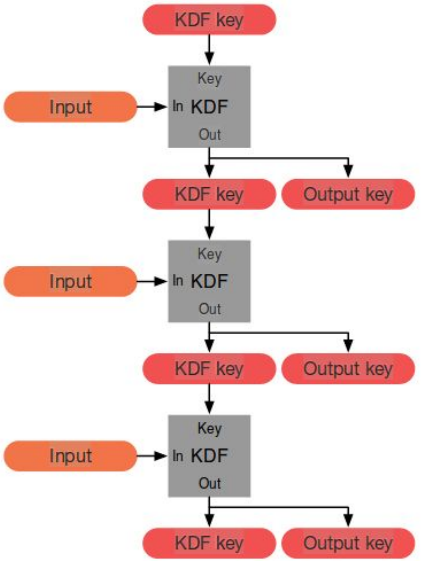
- The Diffie-Hellman Ratchet
  - Elliptic Curve Diffie Hellman
    - Using Curve 25519
    - Fast and 128 bits of security
  - X3DH
- Symmetric Encryption
  - AES
    - Cipher Block Chaining mode
    - Counter mode
- Message Authentication Codes
  - HMAC using SHA-2 (256 bit)
- Hash Ratchet
  - HMAC

X3DH

- Supports X25519 or X448
- Allows for key exchange where one party may be unavailable
  - The exchange happens through an available third party “server”
- Bob places his public identity key, and a signed prekey
  - Alice gets these and forms an initial message with it
  - Bob then processes the message
- The pre-key is replaced frequently
- The protocol has a fallback if no pre-key is published
  - However, replay is possible without a signed pre-key

KDF Chains

- KDF chains
  - “Key Derivation Function”
  - Takes secret, random KDF key and input data
  - Output split into new KDF key and an output key
- Three chains are used
  - Root
    - Input: Diffie-Hellman output secrets
    - Output: Used as KDF keys for other two chains
  - Sending & Receiving
    - Input: Root chain output
    - Output: Used to encrypt messages



A Double Ratchet

- The Diffie-Hellman Ratchet
  - The Root chain is fed with the DH secret output
    - Add resilience to break in
  - The DH keys are changed frequently
    - Deriving the new key forms the first ratchet
  - The Root chain is updated twice each DH ratchet
- The Symmetric Ratchet
  - These chains are ratcheted for each message
  - Ensure each message has a unique key
  - Keys can be deleted after use
  - Keys for missed messages are stored