SIGNAL PROTOCOL

An Insight Into the Protocol and Its Vulnerabilities

Written by: Chinedu Chikezie, Iden Koxhaj, Shihao Dong
Mentor: Shweta Jain, PhD

May 2022

ABSTRACT

This research explores the structure, vulnerabilities and deployment challenges of Signal, an End-to-End Encryption (E2EE) communication protocol that has gained popularity in the last five years The objective is to explore the features of the Signal protocol, reverse engineer its specification, and build a testbed implementation to fully document its attack surface and threat model.

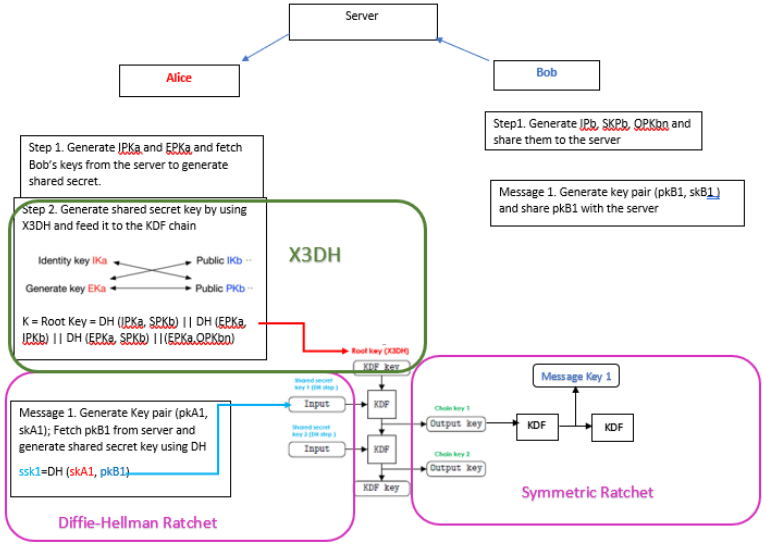
SIGNAL PROTOCOL

Is a cryptographic protocol for instant messaging that aims to offer End-To-End_encryption. It is the core of the Signal instant messaging application and has recently been adopted by other apps such as Whatsapp, Facebook Messenger, and Google Allo, Viber, Skype etc. Even if an attacker is able to decrypt a message, the protocol ensures:

Forward security: he can't get access to the previous ones.

Post-Compromise secrecy: he can't possibly intercept the following messages.

HOW DOES IT WORK?



1. A server stores the public keys of each party for authentication.
2. The user asks for its partner's key information from the server to calculate the initial master secret, from which the first keys can be derived➔ X3DH
3. The user regularly ratchets newly-established secrets in order to generate fresh message keys➔ Double Ratchet Algorithm.

- **X3DH➔**The Extended Triple Diffie– Hellman Key Agreement Protocol establishes a shared secret between two parties who mutually authenticate each other based on public keys and provides forward secrecy.
- **KDF Chain➔** Key Derivation Function chains used by Double Ratchet Algorithm to constantly derive new keys for encrypting each message. Takes as first input the output of the X3DH and continues with the output from the Diffie-Hellman Ratchet on each step. Responsible for the key freshness.
- **Double-Ratchet Algorithm➔** Combines the **Symmetric-key ratchet** for deriving keys for exchanging messages and a **Diffie–Hellman ratchet** to provide secure inputs to the symmetric-key ratchet

VULNERABILITIES

1. It's open source and not standardized.
2. Group messages can easily be hacked.
3. Implementation techniques by instant messaging applications leave it vulnerable to hacking possibilities.

TESTBED IMPLEMENTATION

A small group of people with some technical expertise can setup a private Signal server and client system for their own use. Here's what they need:

1. Open-source code of signal server pulled from GitHub.
2. Locally hosted Signal Server implemented on Ubuntu 20.04 LTS.
3. Using Signal Server version 4.97.
4. Docker container for hosting Signal Server dependencies.
   - MinIO
   - PostgresSQL
   - Redis
   - Coturn Server

REFERENCES:

How Signal Instant Messaging Protocol Works (& WhatsApp etc) – Computerphile; https://www.youtube.com/watch?v=DXv1boalsDI
Double Ratchet Messaging Encryption – Computerphile; https://www.youtube.com/watch?v=9sO2qdTci-s
Van Dam D. "Analyzing the Signal Protocol: A manual and automated analysis of the Signal Protocol" , 2019, Thesis, Radboud University
Johansen C, Mujaj A, Arshad H, Noll J. *"The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications"*, 2021, https://doi.org/10.1155/2021/9965573
Blazy O, Bossuat A, Bultel X, Fouque P.A, Onete C, Pagnin E, *"SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting"*, 2019, IEEE. DOI 10.1109/EuroSP.2019.00030
Bobrysheva J, Zapechnikov S, *"Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm"*, 2020 IEEE Xplore
Cohn-Gordon K, Cremers C, Downling B, Garratt L, Stebila D. *"A Formal Security Analysis of the Signal Messaging Protocol"*, 2017 IEEE European Symposium on Security and Privacy
Kobeisi N, Bhargavan K, Blanchet B, *"Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach"*, 2017 IEEE, DOI 10.1109/EuroSP.2017.38
Chen K, Chen J, Zhang J. *Anonymous Asynchronous Ratchet Tree Protocol for Group Messaging*. Sensors. 2021; 21(4):1058. https://doi.org/10.3390/s21041058
Cohn-Gordon K, Cremers C, Garratt L, Milican J, Milner K. *"On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees"* , CCS'18, October 15-19, 2018, Toronto, ON, Canada
Sukhodolskiy I, Zapechnikov S, *"Analysis of Secure Protocols and Authentication Methods for Messaging"*, 2020 *Procedia Computer Science 169 (2020) 407–411*
Dusane T.P , *"Generation, Verification, and Attacks on Elliptic Curves and their Applications in Signal Protocol"*, 2021, Master of Science in Computer Science Thesis, Rochester Institute of Technology