Frosix: FROST Multiparty Signatures on the Network

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Christian Grothoff
Expert: Markus Nufer

Keeping a private signing key confidential is a challenging task. One of the main reasons for this is that any device could be compromised, making it insecure to handle a private signing key on a single device. The field of multiparty threshold signature schemes aims to address this problem using advanced cryptographic techniques. Frosix is a free software implementation of FROST, a promising threshold signature scheme.

Introduction

In the future, almost everything would ideally be signed with cryptographic signatures to provide integrity, authenticity and non-repudiation. But how to handle a private signing key properly if any device could be compromised? Based on the threshold signature scheme FROST, Frosix provides a solution to this problem.

Theory

Multiparty Threshold Signatures

Briefly, in multiparty threshold signatures the signing key is distributed among n parties, such that $t \leq n$ parties are required to generate a valid signature.

Distributed Key Generation

The primary objective of distributed key generation is the contribution of all parties to the resulting key pair, without combining the signing key in any single place.

Distributed Signing

In distributed signing, each selected party signs with their own share of the signing key, producing a partial signature. These parts can then be combined into one signature. As a result, the private signing key is never constituted on a single machine!

Implementation & Architecture

Frosix consists of two separate applications, the Frosix service provider, a lightweight webserver, connected to a PostgreSQL database and the Frosix client, an application with a command line interface.

Authentication

As the device requesting a signature cannot be trusted, a Frosix service provider always conducts an authentication procedure before providing a signature share. This can involve proving the answer to a security question or solving a challenge.

Results

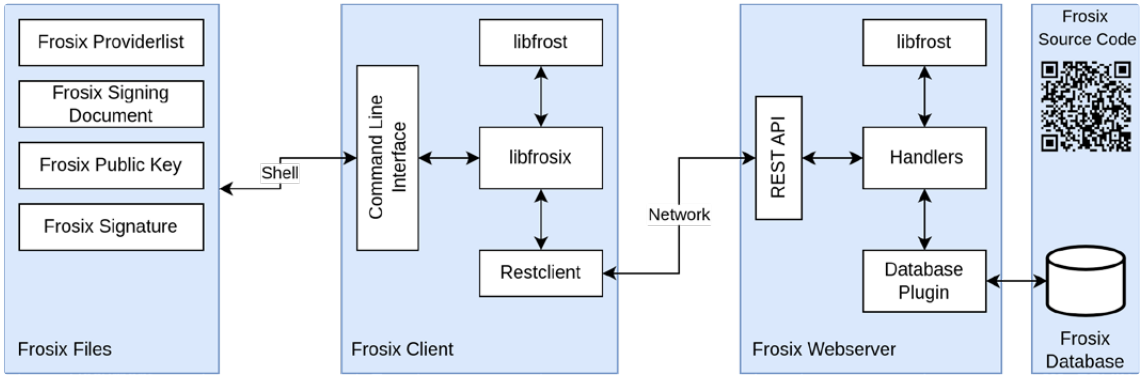
The current implementation of Frosix allows for the generation of a distributed key of up to 254 parties, with a threshold value of up to 253. Furthermore, Frosix supports signing with different authentication methods.

Future Work

There are additional ideas to enhance Frosix and enable it to be utilized as a commercial service:

- support alternative signature algorithms in libfrost
- integrate GNU Taler as a payment system
- develop a GUI or a more user-friendly application
- implement deterministic threshold signatures

Joel Tobias Urech



Frosix System Architecture