CS2361: Blockchain and Cryptocurrencies
Project Milestone 1: M-Pin

Argha Chakrabarty Aarav Varshney

April 13, 2022

Introduction

We need authentication for primarily three reasons:

- authenticate the client to the server,
- authenticate the server to the client,
- and should result in a negotiated encryption key with which subsequent communications can be encrypted.

Until now we've been using Username/Password authentication for authenticating the client and the use of SSL/TLS protocols for authenticating the server. SSL even though now deprecated still had some good ideas but the Username/Password is extremely vulnerable to exploits and that's why there is a massive shift to Multi Factor Authentication (MFA).

The biggest exploit for username/password authentication is that the server stores either the hashe of the password or the password itself in the database which if compromised can be used to gain access to the passwords.

The idea behind M-Pin is that each registered client is issued with a large cryptographic secret. They then prove to the server that they are in possession of this secret using a zero-knowledge proof. This removes the requirement for any information related to client secrets to be stored on the server.

Another crucial attribute of M-Pin is the use of third party authentication. Similar to how SSL uses a CA to verify the certificates, M-Pin uses Trusted

Authority (TA) to store the secrets in contrast to Username/Password where the server performs regular operations as well as authentication.

Plan for the Project

Technical Details

Our implmentation of M-Pin involves

Future Ideas / Plans for expansions

References

[1] Tian Min et al. Blockchain games. https://arxiv.org/pdf/1906.05558.pdf.

[2] Wikipedia. Blockchain game. https://www.wikiwand.com/en/Blockchain_game.