

Device based Authentication System For Secure Web Application

Student: Shreyas Nair

Advisor: Dr. Andrew Novocin

For this project, we are developing a web authentication system that adds a device based verification when a user enters the correct email and password. The system first uses a firebase authentication to verify the users login credentials, after the credentials are confirmed, a FastAPI backend generates a random, short lived and single use authentication challenge. This challenge is then sent to the desktop authenticating agent that is being run locally on the user's computer . The desktop agent then signs the challenge using Ed25519 private key stored on the user's device. The signed response is then sent to the backend, where it is verified using the device's registered public key before the user is granted access to the website. Each approved computer receives a different private key, allowing individual devices to be recognized and revoked if they are lost, stolen or if the device is compromised. The system also rejects any expired or previously used challenges, helping protect against any sort of replay attacks. The testing would examine device registration time, login completion time, signature verification performance, invalid signature attempts, and logins from unauthorized computers. In the future it can be further developed with hardware private key storage, device management controls, security even logging, and honeypot endpoints for detecting automated scanning and suspicious login activity. This system could also strengthen website security by preventing attackers with stolen passwords from accessing an account without also possessing an authorized computer.