A Secure Password Wallet based on the SEcube™ framework

Walter Gallego Gómez

Department of control and computer engineering
Politecnico di Torino

July 23, 2018

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Are passwords still relevant?

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Are passwords still relevant?

Yes, they are the dominant form of authentication.

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Why should people use password managers?

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Why should people use password managers?
So they can use unique strong passwords.

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Why are hardware-based approaches more reliable?

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Why are hardware-based approaches more reliable?
Hardware approaches use two-factor authentication.

Motivation

The need for a hardware-based password manager is justified answering these three questions:

Are passwords still relevant?

Yes, they are the dominant form of authentication.

Why should people use password managers?

So they can use unique strong passwords.

Why are hardware-based approaches more reliable?

Hardware approaches use two-factor authentication.

Outline

Introduction

Software and Hardware components

Design

Outline

Introduction

Software and Hardware components

Design

Software Libraries

The following open source libraries were used:

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

Compatible with C/C++, Cross-platform

Software Libraries

The following open source libraries were used:

SQLite: DataBase management

Software Libraries

The following open source libraries were used:

SQLite: DataBase management

Self-contained...

Software Libraries

The following open source libraries were used:

PwGen: Password generator

Software Libraries

The following open source libraries were used:

PwGen: Password generator

Strong Random or readable

Software Libraries

The following open source libraries were used:

zxcvbn: Password strength estimator

Software Libraries

The following open source libraries were used:

zxcvbn: Password strength estimator

Considers a lot of cases....

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

Compatible with C/C++, Cross-platform
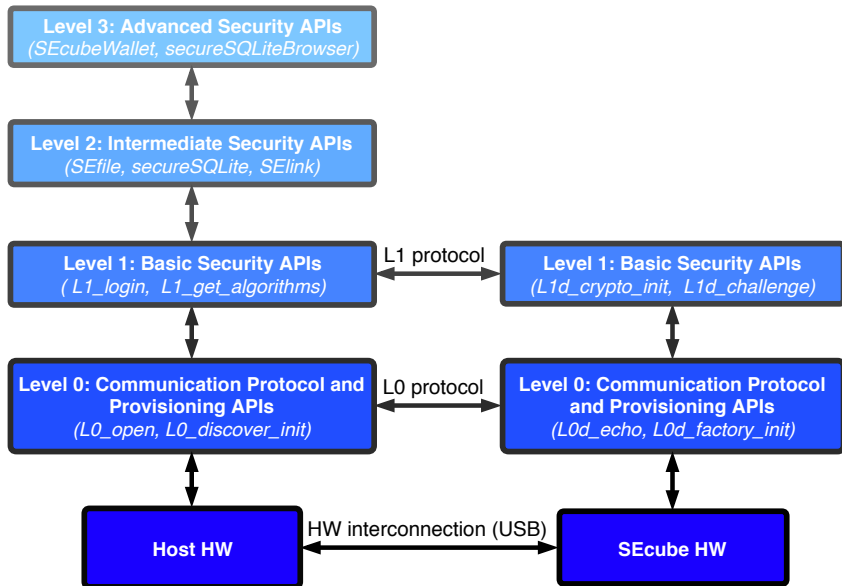
SQLite: DataBase management

Self-contained...

PwGen: Password generator

Strong Random or readable

zxcvbn: Password strength estimator
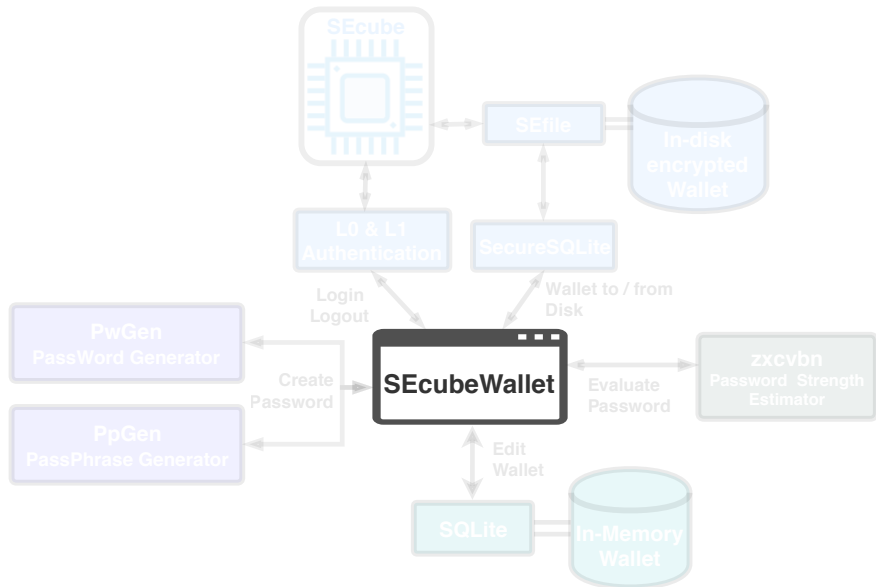
Considers a lot of cases....

SEcube™ APIs hierarchy

Level 3: Advanced Security APIs
(SEcubeWallet, secureSQLiteBrowser)

Level 2: Intermediate Security APIs
(SEfile, secureSQLite, SElink)

Level 1: Basic Security APIs
(L1_login, L1_get_algorithms)

L1 protocol

Level 1: Basic Security APIs
(L1d_crypto_init, L1d_challenge)

Level 0: Communication Protocol and Provisioning APIs
(L0_open, L0_discover_init)

L0 protocol

Level 0: Communication Protocol and Provisioning APIs
(L0d_echo, L0d_factory_init)

Host HW

HW interconnection (USB)

SEcube HW

Outline
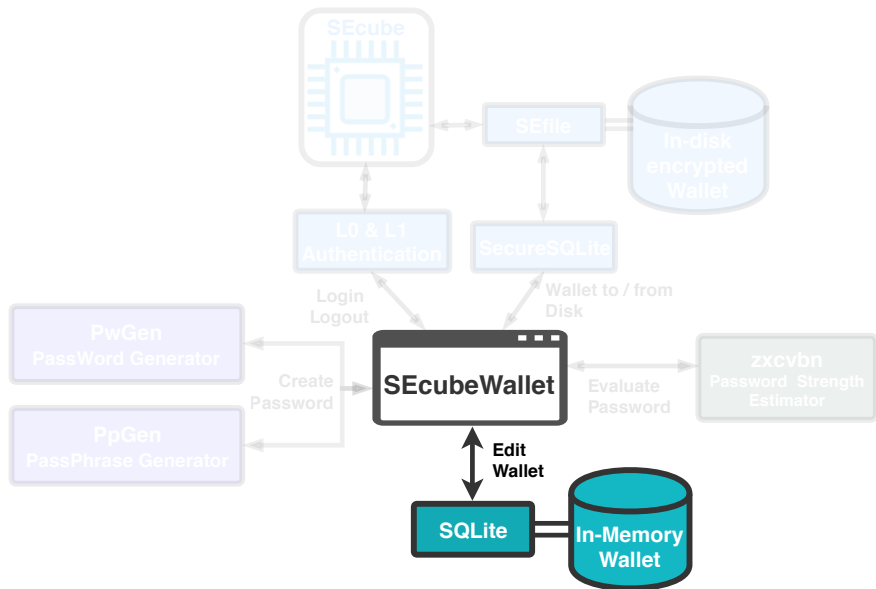
Introduction

Software and Hardware components
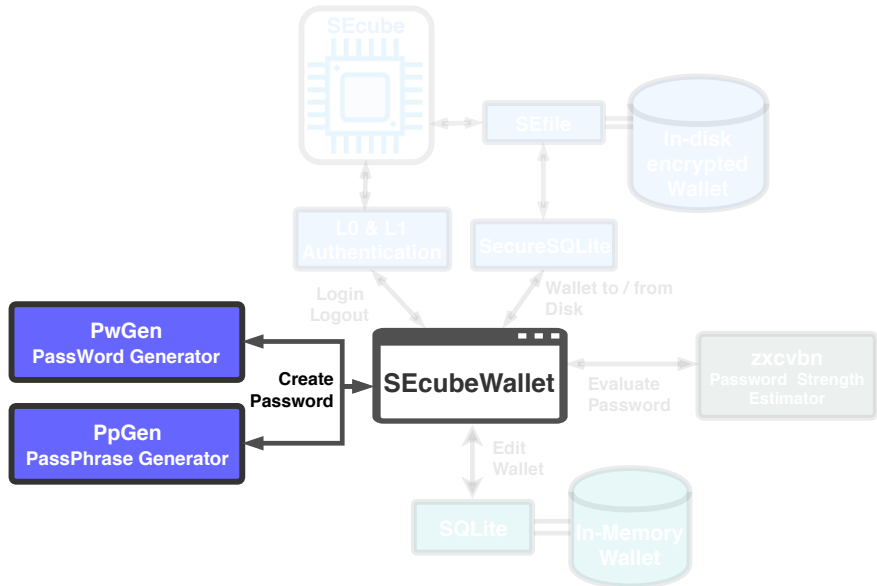
Design

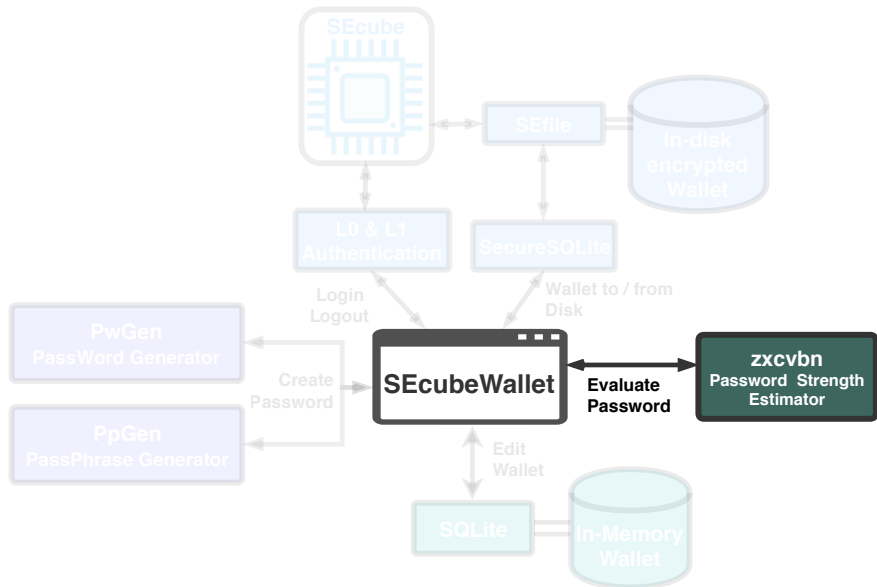# SEcubeWallet Application

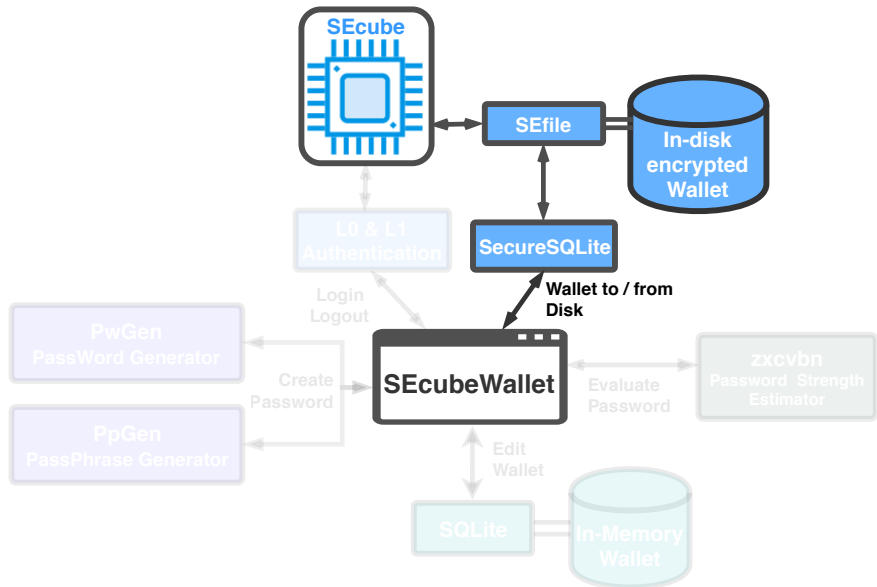# Open device and authenticate
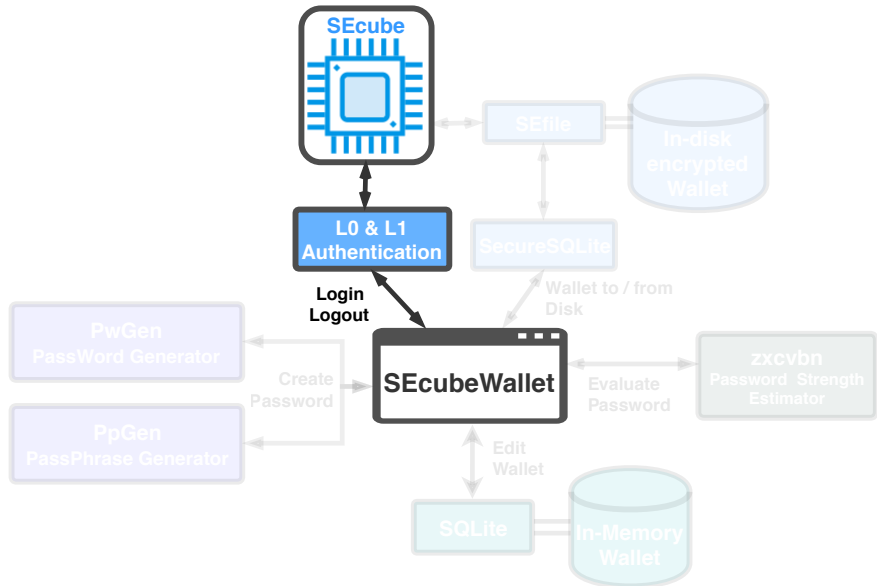
Create In-memory Wallet

Generate Password/Passphrase

Evaluate Strength

Encrypt and Save Wallet to disk

General Architecture