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:

Are passwords still relevant?

Yes, they are the dominant form of authentication.

Why should people use password managers?

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.

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?

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?

To authenticate, Master password + Device are required

Outline

1. Introduction
2. Technologies used
   - Software libraries
   - The SEcube™ Framework
3. Design
4. Demos
5. Conclusions
6. Future Work

Outline

1. Introduction

2. Technologies used

- ▸Software libraries
- ▸The SEcube™ Framework

3. Design

4. Demos

5. Conclusions

6. Future Work

Introduction

Outline

1. Introduction

2. Technologies used
   - ▶Software libraries
   - ▶The SEcube™ Framework

3. Design

4. Demos

5. Conclusions

6. Future Work

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

C++ library, cross-platform, elegant design

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Self-contained, written in C, Transactional

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Self-contained, written in C, Transactional

PwGen: Password generator

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Self-contained, written in C, Transactional

PwGen: Password generator

Configurable, random or readable

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Self-contained, written in C, Transactional

PwGen: Password generator

Configurable, random or readable

zxcvbn: Password strength estimator

Software Libraries

The following open source libraries were used:

Qt: GUI and wrappers

C++ library, cross-platform, elegant design

SQLite: DataBase management

Self-contained, written in C, Transactional

PwGen: Password generator

Configurable, random or readable

zxcvbn: Password strength estimator

Dictionaries, keyboard patterns, sequences, years

The SEcube™ Open Security Platform

Hardware

Software

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Software

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Family

- SEcube™ Chip
- SEcube™ DevKit
- USEcube™ Stick

Software

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Family

- SEcube™ Chip
- SEcube™ DevKit
- USEcube™ Stick

SEcube™ Chip

- **MCU:** STM32F4 (STM)
- **FPGA:** MachXO2-7000 (Lattice)
- **Smart Card:** SLJ52G (infineon)

Software

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Family

- SEcube™ Chip
- SEcube™ DevKit
- USEcube™ Stick

SEcube™ Chip

- **MCU:** STM32F4 (STM)
- **FPGA:** MachXO2-7000 (Lattice)
- **Smart Card:** SLJ52G (infineon)

Software

Developed by European research institutions. Written in C using the Eclipse IDE.

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Family

- SEcube™ Chip
- SEcube™ DevKit
- USEcube™ Stick

SEcube™ Chip

- **MCU:** STM32F4 (STM)
- **FPGA:** MachXO2-7000 (Lattice)
- **Smart Card:** SLJ52G (infineon)

Software

Developed by European research institutions. Written in C using the Eclipse IDE.

Firmware: Developers can customize the firmware to their needs, and load the updated version to the SEcube™ chip.

The SEcube™ Open Security Platform

Hardware

Developed by the Blu5 Group

Family

- SEcube™ Chip
- SEcube™ DevKit
- USEcube™ Stick

SEcube™ Chip

- **MCU:** STM32F4 (STM)
- **FPGA:** MachXO2-7000 (Lattice)
- **Smart Card:** SLJ52G (infineon)

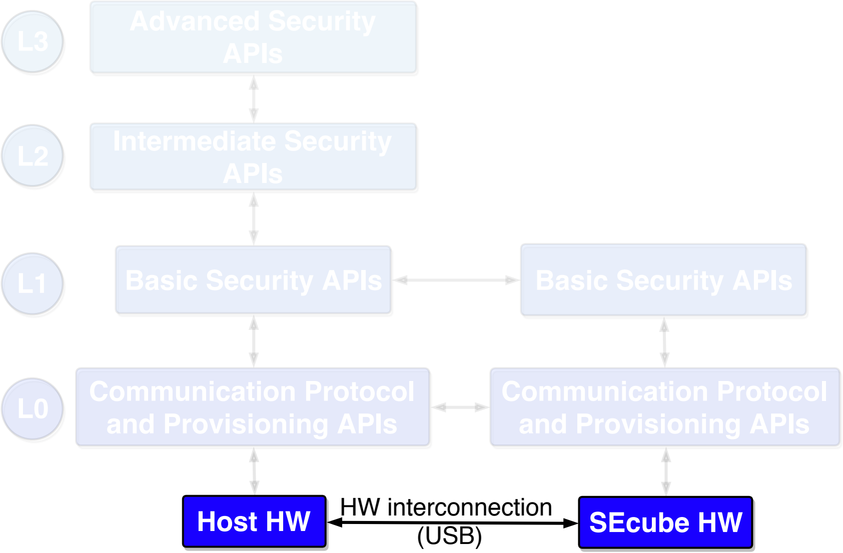
Software

Developed by European research institutions. Written in C using the Eclipse IDE.

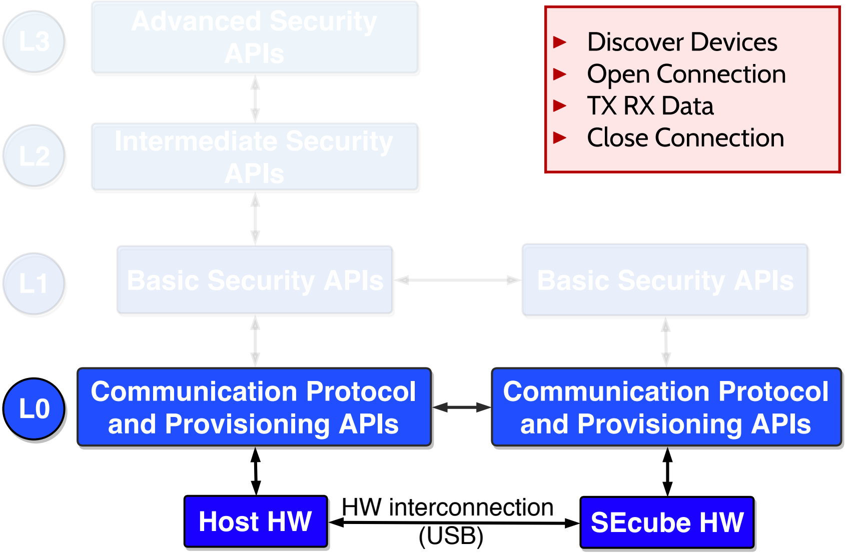
Firmware: Developers can customize the firmware to their needs, and load the updated version to the SEcube™ chip.

Host libraries: Allow to experience the platform as a high-security black box.

SEcube™ APIs hierarchy


L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

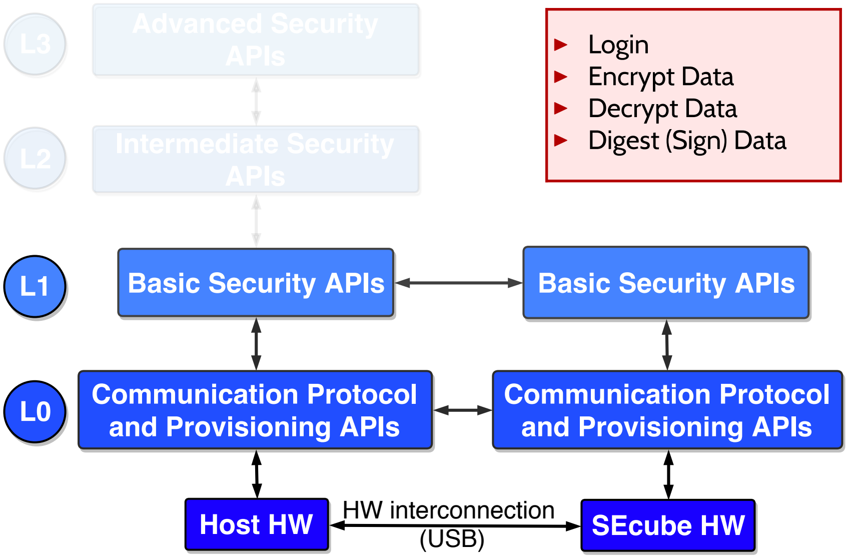
SEcube™ APIs hierarchy



L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

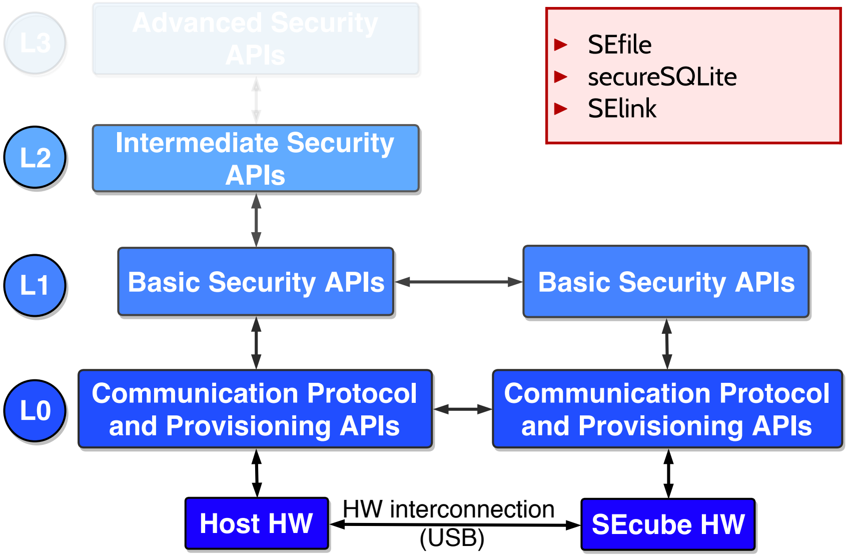
- Discover Devices
- Open Connection
- TX RX Data
- Close Connection

SEcube™ APIs hierarchy


L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

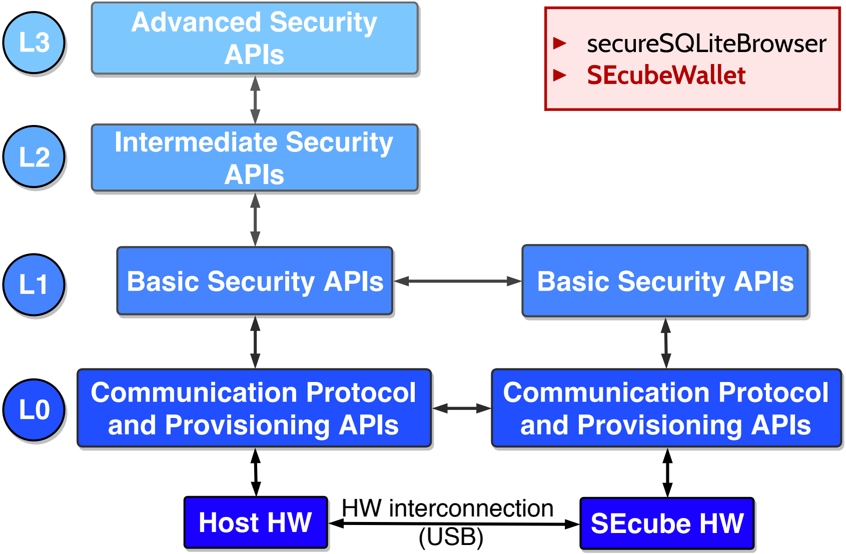
- Login
- Encrypt Data
- Decrypt Data
- Digest (Sign) Data

SEcube™ APIs hierarchy


L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

- SEfile
- secureSQLite
- SElink

SEcube™ APIs hierarchy


L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

- secureSQLiteBrowser
- **SEcubeWallet**

Outline

1. Introduction

2. Technologies used
    - ▶Software libraries
    - ▶The SEcube™ Framework

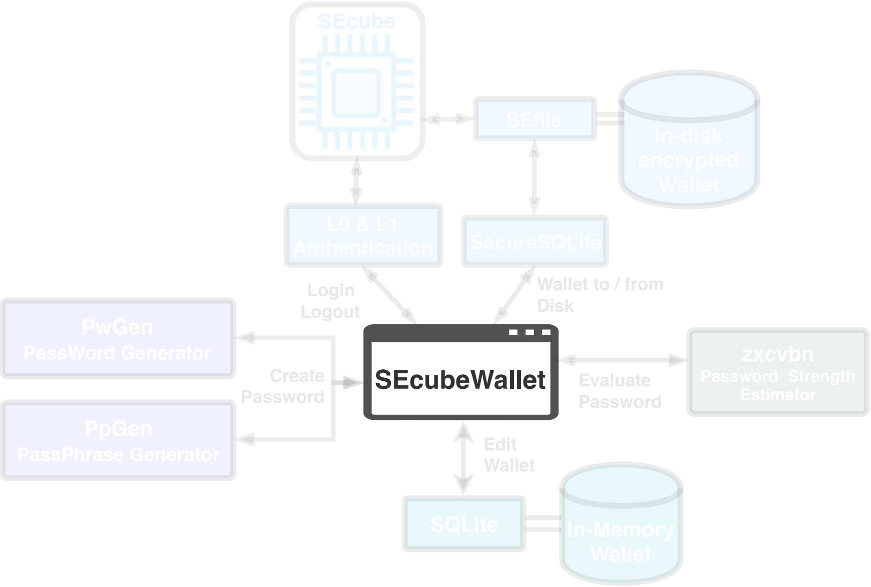
3. Design

4. Demos

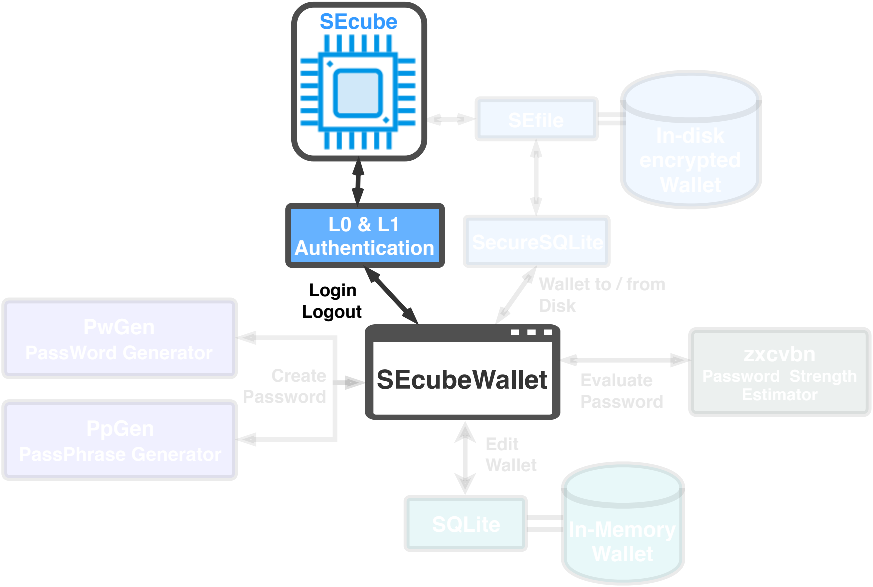
5. Conclusions

6. Future Work

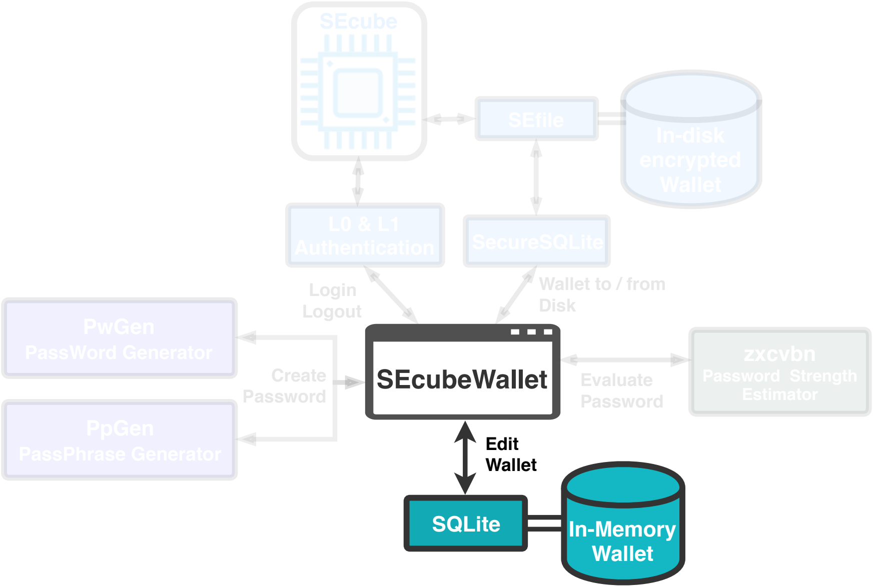
SEcubeWallet Application



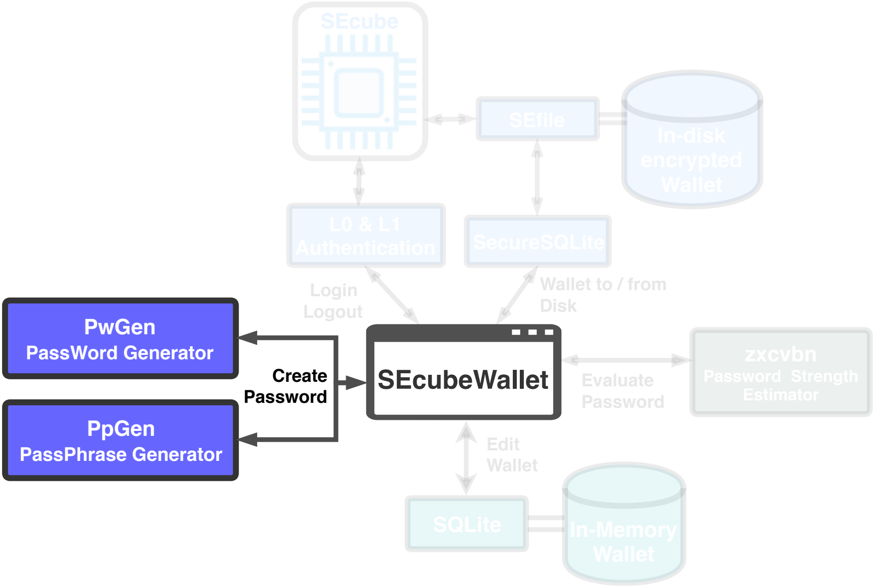
Open device and authenticate



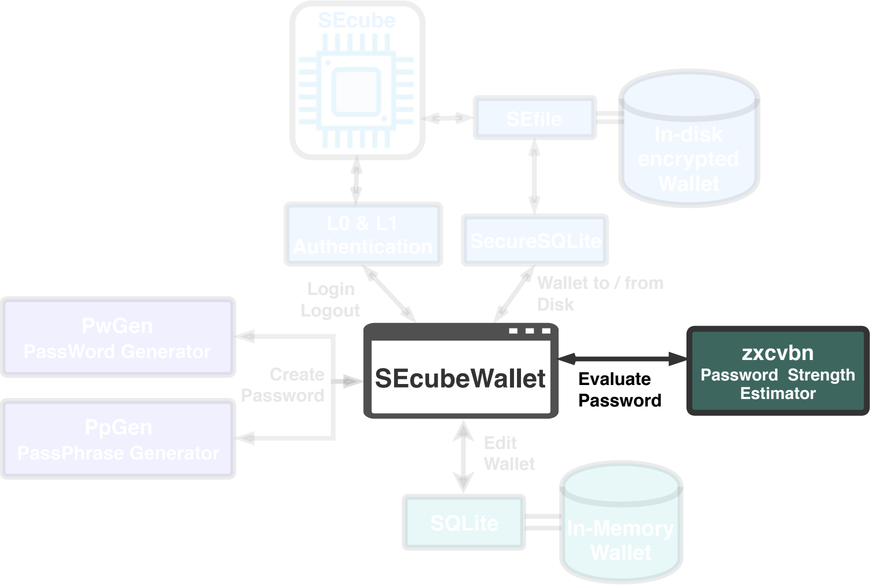
Create In-memory Wallet



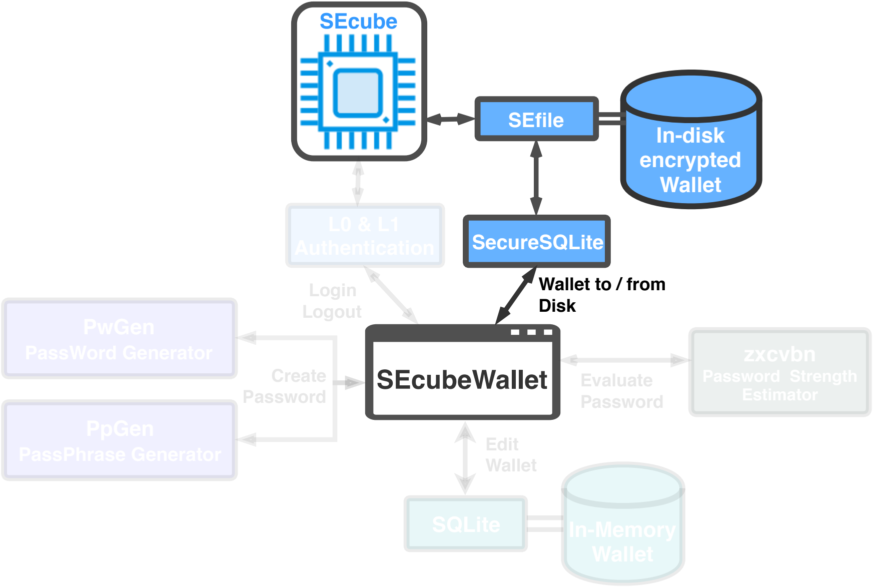
Generate Password/Passphrase



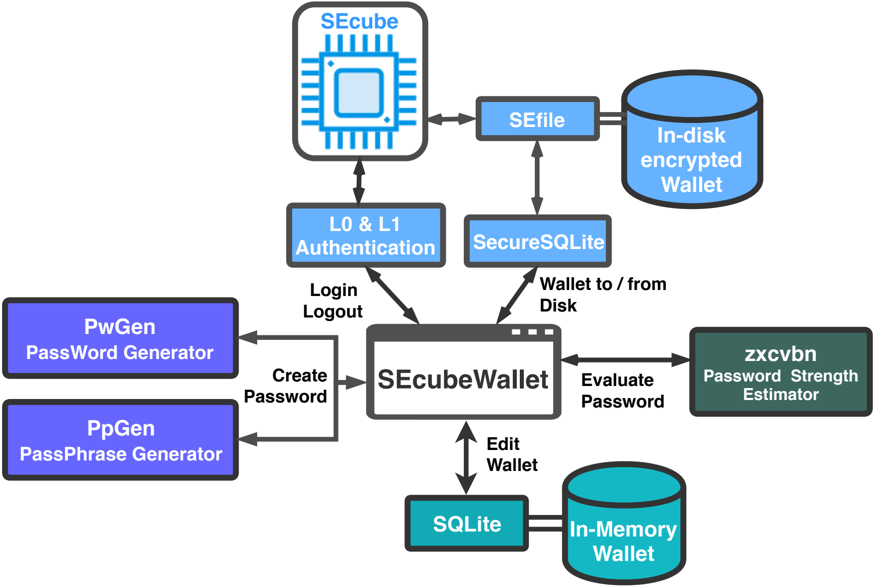
Evaluate Strength



Encrypt and Save Wallet to disk



General Architecture



Outline

1. Introduction

2. Technologies used
   - Software libraries
   - The SEcube™ Framework

3. Design

4. Demos

5. Conclusions

6. Future Work

Login and Open a Wallet

Generate and evaluate password

Outline

1. Introduction

2. Technologies used
    - ▶Software libraries
    - ▶The SEcube™ Framework

3. Design

4. Demos

5. Conclusions

6. Future Work

Outline

1. Introduction

2. Technologies used
   - ▶Software libraries
   - ▶The SEcube™ Framework

3. Design

4. Demos

5. Conclusions

6. Future Work