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?

To authenticate it ask for master password + device

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 it ask for master password + device

Outline

Introduction

Software and Hardware components

- SEcube™ Framework

Design

Outline

Introduction

Software and Hardware components

- SEcube™ Framework

Design

Introduction

Outline

Introduction

Software and Hardware components

- SEcube™ Framework

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

C++ library, cross-platform, elegant design

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, written in C, Transactional

Software Libraries

The following open source libraries were used:

PwGen: Password generator

Software Libraries

The following open source libraries were used:

PwGen: Password generator

Configurable, 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

Dictionaries, keyboard patterns, sequences, years

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

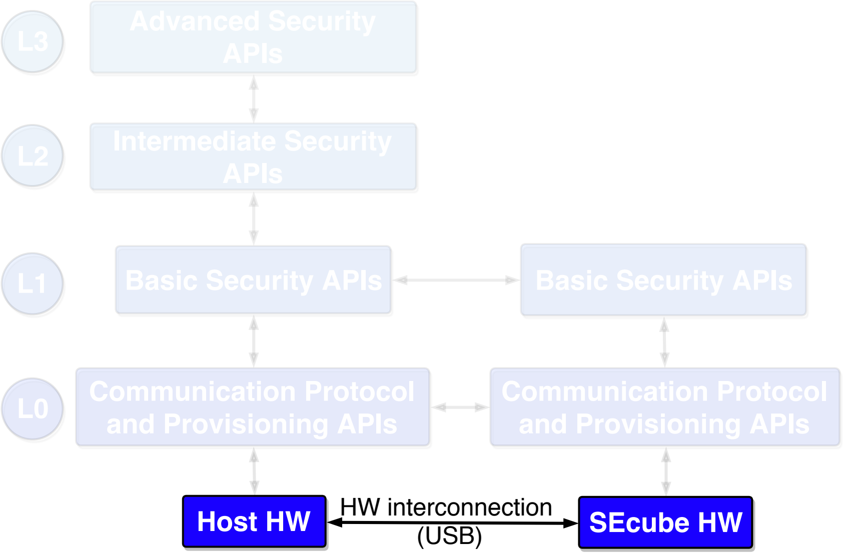
PwGen: Password generator

Configurable, random or readable

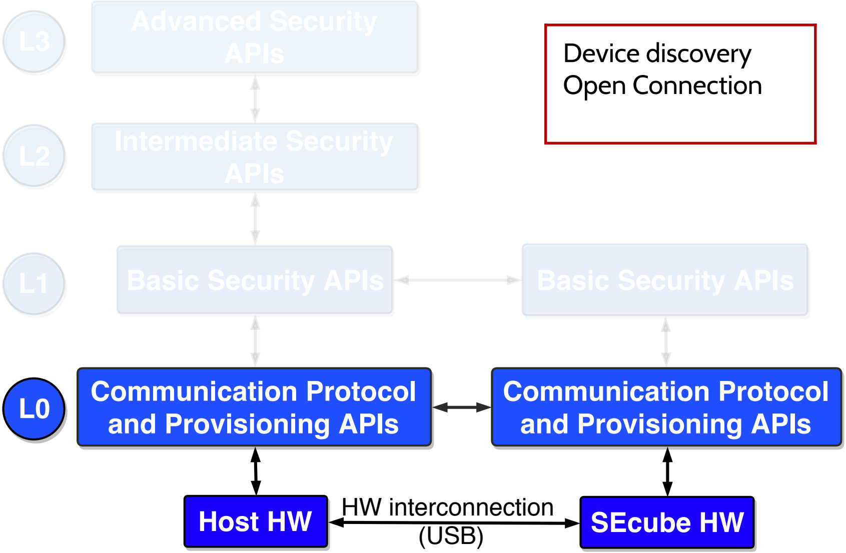
zxcvbn: Password strength estimator

Dictionaries, keyboard patterns, sequences, years

SEcube™ APIs hierarchy

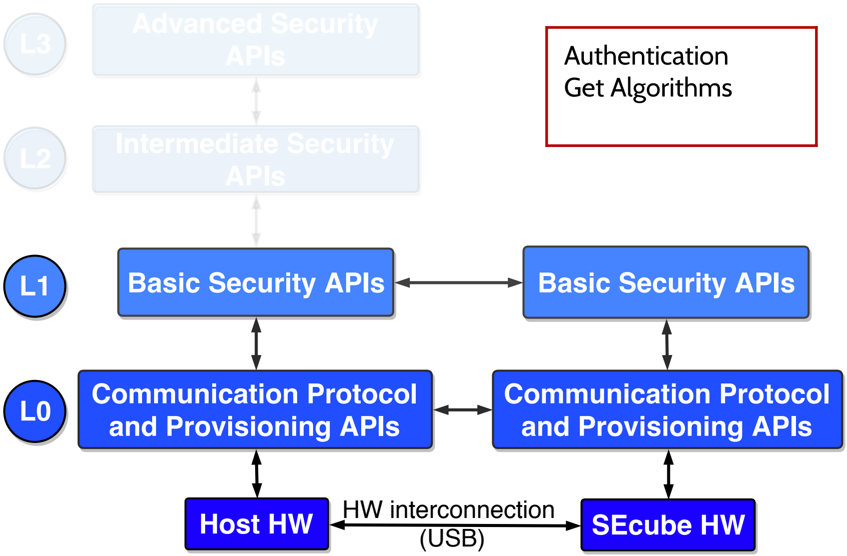

L3
Advanced Security APIs
L2
Intermediate Security APIs
L1
Basic Security APIs
Basic Security APIs
L0
Communication Protocol and Provisioning APIs
Communication Protocol and Provisioning APIs
Host HW
HW interconnection (USB)
SEcube HW

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

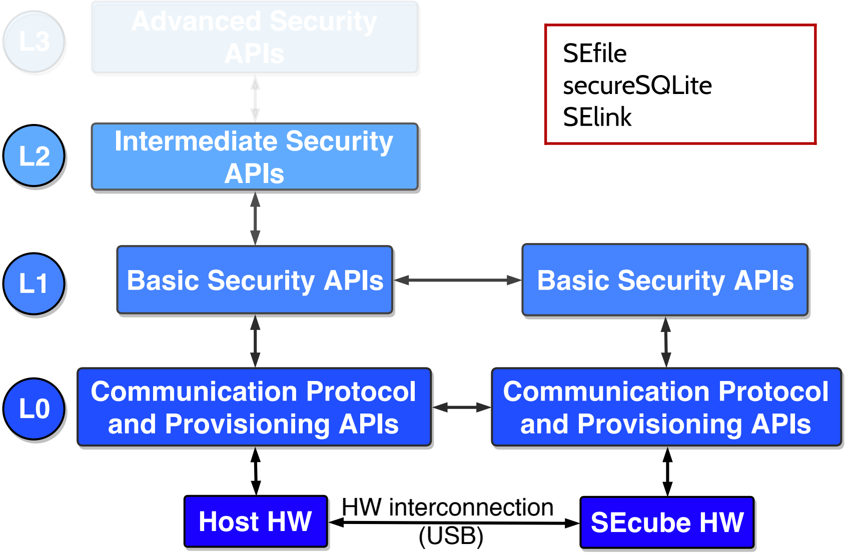
Device discovery
Open Connection

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

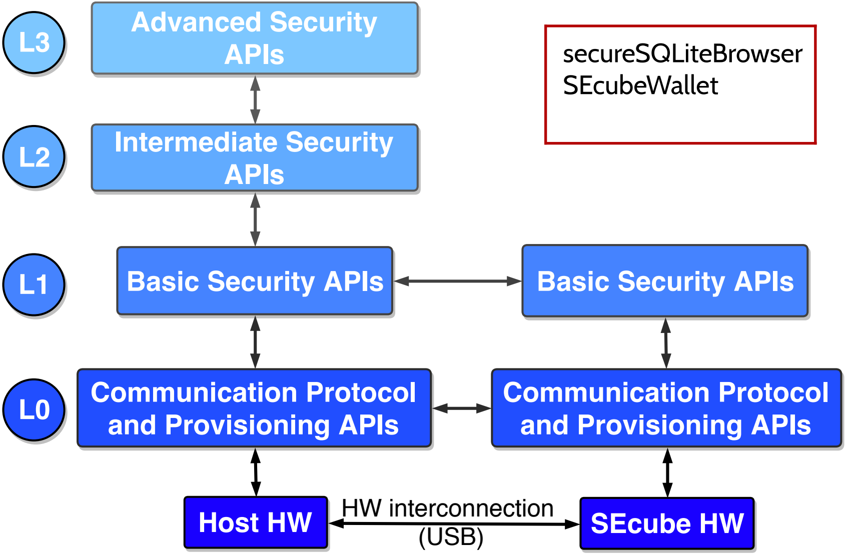
Authentication
Get Algorithms

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

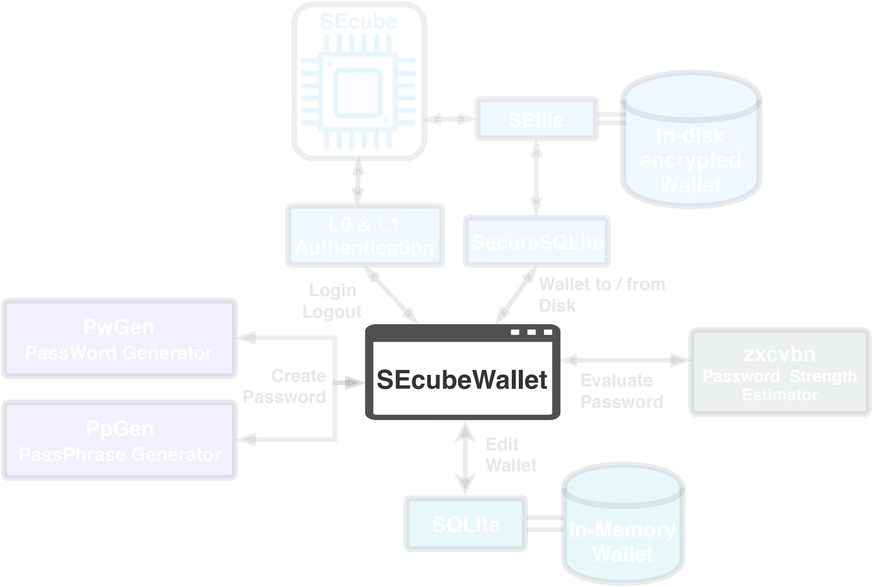
Introduction

Software and Hardware components

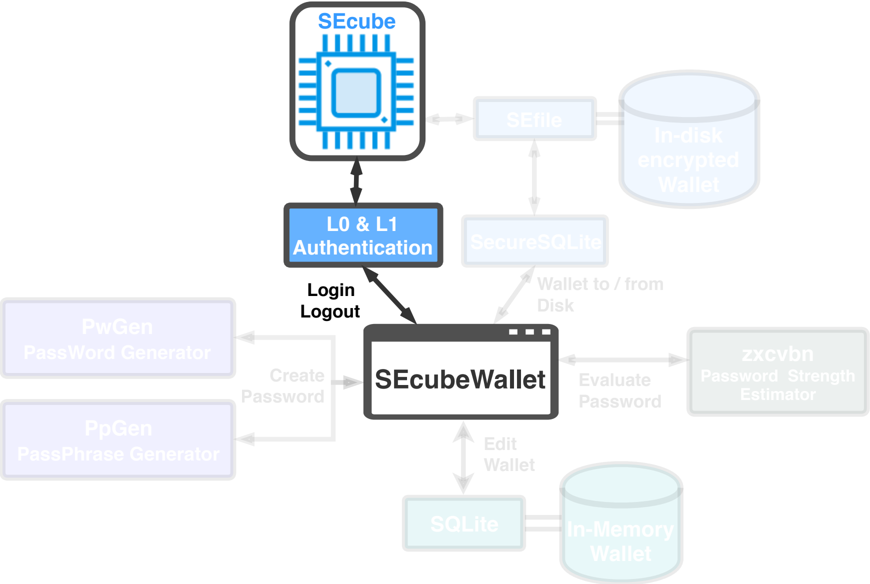
SEcube™ Framework

Design

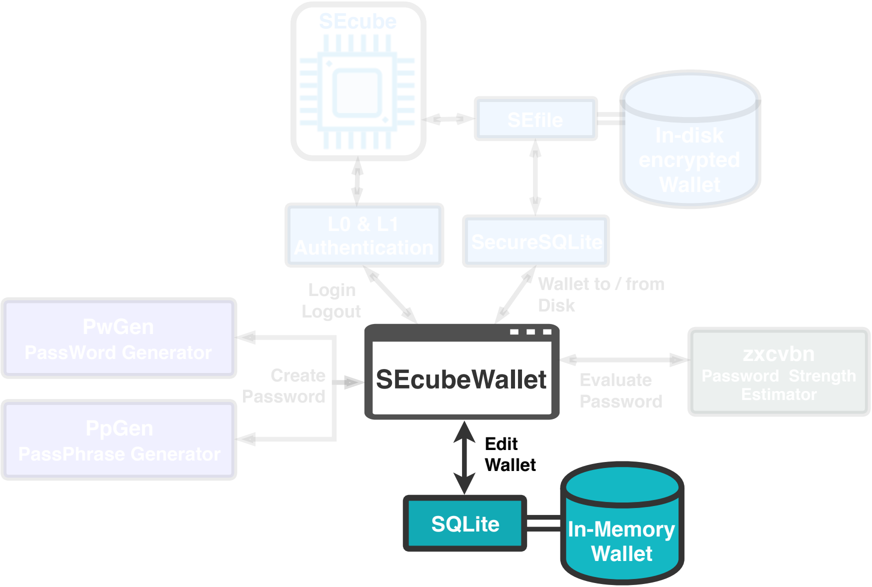
SEcubeWallet Application



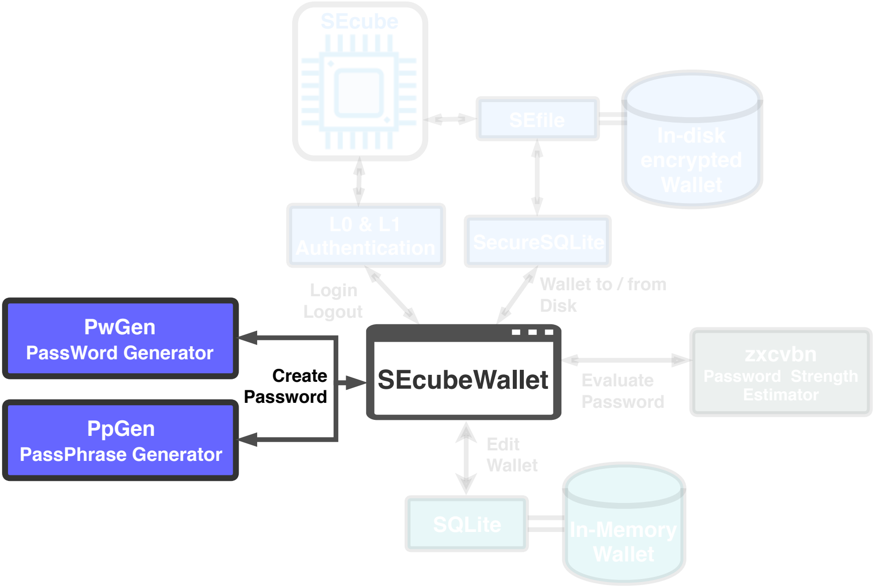
Open device and authenticate



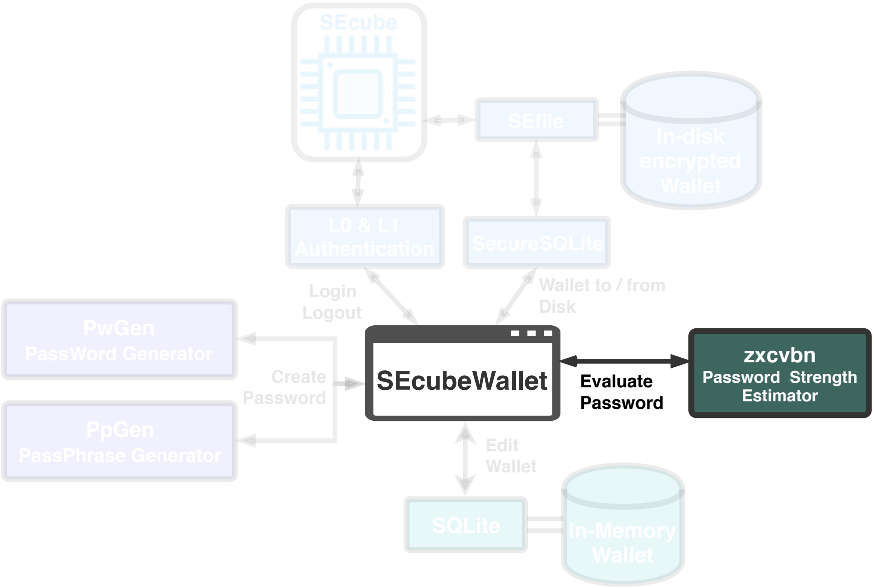
Create In-memory Wallet



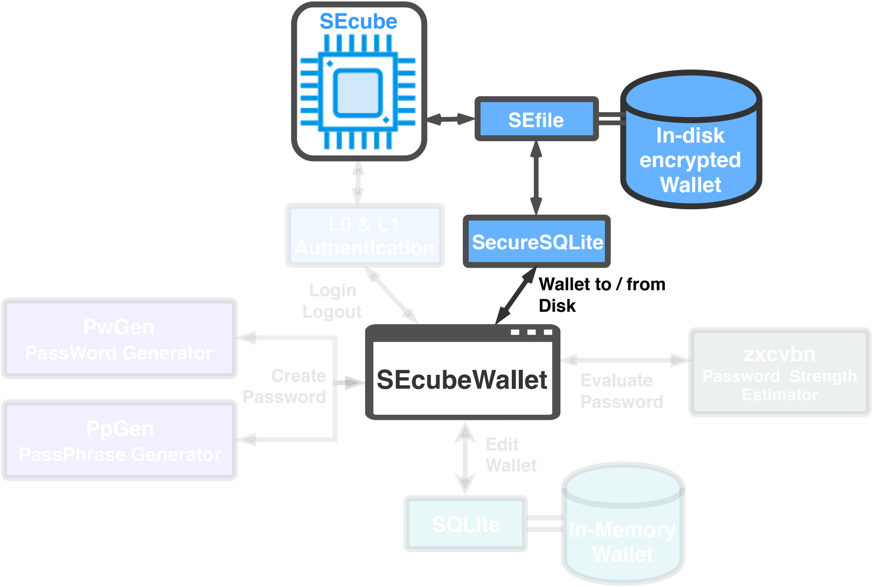
Generate Password/Passphrase



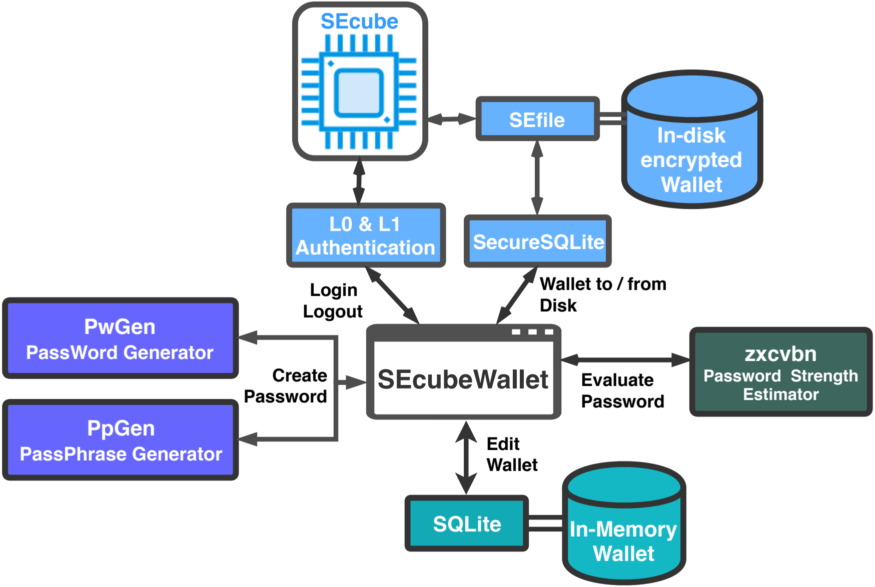
Evaluate Strength



Encrypt and Save Wallet to disk



General Architecture



Login and Open a Wallet

Generate and evaluate password