SecHack365

SecPassBox 物理型パスワードマネージャー

学習駆動コース
今岡ゼミ
渡邉 雄大

概要

パスワードマネージャーを手元に置ける小型独立デバイスとして使えるようにした。
USB/Bluetoothで接続し、キーボードのように振る舞うことで追加ソフトウェアなしで環境に依存せず使用することができる。

制作の動機

・パスワード(PW)を不便な紙で管理する人が多い[1]
・PWマネージャーの機密情報が盗まれないか不安
・CLI環境などではPWマネージャーが使えない
・環境に追加のソフトウェアを入れたくない
→代替手段を用意したい！

利用者はデバイスの認証を行った後、使用したい機器へと接続しID/PWを半自動で入力することができる。

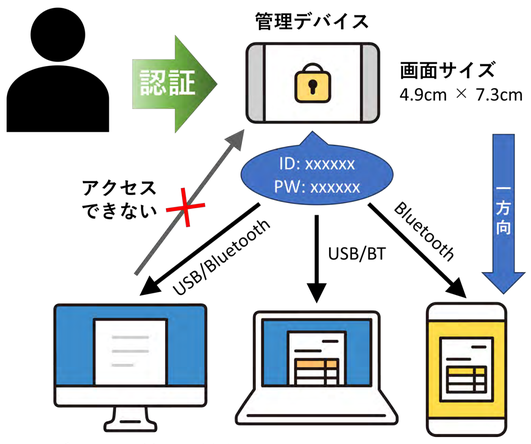


図1 デバイス利用の流れ

図2 PIN入力画面

図3 パスワード選択画面

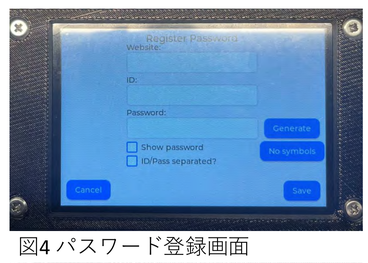


図4 パスワード登録画面

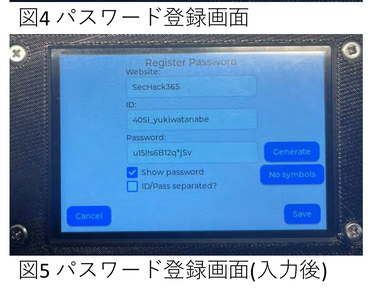


図5 パスワード登録画面(入力後)

デバイスの認証はPIN数字6桁で5回連続で間違えるとマスターパスワードを要求する。
パスワード登録画面ではランダムな英数字を生成して安全なPW管理を実現する。
また、記号の使用を許可していないサービス向けに特殊記号を使わないオプションも作っている。

デバイス紹介

ハード面の工夫

マイコンは指先サイズのものを採用し、ピンヘッダをつけて使用していたが、プリント基板を設計し表面実装を行った。基板設計時に対策を施したことでプロトタイプ時のときより格段にノイズ耐性が向上した。

図6 デバイス内部 (バッテリーなし)

筐体は3DCADを用いて自分で設計し、3Dプリンターで造形した。
自立するように、またタッチペンを収納できるようにするところに苦労した。印刷品質向上のために速度を調整するなど試行錯誤した。

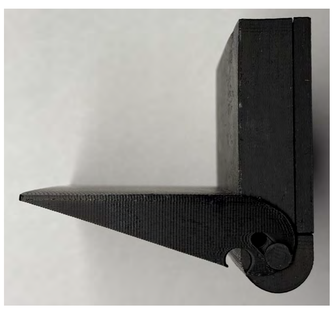


図7,8 穴のおかげでペンを入れている時は蓋が開かない

脅威に対する対策

このデバイスに対して考えられる脅威のうち重要な部分を回路図から考え、右図のように簡略化して表した。
灰色が安全、水色、橙色、赤色と変わるにつれて危険度が高いことを意味する。

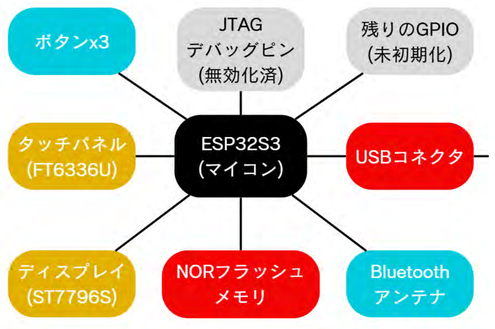
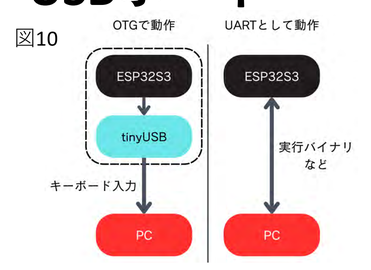


図9 脅威のレベルには差がある

USBポート

図10



OTGモードで動作し、全ての通信はtinyUSBを通るため、バイナリを直接受け取ることのできるモードより自由度が低く安全だと考えられる。

フラッシュメモリ

図11

フラッシュメモリは物理的なアクセスがかなり難しいが、PWを含めた情報がここに含まれている。情報を守るために、内部にあるeFuseを参照しバイナリを復号&検証して起動する構成(Secure Boot)にしておき、NVS(保存領域)はすべて暗号化する。

その他

PINの総当たり
PINが数字6桁であるから100000通り試されると突破されてしまう。
→5回間違えるとマスターパスワードを要求する
乱数の弱さ
暗号学的に安全でない乱数を用いると、極めて可能性は低いが生成したパスワードの規則性を解析されることがあり得る。
→ノイズ由来の乱数を使う

他認証方法との比較/優位性

	SecPassBox	紙・手帳	PW マネージャー	PW 管理デバイス	記憶
PW生成	○	×	○	○	?
暗号化	○	×	△	?	○
利便性	○	×	○	×	×
対ウイルス	○	○	△	○	○
透明性	○	○	△	?	○

表1

※ここでPWマネージャーはブラウザ標準のもの、PW管理デバイスは以前販売されていたものを比較対象としている

PW生成
乱数で安全なパスワードを生成することができるか

暗号化
その媒体が盗まれた時に第三者に内容が見られないか

利便性
PW入力時に手入力する必要があるか、追加のソフトウェアを必要としないか

対ウイルス
マルウェアに感染したときにPWが全て流出といったことにならないか

透明性
仕様が全て公開されていて、確認することができるか

パスキーは?

PWを使わずに認証できる点で良いが、まだ普及しておらずデバイス間の共有も難しいほか、ITに親しみのない人にとって難しい概念と考える。

フィードバック

CSS2024にてデモを行ったとき、SH365の集合回のときに頂いた意見に加えて、親戚や友人に制作途中のSecPassBoxを触ってもらい、UIや筐体を改良した。

課題・今後

・透明性確保のためドキュメント整備, ソースコード公開を行う。
・より多くの意見を集め、機能追加を行う。
・フィッシングサイト対策→ブラウザ拡張機能で対応？

NICT National Institute of Information and Communications Technology

謝辞

SecHack365期間を通して、多くのご支援をいただきました。特にトレーナーの方々の作品に対する意見やポスター制作時のアシスタントの方々の助言は大変参考になりました。トレーニーや運営の方々を含めて、この場を借りて感謝を申し上げます。

[1] IPA「2022年度情報セキュリティの脅威に対する意識調査」