Arduino Password Vault

Úvod

Cílem tohoto projektu bylo vytvořit zařízení na platformě Arduino, které je schopné bezpečně ukládat a spravovat hesla.

Architektura systému

Na rozdíl od cloudových řešení, které jsou vystavena riziku útoku z internetu, pracuje zařízení komletně offline. Arudino hraje roli "hloupého" úložistě dat - samo o sobě neprovádí žádné kryptografické operace (s výjimkou ověřování integrity dat). Veškeré náročné výpočty (odvozování kličů, šifrování dat) probíhají přímo na připojeném počítači. Tím se nejen snižuje riziko zneužití v případě fyziké krádeže, ale také se urychluje provádění složitých operací, protože se využívá výkonu počítače.

Hardware komponenty

1. Arduino MKR Zero

Základem celého projektu je mikrokontroler Arduino MKR Zero. Jeho vestavěný slot pro SD kartu umpžňuje ukládat šifrovaná data bez nutnosti externího modulu. Tento konrétní model neobsahuje žádné moduly pro bezdrátové spojení, čímz se minimalizuje riziko externího zneužití. Jediná podporovaná komunikace je prostřednictvím USB, což usnadňuje integraci s počítačovou aplikací založenou na příkazové řádce (CLI).

2. Microchip ATTEC608A

Jedná se a speciálně navržený kryptografický čip od společnosti Microchip, který je naprosto zásadní pro bezpečné ukládání krypografických klíčů. Takto uložené klíče jsou odolné vůči fyziké extrakci a manipulaci. Čip je mimo jiné schopný generovat a trvale ukládat HMAC klíč, který slouží k ověřování integrity dat.

Kryptografie

1. Šifrování hesel

Hesla jsou šifrována pomocí algoritmu AES-256. Každá šifrovací operace využívá jedinečný iniciační vektor, což zajišťuje, že i při opakovaném šifrování stejných informací, vznikají různá šifrovaná data.

2. Odvozování klíčů

Algoritmus Argon2 se využívá k odvození hlavního šifrovacího klíče z uživatelského hesla v kombinaci s náhodně generovanou hodnotou (salt). Hlavní šifrovací klíč je poté bezpečně uložen na kryptografickém čipu. Při pozdějším ověřování se používají pouze tyto odovezené klíče. Náročnost algoritmu na paměť navíc snižuje efektivitu vůči bruteforce útokům.

3. Ověřování integrity dat

Pomocí algoritmu HMAC-SHA256 je z šifrovaných dat generován hash. Jakákoliv změna dat způsobí odlišný hash, což umožňuje zařízení detekovat neoprávněnou manipulaci s daty. Trvalé uložení HMAC klíče v kryptografickém čipu zarčuje, že se data nemohou změnit bez vědomí systému.

Workflow

1. Inicializace zařizení

- Vygeneruje se náhodný salt (16B), který se uloží přímo na SD kartu
- ATECC608A vygeneruje a trvale uloží HMAC klíč
- Ze zadaného hlavního hesla a saltu se odvodí hlavní šifrovací klíč (Argon2), který je následně také uložen na čipu
- Prázdná databáze hesel je zašifrována (AES-256) a uložena na SD kartu
- Dojde k výpočtu HMAC hashe pro šifrovaná data a uložení výsledku

2. Každodenní provoz

- Uživatel zadá své heslo, na základě kterého odvodí CLI hlavní šifrovací klíč
- Arduino poskytne šifrovaná data, která jsou ověřena pomocí HMAC hashe
- Po úspěšném ověření je datábáze dešifrována a uživateli je umožněn přistup k uloženým heslům

- V případě změny databáze, dojde k novému zašifrování s aktualizovaným iniciačním vektorem a vygenerování nového HMAC hashe, přičemž jsou data opět uložena na SD kartu