Mooltipass, coffre fort numérique

Raoul Hecky
Capitole du libre, Toulouse 2016

Qui suis-je?

- Raoul Hecky <raoul.hecky@gmail.com>
- Créateur et mainteneur du projet de domotique Calaos

Le problème des mots de passe

- Complexe à retenir
- De plus en plus de service avec des identifiants différents
- Utilisation fréquente de “schéma”
- Nous ne sommes pas des machines
- Mot de passe de mauvaise qualité → affaiblissement de la sécurité

Mooltipass

Gestionnaire de mots de passe matériel

—

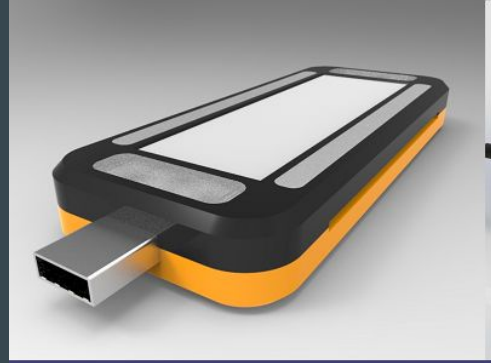
- Génère et sauvegarde vos mots de passe
- Emule un clavier USB pour tapper à votre place
- Coffre fort sécurisé
- Open Source et Open Hardware

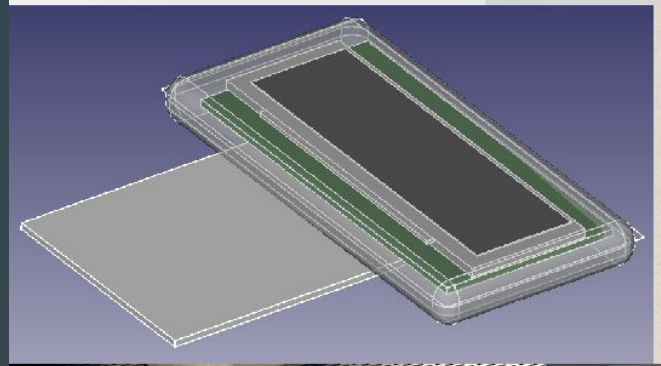
HISTORIQUE

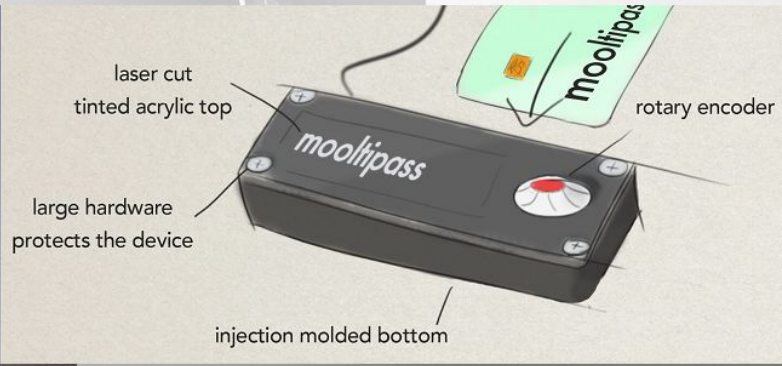
- Projet créé par Mathieu Stephan, ingénieur en électronique
- Lancé sur Hackaday fin 2013
- Formation d'une communauté
- Idée ⇒ produit sur le marché

Mooltipass prototypes

Mooltipass prototypes







Mooltipass v1

Campagne Indiegogo financé à 110% fin 2014.

- Grand écran OLED
- Boutons sensitifs
- Tarif: 170$

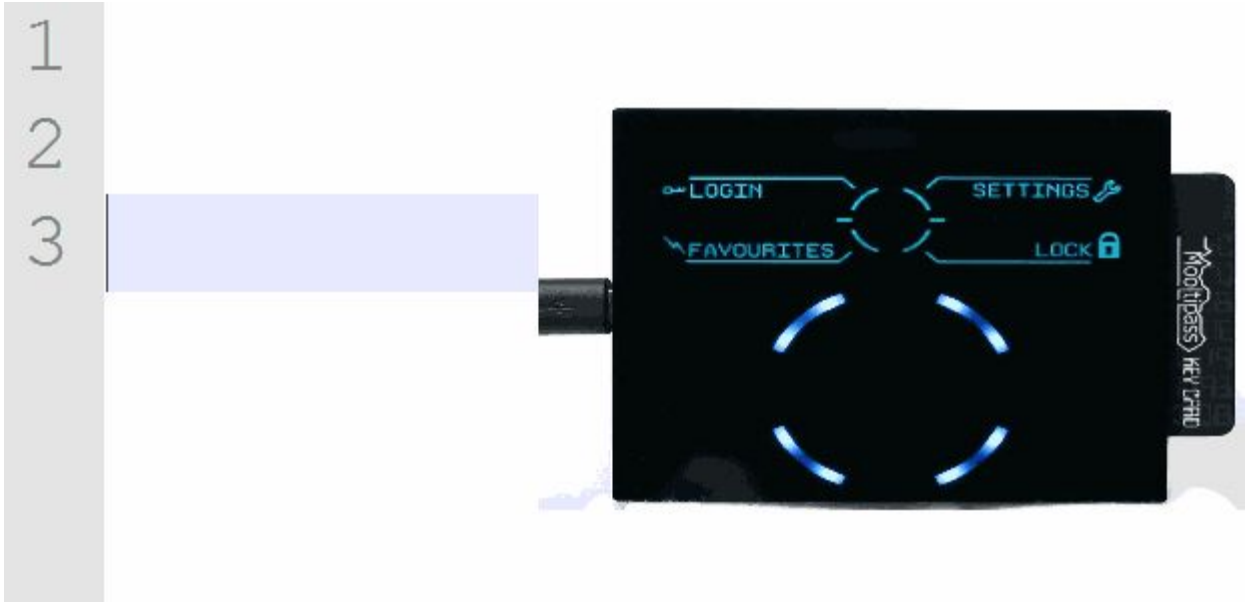
Découverte du projet en 2015

Mooltipass mini

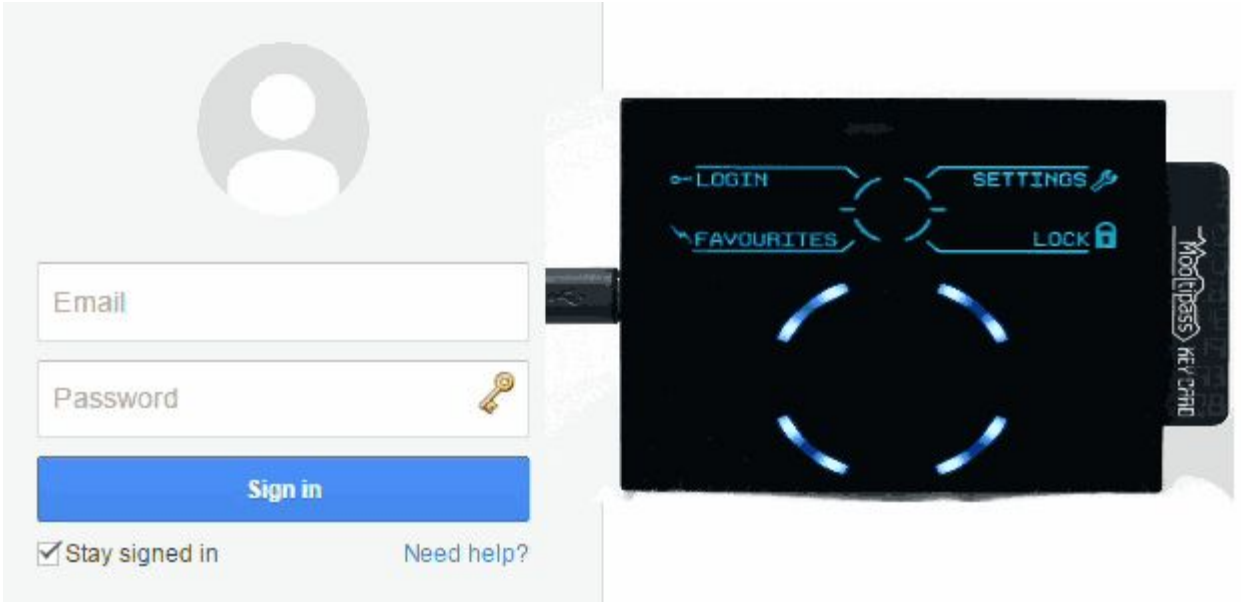
Campagne Kickstarter
financé à 300% en Oct 2016

- Plus petit
- Molette
- Tarif: 70$

Emulation clavier USB HID



Application + Extension du navigateur



Fonctionnement

USB HID

ATMega32U4

écran OLED

FLASH

Boutons

Mooltipass

Smart Card
Verrouillé par code PIN
Contient la clé AES-256

Classe USB HID

- Drivers inclus d'office dans la majorité des OS
- Envoie des KeyCodes via HID (simule une frappe au clavier)
- Utilisation des API HID Set_Report pour communiquer avec le Mooltipass

Stockage chiffré

- Les données sont stockées dans la FLASH (4Mb)
- 2 types de données
  - Mots de passe (32 caractères max.)
  - Données brutes
- La clé AES-256 est stockée dans la SmartCard
- Une SmartCard identifie un utilisateur
  - Plusieurs utilisateurs peuvent utiliser le même mooltipass
- Les données sont chiffrées avec la clé AES + salage

Random Number Generator

- Le mooltipass sert de RNG pour générer les mots de passe
- Utilise le Jitter naturel du timer du watchdog de l'ATMega
- Génère 2 entiers de 32bits par sec. maximum
- L'application utilise ces nombres aléatoires pour générer des mots de passe

SmartCard

- Standard Atmel AT88SC102
- Verrouillé après 4 mauvais PIN
- Mémoire accessible seulement après déverrouillage
- Code PIN de 16bits
- Contient
  - La clé AES-256
  - Un ID pour identifier un utilisateur

Mise à jour du firmware

- Les firmwares sont signés
- Chaque mooltipass mini contient:
  - Un ID unique
  - 2 clés AES générées par appareil (généré au flash usine)
    - 1 pour la signature du firmware
    - 1 pour pour hasher le firmware et vérifier qu'il a pas été altéré

Mise à jour du firmware

- Un firmware (bundle) est unique par device et signé avec la clé AES du mooltipass
- La mise à jour est protégée par un mot de passe généré grâce à la clé AES et l'UID
- Évite certains vecteurs d'attaques:
  - Installation de firmware corrompu
  - Mise à jour sans que l'utilisateur soit au courant
  - Blocage du mooltipass (en cas de mauvais bundle)
- La génération des clés AES et des UID + flash usine est réalisé par Mathieu uniquement et non par l'usine

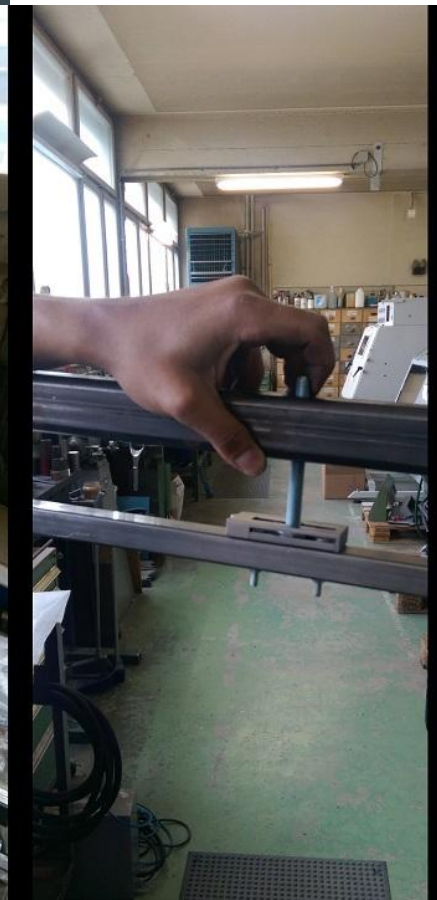
Vecteurs d’attaques

Le nombre de vecteurs d’attaque est réduit, mais existe quand même

- Ecoute du port USB et des paquets HID (Sniff)
  - Fonctionne, mais uniquement lorsque le mot de passe est envoyé
- Altération matérielle (remplacement du PCB, ...)

Test de force

Boitier en Alu collé grâce à une colle haute performance

Test d'ouverture

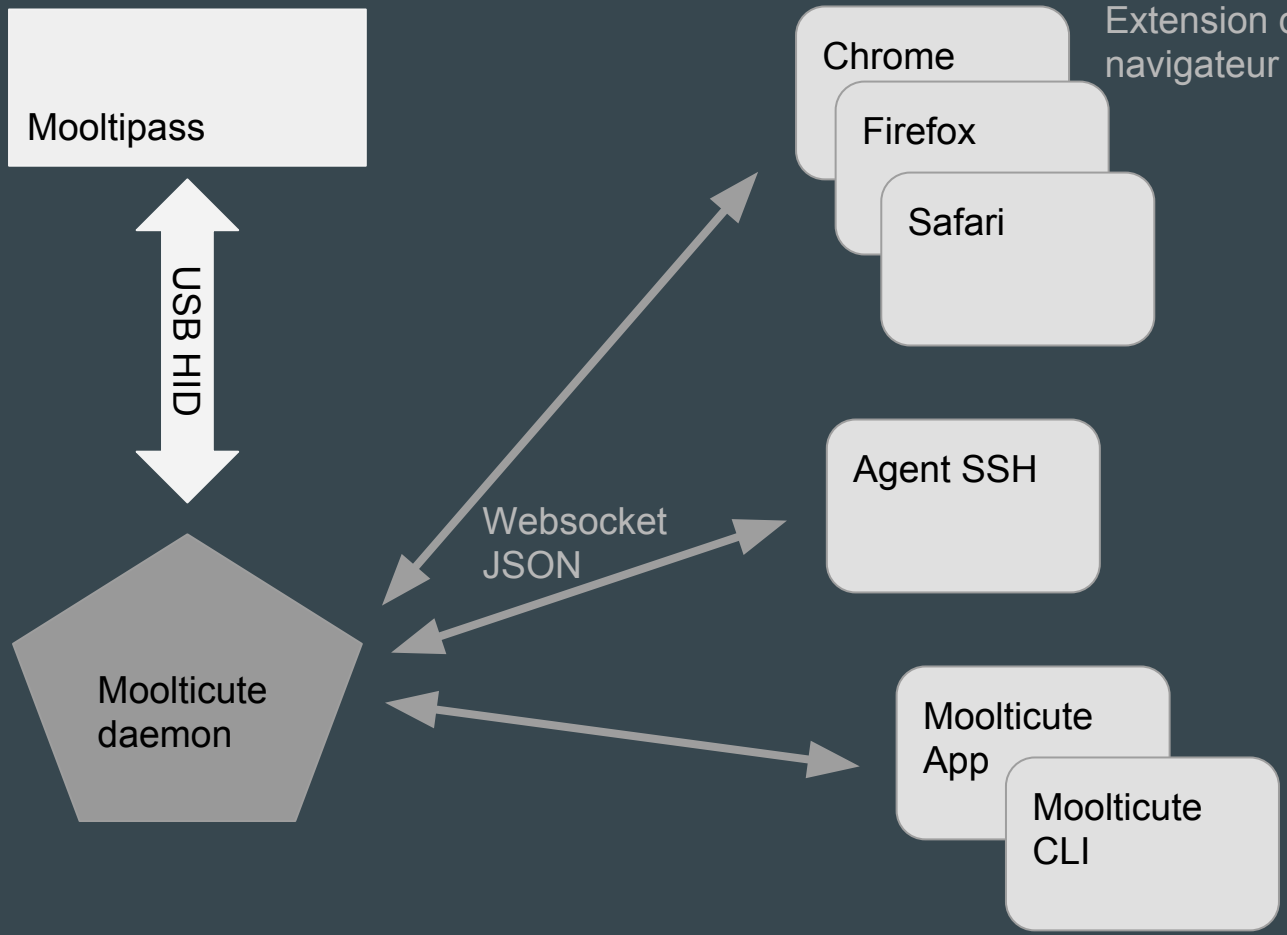
REPAIRABILITY SCORE:

1

OUT OF 10

Moolticute

- App Chrome
  - Google a déprécié les App chrome pour début 2018
- Solution: **Moolticute**
  - Projet créé pour mes propres besoins
  - Va remplacer l'app Chrome officielle
  - Démon qui communique avec l'appareil via les API HID des OS
  - Exporte une API Json simplifié via Websocket
  - Application GUI cliente pour gérer le mooltipass
  - Support d'autre navigateur (Firefox, Safari, ...)
  - Multiplateforme (Linux, macOS, Windows)


Mooltipass
USB HID
Chrome
Firefox
Safari
Extension du navigateur
Agent SSH
Websocket
JSON
Moolticute daemon
Moolticute App
Moolticute CLI

Moolticute

Moolticute

- Client CLI

```
moolticute-cli login get mywebsite.fr raoulh

mysql -u root -p=$(moolticute-cli login get mydb root)
```

Moolticute

- Agent SSH
  - Agent SSH pour stocker ses clés dans le mooltipass
  - Toutes les clés privées sont stockées dans le mooltipass
  - Un agent ssh spécifique a été développé (emulation du protocole SSH-Agent sous linux/macos, emulation du protocole Putty sous windows)

SSH Agent

Questions

https://www.themooltipass.com/

https://github.com/limpkin/mooltipass

https://github.com/raoulh/moolticute

Merci!