ST LOUIS

FLIPPER ZERO

Multi-tool Device for Geeks

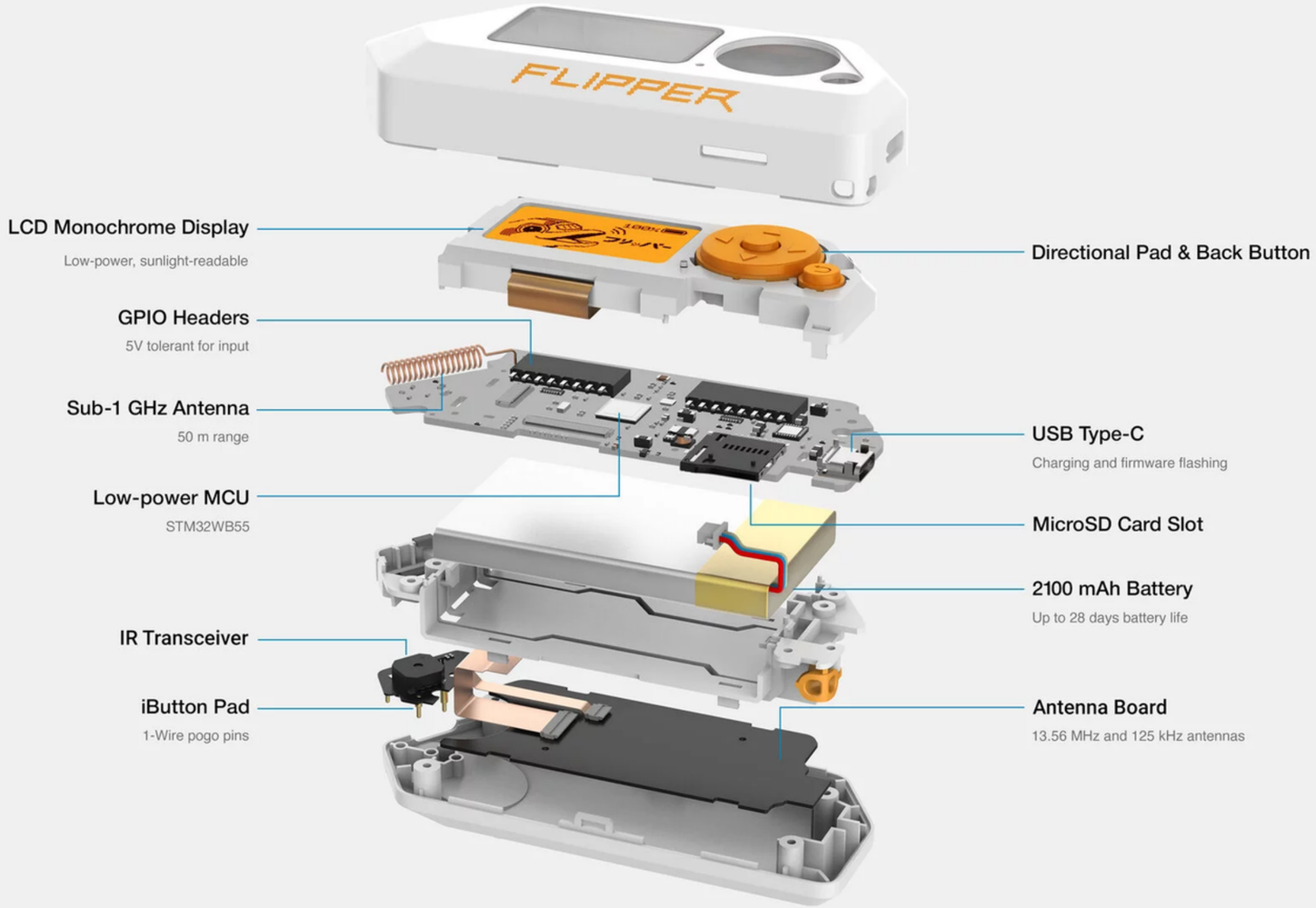
Quentin Parc - Marin Cadro

TABLE
des matières

Introduction

Développé par Alex Kulagin et Pavel Zhovner.
Début du projet : 2019
Financement Participatif sur Kickstarter
4,8 millions $

Sa composition



Fonctionnalités

- **RFID/NFC Tools**

Permet de travailler avec les technologies de communications sans fil RFID (Radio Frequency Identification) et NFC (Near Field Communication).

- **Affichage intégré**

Comprend un écran intégré pour afficher des informations en temps réel ou pour interagir avec l'appareil.

- **Clavier D'émulation**

Peut être utilisé comme émulateur de clavier pour interagir avec des dispositifs comme s'ils s'agissait d'un clavier classique.

- **Ecouteurs et Microphone**

Intègre des fonctionnalités audio pour des applications telles que l'écoute de fréquences radio.

- **Infrarouge**

Dispose d'un émetteur-récepteur infrarouge pour interagir avec des diapositifs utilisant cette technologie

- **Capteurs divers**

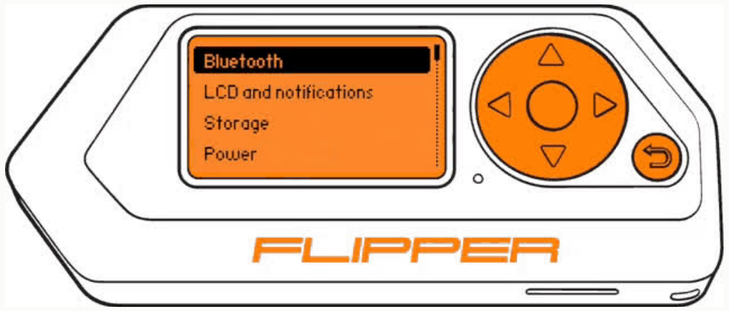
Intègre divers capteurs, tels que des capteurs de mouvement, de température, etc.

- **Open Source**

Le logiciel est Open Source permettant aux utilisateurs de personnaliser et de développer leurs propres applications.

- **Connectivité USB**

Peut être connecté à des dispositifs via le port USB pour une interaction directe.



Usages

1 Éducatif

Sensibiliser les utilisateurs aux vulnérabilités des objets connectés / risques liés à la cybersécurité.

2 Cybersécurité

Permet aux professionnels de la sécurité de tester et d'évaluer la sécurité des systèmes et des dispositifs qui utilisent des technologies telles que RFID ou NFC.

3 Développement de Projets

Utilisation du Flipper Zéro comme base pour développer des projets et des prototypes impliquant des communications sans fil, des capteurs et d'autres technologies.

4 Réparation Matérielle

Peut être utilisé pour des tâches de dépannages et de réparations matérielle en raison de ses capacités de communications et de contrôle.

Dérives

1 Attaque sur la vie privée

Par exemple, en clonant des cartes d'accès RFID ou en exploitant des vulnérabilités de sécurité, peut avoir des conséquences néfastes.

2 Sabotage

Sabotage de systèmes ou l'exploitation de dispositifs connectés à Internet

3 Contournement des dispositifs de sécurité

Contourner des dispositifs de sécurité physique tels que des serrures électroniques, sans autorisation.

4 Attaque sur les Réseaux Sans Fil

Par l'exploitation des capacités RF du Flipper Zéro pour des attaques sur des réseaux sans fil

Conclusion

- Outil important et novateur
- Permet de faciliter l’apprentissage
- Opportunité d'apprentissage et de sensibilisation aux risques liés à la cybersécurité
- Trouver un équilibre entre l'exploration technologique et la responsabilité éthique
- Utilisation potentielle à des fins malveillantes