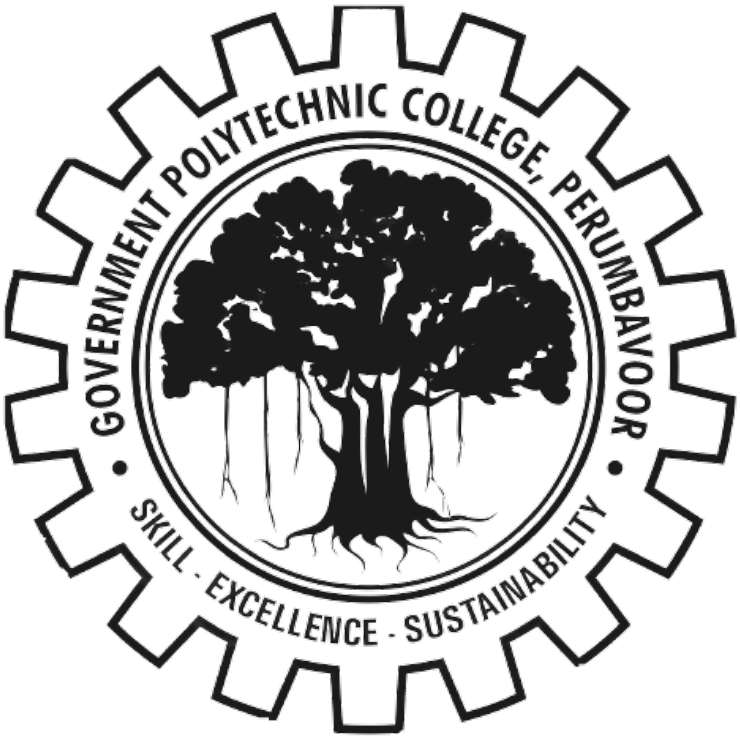
GOVERNMENT POLYTECHNIC COLLEGE PERUMBAVOOR

Koovappady P.O Ernakulam-683 544 Kerala



Semester - VI

Computer Engineering 2022-23

A SEMINAR REPORT

on

FLIPPER ZERO

Submitted by

MANU MOHAN

manumm9526@gmail.com

Lecturer

IVY BALAN

balanivy@gmail.com

ABSTRACT

Flipper Zero is a highly versatile and portable device designed for security testing and digital forensics. It is an open-source device, which means that it can be highly customized and adapted to specific tasks and requirements. Its range of tools and capabilities, including wireless protocol analysis and hardware interface testing, make it an ideal tool for security professionals and digital forensic investigators.

The device is highly intuitive and easy to use, with a simple interface that can be navigated by both novice and experienced users. Its portability is another advantage, making it easy to take on the go and use in a variety of settings. It can also be customized with additional functionality through the use of open-source software and hardware add-ons.

However, as with any technology, there are also some limitations and potential vulnerabilities associated with Flipper Zero. Its hardware capabilities may be limited compared to more specialized tools, and there may be a learning curve for new users. As an open-source device, it relies on ongoing support and contributions from the community to remain up-to-date and secure.

Contents

1 INTRODUCTION **2**

2 DESIGN AND FEATURES **3**

2.1 Multifunctional 3

2.2 Portable 4

2.3 Open-Source 4

2.4 User-friendly 4

2.5 Modular 4

2.6 Long Battery Life 4

2.7 Connectivity 4

2.8 Security 4

3 FUNCTIONALITY **5**

3.1 5

4 APPLICATIONS **6**

5 CONCLUSIONS **7**

6 REFERENCES **8**

Chapter 1

INTRODUCTION

Flipper Zero is a versatile and portable device that is designed for security testing and digital forensics. It offers a range of tools and capabilities, including wireless protocol analysis, RFID scanning, and hardware interface testing. Its open-source design and customizable nature make it an ideal tool for security professionals and digital forensic investigators who are looking for a flexible and adaptable device.

The device's ease of use and portability are also significant advantages. It is designed with a simple and intuitive interface that can be navigated by both novice and experienced users. Its small and lightweight design also makes it easy to take on the go and use in a variety of settings.

Despite its many advantages, it is important to be aware of the potential limitations and vulnerabilities associated with the device. As an open-source device, it relies on ongoing support and contributions from the community to remain up-to-date and secure. Additionally, its hardware capabilities may be limited compared to more specialized tools, and there may be a learning curve for new users.

Overall, Flipper Zero is a cost-effective and flexible solution for security testing and digital forensics. Its range of tools and capabilities, combined with its ease of use and portability, make it an ideal tool for those looking for a versatile and customizable device.

Chapter 2

DESIGN AND FEATURES

Flipper Zero has a sleek and compact design, measuring 86mm x 54mm x 16mm and weighing only 56 grams. It has a white matte finish with a 128x64 monochrome OLED display that displays device status, battery level, and other information. Flipper Zero has a modular design that allows users to add or remove modules based on their needs. The modules include an infrared transmitter, a microphone, an accelerometer, a thermal sensor, and a display module. It is powered by a rechargeable lithium-ion battery that can last up to two weeks on a single charge, depending on usage. Flipper Zero can be connected to other devices via USB, Wi-Fi, or Bluetooth.

2.1 Multifunctional

Flipper Zero is designed to perform various hacking tasks, including sniffing, spoofing, jamming, cracking, and analyzing wireless protocols such as Bluetooth, Wi-Fi, NFC, and RFID.

2.2 Portable

Flipper Zero is a compact and lightweight device that fits in your pocket, making it easy to carry around.

2.3 Open-Source

Flipper Zero is an open-source device, meaning its source code is available for anyone to study, modify, and contribute to.

2.4 User-friendly

Flipper Zero has a user-friendly interface that is easy to navigate and allows for quick access to its various features.

2.5 Modular

Flipper Zero has a modular design, which means that users can add or remove modules based on their needs. The modules include an infrared transmitter, a microphone, an accelerometer, a thermal sensor, and a display module.

2.6 Long Battery Life

Flipper Zero has a built-in rechargeable battery that can last up to two weeks on a single charge, depending on usage.

2.7 Connectivity

Flipper Zero can be connected to other devices via USB, Wi-Fi, or Bluetooth.

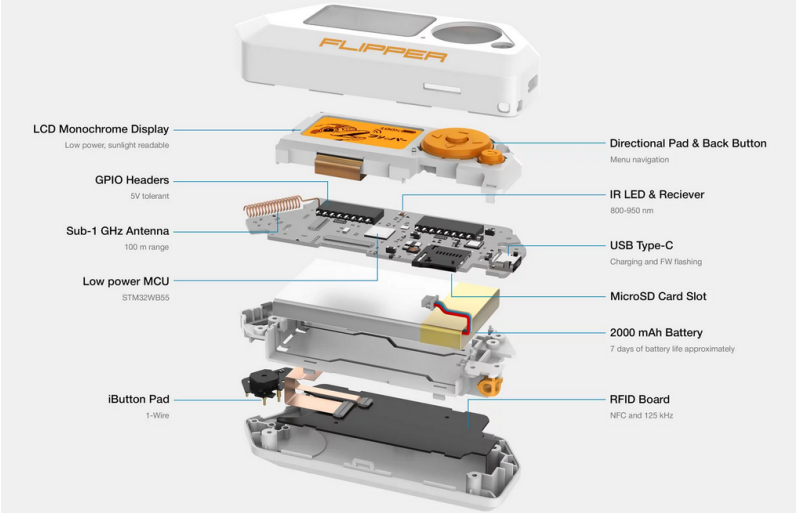
2.8 Security

Flipper Zero is designed with security in mind, and its firmware can be updated to address any vulnerabilities or bugs that may be discovered.

Chapter 3

FUNCTIONALITY

Flipper Zero has a user-friendly interface that is easy to navigate and allows for quick access to its various features. It can perform various hacking tasks, including sniffing, spoofing, jamming, cracking, and analyzing wireless protocols such as Bluetooth, Wi-Fi, NFC, and RFID. It can also be used for physical security testing, such as bypassing electronic locks and cloning access cards. The device's firmware is open-source, allowing users to modify and customize its functionality to suit their needs.



3.1

Chapter 4

APPLICATIONS

Chapter 5

CONCLUSIONS

Homomorphic encryption is a powerful tool for privacy-preserving computation, and has the potential to revolutionize the way we store and process sensitive data. With further research and development, it is likely that this technology will become increasingly important in a variety of contexts, and will play a key role in ensuring the privacy and security of sensitive information.

Chapter 6

REFERENCES

1 Stinson, D. R. (2005). Cryptography: theory and practice (Vol. 55). Boca Raton, FL: CRC press.

2 Boneh, D.,Shacham, H. (2004). Group signatures with verifier-local revocation. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 424-433).

3 Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (1997). Handbook of applied cryptography. CRC press.

4 Goldreich, O. (2001). Foundations of cryptography: basic tools. Cambridge University Press.

5 Bellare, M., Rogaway, P. (1993). Optimal asymmetric encryption—how to encrypt with RSA. In Advances in Cryptology—CRYPTO'93 (pp. 92-111). Springer, Berlin, Heidelberg.