LEXIE THACH

TENGU MARAUDER

Combining Robotics and Cybersecurity

Presented by Lexie Thach and The Tooolbox

WARNING

DURING THE DEMO DO NOT ATTEMPT TO DISRUPT ANY WIRELESS SIGNALS IN THIS ROOM (THAT IS OUR JOB).

Project Overview

Tengu Marauder: Autonomous two-wheeled robot.

- Key Components:
  - RPi , running Marauder
- Main Functionalities:
  - Autonomous movement, WiFi scanning, deauthentication attacks.

Introduction

- My name is Lexie Thach
- I've worked around cyber, tech and development for the past 10 years
- I've done jobs from IT analyst to purple teaming and many more odd jobs in between
- Presented at local conferences and DEFCON
- My specialty is autonomous systems like drones, robotics, ICS/SCADA, and currently getting into AI/ML

Back to Agenda Page

Introduction

- My name is Leo Serrano
- My main focus is primarily on threat modeling and the intersection of security architecture, process, and decision-making.
- I help run a hackerspace in Philadelphia called “The Tooolbox” with my partners where we hopes to showcase the amazing hackers who call Philadelphia home.

Back to Agenda Page

LEGAL CONSIDERATIONS

- FAA Regulations: The FAA regulates drone use, including interception and jamming. Unauthorized use could result in penalties.
- FCC Regulations: The FCC regulates radio frequencies, including those used by drones. Unauthorized interception or jamming is generally prohibited.
- Federal Criminal Laws: Various laws may apply to drone interception and jamming technologies. Interfering with licensed or authorized radio communications is generally illegal.

Back to Agenda Page

Why? To build a drone that can hack.

- 2023 Built a proof of concept using an ardupilot and donated parts
  - Ran into issues with programming and interoperability
  - Learned a lot and wanted to share findings with community
- Goal: Make accessible and crowdsource how to pilot a Flipper Zero
  - Achievable with Raspberry Pis and 3D printed parts
  - Pared down for beginners but can be scaled up
- Learn and educate
  - New intersection of robotics and cybersecurity
  - Understand how law enforcement jamming drones operate

SPECIFIC LAWS

49 U.S.C. § 44801(5): Defines a counter-UAS system as a device capable of lawfully and safely disabling, disrupting, or seizing control of a drone. Does not cover detection-only systems.

Wiretap Act and Pen Trap Statute: These laws may apply to the interception of electronic communications, including those used by drones. Unauthorized interception could result in criminal penalties.

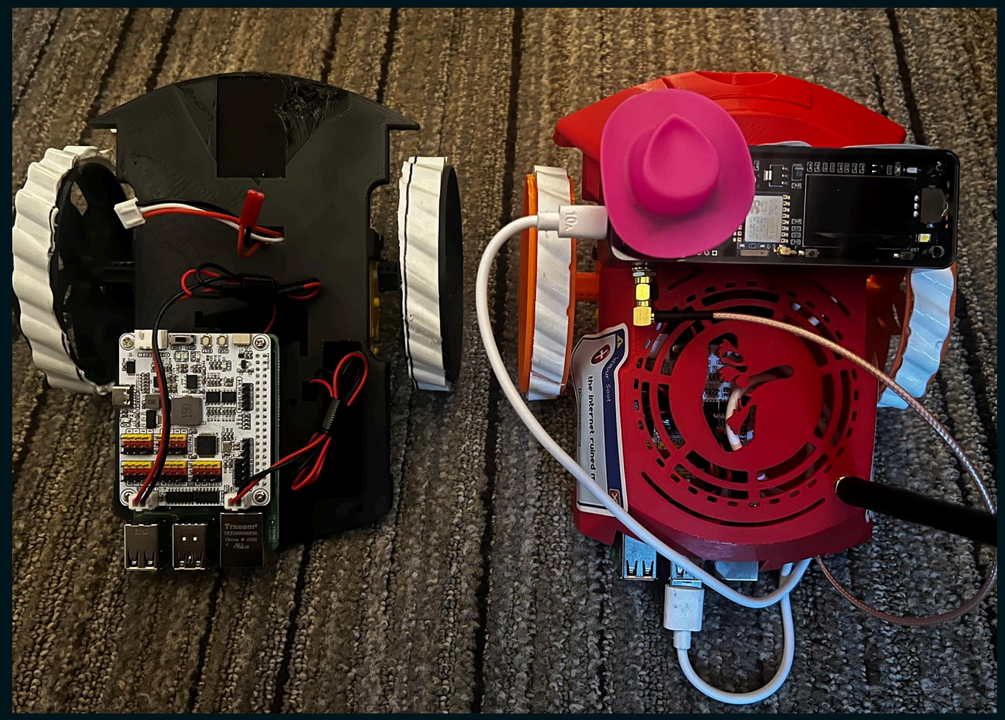
FAA Reauthorization Act: Allows certain government agencies to intercept or take control of drones that pose a security threat. These powers are not extended to private individuals or companies.

DHS Regulations: The DHS has regulations that may apply to drone interception and jamming, particularly in relation to national security and critical infrastructure protection.

Back to Agenda Page

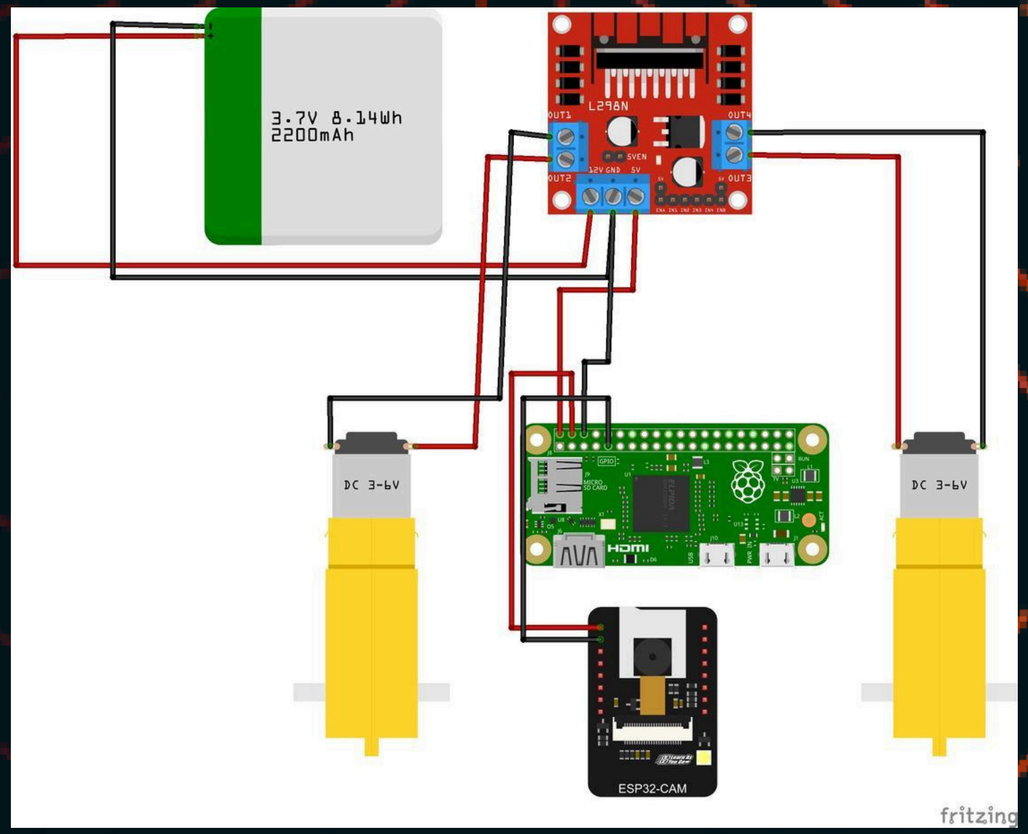
Hardware Components

- RPi: Runs Ubuntu
- ESP 8266: Runs Marauder
- Chassis: Two-wheeled platform with motors and motor driver. Visuals: Images or diagrams of each component.



Communication Protocol Future State

- Serial Communication:
  - RPi and ESP32.
- The communication protocol defines how commands are sent from the operator to the robot and how data is relayed back.
- We have the motor_control node for controlling the robot's movement,
- Future state will use the xbee_comm node for communication, and the esp32_comm node for interacting with the ESP32."
- The command_node wil send automated commands to the ESP32, and the data_processing_node will processes and displays data from the ESP32.
- These nodes communicate through ROS2 topics, enabling modular and scalable interactions.



Back to Agenda Page

Motor Control Node

- Functionality:
  - Controls robot's motors based on commands.

Future state

- Subscriptions:
  - Listens to movement commands (e.g., forward, backward).

- Code Snippet: Key parts of motor_control_node.py showing subscription and motor control logic.

Back to Agenda Page

```python
import rclpy
from rclpy.node import Node
from std_msgs.msg import String
from some_motor_driver_library import MotorDriver

class MotorControlNode(Node):
    def __init__(self):
        super().__init__('motor_control_node')
        self.subscription = self.create_subscription(String, 'cmd_vel', self.cmd_vel_callback, 10)
        self.motor_driver = MotorDriver()

    def cmd_vel_callback(self, msg):
        command = msg.data
        if command == 'F':
            self.motor_driver.move_forward()
        elif command == 'B':
            self.motor_driver.move_backward()
        elif command == 'L':
            self.motor_driver.turn_left()
        elif command == 'R':
            self.motor_driver.turn_right()
        elif command == 'S':
            self.motor_driver.stop()

def main(args=None):
    rclpy.init(args=args)
    node = MotorControlNode()
    rclpy.spin(node)
    node.destroy_node()
    rclpy.shutdown()

if __name__ == '__main__':
    main()
```

Live Demo

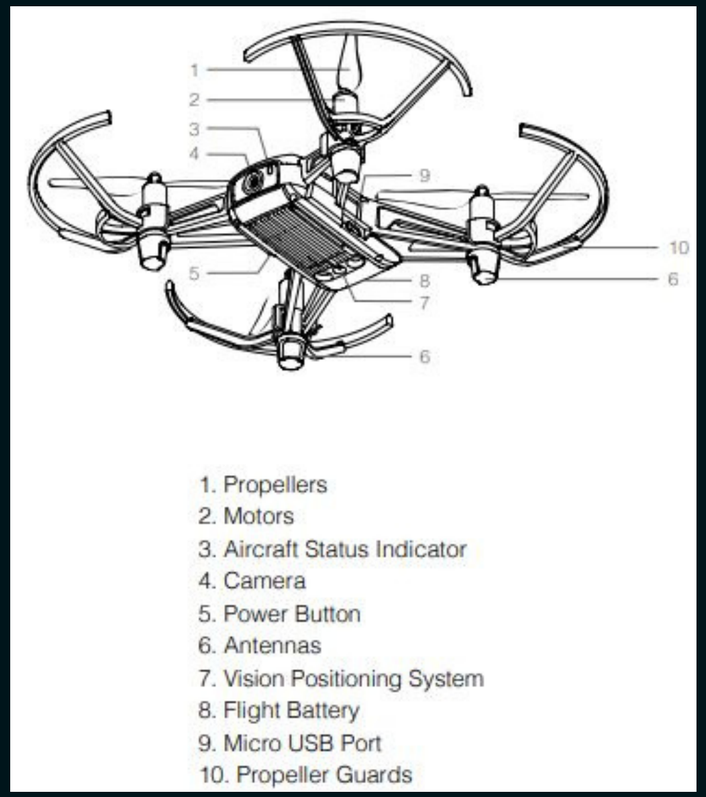
- Step-by-Step Guide:
  - Remote to RPi
  - Use the RPi to send movement instructions via Python script.
  - Initiate WiFi scan and display results.

Demo Script:

```
#Start the Robot: Launch the ROS2 system
ros2 launch tengu_marauder tengu_marauder_launch.py
#Command the Robot: Use the operator interface to send movement commands
python3 operator_interface.py
#WiFi Scan: Send a SCAN command to the ESP32
ros2 topic pub /esp32_in std_msgs/String "data: 'SCAN'"
ros2 topic pub /esp32_in std_msgs/String "data: 'SCAN'"
#Display the scan results processed by the data_processing_node
```

Back to Agenda Page

DEMO



1. Propellers
2. Motors
3. Aircraft Status Indicator
4. Camera
5. Power Button
6. Antennas
7. Vision Positioning System
8. Flight Battery
9. Micro USB Port
10. Propeller Guards

- A DJI Tello connected to a router
- A laptop connecting to the Drone
- Simulates a unified traffic management system (at small scale)

Back to Agenda Page

Results and Analysis

- Analyze the WiFi scan results.
- Discuss potential applications and implications of the Tengu Marauder.
- Highlight any interesting findings from the demo.

Back to Agenda Page


```
{
  "networks": [
    {
      "SSID": "TELLO-1234",
      "BSSID": "60:60:1F:94:84:9E",
      "RSSI": -55,
      "Channel": 6,
      "Encryption": "Open"
    },
    {
      "SSID": "HomeWiFi",
      "BSSID": "34:CE:00:1A:BC:2D",
      "RSSI": -70,
      "Channel": 11,
      "Encryption": "WPA2"
    },
    {
      "SSID": "GuestNetwork",
      "BSSID": "70:3A:CB:3E:1A:C4",
      "RSSI": -80,
      "Channel": 1,
      "Encryption": "Open"
    }
  ]
}
```

Challenges and Solutions

- Throughout the development of the Tengu Marauder, we faced several challenges.

- One major challenge was ensuring reliable communication between the RPI and ESP32 which led us to use an ESP 8266 which was more accessible. A flipper was considered but was found to be insufficient in our tests. May be preferable for for sub gigahertz attacks (NFC, RFID)

- These experiences taught us valuable lessons in hardware-software integration and system design.

Back to Agenda Page

Future Work

- Planned improvements and additional features.
- We aim to integrate more sensors, such as cameras and LIDAR, to enhance its navigation and situational awareness.
- Enhance the the robot with AI for better decision-making and autonomy is also a key goal.
- Additionally, we plan to explore new research directions, such as using the Tengu Marauder for more advanced cybersecurity tasks and environmental monitoring.

Back to Agenda Page

Conclusion

To summarize, the Tengu Marauder is an autonomous security robot that combines commercial off the shelf robotics components with WiFi network security capabilities.
It demonstrates the potential for integrating cybersecurity with robotics to create powerful tools for both fields.
Thank you all for your attention and for attending this presentation. I hope you found it informative and inspiring.

Back to Agenda Page

Contributors

Lourdes Cigarruista , Juan Giarrizzo(Raices)

Don Pellegrino(DeciSym)

Sashur

Kup(Leo N)

Trashp4nda(Leo S)

Riley Carey Lain Chuang

Lexi3cOn(Lexie T)

LEXICON

Do you have any questions?

Feel free to reach out!

Back to Agenda Page

Lexie Thach

@lexiecon121

lexicon21@proton.me