Project Starbeam: An Affordable Approach to Signal Intelligence for Security Applications

Abstract

Project Starbeam is an innovative signal intelligence platform leveraging cost-effective, open-source hardware to deliver advanced capabilities in signal analysis, generation, and manipulation. Central to its design is a custom PCB incorporating the ESP32-WROOM-32D microcontroller alongside multiple radio frequency modules. The system's modularity and compatibility with devices like HackRF One extend its frequency coverage up to 6 GHz, making it a versatile tool for various applications in security testing and operations.

1. Introduction

In the realm of signal intelligence (SIGINT), the demand for flexible, affordable, and efficient tools is ever-increasing. Traditional proprietary systems often come with high costs and limited adaptability. Project Starbeam addresses these challenges by utilizing open-source hardware and software, providing a customizable platform suitable for diverse operational needs.

2. System Architecture

2.1 ESP32-WROOM-32D Microcontroller

At the core of Project Starbeam is the ESP32-WROOM-32D, a powerful Wi-Fi and Bluetooth combination module designed for a wide range of applications. Key features include:

- Dual-core 32-bit processor with adjustable clock frequency (80 MHz to 240 MHz)
- 4 MB of embedded flash memory
- Integrated 2.4 GHz Wi-Fi and Bluetooth capabilities
- Multiple GPIOs for peripheral interfacing

These specifications make the ESP32-WROOM-32D suitable for handling complex signal processing tasks efficiently.

2.2 Radio Frequency Modules

The platform's design allows for configurable RF modules, enhancing its versatility:

- Configuration A: Five NRF24L01+PA+LNA modules
- Configuration B: Three NRF24L01+PA+LNA modules combined with two CC1101 modules

This modularity enables tailored configurations to meet specific operational requirements, facilitating tasks such as frequency scanning and signal generation.

2.3 HackRF One Integration

To extend the system's frequency range, Project Starbeam integrates with HackRF One, an open-source software-defined radio (SDR) peripheral capable of transmitting and receiving signals from 1 MHz to 6 GHz. This integration significantly broadens the platform's capabilities, allowing for comprehensive signal analysis across a wide spectrum.

3. Key Features

- Digital Signal Generation: Users can create custom RF signals for testing and simulation purposes.
- Frequency Scanning: The system can detect and analyze RF signals across multiple bands, aiding in spectrum monitoring.
- Signal Copying & Replay: It captures and reproduces signals, facilitating analysis and testing scenarios.
- Modular Design: The hardware setup is configurable, allowing adaptation to various operational needs.
- Extended Range: With HackRF compatibility, the platform's frequency coverage extends up to 6 GHz.
- Open-Source Architecture: The design promotes customization and expansion, fostering continuous development.

4. Applications

4.1 Tactical Operations

Project Starbeam serves as a valuable tool in secure communications testing, unauthorized transmission detection, counter-surveillance, and communications security assessments for tactical teams.

4.2 Border Security

The platform aids in detecting unauthorized communication devices, analyzing suspicious signal activities, identifying signal-based threats, and monitoring restricted frequencies in sensitive areas.

4.3 Critical Infrastructure Protection

It facilitates vulnerability assessments of wireless systems, detection of potential signal-based attacks, security testing of IoT deployments, and identification of rogue devices on secure networks.

4.4 Training and Simulation

As a cost-effective platform, Project Starbeam supports signal intelligence training, simulation of various RF threat scenarios, hands-on training for technical personnel, and development of countermeasures against signal-based threats.

4.5 Forensic Investigations

The system assists in analyzing RF evidence, signal pattern matching for forensic purposes, documentation of unauthorized transmissions, and reconstruction of communications timelines.

5. Advantages of Open-Source Design

- Cost Reduction: Utilizes affordable, widely available components.
- Local Maintenance: Easier maintenance with locally sourced parts.
- Customization: Adaptable to specific operational requirements.
- Feature Expansion: Open-source architecture allows for continuous improvement.
- Knowledge Transfer: Facilitates technical capacity building for local personnel.
- Vendor Independence: Reduces reliance on external proprietary solutions.
- Community Support: Leverages a global open-source security research community.

6. Future Expansion

The platform's open architecture allows for numerous potential expansions, including integration with additional sensor types, implementation of machine learning for signal classification, development of specialized modules for particular frequency bands, creation of distributed sensor networks, addition of advanced encryption capabilities, integration with existing security infrastructure, and development of custom analysis software for specific needs.

7. Technical Specifications

- Microcontroller: ESP32-WROOM-32D
- RF Modules:
    - Configuration A: 5× NRF24L01+PA+LNA
    - Configuration B: 3× NRF24L01+PA+LNA and 2× CC1101
- Extended Frequency Range: Up to 6 GHz (with HackRF One)
- Power: Specifications depend on configuration and use case
- Connectivity: Wi-Fi, Bluetooth, Serial
- Form Factor: Customizable based on deployment requirements

8. Conclusion

Project Starbeam exemplifies the potential of open-source hardware in developing cost-effective and versatile signal intelligence platforms. Its modular design, extensive feature set, and adaptability make it a valuable asset for military, law enforcement, and security professionals seeking advanced SIGINT capabilities without the constraints of proprietary systems.