Sprint 1 Boeing Bluetooth Protocol Analytical Research

By: Caroline Terre, Matthew Irvin, Gianna Scarangelli, Jonah Rowell, Connal Grace

EMBRY-RIDDLE
Aeronautical University

Why?

Current ways bluetooth is actively used on commercial aircraft

- Refueling process
- Tire pressure
- Entertainment Systems

Advancements that may be added in the future

- Temperature tracking
- Airplane Monitoring System

Bluetooth

- Short range wireless data transfer standard
- Operates at around 2.4 GHz
- Used in tables, smartphones and laptops
- Used for high data transfer rate applications

Zigbee

- Operates around 2.4 GHz
- IEEE 802.15.4-based
- Often used for low power, low data and low cost
- Commonly used in mesh networks

Bluetooth Devices

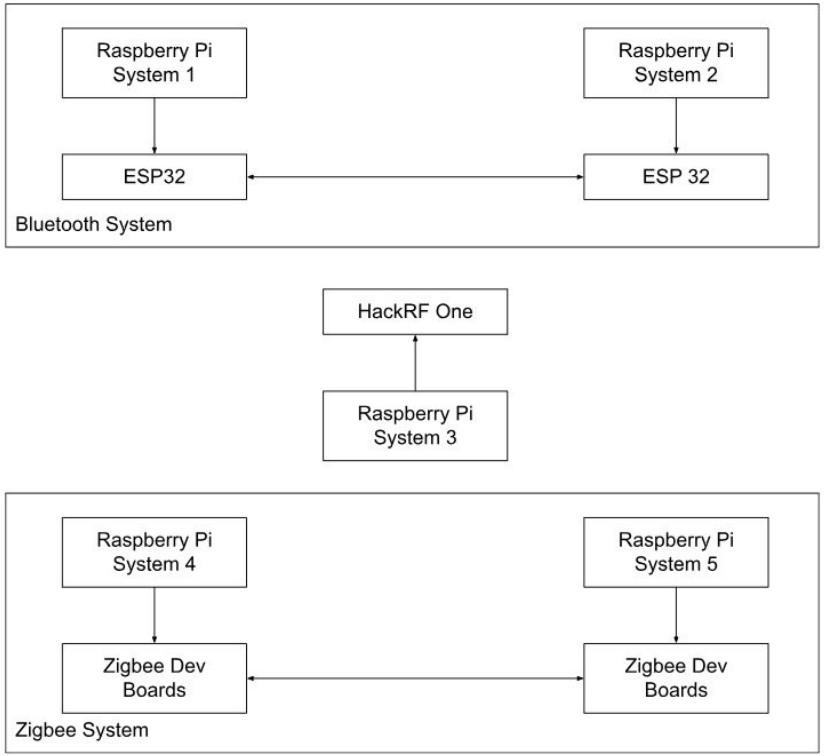
ESP32

HackRF One

Zigbee Dev Board

zigbee

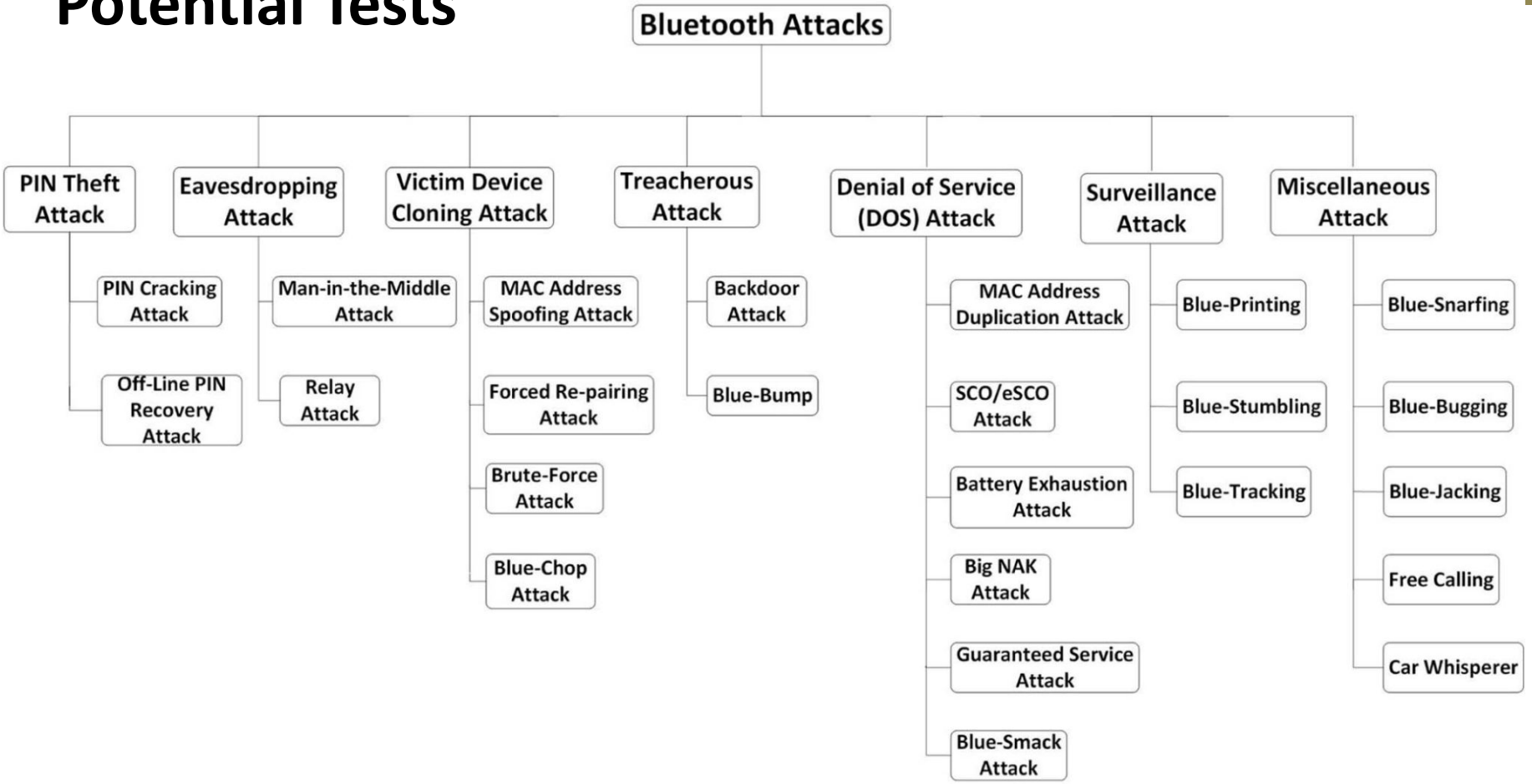
Testbed


Raspberry Pi System 1
Raspberry Pi System 2
ESP32
ESP 32
Bluetooth System
HackRF One
Raspberry Pi System 3
Raspberry Pi System 4
Raspberry Pi System 5
Zigbee Dev Boards
Zigbee Dev Boards
Zigbee System

Bluetooth Vulnerabilities

- Insecure Pairing Methods & Authentication Vulnerabilities => Brute Force Attack
- Eavesdropping Vulnerabilities => Man-in-the-Middle Attack
- Security Vulnerabilities => Bluesnarfing
- Bluejacking
- Blueborne Vulnerability
- Blue Low Energy Vulnerabilities
- Bluetooth Standards => Bluetooth Impersonation Attack
- Bluetooth Protocol => Denial-of-Service Attack
- Lack of Firmware Updates

Potential Tests

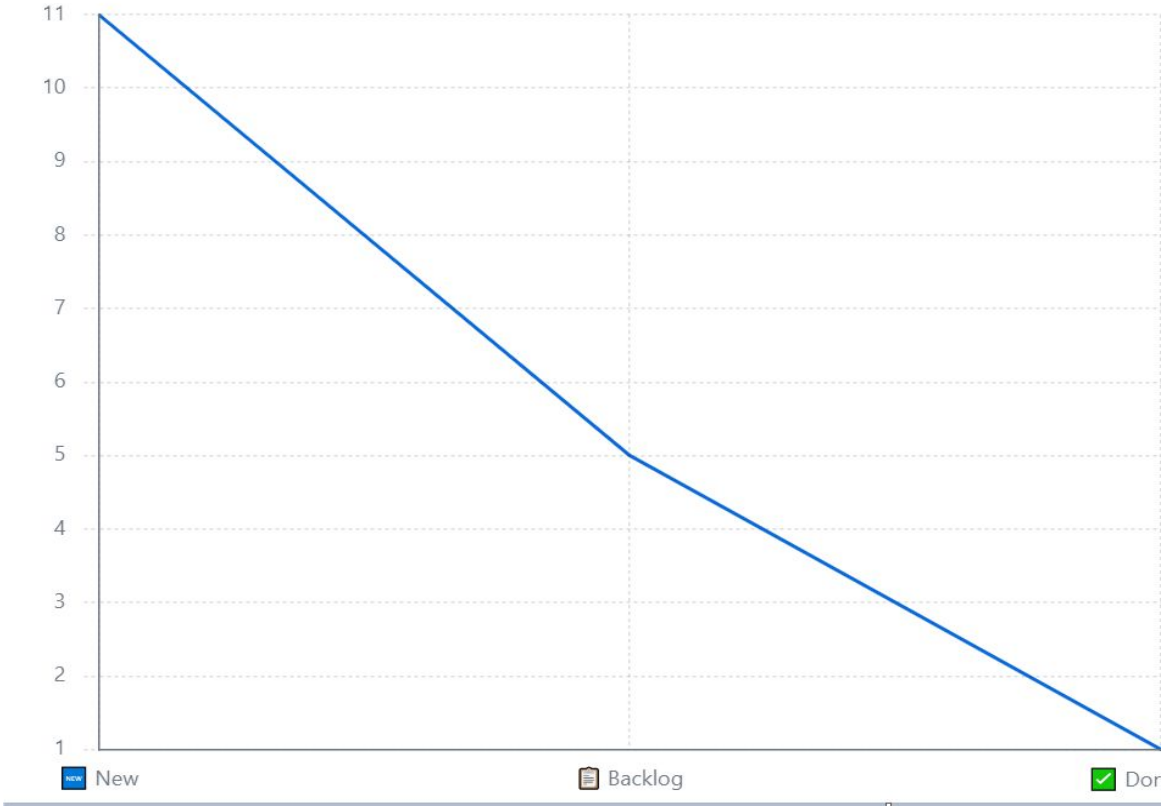


Backlog Items Sprint 1

Sprint 1:

- Create a vision statement
- Explore Bluetooth and Zigbee specifications, including protocol details
- Form an equipment list
- Finish system design document
- Finish system requirement specification document

Burndown Chart



Difficulties with Sprint 1

- Getting equipment from the IT department
- Communicating specifications with Boeing
- Cannot openly access information on Bluetooth and Zigbee vulnerabilities

Future Goals

- Acquire equipment
- Build the testbed
- If things don’t arrive at least be able to show how one would be built in depth
- Eventually demonstrate attacks by the end of the year
- Goal this semester: demonstrate a DoS attack