Blue Hawk

The Bluetooth motion detector

Dor Amit

Co-Founder & CTO at 10Root

Blue Hawk

Bluehawk is a POC RTLS Mobile App
that functions as “virtual proximity sensor”

It’s based on Bluetooth RSSI and comes with
basic automation capabilities.

Intro to RTLS

RTLS stands for Real-Time Location System. It is a technology used to automatically identify and track the location of objects or people in real-time

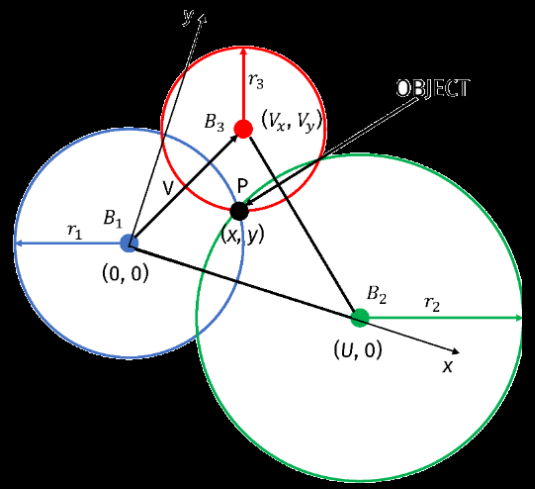
Technology	Accuracy	Cost	Ease of Use	Pros	Cons	Supported Hardware (Transmitter)	Supported Hardware (Receiver)	Supported Bluetooth/Wi-Fi Versions
RSSI	3-10 meters	Low	Easy	Low cost, simple implementation	Less accurate, prone to interference	Mobile phones, laptops, IOT, peripheral equipment	Smartphones, Bluetooth receivers	Bluetooth 4.0+
AoA	Sub-meter	Medium-High	Moderate	High accuracy, real-time tracking	Complex hardware, higher cost	Bluetooth 5.1+ devices with antenna arrays	Bluetooth 5.1+ devices with antenna arrays	Bluetooth 5.1+
DoA	Sub-meter	Medium-High	Moderate	High accuracy, effective in complex environments	Complex signal processing, higher cost	Bluetooth 5.1+ devices with multiple antennas	Bluetooth 5.1+ devices with multiple antennas	Bluetooth 5.1+
UWB	Centimeter	High	Moderate-Difficult	Extremely high accuracy, low power consumption	High cost, specialized hardware	UWB tags	UWB anchors, UWB-enabled devices	N/A (UWB specific)
Wi-Fi RTLS (RSSI)	5-15 meters	Medium	Moderate	Utilizes existing Wi-Fi infrastructure, moderate accuracy	Less accurate than UWB, higher power consumption	Wi-Fi access points	Smartphones, Wi-Fi receivers	Wi-Fi 4 (802.11n) and later

What is RSSI ?

- RSSI stands for “Received Signal Strength Indicator”
- RSSI vs RX
  - RSSI is relative signal strength value. May very between vendors
  - RX is fixed and measured in milliwatts (mW) or decibel-milliwatts (dBm)
- RSSI to Meter formula – Distance = 10 ^ ((Measured Power -RSSI)/(10 * N))
  - Note: N is Constant depends on the Environmental factor and Range 2-4, low to-high strength

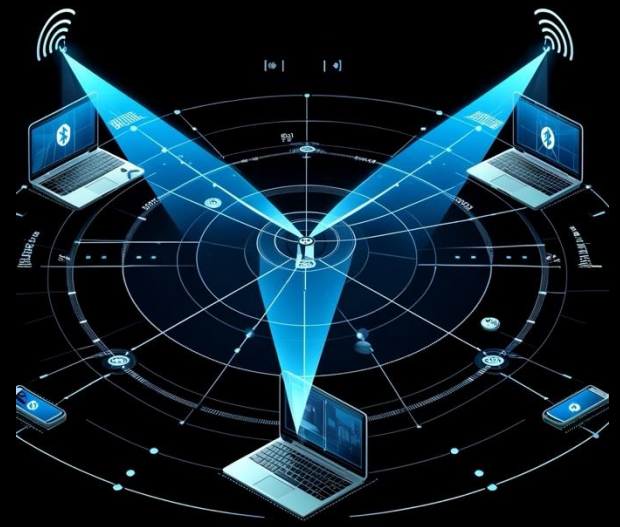
- Examples:
  - Distance for RSSI -80 = 10 ^ ((-69 -(-80))/(10 * 2)) = 3.54 meters
  - Distance for RSSI -69 = 10 ^ ((-69 -(-69))/(10 * 2)) = 1 meter

- RSSI Trilateration - Determines location using distances (unlike Triangulation which Determines location using angles)



Advantages of Bluetooth RTLS RSSI

- Supported transmitter devices – Mobile phones, laptops, IOT, peripheral equipment like smart watches headphones (Discovered by default)
- Supported receiver devices – standard mobile phones etc..
- Low Power consumption
- Less interference & Signal stability then WIFI
- More accurate then WIFI
- Cost\Effective ratio – Low cost BLE Beacons



Use Cases

Asset Tracking and Protection

- **Scenario:** A company needs to ensure that valuable assets (e.g., laptops, servers, specialized equipment) do not leave a designated area without authorization.
- **Implementation:** Equip assets with Bluetooth tags. Use Bluetooth RTLS to monitor the real-time location of these assets within the premises.
- **Example:** If an asset moves outside a predefined geofence, an alert is triggered, and security personnel are notified. This can prevent theft and unauthorized removal of assets.

Physical Access Control

- **Scenario:** A secure facility wants to implement “Intrusion detection system” by monitoring the timeframes and movement of employees and visitors to ensure they do not enter restricted areas or verify arrival at designated place & time.
- **Implementation:** Issue Bluetooth-enabled ID badges to employees and visitors or whitelisted personal mobile device. Use Bluetooth RTLS to track their movements within the building.
- **Example:** If a visitor enters a restricted area or time, an alert is sent to security staff, and access control systems can be used to lock down the area or guide the visitor back to permitted zones.

Enhanced Authentication

- **Scenario:** Implement multi-factor authentication (MFA) that includes physical proximity as a factor.
- **Implementation:** Use Bluetooth RTLS to verify that a user's device is within a certain proximity when they log into secure systems.
- **Example:** During login, the system checks if the user’s Bluetooth-enabled phone is within a certain range. If the phone is not detected nearby, access is denied, providing an additional layer of security.
  Can be combined with TOTP etc..

Contextual Authorization

- **Scenario:** a Define what privileges an identity would poses based physical proximity
- **Implementation:** White list or Black list approach. Use Bluetooth RTLS to verify that a whitelisted Bluetooth device is within a certain proximity when apply privileged action.
- **Example:** If an authorized device has not been discovered within the defined range (IT Manager smartphone) – an attempted user login is approved with restricted access, and an alert is sent to the IT security team.

Offensive Use cases

- Physical Recon
  - Devices & Device types mapping
  - Behavioral Patterns & Trends Recognition (Lunch\Daily meetings..)
- Authorized device spoofing
- Real-Time Movement Tracking for to Avoid detection by security guards
- Exfiltrate data using RSSI as Covert Channel Communication
- Proximity-Based Malware Deployment

```
C:\Demo\Bluetooth>BluetoothScannerFramework.exe
MAC::445CE97E0F09, DeviceName::Unknown, RSSI::-87, Vendor::Samsung Electronics Co Ltd, BluetoothType::BLE
MAC::5929CAD530D8, DeviceName::Unknown, RSSI::-74, Vendor::Apple Inc, BluetoothType::BLE
MAC::435D9870112A, DeviceName::Unknown, RSSI::-91, Vendor::Apple Inc, BluetoothType::BLE
MAC::75823C4EADDD, DeviceName::Unknown, RSSI::-86, Vendor::Apple Inc, BluetoothType::BLE
MAC::2CA774A7FD42, DeviceName::Unknown, RSSI::-97, Vendor::Apple Inc, BluetoothType::BLE
MAC::C3F437DCC0, DeviceName::Unknown, RSSI::-91, Vendor::Samsung Electronics Co Ltd, BluetoothType::BLE
MAC::7929CEFA99D8, DeviceName::Unknown, RSSI::-94, Vendor::Apple Inc, BluetoothType::BLE
MAC::7C2DEACF13, DeviceName::Unknown, RSSI::-76, Vendor::Samsung Electronics Co Ltd, BluetoothType::BLE
MAC::26ACCB138A83, DeviceName::Unknown, RSSI::-96, Vendor::Microsoft, BluetoothType::BLE
MAC::7E5324962B05, DeviceName::Unknown, RSSI::-79, Vendor::Apple Inc, BluetoothType::BLE
MAC::509C3BD84122, DeviceName::Unknown, RSSI::-76, Vendor::Apple Inc, BluetoothType::BLE
MAC::494192A3B52F, DeviceName::Unknown, RSSI::-95, Vendor::Apple Inc, BluetoothType::BLE
MAC::EC297C1FCA57, DeviceName::Unknown, RSSI::-93, Vendor::Apple Inc, BluetoothType::BLE
```

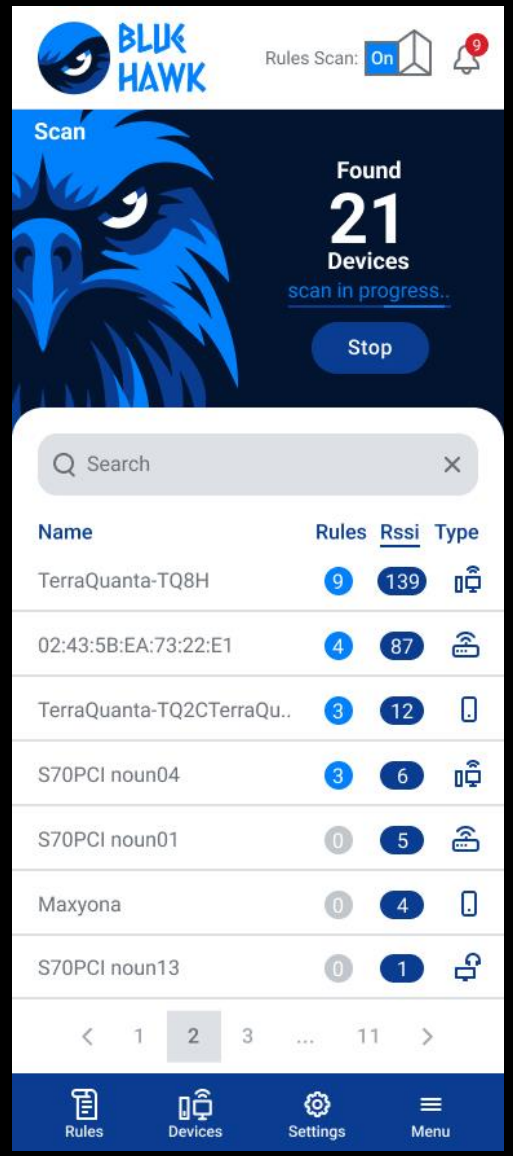
Blue Hawk Research

Bluehawk Mobile App

- Works on any Bluetooth 4.0+ supported smartphone*
- Bluetooth device monitor & RSSI Receiver
- Rule based engine with RSSI proximity-based conditions
- Actions include notifications, Alerts & utilizing mobile device’s sensors like Audio and Video recording

Demo

- Devices Discovery
- Add a new Device
- Configure “Device Discovery” Rule
- Define Video Recording, Notification & Email Alert Actions
- Activate Rule & view results



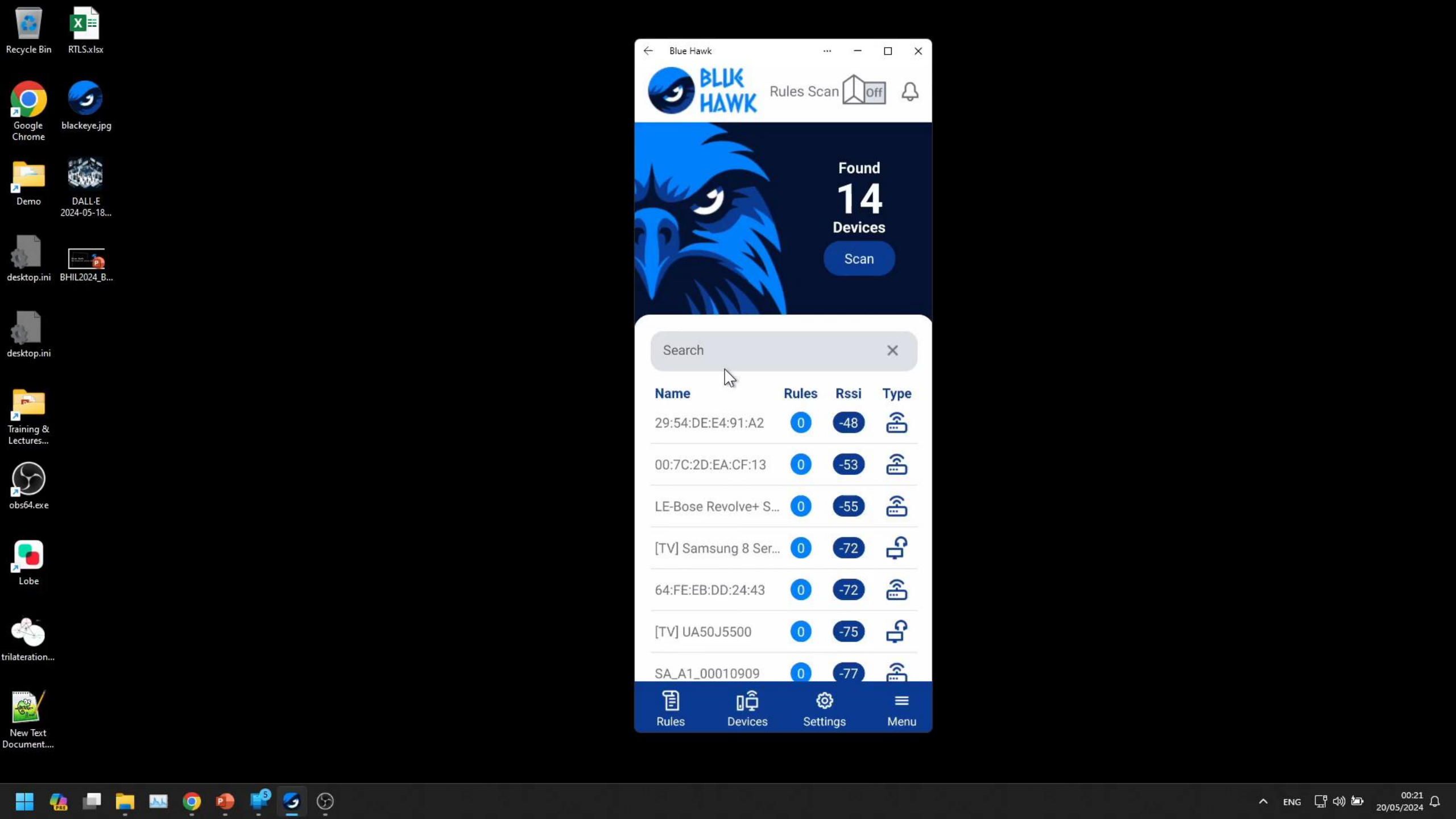
Credits

- David Wolfson

- Alon Kerklies

- Yaniv Radunsky

- Nof Levi


Recycle Bin
RTLS.xlsx
Google Chrome
blackeye.jpg
Demo
DALL·E 2024-05-18...
desktop.ini
BHIL2024_B...
desktop.ini
Training & Lectures...
obs64.exe
Lobe
trilateration...
New Text Document....
Blue Hawk
BLUE HAWK
Rules Scan
Off
Found
14
Devices
Scan
Search
Name
Rules
Rssi
Type
29:54:DE:E4:91:A2
0
-48
00:7C:2D:EA:CF:13
0
-53
LE-Bose Revolve+ S...
0
-55
[TV] Samsung 8 Ser...
0
-72
64:FE:EB:DD:24:43
0
-72
[TV] UA50J5500
0
-75
SA_A1_00010909
0
-77
Rules
Devices
Settings
Menu
ENG
00:21
20/05/2024