How To Detect, Investigate + Resolve RF Devices Entering Your Facilities

Bastille Technical Brief
ISART Conference
August 12, 2020

Presented by:
Dr. Bob Baxley, CTO
Problem Definition and Motivation
4.7 BILLION CELLULAR PHONES

Source: Statistica
8.4 BILLION BLUETOOTH DEVICES

Source: Statistica
9 BILLION Wi-Fi DEVICES

Source: Statistica
IoT Devices Growing Fast and 70% Have Radios (Radio = Radio Frequency Communication Interface)

Today there are ...

22 billion connected devices, and 15 billion have radios

Source: “Internet of Things forecast,” Ericsson
There is Covert Wireless Throughout Today

Vulnerable Wireless Devices in the Enterprise Today
On-Net Device Visibility Exists

Huge Dollars Spent to Monitor 100 Mbps Internet Connections

- Intrusion detection
- Exfiltration detection
- APT detection
- Next gen firewalls
- SIEMs

Off-Net RF Devices are Invisible

5 Gbps are Leaving via Radio Signals

- Corporate phones
- Personal phones
- Hotspots
- Wearables
- Thermostats
- Sensors
- IoT

NOBODY IS WATCHING!
What Does Bastille Do?
Sense & Locate Cellular, Wi-Fi, Bluetooth, BLE and other RF devices/networks through Software Defined Radio (SDR)
Bluetooth Pairing Policy Enforcement

- Nuanced policies for wearables in restricted spaced
- Differentiation between paired and unpaired devices
- Alerting on pairing violation
Cell Phone Location

*Bastille Persistently & Accurately Locates Individual Devices in Real Time*

- Bastille accurately locates individual phones and other devices and puts real time dots on a map
- Digital demodulation means that we can localize co-located phones

*Bastille stores location/device history for after-event analysis and forensics*
How does Bastille do that?
Bastille Sensor Arrays

- 25 MHz - 6 GHz visibility
- FPGA on-board for pre-processing
- UL Certified to work in the Plenum space above ceiling tiles
- FCC Certified as 100% passive
- **No Moving Parts**
  - Absolutely no fans. Fan failure can lead to sensor overheating and failure.
  - Advanced sensor power management can use POE+ or wall power barrel connector
- Real-Time Sensor Health Monitoring and Fail Safe
  - Automatic alerting if an individual sensor fails
  - Identification of which sensor has failed
  - System operation continues if a single sensor fails
Bastille Distributed Enterprise Architecture

1. Customer Site
2. Private Customer Cloud
3. Bastille Secure Cloud

Fusion Center

Analytics / Machine Learning

API