Bastille
Wireless Threat Intelligence

WHITE PAPER

Radio Frequency & Cellular Intrusion Detection

Table of Contents

SECTION 1: Bastille's Accurate RF Device Location Technologies **4**
Location or Localization of RF emitters 4
Path Loss and Signal Strength 5
Lateration 5
Angulation 7
Lateration with Shadowing Objects 9
RF Tomography 11
Tracking 12
SECTION 2: Advantages of Bastille's FPGA-based Decoding **13**
SECTION 3: Bastille's Sensor Arrays **14**
SECTION 4: Bastille's Cellular Detection Technologies **17**
Introduction 17
Basic Concepts 17
RF signal modulation bandwidth 17
RF Center Frequency 18
RF Modulation and Coding 19
Medium Access Control (MAC) 19
Passive Emitter Detection 20
Diode Detection 20
Filtered Diode Detection 21
Hardware Radio Receivers 21
Software Defined Radio (SDR) Receivers 22
Distributed Persistent SDR Receivers 22
Bastille 22
Emission Association 22
Localization: Heatmaps versus Dots 23
SECTION 5: Bastille Architecture **24**
Sensor Arrays 24
Concentrator 25
Fusion Center 26
SECTION 6: Bastille's APIs & Integrations **26**
Device Event Stream 27
Device API 27
Integration Templates and Recipes 28
Example integrations 28

Video Camera Systems 28
ELK Stack 29
SPLUNK 30
Incident Response (IR) and Endpoint Detection and Response (EDR) Systems 31
SIEMs 32
Routers and Other Network Systems 34
MDM 34
APPENDIX 1: Bastille Unique, Trade Secret and Patented Technology (32 Issued) 39

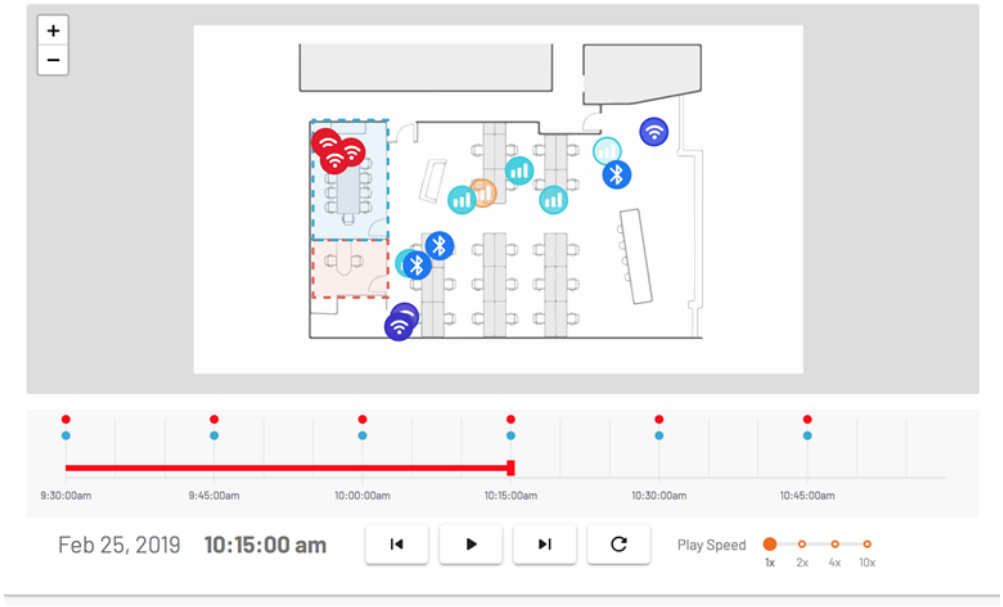
SECTION 1: Bastille's Accurate RF Device Location Technologies

Location or Localization of RF emitters

Core to the Bastille solution is the accurate localization of cell phones and other RF emitters within the area under observation. Previous generations of solutions based on spectrum analyzer approaches or basic SDRs with limited analytics have only been able to present clouds of cellular energy which may contain one or ten devices, one meter or ten meters away.

Bastille's breakthrough, patented work provides Bastille the ability to disambiguate multiple cell phones and accurately locate those devices with one to two meters of accuracy in real-time.

The following sections define the challenges behind accurate individual cell phone location and explain in detail the techniques Bastille employs to detect, locate and alert in real-time for presence and location of cell phones within buildings.



Bastille UI screenshot showing accurate real time location on a floor plan of cellular, Wi-Fi and Bluetooth devices

There are a taxonomy of possible techniques for passive localization of RF emitters. The main idea behind all of the techniques is to transform an RF measurement into a distance or angle representation which can then be used in a geometry calculation to determine the emitter

position. Sometimes this RF-to-geometry transformation is not an explicit step in the algorithm and is instead implicit.

Path Loss and Signal Strength

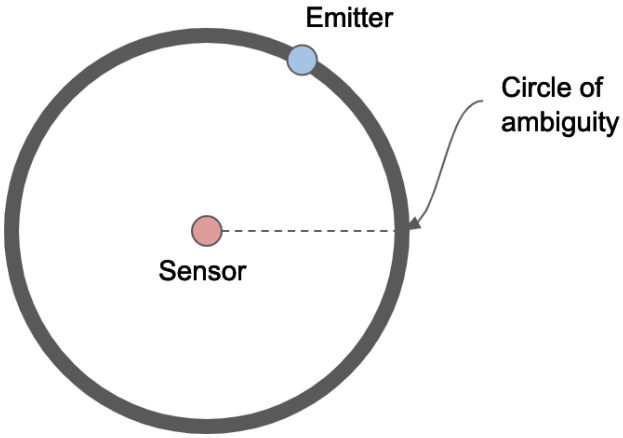
The first RF measurement that is useful for localization is signal strength. We can relate the signal strength of a reception to the distance between the emitter and the receiver with a “path loss model”. More accurate models lead to more accurate localization. For example, a simple path loss model for an indoor environment with many obstructions is not a good fit and will lead to poor localization performance.

The canonical path loss model models path loss in free space and is called the “free space path loss model”. In that model, signal power decreases with the square of the distance between emitter and receiver. The FSPLM is also isotropic, which means that the path loss does not depend on the angle between the transmitter and receiver.

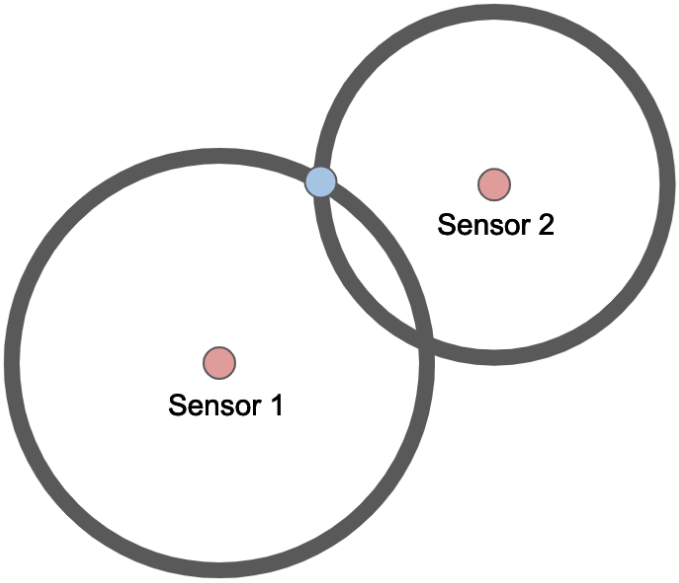
More sophisticated path loss models exist that either rely on statistical surveys of physical environments (Okumura model and Hata Model), simplified ray-bounce physics (two-ray ground reflection model), or detailed ray tracing of a 3-D model of a physical environment. One of Bastille’s innovations, as we will describe later, is our real-time online estimation of the path loss model using a ray-tracing-like mechanism without having to actually have a physical building model. Instead, we infer the building model using passively collected signal information from all of the emitters in a space.

Lateration

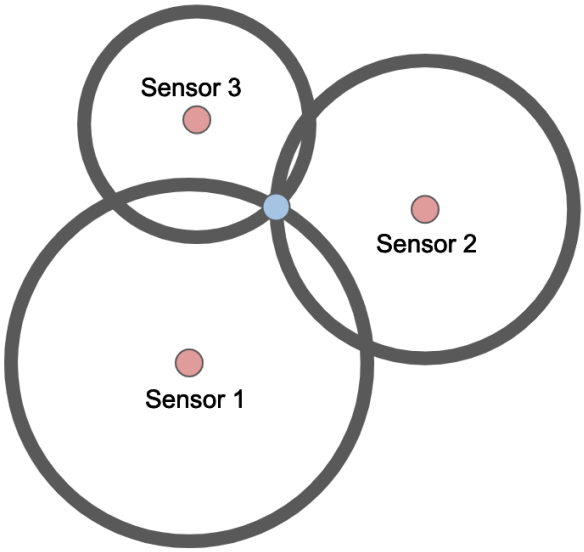
Once we have modeled the path loss, we can make a signal strength measurement from a sensor and use this measurement and the inverse model to determine the distance between the sensor and the emitter. For example, if the distance estimate is 50 meters and the antennas and system is isotropic--that is, equally sensitive in all directions--then we know that the emitter is somewhere on the circle that outlines the sensor at a distance of 50 meters.



To narrow down the position further, we need another sensor to make a signal strength measurement from a different location. If the second sensor's measurement indicates that the sensor is 30 m away, with a second radius, we can draw both of our circles on the map. The circles will intersect at zero, one, or two points, depending on the location of the sensors. Those points of intersection indicate possible emitter positions. By adding a sensor, we have reduced our ambiguity from the circumference of a circle down to one or two points.



We can further reduce ambiguity by adding a third sensor. If that sensor is placed far away from the other two sensors, then we will likely only have one intersection, which will be the position of the emitter. We can add more spatially separated sensors in order to provide a refined emitter position estimate.



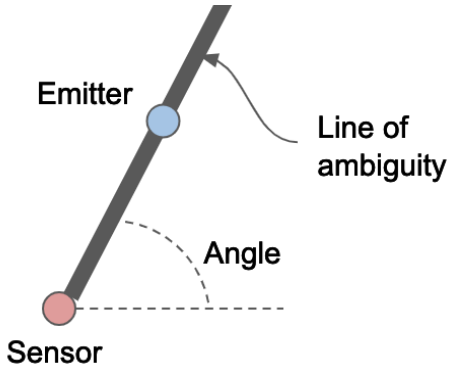
This process of localizing an emitter using lateral distance measurements is called lateration. Lateration with 3 sensors is called trilateration. The generalization to multiple sensors is called multilateration. In practice, noisy measurements make it so that the circles do not quite intercept at a common point and other math is required to find the location that best fits the circles. Specifically, when noise is added to the system, we can use minimum mean squared error regression to find the location that best fits the noisy data. More sensors will tend to increase the accuracy of the location estimate when noise is present, which is the case in practice.

In summary, lateration is the act of localizing an emitter using multiple signal strength measurements that are converted to distance measurements. Bastille uses a form of lateration in combination with online channel modeling and emitter velocity tracking.

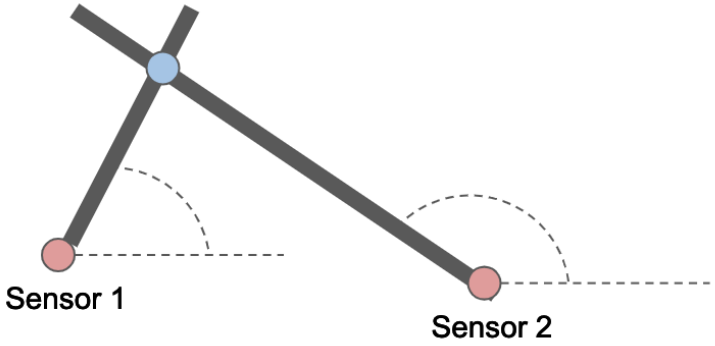
Angulation

The more familiar type of RF localization is called angulation--for instance triangulation. In angulation, the relevant RF measurement is the angle of the emitter with respect to the sensor. For example, if a sensor had a rotating antenna or a phased array, as radars commonly do, then we could measure the angle of the emitter.

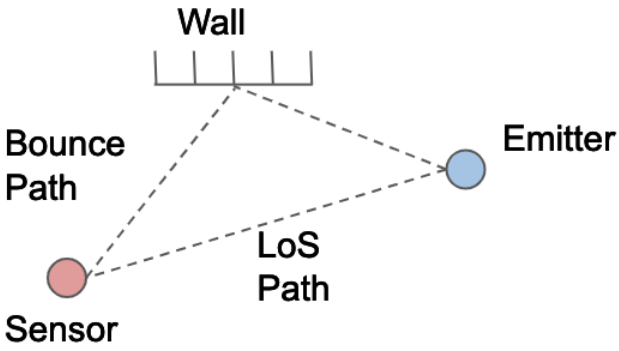
With only a single sensor and a single “line of bearing” or LoB reading, our position estimate would be ambiguous along a line.



To disambiguate the emitter position we need one more sensor in 2D localization and 2 more sensors in 3D localization. With enough sensors, the emitter position is simply the intersection of the line of bearing points.



Angulation tends to not be accurate indoors since it is difficult to distinguish a signal that is received along the line-of-sight path versus a signal that is received after having bounced off of a wall. The issue is that the bounce path and the line of sight (LoS) path will have different arrival angles causing the angle estimation procedure used by angulation to be confused and give a poor angle estimate.

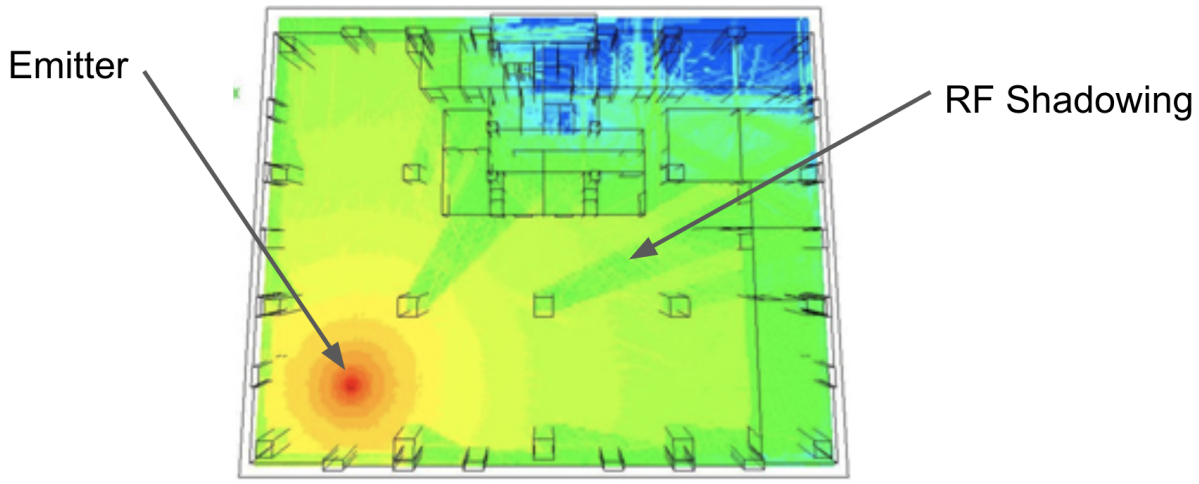


In practice, for indoor environments with many walls, there are so many bounce paths that angulation is not usable. It is possible to disambiguate the bounce paths in time, but only for very wide-bandwidth signals. For commercial signals that are only tens of MHz wide, the bounce path or multipath problem is very difficult to overcome without imposing unreasonable constraints about the environment physics.

Lateration with Shadowing Objects

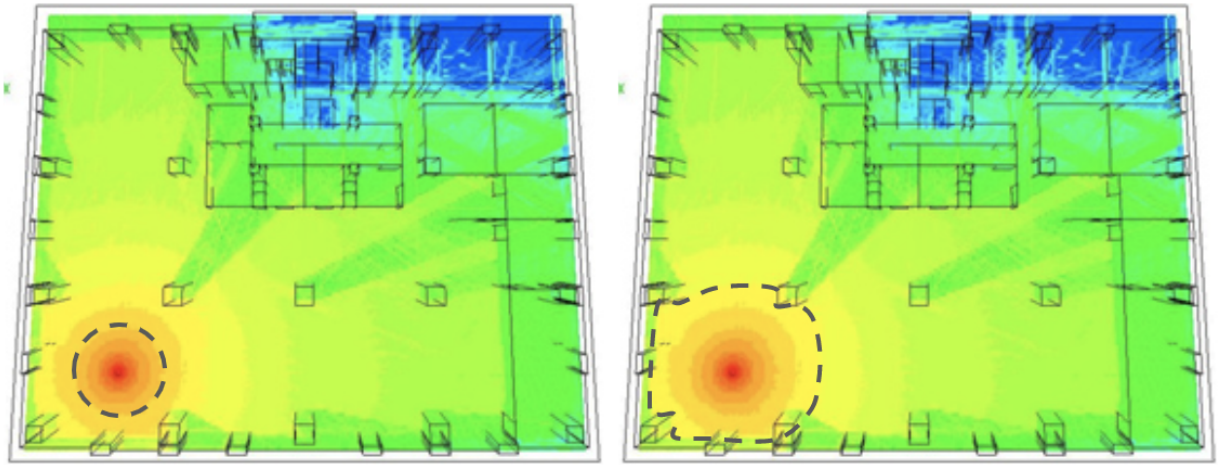
While lateration is straightforward for environments with no obstructions, it becomes much more difficult indoors where walls and other obstructions are present. The main difficulty is that the path loss model is no longer a simple equation that is isotropic. Instead, the path loss model needs to take into account positions and shadowing properties of walls and other objects in the space.

The figure below shows the signal strength heatmap for an indoor floor plan that has one emitter transmitting in the lower left corner of the space. It is clear that for the regions near the emitter where there are no obstructions, that the power is distributed radially around the emitter. It is also clear that in the shadow of a pillar, the signal strength is significantly reduced. That is, the colormap is more green directly behind each pillar.

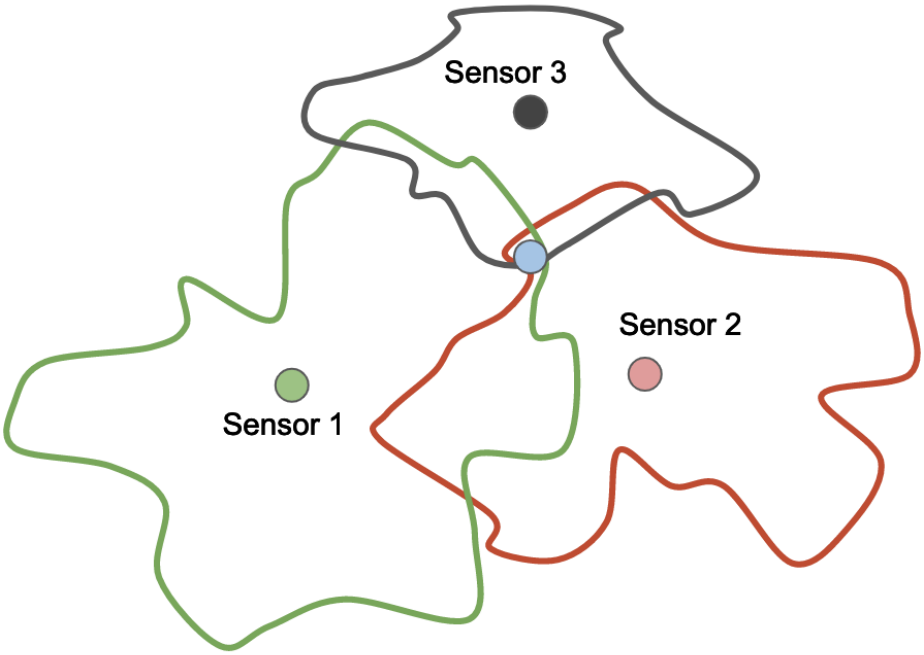


Simple isotropic path loss models do not capture this shadowing nuance. Instead, in order to do lateration in this environment, we must first create a path loss model that takes the shadowing objects into account. Once we have that model, the circles of ambiguity in the multilateration problem begin to look more like amoebas of ambiguity that follow the curves of constant pathloss throughout the floor plan. For areas where there are no shadowing objects, the curves are still circles. The plot on the left below shows that the contour of constant-pathloss near the

emitter is still a circle, while the plot on the right shows a contour that follows the outline of the shadowing objects.



The resulting multilateration problem can be visualized below. Because the curves of ambiguity no longer contain a convex region, there is no longer a guarantee that three sensors will lead to an unambiguous position. Accordingly, Monte Carlo gradient descent solvers are needed to find the intersecting that is most likely to be the emitter location.

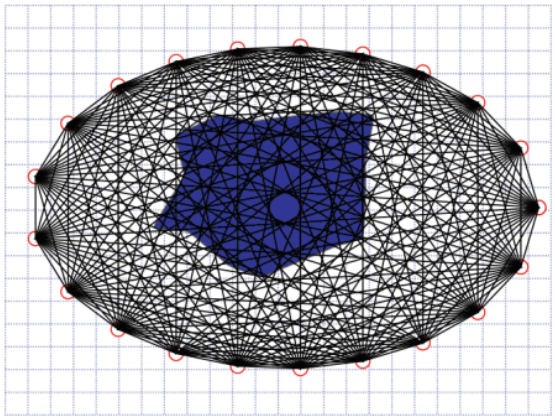


RF Tomography

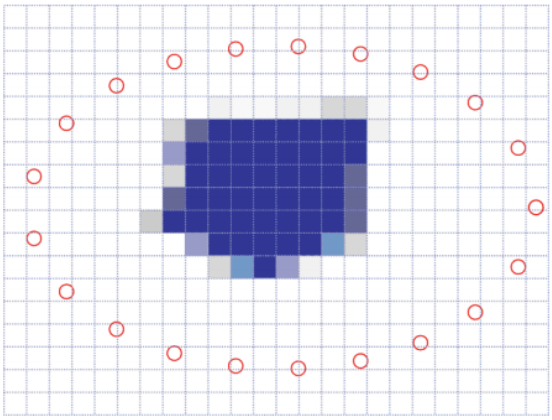
The previous section pointed out the difficulty of using multilateration in a shadowing loss environment if the shadowing loss path loss model is known. In practice, we do not have access to this path loss model. The mechanism for estimating a shadowing loss model, or more specifically, for estimating the shadow loss field, is called RF tomography.

Tomography is the act of imaging a volume using transmission of electromagnetic waves such as RF signals. The cousin of tomography is radar, which is the act of imaging a volume using reflection of RF signals. Tomography is familiar from the medical setting where CT (computed tomography) scans are used to image the cross-section of a human body by transmitting X-Rays at various angles through the body and observing the pathloss of the X-rays after they have passed through the body. The Radon transform is a mathematical tool that converts a collection of radial X-ray readings that have passed through an object and reconstruct the cross-sectional image of that object.

Bastille's Chief Technology Officer, Dr. Baxley, was one of the pioneers in demonstrating the feasibility of performing tomography using RF signals for buildings (Hamilton, B.R., Ma, X., Baxley, R.J. and Matechik, S.M., 2014. Propagation modeling for radio frequency tomography in wireless networks. *IEEE Journal of Selected Topics in Signal Processing*, *8*(1), pp.55-65.).



a) Signal strength measurements of shadowing from an object



b) Tomographic reconstruction of the object from the measurements

Bastille has created a new localization paradigm that involves 1) estimating the tomographic image of a space from opportunistic emitters in the environment, and 2) using the shadow loss field estimates from the localization to create emitter position estimates. This is an iterative process that first estimates the positions of each emitter in the space with an isotropic path loss model. Next, those hypothesized positions are used to estimate the shadow loss field. Next the

shadow loss field is used in the localization algorithm to obtain more refined location estimates. The refined positions are then fed back to the tomographic algorithm and the process continues on in iterations until it converges.

Tracking

The final element of the Bastille localization system is particle filter tracking, which simultaneously smoothes noisy position estimates and estimates the velocity of moving emitters in the environment. Bayesian tracking like this is critical in order to get high-accuracy localization. Specifically, Bastille uses a particle filter to track the position of devices as they move through the space. The particle filter is simultaneously tracking position, velocity, and shadowing loss field parameterization for all devices in the space.

SECTION 2: Advantages of Bastille's FPGA-based Decoding

One of the differentiators of the Bastille sensor array is the massive amount of FPGA processing power that is available. With a 480k logic element Arria 10 SoC, the Bastille sensor array is capable of instantiating over 100 distinct protocol decoders in parallel that can simultaneously process the full 120 MHz RF bandwidth that is captured by the two SDR front-ends in the array. No other sensor on the market has this much processing power.

Bastille has also developed a suite of more than 2 dozen FPGA protocol decoders that can be configured to run on the sensor.

Bastille's sensor arrays provide advanced detection and location across a range of RF protocols. For example, for the Bluetooth protocol, Bastille sensor arrays constantly demodulate all 79 Bluetooth channels all the time. This is made possible with Bastille's proprietary Bluetooth software-defined demodulators that run in the sensor array FPGA.

Bastille's Bluetooth detector contrasts to other technologies that only listen to one Bluetooth channel at a time. That is, other devices can only see 1.2% of the traffic that Bastille can see. Moreover, by listening to all channels, all of the time, Bastille's patented device and traffic fingerprinting machine learning technology can determine the types of data traffic being conveyed by each Bluetooth network. For example, Bastille can tell the difference between a Bluetooth tethering event which is malicious and one which is innocuous, such as one to a music streaming device.

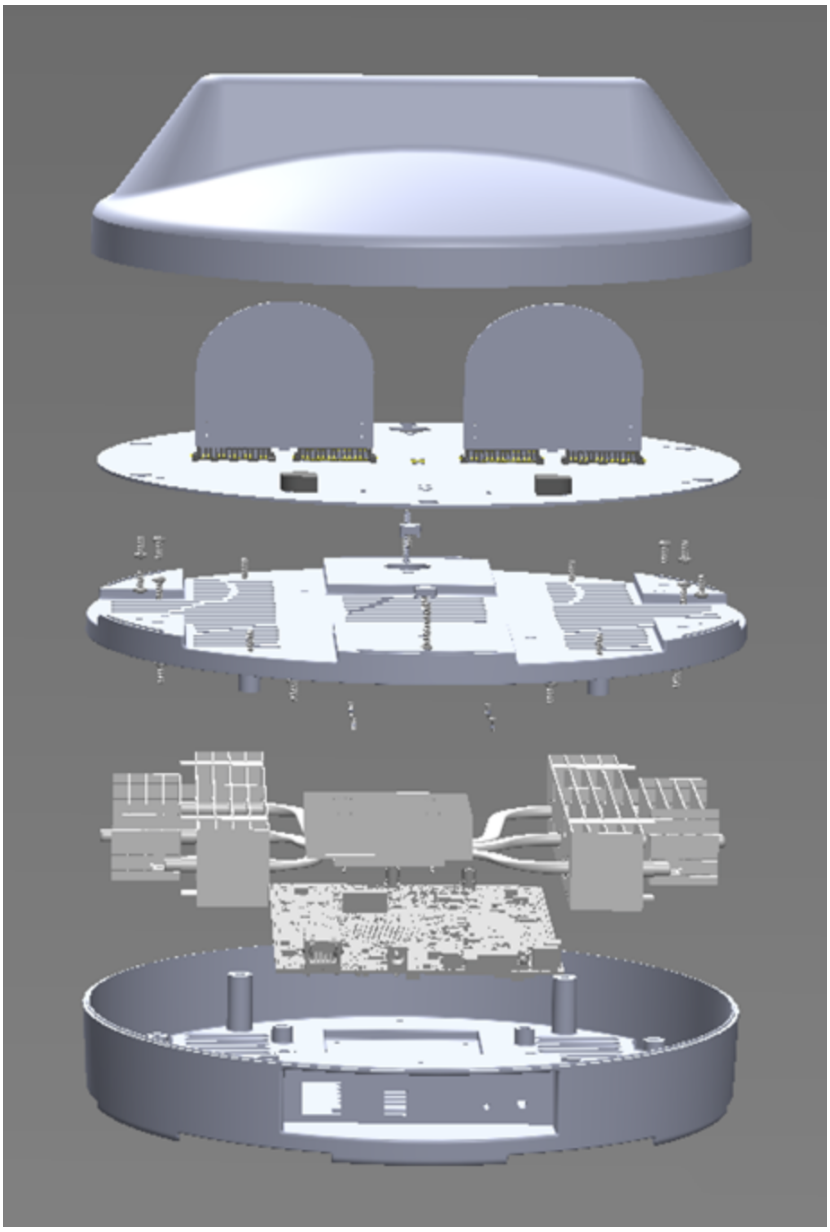
The FPGA sensor decoders can be upgraded through a firmware update. As protocols such as Bluetooth, DECT, Z-Wave, goTenna, Zigbee and others evolve, Bastille will be able to handle such changes without requiring a hardware upgrade.

SECTION 3: Bastille's Sensor Arrays

Bastille's Sensor Arrays were designed from the beginning to be a part of an RF Tomographic Network with the ability to provide enterprise wide 24/7 device detection, location and alerting. The Sensor Arrays work in conjunction with the Bastille Fusion Center (See Section 5 - Bastille Architecture)

The Bastille Sensor Array is the 4th-generation Software Defined Radio (SDR) sensor array from Bastille. It contains two scanning 802.11ax Wi-Fi receivers, two SDR receivers front ends that can each sample at 61.44MSps and sense from 25 MHz to 6 GHz, and an array of bespoke internal antennas that have been optimized to maximize detection and localization performance.

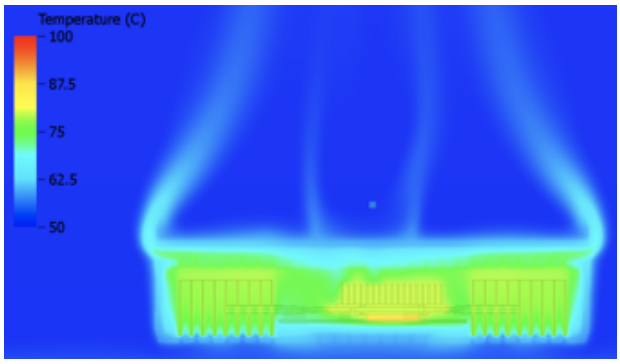
Bastille's Sensor Array is now in its 4th generation, is entirely passive (does not emit any radio signals), and was designed and built in the USA

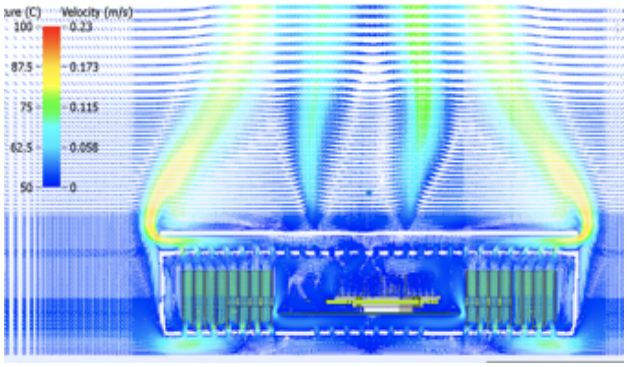


*Bastille's sensor contains no moving parts; the Analog Devices radio front ends and Altera/Intel FPGA are passively cooled by a custom heat-sync which replaces the fans used in most other RF sensor***s**

The Bastille Sensor Array is fully UL 2043 certified to operate in the building plenum. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. This Class A digital apparatus complies with Canadian ICES-003.

The Bastille Sensor Array is passively cooled and is capable of operating from 0 – 40°C. Bastille devoted significant engineering effort to ensure the dependable and reliable operation of the Array for any condition in its operating envelope. That includes extensive thermal testing, modeling and simulation. The plots below show an example heat and airflow velocity measurement and simulation for the Sensor Array.





The Sensor Array is powered by Power-over-Ethernet (PoE) that is compliant with 802.3at PoE+ specification. Alternatively, it can also be powered from a DC power supply (i.e. a wall wart). that provides 44VDC to 56VDC and a minimum of 26W of power.

Category	**Specification**
Size	298mm x 298mm x 132mm
Weight	6.2 lbs
Operating Environment	0 – 40°C, 0-90% RH
Power Consumption	20W typical at 25°C, 25W maximum
DC Input Jack	44-56V, 25W min (use CUI SD150-48-U-P5 AC Adapter or equivalent)
POE	802.3at compliant
Indications	Ethernet LINK/ACT LED, RGB status LED
Control	Reset button
Connectors	RJ-45, Auxiliary DC Input Jack
SDR Bandwidth	2 X 60.44 MHz
SDR Frequency Range	25 MHz to 6 GHz
Decoders Available	Cellular (LTE, GSM, UMTS) , Wi-Fi, BT, BLE, Zigbee, RF4CE, Z-Wave, DECT, goTenna, Microsoft mouse & keyboard (MK), Logitech MK, Amazon MK, Lenovo (4 variants) MK, HP MK, Dell MK, analog bug detection
Hardware Decoders	2 X Wi-Fi scanners. Visibility into 2.4 GHz and 5 GHz IEEE 802.11abgn, 802.11ac, 802.11d, 802.11e, 802.11i, 802.11h, 802.11w

SECTION 4: Bastille's Cellular Detection Technologies

Introduction

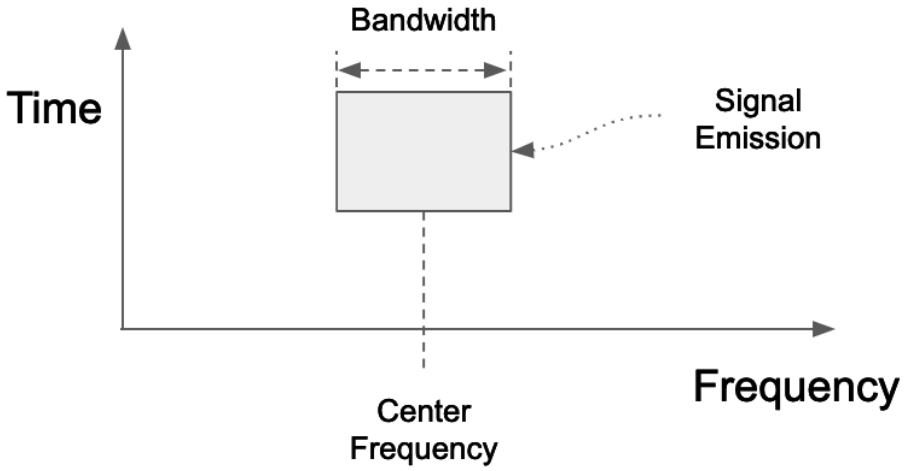
Detecting cell phones from their RF emissions is a challenging problem. Even naive detectors are not trivial. At Bastille we are proud to have 6 Patents Pending that cover our cell phone detection IP. The following is a brief summary of the elements of that IP and how it is differentiated from other solutions.

Basic Concepts

In order to understand the strengths and weaknesses of RF signal detectors available in the market, it is necessary to understand the basic concepts in RF signal detection. The following subsections briefly discuss the signal characteristics relevant to RF signal detection.

RF signal modulation bandwidth

Communications RF signals all have a bandwidth which is defined as the width in frequency of a given RF emission. For instance, a Wi-Fi emission is 20 MHz wide for 802.11 a/g/n and can be larger (40 MHz or 80 MHz) for 802.11ac. LTE signals are anywhere from 1.4 MHz to 20 MHz wide. Bluetooth signals are 1 MHz wide. FM audio radio station signals are 200 kHz wide. Most consumer devices have bandwidth between a few kHz and tens of MHz.



There is an interplay between signal bandwidth and other important aspects of communications signals. First, the RF bandwidth is limited by the digital-to-analog converter (DAC) sample rate at

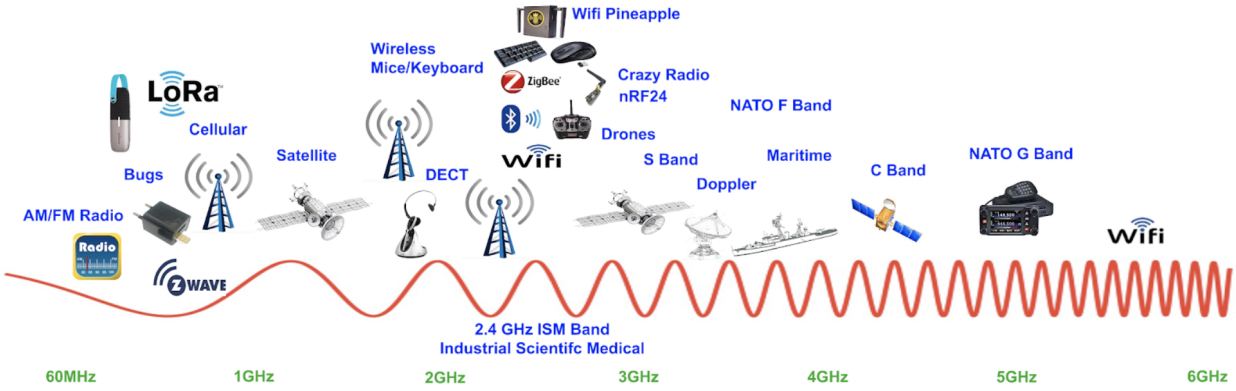
the transmitter and the analog-to-digital converter (ADC) at the receiver. Depending on how the DAC/ADC specification is worded, the RF bandwidth is either the sample rate or one half of the sample rate. Price and power consumption of DACs and ADCs increase for higher-rate devices.

The communication bit rate is also dictated by the signal bandwidth. Specifically, in his famous 1948 work (Shannon, C.E., 1948. A mathematical theory of communication. Bell system technical journal, 27(3), pp.379-423.) Claude Shannon showed that the information rate of a communication signal can be no faster than capacity, defined as C = BW * log_2 (1 + SNR), where BW is the RF signal bandwidth and SNR is the signal to noise ratio. As an aside, it is clear from the equation that the capacity is linearly increasing in BW but only logarithmically increasing in SNR, which indicates that BW is the critical parameter for sending high-rate information.

RF Center Frequency

The second component of a communication signal that is relevant for detection is the center frequency of the signal. Center frequency is also sometimes referred to as the “tuning frequency” or simply the “frequency” of a signal.

The FCC tends to designate certain frequency bands for certain applications. For instance, 407 MHz to 806 MHz used to be reserved for licenced television transmissions (in 2008 the FCC decided to open these bands to other uses). As another example, the frequencies between 2.4 GHz and 2.5 GHz are one of the ISM (industrial, scientific and medical) bands, which allows for unlicensed RF transmissions.



Unlike RF bandwidth, there are few hardware limitations that dictate cost or power tradeoffs in the center frequency. Instead, the biggest decider is regulatory--that is, devices can only transmit in bands where they are allowed.

There are, however, physics tradeoffs to consider in the choice of center frequency. A transmitted signal attenuates as it travels through the air. That attenuation is a function of the

properties of the medium (e.g. air) as well as the center frequency. The higher the frequency, the more antennuation--or path loss--there is. The practical effect of a reduced path loss is that a receiver receives the signal with a lower power, thus decreasing the reception SNR.

Because of this phenomenon, the UHF TV channels are thought to be “beachfront property” from a cellular service perspective because the band was low enough to provide several square kilometers of coverage from a signal base station, while being high enough to afford room to allow many multi-MHz channels.

RF Modulation and Coding

RF center frequency and bandwidth determine the important physical aspects of a signal emission, but they say nothing about how data is conveyed over those emissions. To understand that, we need to specify the signal modulation, which specifies how bits are converted from 1s and 0s to voltages that excite an antenna. While there are hundreds of modulation schemes that have been proposed over the decades, most modern devices use a narrow set of modulations.

Inexpensive narrow-band (i.e. low-rate) transmissions tend to use a frequency shift keying (FSK) modulation variant such as GFSK, MFSK, CPM, etc. Higher rate signaling is almost exclusively accomplished with orthogonal frequency division multiplexing (OFDM) modulation. OFDM has a couple of advantageous properties such that it is robust in environments where there are many reflections caused by walls and other obstructions in an environment.

Correcting the effects of these reflections is called equalization. The higher the RF bandwidth, the harder and more computationally complex equalization generally becomes. OFDM is distinguished because its equalization mechanism is particularly robust and low on computational complexity, especially compared to competing protocols like CDMA.

Medium Access Control (MAC)

The final component that affects signal detection that we will discuss is the medium access control (MAC). A protocol’s MAC algorithm dictates how, when, and where in the spectrum an emitter decides to transmit. For example, Bluetooth’s MAC involves pseudo-randomly hopping amongst up to 79, 1 MHz channels and transmitting for a very short period of time in each of those channels. This is called frequency hopping. So, while each Bluetooth emission is only 1 MHz in RF bandwidth, a Bluetooth emitter might be transmitting over a 79 MHz spectrum swath if it is observed for a long enough period.

Similarly, Wi-Fi devices in the 2.4 GHz band are 20 MHz wide, but can have a center frequency that is one of 14 values--one for each possible Wi-Fi channel. Some Wi-Fi devices perform spectrum sensing to dynamically decide which channel to use, while other devices only transmit a signal on a fixed frequency set by the user. In the time dimension, Wi-Fi devices randomly

select time-slots to transmit in an attempt to avoid collisions with other Wi-Fi signals in the same band.

Generally, MAC mechanisms can be described by either frequency, time, or space (for multi-antenna systems) deconfliction mechanisms--commonly called frequency division multiple access (FDMA), time division multiple access (TDMA), and space division multiple access (SDMA). There is also code division multiple access (CDMA), which uses coded sequences in time and frequency to allocate medium access to users.

Passive Emitter Detection

There are various flavors of emitter detection that have varying benefits and capabilities. The most basic level of capability is determining whether any RF emitter is in the vicinity of an area under observation (AUO). The most sophisticated capability is being able to determine distinct devices that are collocated in time and frequency and determine persistent identifiers and other meta digital metadata about those devices. The list below describes the components of detection in order of usefulness.

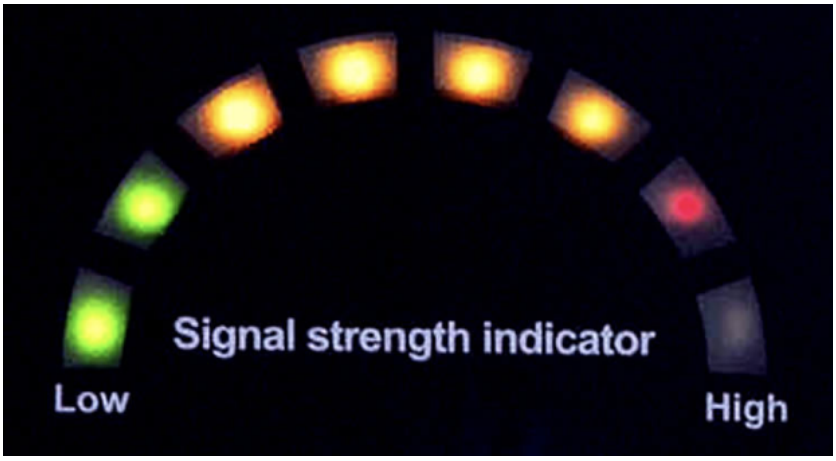
1) Presence of device in any frequency
2) Presence of device in a given frequency
3) Device classification using fuzzy frequency look-up tables
4) Device type identification using digital demodulation
5) Device identifier identification
6) Device metadata decoding
7) Device localization

In the following subsections, we describe various device detection technologies and how they meet these levels of capability.

Diode Detection

The most basic detection systems are available for less than $100 from spy shops. These devices use what amounts to a simple diode wide-band power detector in order to sense cellular RF energy. Diode detection has the advantage that diodes are sensitive over a very wide range of bandwidth (e.g. gigahertz), however they are unable to distinguish energy in different bands. Thus, a diode detector will be triggered by TV tower emissions, cell phones, and 2.4 GHz Wi-Fi devices all at once. In busy RF environments where only a subset of devices need to be detected (e.g. cell phones), diode detectors are mostly useless unless you are using them in very close range.

The resulting signal indication from a diode-like detector is usually visual LEDs that lights up in proportion to the signal strength.



Filtered Diode Detection

A slight modification to a diode detector is a diode detector plus a filter. For example, to detect 2.4 GHz devices, one possibility is to place a filter that only passes 2.4 GHz signals between an antenna and a diode detector. The resulting detector would only be sensitive to 2.4 GHz signals.

Most cell-phone detection products on the market today are a variation of this approach. Where one or more filtered diode detectors are used to determine signal presence in a predetermined set of cellular bands. The resulting band detections can be compared to a lookup table of cellular carrier frequency allocations to estimate the carrier that the emitter is using. This sort of detector is better than nothing, but it is brittle because cellular band allocations are area specific and constantly changing. By predetermining the filter-diode bank, these devices lack the flexibility to sense in new band allocations. They also suffer from the problems inherent in diode detectors which is that it is *impossible to distinguish one nearby device from many devices that are further away.*

Hardware Radio Receivers

Hardware radio receivers refers to ASIC chips that are designed to detect and demodulate one type of protocol or modulation. Example receivers include promiscuous-mode Wi-Fi cards, hacker devices like the Ubertooth, and flexible receivers like the nRF24 or the CrazyRadio. These hardware modules are typically only capable of tuning to a relatively narrow band of the spectrum such as the 2.4 GHz ISM band. But within that spectrum, they are able to completely demodulate a protocol or a class of protocols. The advantage of these devices is that they are inexpensive and work very well for the protocols that they target.

For instance, a promiscuous Wi-Fi receiver can passively demodulate all Wi-Fi traffic on a given channel and report back all unencrypted information like the MAC address, the security capabilities, the device capabilities, etc.

Similarly, a CrazyRadio can tune to the 2.4 GHz band and do arbitrary demodulation of FSK-class modulations that have a bandwidth up to 2 MHz. In order to decode a specific protocol, one has to do more work to create a protocol decoder that will convert demodulated bits into useful information.

In summary, hardware radios can be very useful if they exist for the protocol of interest.

Software Defined Radio (SDR) Receivers

There are two disadvantages in hardware radio receivers: 1) they only decode one protocol, 2) if that protocol evolves, an upgrade requires a hardware change, not a software change. SDR receivers solve both of these problems. As background, a SDR is a radio device that is capable of capturing raw RF samples and processing them with arbitrary "software-defined" decoders. The decoder processing is either performed on a general purpose processor like a general purpose processor chip, or on an FPGA.

SDRs are characterized by their tuning range, which is the range of center frequencies that they can receive, their RF bandwidth, which is the width of the RF spectrum they can receive at once, and their processing power.

For a SDR to be useful for signal detection, someone must write the demodulation software/firmware that converts raw RF signals into useful packet-level information. Moreover, general-purpose processor-based decoders are typically too slow to run in parallel, so for production applications, FPGA-based decoders are required.

Distributed Persistent SDR Receivers

Device localization is also desirable in a signal receiver system so that an operator can determine the presence and position of a device in the AOU. For localization to be possible multiple spatially distributed must be installed that are capable of synchronously receiving signals.

Bastille

Bastille sensor arrays are the combination of all of these things. The Bastille sensor array combines two stand-alone SDRs and two stand-alone hardware defined Wi-Fi receivers to provide comprehensive and persistent signal detection coverage in an AOU.

Emission Association

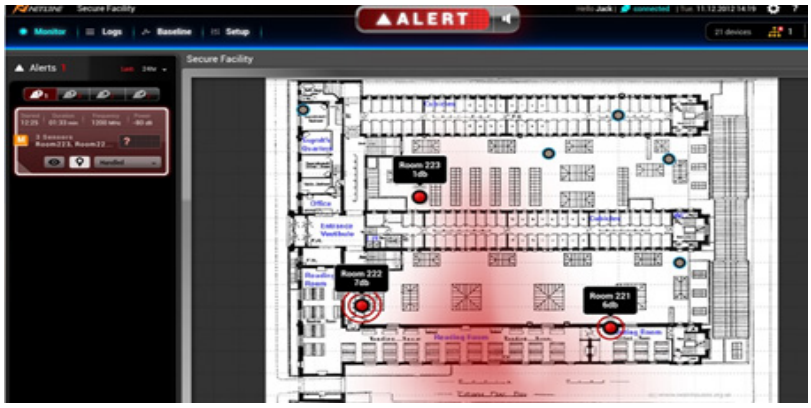
Bastille is the only technology that can associate every emission with a distinct device. This differs from competing technology in a couple of ways. First, some cellular detection

technology is *only able to identify network association packets that are only emitted when a phone joins a network or resets its connection to a network*. This sort of event might happen as rarely as once per day. So, a technology that relies on network association packets precludes *real-time* insight into a device position and activity. The reports they generate can be summarized as "there was a distinct cellular device here earlier today."

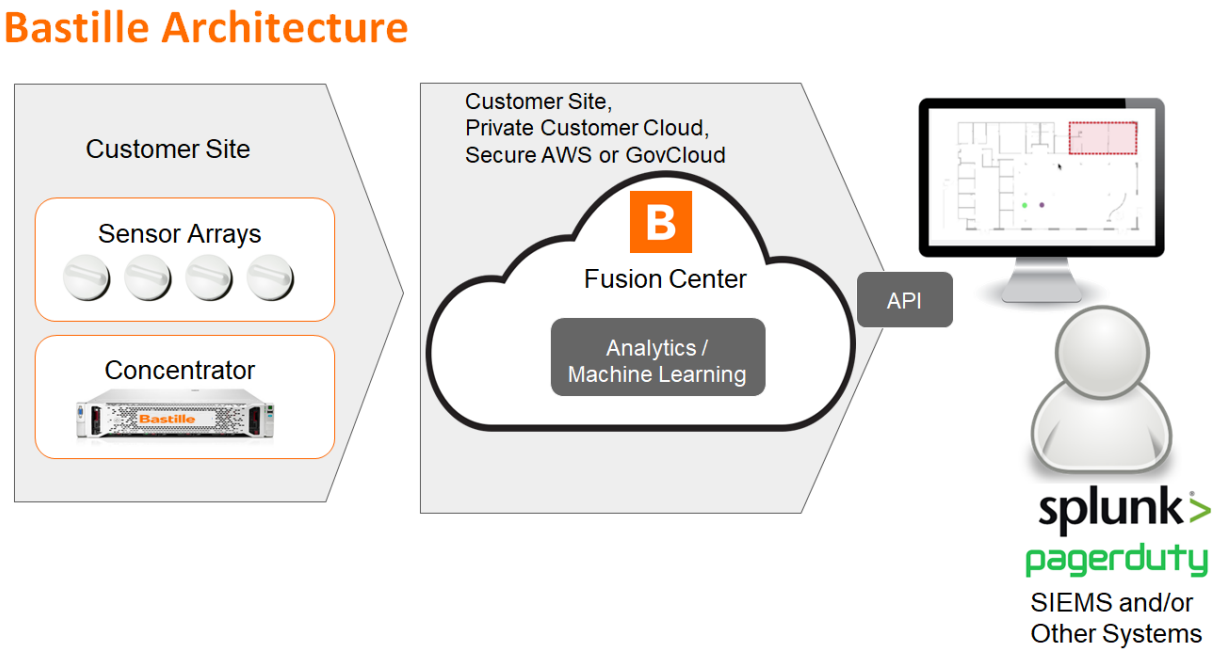
Even less sophisticated technology like diodes or power detectors, are unable to separate out the fact that RF emissions come from a distinct device. Without that association, competing technology simply aggregates all emitted energy in a given LTE band and reports that back. But this sort of aggregated energy reading is unable to distinguish the number of users and is unable to determine if there are many users that are far away or one user that is close by. The reports from these technologies can be summarized: "There is one or more emitters at a certain frequency somewhere close enough to a sensor that we can detect it."

Localization: Heatmaps versus Dots

The fact that Bastille is able to do real-time emitter differentiation of all cellular emitters, contributes to Bastille's industry-leading cellular localization performance. Bastille can put a dot on the map for each cell phone in an area. By assigning each RF emission to a specific emitter, Bastille is able to localize each emitter distinctly even if there are two phones on the same person or desk. The result is that Bastille provides 2m-accurate LTE emitter locations for each emitter. This is in contrast to competing products that can only provide a "mist" or heatmap of LTE energy overlayed on a floor plan. Heatmaps of energy that require a sophisticated signals intelligence operator to determine if there is one phone or 10 are not actionable with deterministic alerts. Moreover, heatmaps do not provide the discrete position estimate for each LTE emitter in the space.



SECTION 5: Bastille Architecture



The Bastille architecture and data model is composed of several components.

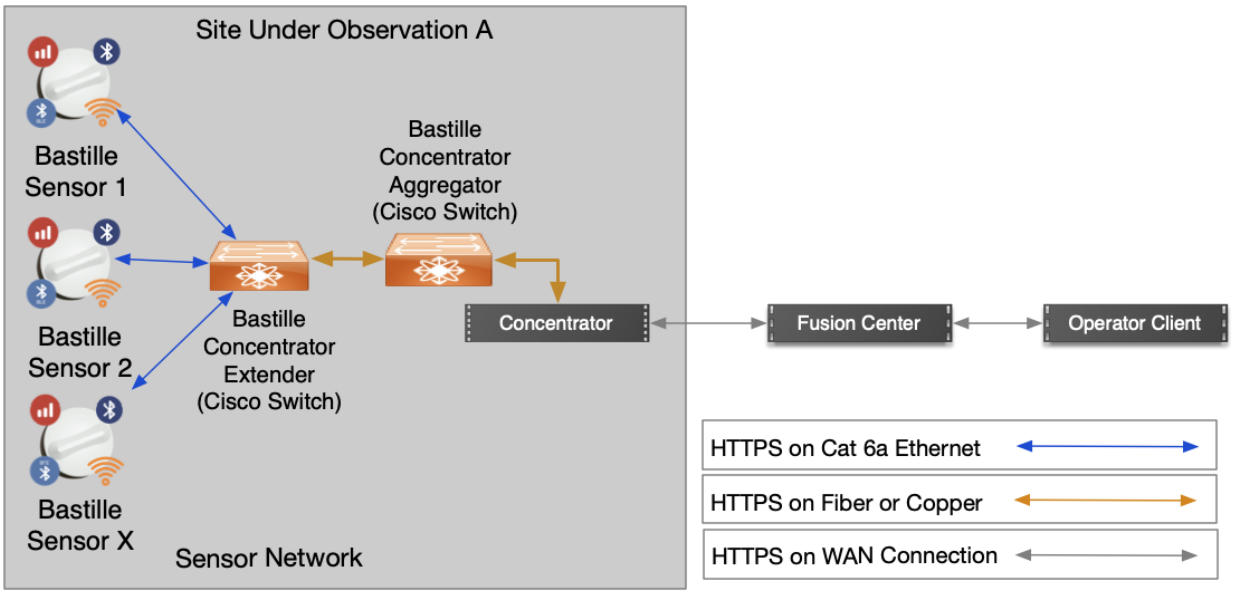
Sensor Arrays

Each Sensor Array can cover an area of 3,000 square feet and they are typically deployed at a client site, one every 50-100ft along the perimeter of the Area Under Observation (AOU) The Bastille Sensor Array is fully UL 2043 certified to operate in the building plenum. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. This Class A digital apparatus complies with Canadian ICES-003. Given their plenum certification, Bastille sensors can be, and are typically installed above the ceiling tiles. Alternatively, they can be suspended from a ceiling or placed on top of shelves, credenzas etc.

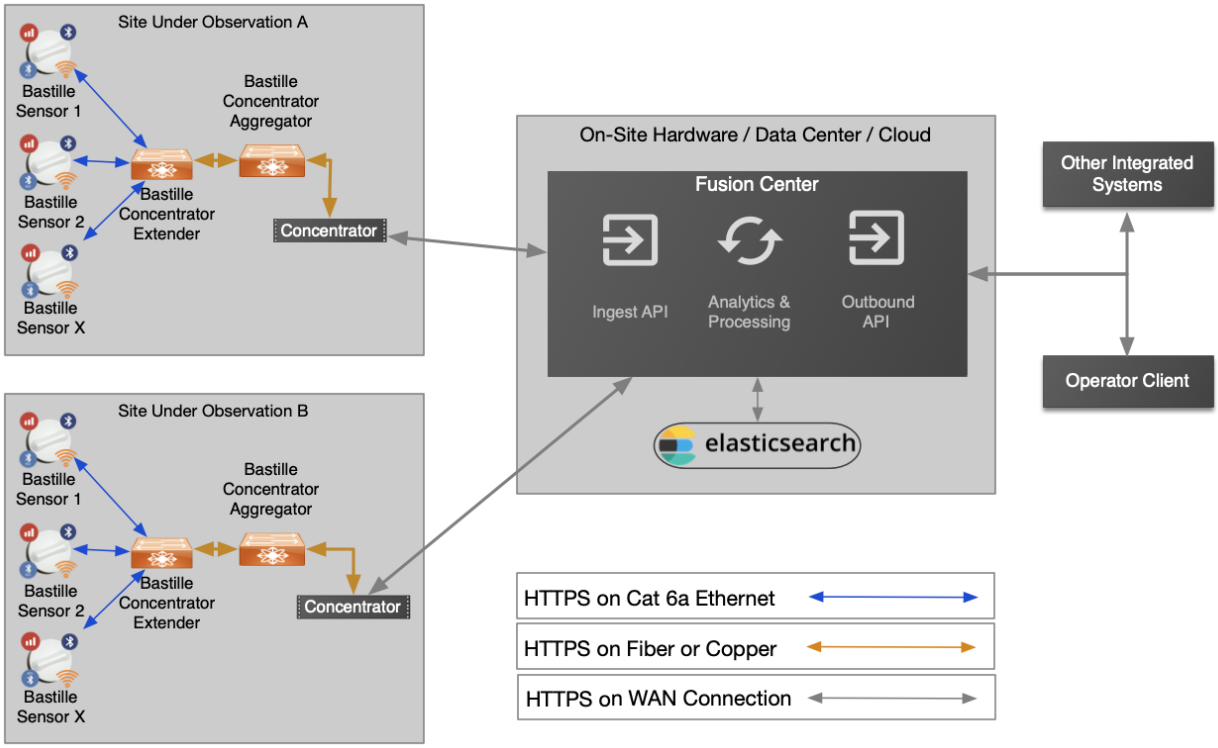
For a complete description of the Bastille Sensor Arrays, refer back to Section 3 of this document.

Concentrator

The sensor arrays are connected to a local appliance onsite called the Bastille Concentrator. That Concentrator collects data from Sensors connected to it and condenses that data. The Concentrator then backhauls aggregated data to the Bastille Fusion Center.



Fusion Center



The Fusion Center is available in several options to permit on-site, on-premise, or cloud deployment as required. The Bastille Fusion center can be installed on-site as a second appliance, installed as a virtual appliance in a private cloud, or can function as a SaaS client in the Bastille AWS Cloud or AWS GovCloud. The Fusion Center hosts Bastille APIs and can be accessed using HTTPS Rest commands.

A single Fusion center is horizontally scalable and can support multiple sites (and Concentrators). When deployed in scaling mode, the Fusion Center becomes a cluster of individual Fusion Center nodes. Using virtualization orchestration software like VMWare vCenter, a Fusion Center cluster can be configured to support both infinite horizontal scaling and robust automatic failover.

SECTION 6: Bastille's APIs & Integrations

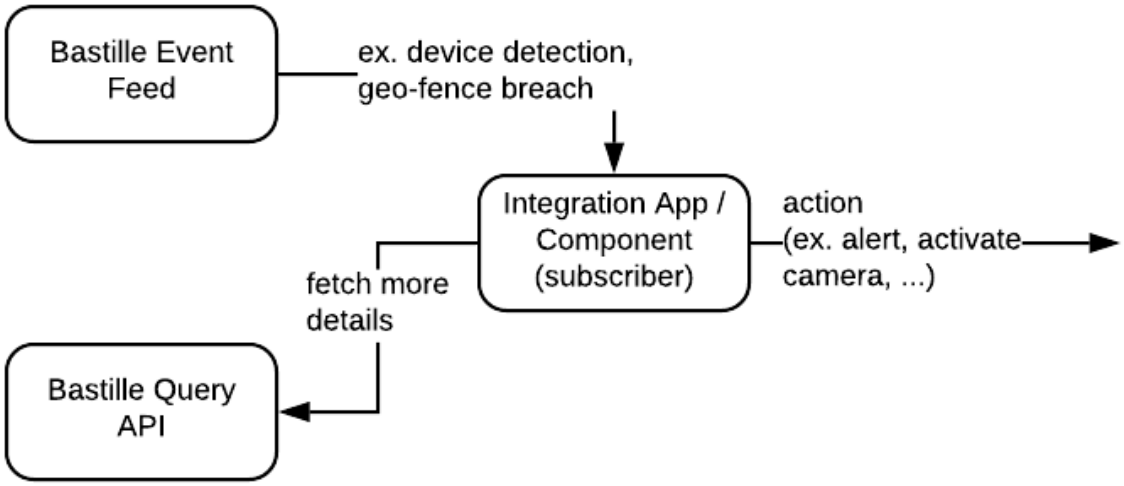
Organizations don't want applications that create more data islands. Systems need to be inter-connected. Particularly in modern IT Security stacks where security is a team sport across vendor products. Bastille's APIs and event streams are "first class citizens" in that all Bastille user interfaces and integrations exclusively use the same APIs and event streams available to

customers. Furthermore, Bastille APIs and event streams use industry standard and best practices.

Bastille's APIs and event streams can be used to build:

- user interfaces
- command lines tools and automate processes
- integrate with incident response and alert systems
- integrate ETL jobs and data warehouses (and enable custom analytics)
- build a rich security fabric, combining a set of security components

Bastille provides a Device API and event data streams. A common application integration workflow might be:



Device Event Stream

The Fusion Center will emit events, such as new device detection or a geo-fence breach. These events are published via a *http webhook*. In addition, Bastille can emit events directly to Splunk, letting organizations leverage existing business rules and alerting mechanisms, common to the Splunk platform.

Device API

Bastille's Device API uses the Elasticsearch Query DSL. This provides a common search language that many organizations are already using and understand. The Device API provides all event and detailed data available in the Bastille platform, such as

- device details, such as identifiers , manufacturers, networks and protocols
- device locations
- device events

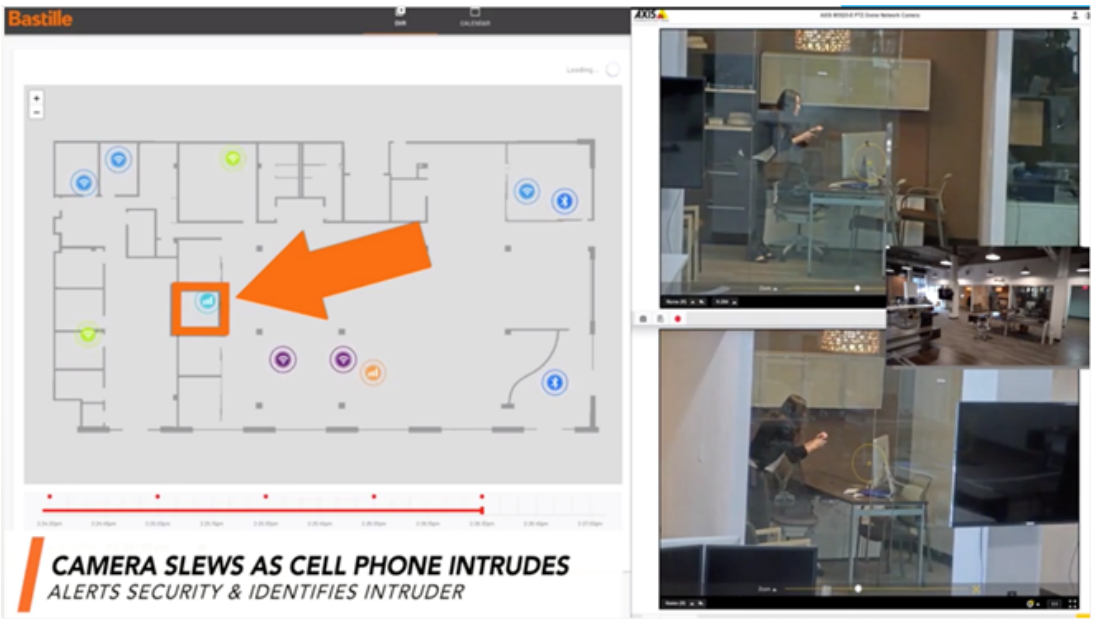
Integration Templates and Recipes

Bastille provides ready-to-use integration templates, recipes and sample applications. While this repository continues to grow, examples include:

- Incident responses workflows, using systems such as PagerDuty, Securonix, QRadar, and LogRhythm
- Camera integrations (cue and slew a camera based on a geo-fence breach)
- Data snapshots and ETLs
- Zero Trust Framework integrations with network access control (NAC) systems such as Aruba ClearPass
- Data logging and SIEM integration into system such as Splunk and ELK

Example integrations

Video Camera Systems



Bastille can "Cue to Slew" a Pan Tilt Zoom (PTZ) Video Camera System (Link to video)

Bastille locates a cell phone and in real-time sends the coordinates of the cell phone to the 3rd party PTZ video camera system via the ONVIF open API standard . ONVIF is a standard that all modern enterprise and consumer class cameras conform to. With the Bastille integration, the closest PTZ video camera "slews to the emitter cue provided by that Bastille system." As the

camera slews, it also zooms in and focuses on the individual with the cell phone. The resulting video recorded can be used in conjunction with Bastille's DVR record of the device and its characteristics.

The input to the camera location is the position and orientation of the camera. The Bastille-to-ONVIF connector performs a simple geometric transform to convert the x/y/z coordinates produced by the Bastille localization and alerting system into a pan/tilt/zoom command.

When an individual with a cell phone enters a geo-fenced area, an alert is sent via SMS, or to an Incident Alert System and/or Bastille "cues and slews" a PTZ video camera

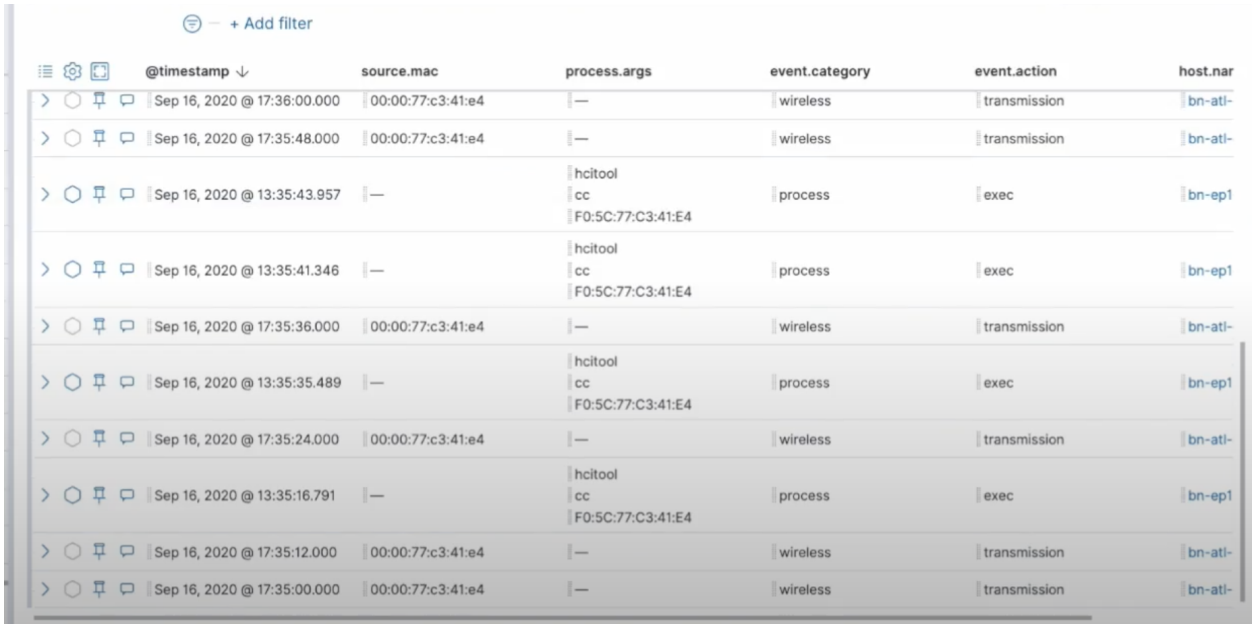
In environments where there are multiple fixed position cameras covering a facility or campus, Bastille can send the coordinates of the suspect with the phone and an alert which causes the current image of a particular camera to be served to security personnel.

The same API which activated the video cameras can send information and/or a real time alert to any other system such as a SIEM or Incident Response System (see below).

Bastille's enhancement of video surveillance systems delivers 24/7 security and surveillance, ideal not just for perimeter security, but also to protect sensitive areas or rooms inside a building which can be geo-fenced using Bastille.

ELK Stack

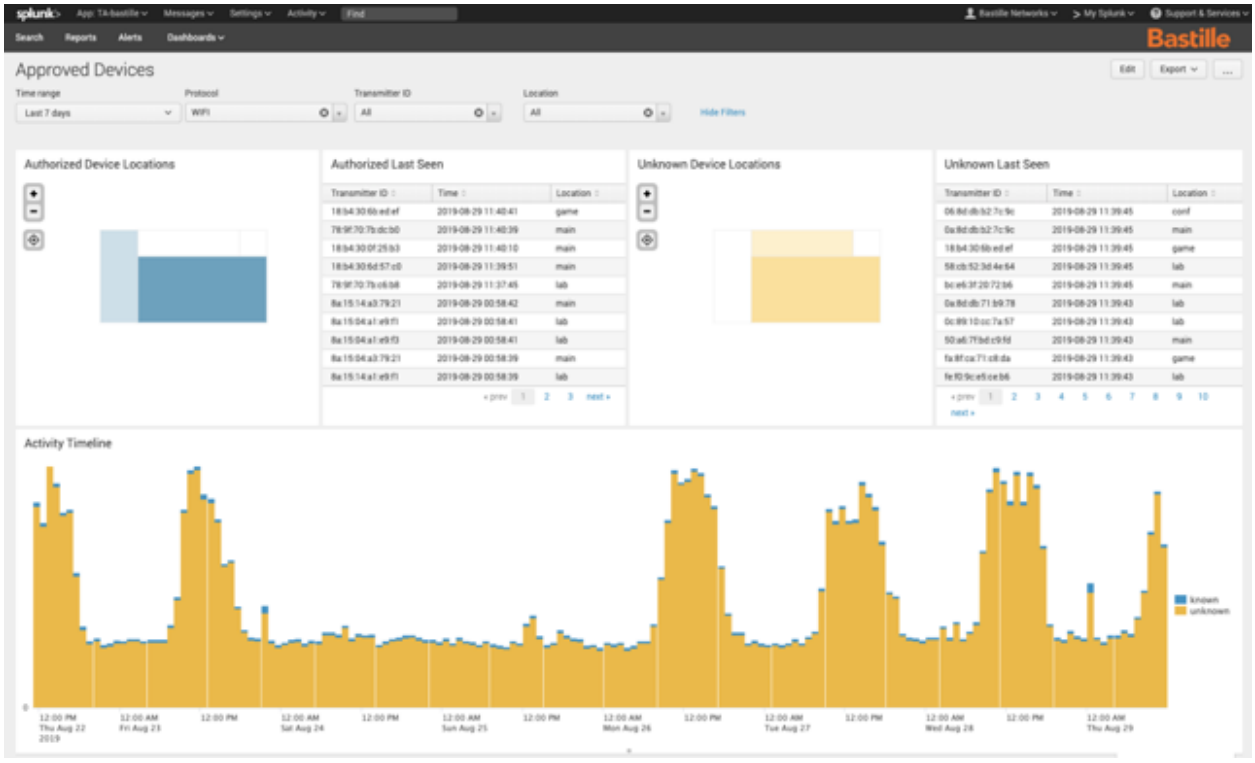
Elasticsearch, Logstash, and Kibana (ELK) have become a very popular stack of tools for storing, processing, and analyzing cyber security information. Specifically, our threat hunting customers seem to exclusively use ELK to collect data from various security feeds and then cross-correlate that data to find advanced persistent threats. As with other SIEM systems, Bastille can seamlessly push data to ELK through our Streaming API that uses HTTPS webhooks.



View of Kibana showing event data from both Bastille and Elasticsearch Endpoint Security for a single endpoint. The view shows a correlation of the local Bluetooth events on the endpoint and the network Bluetooth events observed by Bastille. By viewing these together, it is clear not only that data was being exfiltrated over Bluetooth, but that also, with the Bastille data, it is clear where that data was being sent. (click to watch the demo video)

SPLUNK

Splunk is a popular SIEM used in production SoCs to parse, search, correlate, and visualize log and event data. Bastille provides a customized Splunk integration that uses the Bastille Device Event Stream API to send data from a customer's Bastille Fusion Center to Splunk. Customers have used the Splunk integration for a variety of simple tasks like searching, monitoring, and alerting, as well as more advanced multi-layer integrations. That is, once a customer's Bastille data is in Splunk, that customer can leverage the vast constellation of existing Splunk integrations to connect Bastille data with other sources of data or other external systems. The figure below shows a Dashboard from the Bastille Splunk App.



Incident Response (IR) and Endpoint Detection and Response (EDR) Systems

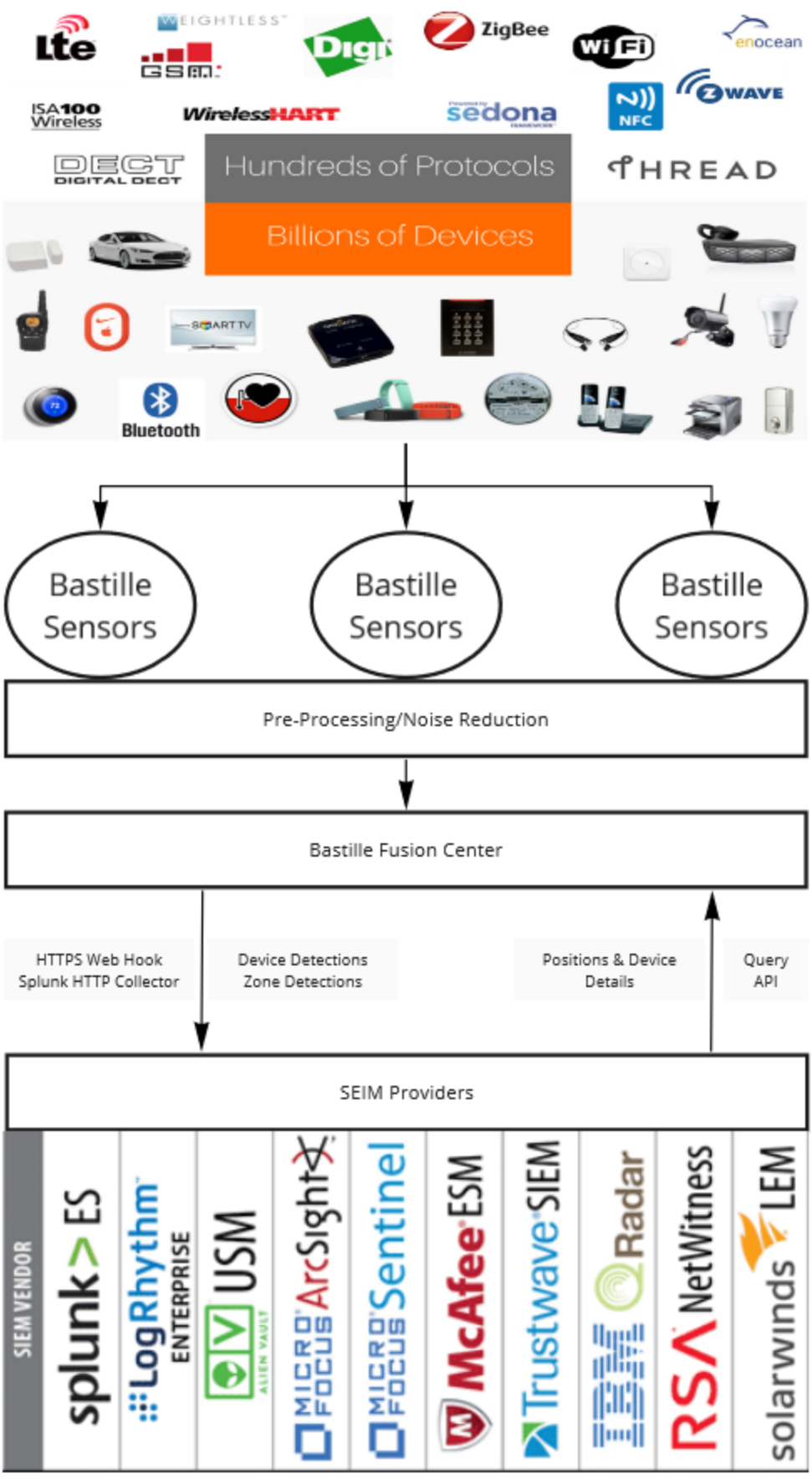
Incident Response and Endpoint Detection & Response addresses the need for constant monitoring and response to threats. When enhanced from Bastille's event stream, they can provide further context to a new attack, allowing security operations staff to respond faster. For response to incidents, applications such as PagerDuty are used for creating tickets and sending alerts to people and systems via email, text, slack, phone call, app push notifications and other mechanisms.

Bastille provides a PagerDuty integration for quick incident response. With the PagerDuty integration, our customers get the advanced RF detection capabilities that Bastille provides paired with the advanced ticketing, tracking, and notification engine provided by PagerDuty. With PagerDuty and Bastille you can, for instance, assign specific geofence breach alerts in Bastille to specific users in charge of adjudicating those breach events. Each has a comment thread so that actions and observations about an event can be recorded and saved for future analysis.

PagerDuty is just one example of an enterprise's EDR tools that are easily integrated with our open architecture.

SIEMs

The Bastille Device Event Stream API can be used to push data to any SIEM, not just Splunk. The Device Event Stream publishes events via a webhook, which is an open interface supported by every SIEM. Once the webhook is configured, Bastille event data will flow into the SIEM, and all of the power of the SIEM's data manipulation can be brought to bear to monitor an enterprise's RF environment. SIEM's, in turn, will typically take data from the Bastille Device Event Stream such as the time and location of the incident and cross-match it with personnel that have recently entered the area via the building access control systems, or has recently logged in to a nearby workstation. Common candidates for integration with Bastille include LogRhythm, QRadar, Exabeam, McAfee, and Securonix.

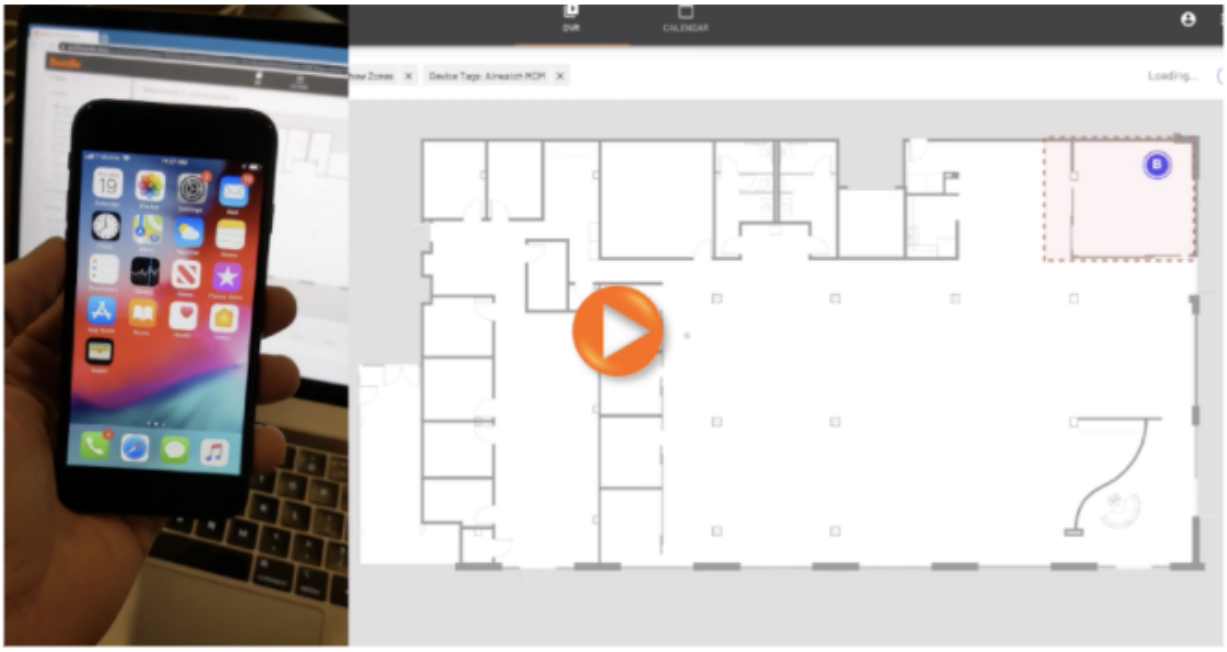

Hundreds of Protocols
Billions of Devices
Bastille Sensors
Bastille Sensors
Bastille Sensors
Pre-Processing/Noise Reduction
Bastille Fusion Center
HTTPS Web Hook
Splunk HTTP Collector
Device Detections
Zone Detections
Positions & Device Details
Query API
SEIM Providers
SIEM VENDOR
splunk> ES
LogRhythm ENTERPRISE
USM
MICRO FOCUS ArcSight
MICRO FOCUS Sentinel
McAfee ESM
Trustwave SIEM
Radar
RSA NetWitness
solarwinds LEM

Routers and Other Network Systems

The data that Bastille collects can be enriched by other external network device data and inventory systems. For instance, Bastille has demonstrated integrations with both Cisco Meraki and Mist access points, where Bastille data is enriched by the layer 4-7 data available for devices that have enrolled in the access point network. For example, an access point can decode the host name, the operating system, and other metadata that is only available at the application layer and is not observable at the PHY or MAC where Bastille does its sensing. With the Bastille Access Point Integration, Bastille customers can join the Bastille data, including hyper-accurate localization, with the access point information to provide very rich visibility in a device at all layers of the OSI stack.

MDM

Mobile Device Managers like VMWare Workspace One, Good, MobileIron, and others are popular tools for managing enterprise devices. One issue with all of these MDMs is that they can only geolocate devices at a building-level granularity. However, many use cases involve fine-grain indoor geolocation-based access control. With the Bastille MDM integration, customers can fuse data from their MDM system with Bastille RF data to enable these kinds of indoor granular location-based access control rules. . For instance, all MDM devices might be “whitelisted” devices that should not trip a geofence breach alert. Maintaining the list of these MDM devices is simple with the MDM integration as the data is updated in real time as the MDM data changes.



Demonstration of Bastille-MDM integration to remove the camera application from a phone when it enters a geofenced zone: link.

Cisco SecureX

Cisco SecureX connects security tools and data from customers' security portfolios to enable a simpler, more consistent experience across endpoints, cloud, network, and applications. Threat Response is a component of SecureX that aggregates intelligence from both Cisco security product data sources and third-party sources via APIs to identify whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious. Bastille is a Cisco Technology Partner and has an integration with SecureX. The integration allows for a security operator using SecureX to query their Bastille system to extract any and all information that Bastille has observed about a device.

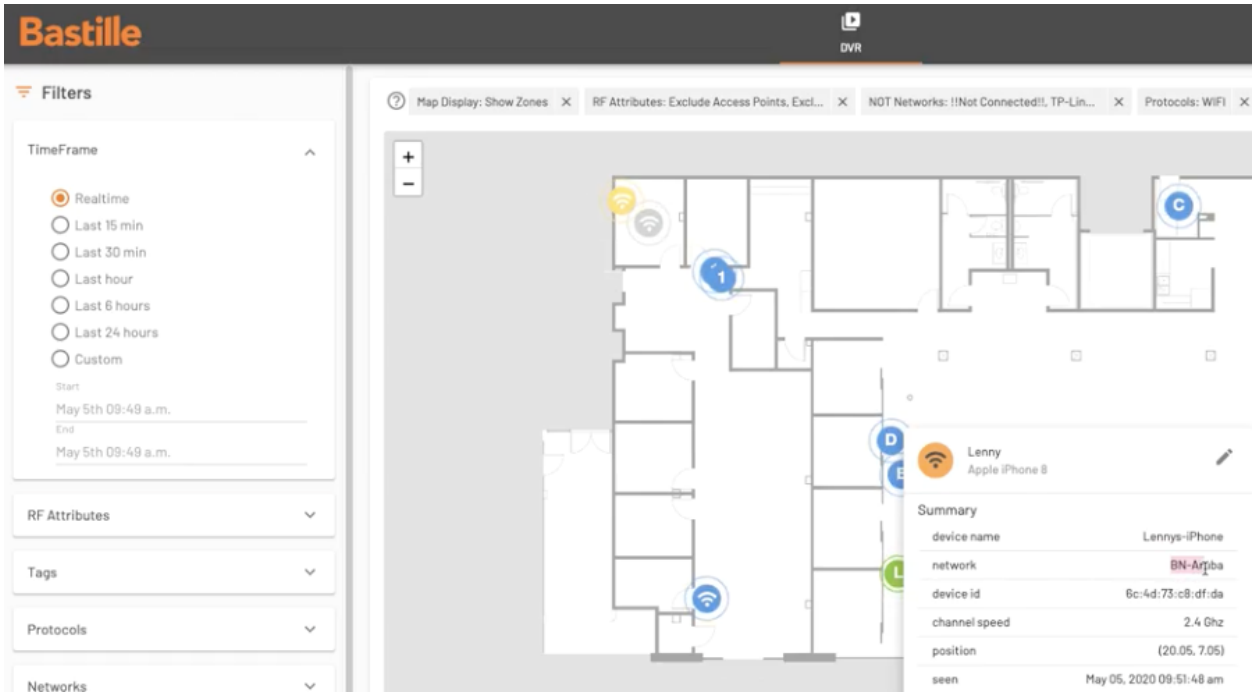
For example, there are a class of threats that involve both a wired network component as well as a RF component. An operator may understand that a device is on the enterprise wired network using their non-Bastille network monitoring tools. To understand whether that device also has a RF interface, an operator could click on a context menu in SecureX, which will poll Bastille's API and return any data available about RF interfaces present on that device.

Cisco SecureX-Bastille integration example shows how SecureX can be used to quickly pivot into Bastille to learn what RF emissions are emanating from a device: link.

Palo Alto Networks Demisto

Demisto is perhaps the most popular security orchestration, automation and response (SOAR) system on the market. Demisto uses playbooks and bots to determine what information is needed and to fetch it, and in some cases, to automatically respond in order to minimize what a human analyst needs to do. As an example, if an alert from an endpoint product indicates a user has a suspected phishing message, Demisto can run automatic logic for triage.

The Bastille-Demisto integration brings Bastille's data into the realm of Demisto's purview. So, for example, if Bastille detects a forbidden device has entered a facility, Demisto can be used to orchestrate creating an incident response ticket, sending a SMS to the operator on duty, NACing the device from the network, and tagging it in Bastille as unauthorized. Moreover, Demisto can be used for security investigations, where an operator or threat hunter can use the Demisto interface to pull Bastille data and wired network data together to find patterns.



Demisto-Bastille can orchestrate API connections between various Bastille and other systems. In this example, Demisto is the connection glue that polls Cisco Meraki Access Points for their MAC addresses and then tags those MAC addresses in Bastille: link.

Zero Trust and Network Access Control (NAC) Integration

Zero Trust centers on the belief that we should not automatically trust anything inside or outside our perimeters. Instead of trusting a device's authenticity, we must continuously verify anything and everything that may attempt to connect to systems before granting access.

Bastille provides full visibility into devices as they enter and exit your facilities. While devices may authenticate, many may not, and yet they are still inside your buildings, forming a shadow IT infrastructure capable of data capture and exfiltration. These devices should be under the same policy as your authorized devices that use Zero Trust policies. Bastille provides both the visibility and data feeds that enable you to implement and automate your Zero Trust policies across these otherwise-invisible devices.

Integration of Bastille with your NAC system to ensure Zero Trust policies are maintained
Bastille will show you the authorized and unauthorized devices operating in or close to your environment. When integrated with a NAC such as Cisco ISE, Forescout, or Aruba ClearPass this enables a complete Zero Trust policy to be maintained over all devices, whether they are already known to be using facility Wi-Fi, or radio systems beyond existing Zero Trust policies, such as Bluetooth, Cellular and IoT devices.

Bastille + ClearPass: Real-Time Geofence NAC Policy Enforcement

Bastille:

Detect and accurately locate authorized and rogue Cellular, Bluetooth, BLE, WiFi or IoT devices

Bastille + Aruba ClearPass:

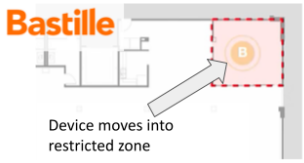
Example Rule: Cut off network access for devices that breach a Geofence.

Workflow: Bastille identifies the device location and applies the geofence rule. Aruba ClearPass applies the Network Access Control.

Example Devices Bastille Detects:

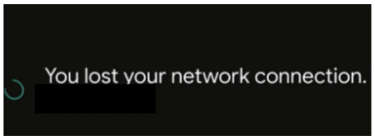
Integration Workflow Example:

1) Device detected in Geofence by Bastille



2) Bastille sends alert to ClearPass

3) ClearPass removes device's network access



Bastille

14

Cisco Identity Services Engine (ISE), Forescout and Aruba ClearPass are now broadly deployed to permit policy based network access control, which can be extended to RF based device via integrations with Bastille

APPENDIX 1: Bastille Unique, Trade Secret and Patented Technology (32 Issued)

Bastille Patent Summary

Cellular

Unique Technology and Customer Benefit

- Digital detection of phones
- Association of phones with their carrier-assigned temporary identifier
- Ability to differentiate co-located phones that are using the same band
- 1 to 3 meter accurate cell phone localization
- Continuous phone visibility (not just visibility when a phone joins a cell)
- Phone position and trajectory over time
- Phone-to-tower network connection data volume detection
- Automated smart cell tower scanning and monitoring
- Fast channel scanning for phones

Cellular Patents

US #10,473,749 - Localization of Mobile High-Speed Wireless User Equipment from Uplink Channels

- Derive position estimate on signal strength clusters using physics/DSP-based model.
- Unsupervised machine learning model for grouping signal strength clusters.

US #10,564,251 - Localization of Mobile High-Speed Wireless User Equipment from Downlink Channels

- Use both uplink and downlink cellular signal information to distinguish cellular users
- Group the signals from each user and localize the user devices

US #10,567,948 - User Equipment Identification from Mobile High-Speed Wireless Uplink Channels

- Estimate the number of RF users in the vicinity of a sensor using machine learning to cluster spectrum features
- Localize users with only the uplink signal information

US #10,705,178 - Localization Calibration and Refinement in High-Speed Mobile Wireless Systems

- Mechanisms to use a mobile autonomous robot to collect RF signal strength and feature data in a facility
- Machine learning techniques to use the collected data to refine localization models

US Application [In Progress] - Mobile Communications Base Station Site Survey

- Cellular Tower Identification and Survey

Bluetooth (BT) & Bluetooth Low Energy (BLE)

Unique Technology and Customer Benefit

- Continuous simultaneous monitoring of all 79 BT Classic channels and all 40 BLE channels. This allows Bastille sensors to see all BT/BLE network connections even as the BT/BLE devices hop frequencies every 625 microseconds.
- Network & Device pairing alerting and monitoring for BT Classic
- Network & Device pairing alerting and monitoring for BLE
- Comprehensive visibility with no active transmission of inquiry packets. Bastille sensors are completely passive, but still see BT/BLE better than active systems.
- BT Classic inquiry packet detection and alerting
- BLE inquiry packet detection and alerting
- BT/BLE connection type detection using machine learning traffic signatures. For instance to differentiate a BT audio tether from a data tethering connection

BT and BTLE Patents

US Application 16/412,411 - Traffic and Threat Classification for Short-Range Wireless Channels

- Machine learning training and inference to determine the type of traffic in a bluetooth piconet

US Application 16/785,644 - Passive Determination of Pairing and Channel Parameters for Short-Range Wireless Communications

- Inference of pairing connections between Bluetooth low energy devices
- Alerting on the existence of a pairing event

WiFi

Unique Technology and Customer Benefit

- Smart scanning of all WiFi channels including 80MHz WiFi 6 channels
- Bandit search mechanism to optimize dwell time in each channel to maximize WiFi device detection
- Detection of all WiFi access points and networks
- Network map of all WiFi networks including clients connected to each AP
- WiFi Direct detection
- Detection of unconnected WiFi clients
- Device fingerprinting to detection device characteristics like device type

WiFi Patents

US #10,338,191 - Sensor Mesh And Signal Transmission Architectures For Electromagnetic Signature Analysis

- Distributed and adaptive sensor RF hop scheduling based on the signals in the environment
- Mechanisms to more efficiently scan for RF signals using bandwidth-constrained sensors

US #9,739,868 - Electromagnetic Signature Analysis For Threat Detection In A Wireless Environment Of Embedded Computing Devices

- Alerts based on RF network behavior of devices
- Over-the-air RF threat identification and alerting

Localization and Geofencing (for All Protocols)

Unique Technology and Customer Benefit

- Network and Device Location within 1 to 3 meters
- Multilateration signal-strength based algorithm that approaches the theoretical limits of signal-strength based RF device geolocation
- RF Tomographic algorithm to infer the shadow loss field of a facility in order to improve the multilateration location estimation
- Kalman and particle filter smart device trajectory optimization to maximize location accuracy of moving devices
- A machine learning model that incorporates human position correction information to improve location accuracy
- Alerts based on device position in a floorplan
- Alerts based on the relative proximity of two devices with respect to each other
- Overlay of RF device positions on AR and VR visualization headsets
- Location estimation of a single device using the RF emissions from multiple radios on that device. For example, using both Bluetooth and WiFi emissions from a single phone to improve the phone's position accuracy.

Localization and Geofence Patents

US #9,485,266 - Security measures based on signal strengths of radio frequency signals

- Infer position and trajectory of devices based on their RF emissions
- Alert using thresholds on the position and trajectory of devices

US #9,485,267 - Anomalous behavior detection using radio frequency fingerprints and access credentials

- Alerts on IT policy violation based on observations from RF devices and personas
- Tailgating detection and geofencing using RF signatures

US #9,551,781 - Efficient localization of transmitters within complex electromagnetic environments

- Bastille RF signal localization algorithm
- Includes elements of kalman filters, particle filters, and tomographic shadow loss field estimation

US #9,560,060 - Cross-modality electromagnetic signature analysis for radio frequency persona identification

- Grouping multiple radios on a single device into a persona
- Associated multi-radio alerting and analytics

US #9,736,175 - Anomalous Behavior Detection Based on Behavioral Signatures

- People analytics and alerting using RF data; enforce device-proximity rules

US #9,945,928 - Computational Signal Processing Architectures For Electromagnetic Signature Analysis

- Distributed sensor collection and analysis system/architecture for RF signal detection
- Mechanisms for storing, aggregating, and distributing RF signal information

US #9,880,256 - Diverse Radio Frequency Signature, Video, and Image Sensing for Detection and Localization

- Overlay RF device localization on real-time video feeds
- Combined RF-video forensic analytics to find devices and people

- Refine localization model using feedback from the position of objects identified in a video feed

IoT

Unique Technology and Customer Benefit

- Library of FPGA-based protocol decoders for more than a dozen IoT protocols.
    - Cellular (LTE, GSM, UMTS) (3 protocols)
    - Wi-Fi 802.11b - 802.11ax (WiFi 6) (5+ protocols)
    - Bluetooth Classic / Bluetooth Low Energy v1 - v5 (2 protocols)
    - 802.15.4 Protocols - Zigbee, RF4CE, Thread, 6LoWPAN, WirelessHART, ISA100.11a, and proprietary variations (6+ protocols)
    - DECT (1 protocol)
    - goTenna (1 protocol)
    - Mouse Keyboard (MK) - Logitech MK, Amazon MK, Lenovo (4 variants) MK, HP MK, Dell MK, Generic MK (9+ protocols)
- Detection of long-range backhaul attacks like ATM card skimmer detection.

IoT Patents

US #10,104,098 - Electromagnetic Threat Detection And Mitigation In The Internet Of Things - 2

- Cellular and skimmer focused attack detection, alerting, and analytics
- Baselining an RF environment and then alerting on deviations from the RF signal baseline

US #10,122,736 - Ground And Air Vehicle Electromagnetic Signature Detection And Localization

- Drone detection and localization through RF signal analysis
- Drone fingerprint database for threatening drone signals and physical trajectories

Spectrum Analysis

Unique Technology and Customer Benefit

- Spectrum device fingerprinting to differentiate devices where no digital decoder for the device exists
- Blind classification of a device and its modulation using only analog spectrum measurements
- Smart spectrum sweeping algorithms to optimize dwell times in each band in order to maximize signal detection
- Spectrum persona estimation to group spectral signatures from a signal device even if the device is emitting signatures on multiple radio interfaces.

Spectrum Patents

US #9,591,013 - Radio frequency fingerprint detection

- Identify a device by its RF signature and signal strength variations
- Maintaining and cross-referencing a device fingerprint database for device data enrichment

US #9,625,564 - Blind Signal Classification And Demodulation In A Multimodal Radio Frequency Environment

- Machine learning to determine characteristic of a device using RF features; e.g. modulation type, manufacturer, hardware components
- Identify RF threats using blind signal classification

US #9,635,044 - Electromagnetic Persona Generation Based on Radio Frequency Fingerprints

- RF Persona generation using only RF-sensed data/events through device correlation analysis
- RF Persona to entity association with time series cross-correlation

European Patents

In addition to US patents, we also have the following EU patents issued that cover roughly the same intellectual property as our US patents:

- EU #3,149,597
- EU #3,149,986
- EU #3,285,196
- EU #3,296,917
- EU #3,287,934
- EU #3,327,609
- EU #3,276,527
- EU #3,296,916