Bastille

Security for the
Internet of Radios

Bastille

bastille.net

Bastille

Security for the Internet of Radios

Internet of Radios

Gartner predicts that there will be 20 billion devices connected by 2020. Cisco forecasts the "Internet of Everything" market impact at $19 trillion by the same year. And what do 15 billion (75%) of these devices have in common? ... Radios!

We all know Wi-Fi uses radio to communicate, but so do the other 99 plus protocols that make up the world of mobile, cellular and the Internet of Things (IoT). All these new radio enabled devices bring with them new invisible threats. Enterprises will need to be able to react to new threats entering their environments through the Internet of Radios.

We often hear about the dangers of the Dark Web. The Internet of Radios is not merely "Dark" it's invisible!

Forward leaning security professionals have come to realize that the new attack vector presented by the Internet of Radios is also a powerful new tool they can harness to provide situational awareness of threats inside their environment.

Bastille provides full visibility into the Internet of Radios inside an enterprise's corporate airspace. Through its patented software-defined radio and machine learning technology, Bastille senses, identifies and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger to customer data and network infrastructure.

Bastille: Security for the Internet of Radios

Bastille is the first company to enable enterprise security teams to assess and mitigate the risk associated with the growing Internet of Radios. Bastille's patented software and security sensors bring visibility to devices emitting radio signals (Wi-Fi, cellular, wireless dongles and other IoT communications) in your organization's airspace.

Bastille's technology scans the entire radio spectrum, identifying devices on frequencies from 60MHz to 6 GHz. This data is then gathered and stored, and mapped so that you can understand what devices are transmitting data, and from where in your corporate airspace. This provides improved situational awareness of potential cyber threats and post-event forensic analysis.

Bastille Protects against Threats

The Bastille Research Team proactively monitors for new radio-borne threats. Their breakthrough research and discoveries such as MouseJack and KeySniffer help to keep not just Bastille clients, but the larger ecosystem safe. Each month, Bastille Research reports on the most prevalent and most pernicious attacks.

KEY BENEFITS

- SENSE
  Continuously monitor your corporate airspace across the entire wireless spectrum from 60MHz to 6GHz
- IDENTIFY
  Detect vulnerabilities and malicious behavior on wireless, cellular and IoT devices
- LOCALIZE
  Pinpoint on a floorplan of your premises where the malicious device is, and where it has been
- OPEN STANDARDS
  API for integration with existing SIEM and Analytic systems

KEY FEATURES

- NEW SITUATIONAL AWARENESS
  Know what's in your environment and detect unauthorized devices
- PREVENT DATA EXFILTRATION
  Secure your customer data and intellectual property
- SAVE SECURITY TEAM TIME
  Enable staff to quickly know where to go and what to look for in real time and forensically

TOP 10 INTERNET OF RADIOS VULNERABILITIES	
1. **ROGUE CELL TOWERS** *('stingrays', 'IMSI catchers')*	Rogue cell towers are used to hijack cellphone connections, allowing attackers to listen to calls and read texts. An attacker can even push malware to a vulnerable phone to hack it. A common use of Rogue Cell towers is to break 2-factor authentication
2. **ROGUE WI-FI HOTSPOTS** *(and Wi-Fi pineapples)*	Rogue Wi-Fi access points (including Wi-Fi Pineapples) can impersonate legitmate Wi-Fi networks, and can be used for Man-In-The-Middle attacks to sniff network traffic and steal credentials. Can someone in your building by-pass all your Wireless Intrusion Detection Systems by opening a Wi-Fi hotspot which detours your data around your expensive Wi-Fi anomaly detection?
3. **BLUETOOTH DATA EXFILTRATION** *(tethering)*	Bluetooth tethering can be used to pair a network device with a cellular data path (e.g. 4G LTE) which bypasses your traditional network security. How do you detect when someone starts Bluetooth tethering in your building? How do you avoid false alarms when the Bluetooth is only being used to connect a headset?
4. **EAVESDROPPING/ SURVEILLANCE DEVICES** *(e.g. conference room bugs)*	Voice-activated FM & GSM bugs and other radio bugs cost as little as $20 on eBay®.
5. **VULNERABLE WIRELESS PERIPHERALS** *(mice/keyboards)*	Low-end wireless keyboards allow sniffing all keystrokes out of the air from 250 feet away because they do not implement encryption. A vulnerable wireless mouse dongle can expose the computer to which it is connected to an external attack through keystroke injection. Once the computer is itself compromised, it can expose the larger network to insider attacks.
6. **UNAPPROVED CELLULAR DEVICE PRESENCE**	(2G GSM, 3G WCDMA, 4G LTE) It's one thing to have a "no cell phones in this area" policy. It's another thing to detect policy violations!
7. **UNAPPROVED WIRELESS CAMERAS** *(using Wi-Fi and other protocols)*	Inexpensive wireless cameras are great for security when your security department installs them. But if someone else installs them then they can be used to plan security breaches. Know every camera operating in your facility and whether it works for your security team or someone else.
8. **VULNERABLE WIRELESS BUILDING CONTROLS** *(e.g. default credentials)*	Many new pieces of equipment ship with two consoles: Ethernet and "Radio Ready" Consoles. You know about your Ethernet console but is there another console on your equipment set up with default configuration and broadcasting for instructions?
9. **UNAPPROVED IoT EMITTERS**	New thermostats and building sensors often have multiple data radios. Wi-Fi is the one you know about. But is your sensor also transmitting on other frequencies like Zigbee (short range) or LORA (up to 1 mile range)? What data is beaming down the street that you don't know about?
10. **VULNERABLE BUILDING ALARM SYSTEMS**	Many Window, Door and Motion detectors can be ordered to "pay no attention to the man climbing in the window" by someone carrying a $10 radio jammer, or $300 Software Defined Radio, which can also simulate any alarm event. Security professionals need to be alerted when someone attempts to jam any part of their alarm system.

These vulnerabilities are exploited individually and combined to access files and customer data, listen into and record sensitive conversations or take over industrial control systems. And just because a CISO didn't approve radio enabled devices to be used inside the company, it doesn't mean they aren't installed or brought in daily as wearables.

The "Radio Ready" Phenomena: many pieces of equipment inside the enterprise are "wired" into the secured network or connected by 'secure' Wi-Fi but also have other radio-capabilities, which might not be in use by the enterprise – or even known by the enterprise – but can be exploited by a hacker. Those devices are, more likely than not, using the default username and password.

How It's Deployed

Bastille is delivered as a SaaS (Software as a Service) solution. There is no separate purchase of sensor hardware, Bastille installs the number of sensors you need for the solution you order.

Bastille's proprietary sensors are usually installed in the space above the dropped ceiling of the area to be protected. The sensor units are powered by POE (Power Over Ethernet). The sensors are constructed of a special custom polymer which both permits them to perceive the full spectrum of radio emissions, but is also rugged enough to allow them to be placed inside the false-ceiling plenum of a building, and they have been UL, FCC and CE certified to safely exist in that environment. Where you prefer, the sensors can be installed below the ceiling or on desktops and cubes.

The number of sensors required depends on the nature of the building to be monitored and the use case (problem) which is being solved. A good rule of thumb is that sensors are deployed in about the same density as you would use to deploy Wi-Fi access points.

Installation takes minutes, and does not require extremely close sensor positioning or calibration, as all the configuration is done post installation via the Bastille platform in our Secure Virtual Private Cloud.

Bastille's Differentiating Technology

At Bastille's core, to protect organizations against the threats which already exist and the new threats which are emerging via the radio spectrum there are 3 areas of technology across which Bastille has 14 patents approved and pending. These technologies permit Bastille to SENSE, IDENTIFY & LOCALIZE threats as follows:

SENSE

Collaborative Bandit Sensing is Bastille's patent pending technology[1] to quickly and accurately scan the spectrum for emitters and threats. Collaborative Bandit Sensing utilizes a variant of the Multi-Armed Bandit (MAB) problem to allocate sensor time watching various parts of the spectrum. The classic MAB problem is one where an actor has to balance exploitation of a reward function with exploration of other possible activities that might lead to a higher payoff. The challenge is that exploration has opportunity costs, while premature exploitation can lead to a low payoff rate. In Bastille's context, our sensors are intelligently making distributed decisions about when they should continue to observe a known signal (exploitation) versus scanning another part of the spectrum to find unknown signals (exploration). Bastille has solved this problem by combining a stochastic model of the signal environment, an array of intelligent distributed search algorithms, and collaborative optimization based on gossiping algorithms.

Researchers Hack Air-Gapped Computer with Simple Cell Phone

Researchers have devised a new method for stealing data – using the GSM network, electromagnetic waves and a basic low-end mobile phone.

—WIRED, 7.27.15

Hackers show off long-distance Wi-Fi radio proxy at DEF CON

The device uses the 900MHz band, but hides the data in the back-ground radio noise.

—PC WORLD, 8.10.15

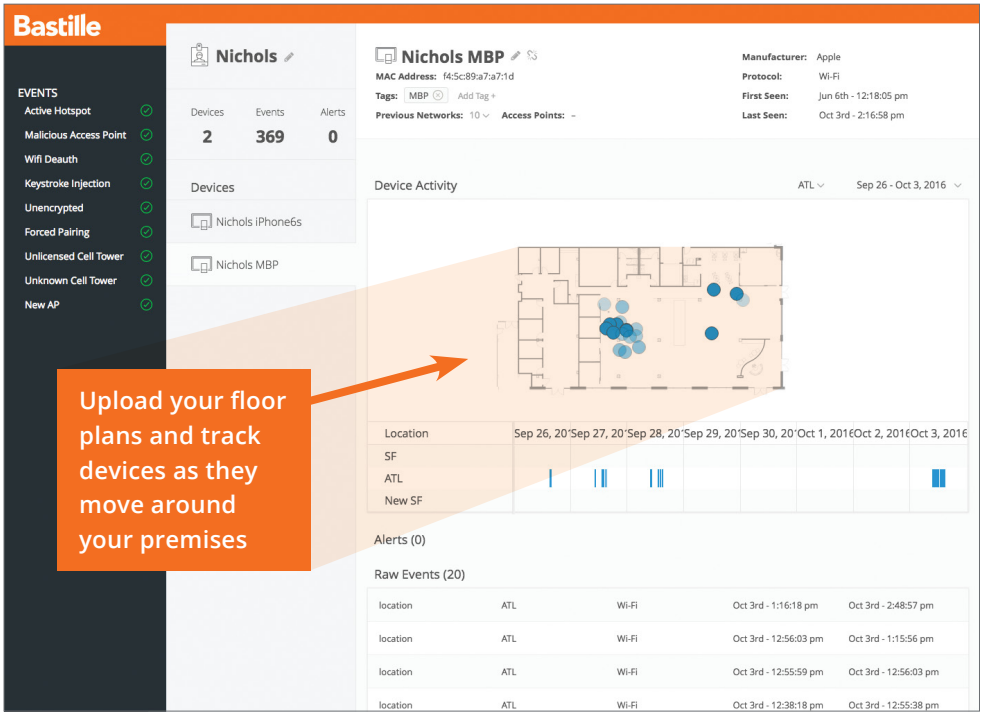
IDENTIFY

Bayesian Device Fingerprinting is a suite of patent pending technology[2] that Bastille uses to detect and identify devices in an Enterprise airspace. Bayesian Device Fingerprinting relies on Probabilistic Graph Models of possible device characteristics to track and estimate device meta-information. The probability states are updated as new observations are made both in radio frequency space and through other input systems like access control, MDM, video surveillance, or SSO. With Bayesian Device Fingerprinting, Bastille Enterprise can resolve emitter, device, and people-device entities to produce never-before-seen situational awareness of your RF and physical space.

LOCALIZE

Distributed Tomographic Localization is Bastille's patent pending technology[3] to provide actionable position information of all emitters in your corporate airspace. Like Computer Tomography (CT scans) uses path loss in the medical world, Bastille uses passive Radio Tomography in the corporate airspace to account for the location of walls. This allows Bastille to locate radio emitters much more accurately than other technologies to 1 metre of accuracy.

Bastille's approach to localization uses two unique innovations to achieve industry-leading location accuracy. The first is Distributed Tomography, which allows Bastille to estimate the positions of the walls and other objects in the environment which we then incorporate into our localization model. The second is Bayesian filtering coupled with Ensemble Machine Learning algorithms to do precise perimeter detection. Bastille Enterprise customers can use Distributed Tomographic Localization to geo-fence spaces and set localization based alerts for sensitive areas.



100+ PROTOCOLS

The Internet of Radios is comprised of more than 100 communication protocols, many of which are 'Proprietary' and have not been hardened from a security perspective by input from the community or reviewed by standards committees.

Organizations are deploying Bastille to protect their most valuable assets. Bastille's ability to SENSE, IDENTIFY and LOCALIZE threats makes it valuable for a range of use cases across the enterprise.

SOLUTIONS	
C-SUITE OFFICES AND MEETING ROOMS	The C-Suite has the most access to valuable information about strategy, financial results, customers, partners, employees, and intellectual property. In particular, executive boardrooms, suites, and even homes hold, carry, and publish very sensitive information in both oral and written format. Whether you are a Fortune 500 corporation or a mid-sized business, keeping the C-Suite protected is a top priority.
FACILITY/CAMPUS HEADQUARTERS	Many organizations are interested to understand employee behavior and what types of devices are entering their offices and campuses. Large organizations with sensitive data want to know the movements of devices in their environment in order to get a holistic view of all the activity in the radio frequency spectrum within their combined premises.
CALL CENTERS	Call Centers deal with very sensitive customer data such as personally identifiable information including social security numbers, bank financial records such as credit card details, and the like. The top priority is keeping that data protected. The attack vector that Call Centers are most vulnerable to are their employees and the devices that they bring along.
DATA CENTERS	The Data Center contains the crown jewels for an organization. In addition to the IT equipment we think about, Data Centers are loaded with Industrial equipment (chillers, lighting, power, etc.) and often frequented by contractors. Many vectors expose a Data Center to risk, and as a result, Data Center security has long been the recipient of significant budget and attention from both physical and cyber security organizations. Data Centers have the highest physical security for any organization, often employing mantraps, biometrics, and expanded video coverage. On the cyber side, large budgets are deployed for endpoint security and intrusion prevention for the wired infrastructure. However, there is an attack vector capable of penetrating Data Center walls and bypassing the firewalls, namely radio frequency (RF) based attacks.

Bluetooth and Its Inherent Security Issues

Bluetooth flaw in native security can subject a user to threat vectors: default configuration, theft and loss, eavesdropping and impersonation, person-in-the-middle attack, piconet/service mapping, and denial-of-service attacks.

—SANS

Researchers Find Major Security Flaw with ZigBee Smart Home Devices

By making it easier to have smart home devices talk to each other, many companies also open up a major vulnerability with ZigBee that could allow hackers to control your smart devices.

—ENGADGET, 8.7.15

Bastille Customer Testimonial

Jon Miller: Chief Research Officer, Cylance

VISIBILITY

"At Cylance, we've been using Bastille for a little over a year now. For me, the promise of Bastille to Cylance was visibility. We were going through quarterly audits of our corporate headquarters looking for covert listening devices, rogue access points, anything that could be used by an attacker to bridge the gap between the physical and the data layer and extract information out of our enterprise. The reason that we went with Bastille was that Bastille gave us the ability to do real time inspection of that space, and instead of dealing with something after it's been there for a while and you find it. We can detect it and remediate it the second it gets turned on."

"Bastille gives Cylance the ability to, in real time, detect something that is potentially malicious or unwanted on our network and remediate it before we have to worry about the threat of exfiltration."

RADIO (RF) IS THE NEW FRONTIER

"As enterprises continue to grow and we're getting new smart devices, the boundaries are essentially eroding on a traditional perimeter. A firewall's not going to protect you from an RF based attack and Bastille is the only tech on the market that gives an enterprise the ability to not only monitor but protect all of the RF airspace at the same time."

ADVANTAGE OVER SOPHISTICATED ATTACKERS

"One of the reasons that I'm very fond of Bastille is normally when you're dealing with a sophisticated attacker, they're not going to attack you with the same attack that's been around for 10 years. They're funded, they're skilled. They can infiltrate things like supply chains. They can infiltrate corporate networks. And having that next generation of technologies where the attackers themselves don't realize that you're doing protection or monitoring there, essentially gives you a leg up. It gives you the ability to detect an attacker via a vector that they're not aware that you have capabilities to protect."

TRADE-SECRETS CAN BE EXFILTRATED BY VOICE AND DATA

"Any type of covert listening device that could monitor our data science team or bridge the gap between our network and start to ex-filtrate trade secrets out over RF is a major, major concern. Not just from a customer privacy perspective, but from a competitive advantage. If you can't keep a hold of your company's intellectual property, it's gonna start popping up in competitive products."

"Bastille was actually able to identify a bunch of vulnerable RF devices in our network on the initial POC, and we were able to go around and get everything replaced."

Forbes

The IoT Gives Criminals Superpowers

"The Internet of Things will give superpowers to a new class of entrepreneurs able to forge the future of connected communications. Unfortunately, some of them will be criminals.

Internet of Things security has been a pressure point among researchers for a while. In an effort to keep costs low and the learning curve lower for neophyte consumers, manufacturers have rushed connected things to the market. Many have generic firmware and, worse, default passwords. Creepy hackers have easily commandeered everything from home security cameras to baby monitors. The jump to using connected devices as weaponry was just a matter of time.

In the [James] Bond films, despite villain superpowers, the forces of good always win. Then again, there is usually just one villain and they can't rent superpowers for just $30 a month. Cyber security trouble is not going away."

—FORBES, 10.11.16

Bastille Service Versions

We provide service versions which you can run for a week, a month or full time for continuous protection. All solution versions will provide:

- Inventory: Show radio capable devices in the environment
- Insight: Detail the threat capabilities of those devices
- Threat Scan: Alert on active threats

SERVICE VERSION	OVERVIEW
BASTILLE ENTERPRISE Full solution deployment from one floor to enterprise wide. Bastille installs the sensors.	• Sensors installed throughout the area you want to secure in the same density as Wi-Fi access points, minimum 4 sensors per area for premium threat localization • Discovers and LOCALIZES device/threat source
BASTILLE AUDIT A one-month audit of the airborne threats in a single part of your environment up to 25,000 square feet. Bastille installs the sensors.	• Up to 10 sensors • 1 month Audit and detailed report of everything we find • Discovers and LOCALIZES device/threat source
BASTILLE DESKTOP A one week audit of the airborne threats in a small area e.g. 2,500 square feet. Does NOT localize threat. No installation required, sits on desktop.	• 1 sensor in 1 location • 1 week Audit and detailed report of everything we find • Discovers but CANNOT LOCALIZE device/threat source (multiple sensors needed for localization)

Bastille Research Team

The Bastille Research Team is a globally renowned group investigating threats on the cutting edge of radio based security. To learn more about the latest vulnerabilities from the Bastille Research Team, or to subscribe to their Threat Newsletter, go to bastille.net/research.

[1]*USPTO APP #20160127404,* [2]*USPTO APP #20150348341,* [3]USPTO APP #20160127931, and eleven additional patents pending.

COMPANY RECOGNITION

Gartner Cool Vendor 2016

CRN SECURITY 100 2016

RED HERRING N. AMERICA 100 WINNER

CRN The 2015 Internet of Things 50

RSAC Innovation Sandbox 2016 FINALIST

2016 SILVER STEVIE® WINNER AMERICAN BUSINESS AWARDS

10 Innovative Network Security Startups InformationWeek NETWORK Computing

BEST PRODUCT WIRELESS SECURITY SOLUTION 2016 CDM

NETWORKWORLD 10 More Security Companies to Watch 2015

TEAM AWARDS

- Darpa Spectrum Challenge
- Darpa Shredder Challenge
- GNU Radio Hacking Challenge

ABOUT BASTILLE — Launched in 2014, Bastille is the leader in enterprise threat detection through software-defined radio. Bastille provides full visibility into the known and unknown mobile, wireless and Internet of Things devices inside an enterprise's corporate airspace–together known as the Internet of Radios. Through its patented software-defined radio and machine learning technology, Bastille senses, identifies and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger to network infrastructure. For more information, visit www.bastille.net and follow on Twitter @bastillenet.

Bastille

497 LAKE AVE, SANTA CRUZ, CA 95062
INFO@BASTILLE.NET / 800.530.3341