Bastille RESEARCH

Wireless Zero Trust

Dr. Brett Walkenhorst, CTO, Bastille

Table of Contents

Zero Trust	2
The Wireless Problem	2
Bringing Visibility to the Invisible Wireless Attack Surface	3
Solving the Wireless Problem	5

© 2024 Bastille Networks. All Rights Reserved. All Other Trademarks And Logos Are The Property Of Their Respective Owners

Zero Trust

Zero Trust has been an important paradigm for advancing network security for almost 15 years, incorporating tenets that move beyond perimeter-based control toward a multi-layered approach that seeks to minimize risk in the modern world. Although the paradigm is complex, the basic idea behind Zero Trust is to shift our mindset from defending our perimeter to assuming an attacker has already penetrated it. This requires us to bring visibility to our network, limit access to network resources, and automate the response to incidents aided by analytics.

As a security community, we are making progress implementing this paradigm shift, but one key area that is often overlooked is the wireless attack surface of our networks. Without addressing the wireless problem, our Zero Trust posture is incomplete.

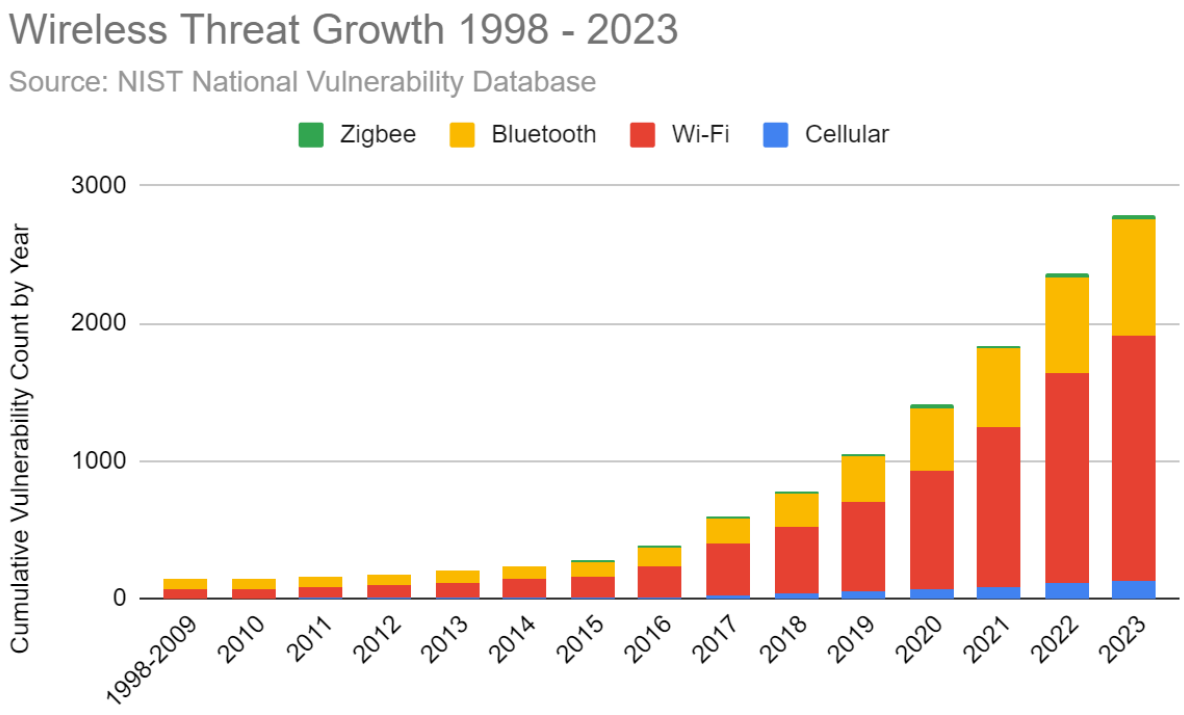
The Wireless Problem

Wireless devices number in the tens of billions worldwide, and their presence continues to grow. Protocols include Wi-Fi, cellular, Bluetooth, IoT, and others. Much of this wireless space is not monitored or even visible within our security tools. Devices may include shadow IT equipment, industrial control systems (ICS), personal/corporate smartphones, peripherals, wearables, and many more. All of these devices have the potential to connect to our networks in some way, and yet their wireless interfaces are largely unmonitored. In our efforts to shift to a Zero Trust mindset, it is critical that we bring visibility to these wireless technologies in addition to the wired components of our networks.

Wireless devices are ubiquitous. They utilize electromagnetic waves to communicate with each other and with network infrastructure. These waves travel at the speed of light; they penetrate walls and other physical barriers, bypassing our physical security perimeter; and they are invisible to the eye. As critical 1's and 0's modulate these invisible waves, we must find ways to make them more visible to defend against the many vulnerabilities that exist within these wireless protocols. Nearly 3,000 wireless CVEs have been published to date. And that is only what has been discovered. The trend of these discoveries is one of exponential growth. Clearly, the wireless attack surface is an area of growing concern.

The forms of wireless-based attacks vary widely. They include machine-in-the-middle (MitM) attacks to crack credentials and/or compromise clients/peripherals; denial of service (DoS), eavesdropping, malware injection, data exfiltration, and many more. Many affordable tools (both hardware and software) exist that have lowered the barrier to entry for people to conduct such attacks. Attack devices include Wi-Fi pineapples (Evil Twin attack devices), O.MG and USB Ninja cables and Wi-Fi Rubber Duckies (wireless-controlled keystroke injection and exfiltration cables/dongles), wireless network interface controller (NIC) dongles, Bluetooth development

kits/dongles, software-defined radio kits/dongles, and more. The more sophisticated devices are typically around $100, but many very capable devices can be purchased for $10 or less.



Bringing Visibility to the Invisible Wireless Attack Surface

Wireless signals use electromagnetic (EM) waves to communicate. EM waves are invisible, but electronic systems can be built to both create and detect them. To make those invisible waves visible, then, we need a suitably capable detector. While radio technology has been around since the late 19th century, modern developments involving higher frequencies and digital modulation have made wireless communication increasingly efficient and effective, allowing us to use different bands of the EM spectrum to support tens of billions of devices speaking many different protocols. A wireless detection system must be equally capable by employing modern tools like software-defined radio technology and highly-capable processors to digitally demodulate and decode the many wireless packets from many protocols.

The Bastille System

Bastille uses broadband, multi-channel software-defined radio sensors to detect multiple wireless signals simultaneously. The sensors digitally decode the headers of many wireless packets in parallel to extract metadata for individual wireless detections, and then feed their data to a central server to localize the emissions in space. In this way, the system can detect and locate all wireless emissions within a facility. This gives a user visibility into the wireless signals in terms of their temporal, spatial, and behavioral characteristics. But visibility is only the first step. To enable Zero Trust, we need to add analytics and automate the response.

Analytical tools transform data into actionable insights. Applied to wireless data, we need to identify unhealthy behaviors in the wireless transmissions, classify their severity, and provide tools for users to take action. Dimensions over which we can analyze wireless devices include time, space, and many dimensions of behavior. The metadata available from the wireless packet headers offers a rich set of data from which we can infer connectivity, device information, data transmission volume, and much more. Bastille's back-end processing leverages the rich set of data provided by the sensors to identify malicious behavior and improper security settings.

Once a vulnerable behavior is identified, the Bastille system can alert on that behavior and automate the response if appropriate. Such automation may include shutting off a device's network access, disabling certain functions of the device, populating an alert list in a security operations center (SOC), issuing an incident response alert, focusing physical security cameras on a specific area, flashing a light, locking a door, and many other actions. To enable those kinds of responses, Bastille's wireless detection system readily integrates with a host of other security tools including security information and event management (SIEM) systems, security orchestration automation and response (SOAR), network access control (NAC) systems, unified endpoint management (UEM) systems, physical access control systems, etc.

Key Differentiators

In addition to the above capabilities, Bastille offers some key differentiators including the following:

- Bastille differentiates among individual 4G/5G cellular devices and localizes them based on their traffic channels
  - Other wireless detection systems detect only certain control channel packets such as a random-access channel (RACH) packets, but these are few and far between, so they miss most of the relevant data

- Bastille detects and locates Bluetooth devices when they're connected to other devices
  - Bluetooth signals hop in frequency when they're in a connected state, so many single-channel sniffers aren't capable of seeing them
  - The inability to detect connected Bluetooth devices is a big limitation from the perspective of mitigating data exfiltration threats
  - Bastille is the only wireless detection system on the market with this capability
- Bastille provides accurate localization of indoor signals
  - Indoor environments have a lot of noise and multipath (EM waves bouncing off of various physical materials) making accurate localization extremely challenging
  - Many indoor localization systems provide accuracies of 10m or more, which limits their utility
  - Bastille provides accuracies of 1-3m allowing precise location to aid interdiction

Event Detection Examples

Providing wireless visibility is essential for implementing a Zero Trust architecture. The following examples highlight the necessity for such visibility; they are just a few examples of events that Bastille customers have detected and located using Bastille's system:

- A USB Ninja cable on an executive floor of a Fortune 10 company
  - This cable is a hacking tool that looks and acts like a standard USB cable
  - It can wirelessly connect to a controller to enable an attacker to inject keystrokes and exfiltrate data from a target system
- A laptop connected to a server in a secure data center beaconing Wi-Fi and Bluetooth packets
- An active, unencrypted Zigbee transceiver in industrial chillers that had wired access to the core network inside a data center
- Excessive RTS and connection request packets from devices indicating misconfiguration and/or a potential DoS condition
- Intermittent WEP encryption advertised through beacons from an access point that otherwise used WPA2 encryption
  - WEP is a very old Wi-Fi encryption scheme that was cracked in 2001
  - No access point should ever be using it
- Bluetooth-enabled RFID readers that were susceptible to wireless DoS attacks that could shut down physical access to the facility

- Fitbits, phones, smartwatches, and many other devices are detected on a daily basis in various government and secure commercial facilities where the presence of such devices is prohibited due to security concerns

The ability to detect these kinds of threats allows operators to identify potential problems before they become incidents and take corrective action. For many of the examples above, physical security interdiction is the appropriate response, and the wireless detection system's ability to locate the wireless devices spatially is critical. For others, some action to correct device misconfiguration or simply shutting down a specific wireless mode is sufficient. For such cases, the system's ability to identify device details such as MAC address, device name, manufacturer, etc and integrate with a UEM/NAC system are all that is needed to identify and correct the problem. Whatever the case, a wireless detection solution can not only provide real-time monitoring of the wireless attack surface to identify malicious incidents as they occur, but it can serve to shore up an organization's security posture to prevent attacks from occurring at all.

Solving the Wireless Problem

Wireless devices are ubiquitous, vulnerable to attack, and invisible to most security tools. Their growing presence and vulnerability along with the trend toward democratizing RF hacking tools and capabilities necessitates improved vigilance on the part of network administrators and the entire security industry. Bastille's wireless detection and localization solutions can monitor these wireless signals, providing insight and automated response to threatening wireless behavior.

The ability to detect, localize, analyze, and respond to wireless threats is the next phase in the implementation of Zero Trust. It is time to plug this increasingly dangerous gap in our network security posture.

For more information on Bastille, please visit bastille.net. To read the full SECDEF memo please visit https://bastille.net/secdefmemo