Wednesday, October 23, 2024

10:30 am - 10:50 am

The Rise of Wireless Threats: Protecting Classified Information from Invisible Wireless Attacks

Brett Walkenhorst

Chief Technology Officer

Bastille

Abstract:

The United States Department of Defense has long recognized the risks associated with wireless capabilities, prompting policies to exclude electronic devices from secure areas, whether stationary or forward-deployed. Today, those risks are greater than ever, driven primarily by three factors: 1) the ubiquity of wireless-capable devices, 2) the invisibility of the signals they send, and 3) the vulnerability of the protocols they utilize.

For the malicious insider, the first two drivers are sufficient to cause significant damage. The ubiquity (and affordability) of wireless technology lowers the barrier to entry for would-be attackers, putting powerful tools into the hands of less sophisticated actors than ever before. The invisibility of the signals those devices send allows such attackers to act without fear of detection. Until recently, robust solutions to this problem were not available, but today, we can and must do better in bringing visibility to the invisible wireless attack surface.

For the unwitting insider, the unintentional introduction of electronic devices can be just as damaging due to the third driver: vulnerability. To date, almost 3000 wireless-related CVEs (Common Vulnerabilities and Exposures) have been published in the NIST database with ever-increasing numbers in recent years. These numerous vulnerabilities represent a fraction of what could potentially be exploited. With low-cost hardware and openly available code repositories that implement various attacks, the barrier to entry is lower than ever, enabling bad actors to compromise an insider's electronic devices in numerous ways. Today, every well-meaning person with access to classified information has the potential to unintentionally introduce compromised electronic devices into secure spaces where they become as dangerous to the security of classified information as the malicious insider.

This presentation will examine various wireless devices and threats, including how smartphones become sophisticated surveillance devices against their own users; Wi-Fi pineapples emulate trusted networks, capture devices, and steal credentials; Bluetooth peripherals are appropriated for data exfiltration; IoT devices become unwitting pawns in network-based attacks; and many more. Additionally, we will review hardware and software tools used to conduct wireless attacks and explore how they lower the barrier to entry, making such attacks more feasible to a larger group of bad actors.

Finally, we will present a wireless detection and localization system and discuss its use in identifying and alerting on malicious wireless devices and behaviors. We will review the system architecture, highlight key system components, and discuss analytics tools that are used to bring visibility to the increasingly problematic and invisible wireless attack surface.