How Public and Private Research Pioneered Next-Gen Wireless Detection

EPIQ SOLUTIONS

Table Of Contents

Introduction

In this paper, we'll discuss how years of cooperative research between the US government and private industry have helped usher in extremely effective methodologies to identify and take action against wireless threats.

In May 2020, while the world was still adjusting to the realities of living with the COVID-19 pandemic, astronauts Robert Behnken and Douglas Hurley lifted off from Kennedy Space Center aboard a SpaceX Falcon 9 rocket. This marked the first time a commercially built spacecraft carried NASA crew into orbit. The SpaceX Demo-2 mission represents a remarkable partnership between the public and private sectors, but it's far from the first time government and private research have combined to solve a problem.

In this whitepaper, we'll discuss how years of cooperative research between the US government and private industry have helped usher in extremely effective methodologies to identify and take action against wireless threats. We'll explore the genesis of current wireless detection solutions, how Epiq Solutions became part of this pursuit, and look at some of the technical challenges that were encountered and overcome along the way.

Ubiquitous Wireless Connectivity and the Birth of Flying Squirrel

Knowing a Wi-Fi network is under attack is important, but being able to survey all active Wi-Fi devices and identify and locate potential attackers became an area of focus for the DoD cybersecurity community.

Wi-Fi® has connected everything and altered virtually every aspect of how we manage day-to-day life. From asset tracking to smart factories, constant connectivity has left virtually no industry untouched by the benefits it offers. Government organizations are no exception, but driven primarily by the need for security on these networks, it took time for the Department of Defense (DoD) to formalize an approach to deploying Wi-Fi networks. In order to protect against intrusion on these new wireless networks, the DoD mandated the use of Wireless Intrusion Detection (WIDS) and Wireless Intrusion Prevention (WIPS) systems. These systems protect the network by using heuristics to identify exploit attempts by looking for unusual network activity or malformed packets. This approach provides effective network-based defense and is required by DoD Instruction (DoDI) 8420.01.

Knowing a Wi-Fi network is under attack is important, but being able to survey all active Wi-Fi devices and identify and locate potential attackers became an area of focus for the DoD cybersecurity community and an active area of research for the United States Naval Research Laboratory (NRL) Center for High Assurance Computer Systems. Their Flying Squirrel program was the product of this research and brought real-time discovery, analysis, and mapping of 802.11 wireless networks to wireless detection. This immediately strengthened the government's ability to protect its wireless networks, and for the first time operators responsible for protecting networks could identify an attack, know where it was coming from, and take action. Using reconfigured off-the-shelf access points and designed to run on a standard laptop, Flying Squirrel was the right tool for the job with passive operation and 24/7 capabilities. In many DoD facilities where wireless networks are present, Flying Squirrel is in operation.

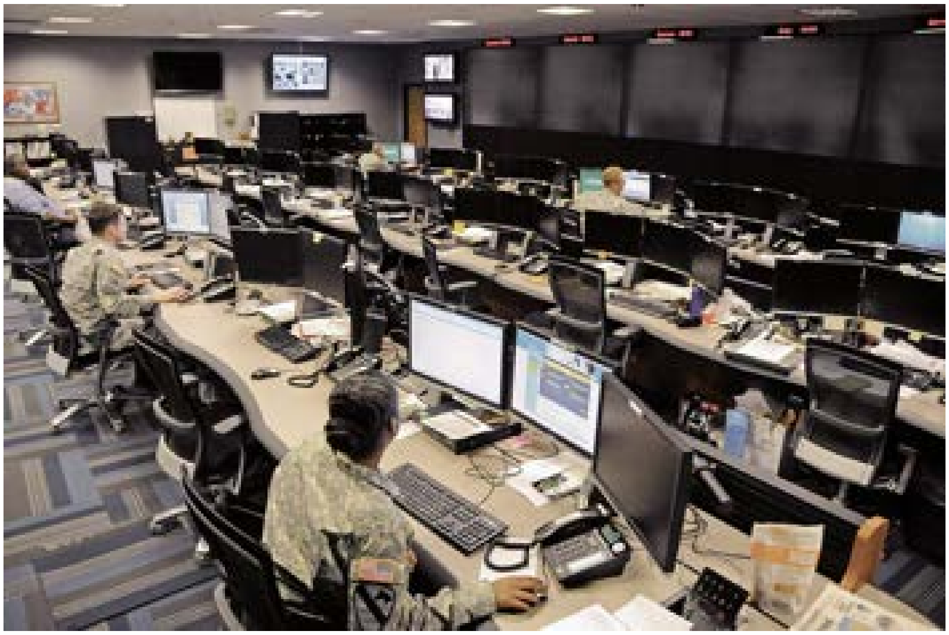
Extending Protection from Wireless Networks to Physical Spaces

The Flying Squirrel wireless detection technology that proved effective in detecting Wi-Fi devices gained interest from those looking to protect secure spaces. The need then evolved from protecting wireless LAN networks to detecting portable electronic devices (PEDs) in secure spaces where they are prohibited. The U.S. government operates hundreds of sensitive compartmented information facilities (SCIFs) around the world. These specially-built facilities are painstakingly designed so sensitive topics can be discussed or shared without the presence of any electronic devices that might intercept, collect, and transmit sensitive information to the outside world. In addition to the extensive physical and technical security measures required for accreditation, each SCIF requires a TEMPEST countermeasures review and Technical Surveillance Countermeasures (TSCM) survey and evaluation.

"TSCM involves techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to National Security Information (NSI), restricted data, and sensitive but unclassified information. TEMPEST is a short name referring to investigation, study, and control of compromising emanations from telecommunications and automated IS equipment. The aim is to minimize the likelihood that these emanations will ever be intercepted by adversaries of the United States." From DoDM 5100.21-v2: Sensitive Compartmented Information (SCI) Administrative Security Manual.

While the DoD and the intelligence community make substantial investments in safeguarding SCIFs from technical exploitation, perhaps the biggest technical threat comes from common devices such as smartphones that are carried by those who work inside SCIFs.

While the DoD and the intelligence community make substantial investments in safeguarding SCIFs from technical exploitation, perhaps the biggest technical threat comes from common devices such as smartphones that are carried by those who work inside SCIFs.



Keeping SCIFs free of unauthorized PEDs is a growing concern for DoD and government organizations. Photo courtesy of U.S. Army Cyber Command.

Being blind to the presence of PEDs creates two risks. The first is if someone intentionally brings a device into a SCIF with malicious intent, which might include the exfiltration of protected information or the introduction of malware into the environment. The second risk is less obvious: someone simply forgetting they have a PED with them and walking into a sensitive environment. Think about the apps we use on our smartphones and the terms of agreement we sign in order to use those apps. These agreements can, unknowingly to us, provide the company that made the app access to all of the device's peripherals including the camera and microphone, as well as keystroke history and location data. Even with no ill-intent, accidentally bringing a PED into a SCIF puts secure information at risk.

Countering wireless threats associated with SCIFs became the next area of focus for NRL's Flying Squirrel team and brought with it a new set of challenges.

Countering wireless threats associated with SCIFs became the next area of focus for NRL's Flying Squirrel team and brought with it a new set of challenges.

Detecting and decoding cellular signals is usually done in a cellular base station or a mobile device, both of which have been highly optimized for their specific functions.

A Lack of Commercially Available Solutions and the Move Toward Software-Defined Radios

While the Flying Squirrel Wi-Fi security solution made use of inexpensive and readily available 802.11 hardware, providing a reliable detection and location solution for SCIFs that could address Bluetooth®, Wi-Fi® and cellular signals required something more.

Detecting and decoding cellular signals is usually done in a cellular base station or a mobile device, both of which have been highly optimized for their specific functions. The cellular radio modems in mobile phones are highly integrated and optimized for size, cost, and power. They can't be used to decode arbitrary cellular signals or tune to arbitrary channels. Cellular base stations, on the other hand, have been designed to implement the other end of the cellular link in a way that is best for reliability, where cost and size are not primary concerns. The NRL needed something, not commercially available, that could detect, decode, and locate cellular devices and yet be small, lightweight, and cost effective.

Reliably detecting and decoding Bluetooth posed a similar challenge. Bluetooth devices and chipsets are small and inexpensive, but have optimizations built in for how devices are meant to work in practice. For example, Bluetooth Classic devices pair with hosts by awaiting and responding to inquiry packets of hosts wishing to pair. However, these devices won't respond to inquiry packets after they are paired with a host. In order to detect these paired devices, something that can decode Bluetooth signals without acting as a Bluetooth device or host is necessary.

SDRs implement communications protocols in software where they can be programmed to function beyond the capabilities of traditional, hardware-based, commercial off-the-shelf (COTS) devices.

To address these challenges, the Flying Squirrel project team at NRL turned its focus toward software-defined radios (SDRs). SDRs implement communications protocols in software where they can be programmed to function beyond the capabilities of traditional, hardware-based, commercial off-the-shelf (COTS) devices. NRL was looking to solve challenges in the RF domain that sought to combine SDRs, commercial communications protocols, and small form factors, the very same RF challenges that Epiq Solutions specializes in overcoming. Thus began NRL's partnership with Epiq Solutions.

Photo courtesy of U.S. Army Cyber Command

Government and Private Industry Come Together to Develop Flying Fox™

Seeing how Epiq Solutions could make a single sensor from a few SDRs that could be reprogrammed on the fly to accomodate for different frequencies and waveforms, NRL knew SDRs would be key to detecting devices that are not all on one carrier and that spanned multiple cellular generations. It became clear to both NRL and Epiq Solutions that, together, they could utilize SDR technology to adapt a sensor network to ever changing cellular frequencies, technologies, and standards. They called the product of their collaboration Flying Fox.

NRL knew SDRs would be key to detecting devices that are not all on one carrier and that spanned multiple cellular generations.

Moving forward to address the challenge of developing a sensor that could cover all of bands and channels in the cellular spectrum, Epiq Solutions needed to address three solution criteria:

- Detect and identify wireless threats
- Be fully passive, meaning sensors would not transmit
- Able to cover the full spectrum of RF frequencies in use by modern wireless/cellular devices

Epiq Solutions worked to develop the scanning algorithm, which not only provided the ability to detect, identify, and locate cellular devices, but also allowed real-time sensing of active cellular channels and decoding of signals to provide the detailed insight needed to accurately identify and reliably locate wireless devices.

To overcome the challenges associated with reliably detecting Bluetooth, again the team turned to an SDR-based solution.

Epiq Solutions implemented a Bluetooth protocol stack in an SDR which allowed the detect and decode transmissions between the paired device and the host device. This approach made it possible for to meet these challenges of detecting Bluetooth Classic and Bluetooth low energy devices with a fully-passive approach.

A passive-only Bluetooth detection system can have its drawbacks, too. Bluetooth Classic devices that are not in a piconet will not “speak until spoken to.” This means that the unpaired Bluetooth headset in the backpack would be undetected by a passive-only scanner. The system needed to have the best of both worlds – active and passive detection where possible, as an example in a building entry, and passive only where needed – inside the SCIF.

Once the team developed the approach using SDR for cellular and Bluetooth detection and integrating it with the existing work from Flying Squirrel that used COTS Wi-Fi radios, the architecture of the sensor could take shape.

The Sensor Takes Shape

With an SDR-based approach to cellular and Bluetooth detection, and by integrating it into the existing work from Flying Squirrel that used COTS Wi-Fi radios, the architecture of the sensor could take shape. Epiq Solutions' Sidekiq MiniPCIe card forms the basis of the flexible radio, with four of these SDR cards coupled to a carrier board to cover all of the required wireless technologies in a sensor that's only about the size of a paperback book (6.5" x 4.2" x 1.5") and consumes 22 watts – a major technical achievement and great government/industry team outcome.

Making Flying Fox Operational

Having accomplished the goal of devising a method for reliable detection of PEDs in secure locations, the Epiq Solutions team knew the work wouldn't be very useful if it remained a research project. Flying Fox needed to be taken out of the lab and made operational in order for it to fulfil its potential for DoD and federal government applications. Bringing these challenges to a product that would work in the real-world presented a new set of challenges.

Flying Fox embarked on a five-year government-off-the-shelf (GOTS)/ commercial-off-the-shelf (COTS) collaboration that culminated in Flying Fox™ Enterprise, an operational wireless detection and geolocation solution.

Flying Fox embarked on a five-year government-off-the-shelf (GOTS)/commercial-off-the-shelf (COTS) collaboration that culminated in Flying Fox™ Enterprise, an operational wireless detection and geolocation solution. Always-on, passive monitoring, geolocation, alerting, recording, and logging of cellular, Bluetooth and Wi-Fi transmissions had been the goal of NRL research and was brought to life through this partnership. The SDR-based approach means Flying Fox can keep up with always-changing wireless standards and represents a milestone in public/private cooperation that resulted in a highly innovative, highly effective commercial solution. Flying Fox Enterprise is web-based, multi-user application and users can set up zones for geofencing for facilities or buildings where some areas allow PEDs and some don't, further addressing the issue of false positive readings.

There have been a number of successful deployments, from very large operational missions to very small, and Epiq Solutions is very proud of what we've been able to accomplish working in coordination with the NRL.

Conclusion

Advancing RF situational awareness from a government research project focused narrowly on Wi-Fi intrusion detection, to ultimately realize a fully commercial product providing full-spectrum visibility and detection of any device is a testament to the power of private and public expertise coming together. To read about how Flying Fox Enterprise is being deployed, read a case study based on a real-world application at a DoD Joint Base here.

READ THE CASE STUDY

With more than a decade in business, Epiq Solutions understands how important speed, cost, and performance are for defense and security applications. Our radically small SDR transceiver modules and turnkey RF sensing tools lead the way in size, weight, and power consumption. Whether you're developing mission-critical defense applications for the battlefield or protecting sensitive information, you can trust us to get you there fast.

LEARN MORE

EPIQ SOLUTIONS
epiqsolutions.com