1600 - Radio Exploitation 101: Characterizing, Contextualizing, and Applying Wireless Attack Methods

Friday at 16:00 in 101 Track
45 minutes | Demo
Matt Knight*Senior Software Engineer, Threat Research at Bastille*

Marc Newlin*Security Researcher at Bastille*

What do the Dallas tornado siren attack, hacked electric skateboards, and insecure smart door locks have in common? Vulnerable wireless protocols. Exploitation of wireless devices is growing increasingly common, thanks to the proliferation of radio frequency protocols driven by mobile and IoT. While non-Wi-Fi and non-Bluetooth RF protocols remain a mystery to many security practitioners, exploiting them is easier than one might think.

Join us as we walk through the fundamentals of radio exploitation. After introducing essential RF concepts and characteristics, we will develop a wireless threat taxonomy by analyzing and classifying different methods of attack. As we introduce each new attack, we will draw parallels to similar wired network exploits, and highlight attack primitives that are unique to RF. To illustrate these concepts, we will show each attack in practice with a series of live demos built on software-defined and hardware radios.

Attendees will come away from this session with an understanding of the mechanics of wireless network exploitation, and an awareness of how they can bridge their IP network exploitation skills to the wireless domain.
Matt Knight
Matt Knight is a software engineer and applied security researcher at Bastille, with a background in hardware, software, and wireless security. Matt's research focuses on preventing exploitation of the myriad wireless networking technologies that connect embedded devices to the Internet of Things. Notably, in 2016 he exposed the internals of the closed-source LoRa PHY based on blind signal analysis. Matt holds a BE in Electrical Engineering from Dartmouth College.

@embeddedsec
Marc Newlin
Marc Newlin is a wireless security researcher at Bastille, where he discovered the MouseJack and KeySniffer vulnerabilities affecting wireless mice and keyboards. A glutton for challenging side projects, Marc competed solo in two DARPA challenges, placing third in the

DARPA Shredder Challenge, and second in the first tournament of the DARPA Spectrum Challenge.

@marcnewlin

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday