1200 - The Black Art of Wireless Post Exploitation

Sunday at 12:00 in 101 Track
45 minutes | Demo, Tool
Gabriel "solstice" Ryan*Gotham Digital Science*

Most forms of WPA2-EAP have been broken for nearly a decade. EAP-TTLS and EAP-PEAP have long been susceptible to evil twin attacks, yet most enterprise organizations still rely on these technologies to secure their wireless infrastructure. The reason for this is that the secure alternative, EAP-TLS, is notoriously arduous to implement. To compensate for the weak perimeter security provided by EAP-TTLS and EAP-PEAP, many organizations use port based NAC appliances to prevent attackers from pivoting further into the network after the wireless has been breached. This solution is thought to provide an acceptable balance between security and accessibility. The problem with this approach is that it assumes that EAP is exclusively a perimeter defense mechanism. In this presentation, we will present a novel type of rogue access point attack that can be used to bypass port-based access control mechanisms in wireless networks. In doing so, we will challenge the assumption that reactive approaches to wireless security are an acceptable alternative to strong physical layer protections such as WPA2-EAP using EAP-TLS.
Gabriel "solstice" Ryan
Gabriel is a pentester, CTF player, and Offsec R&D. He currently works for Gotham Digital Science, where he provides full scope red team penetration testing capabilities for a diverse range of clients. Previously he has worked at OGSystems and Rutgers University. He also is a member of the BSides Las Vegas senior staff, coordinating wireless security for the event. Things that make him excited include obscure wireless attacks, evading antivirus, and playing with fire. In his spare time, he enjoys live music and riding motorcycles.

@s0lst1c3
github.com/s0lst1c3
solstice.me
blog.gdssecurity.com

#defcon25/by_track/101/Sunday #defcon25/By_Day/_Sunday