Top Wireless Threats

WIRELESS THREAT	DETAIL
ROGUE WI-FI HOTSPOTS *(and Wi-Fi pineapples)*	Can someone in your building by-pass all your Wireless Intrusion Detection Systems by opening a Wi-Fi hotspot which detours your data around your expensive Wi-Fi anomaly detection?
WI-FI PINEAPPLES	Wi-Fi Pineapples can insert themselves into legitimate Wi-Fi networks, and can be used for Man-In-The-Middle attacks to sniff network traffic and steal credentials.
BLUETOOTH DATA EXFILTRATION *(tethering)*	Bluetooth tethering can be used to pair a network device with a cellular data path (e.g. 4G LTE) which bypasses your traditional network security. How do you detect when someone starts Bluetooth tethering in your building? How do you avoid false alarms when the Bluetooth is only being used to connect a headset?
EAVESDROPPING/ SURVEILLANCE DEVICES *(e.g. conference room bugs)*	Voice and motion-activated bugs cost as little as $20 on eBay.® These devices are getting smaller, yet with ever more sophisticated capabilities. They can exfiltrate voice and video across multiple radio bands, using FM, cellular and/or Wi-Fi.
VULNERABLE WIRELESS PERIPHERALS *(mice/keyboards)*	Low-end wireless keyboards, even from top manufacturers, allow sniffing of keystrokes out of the air from 250 feet away because they do not implement encryption. A vulnerable wireless mouse dongle can expose the computer to an external attack through keystroke injection. Once the computer is itself compromised, it can expose the larger network to insider attacks.
UNAPPROVED CELLULAR DEVICE PRESENCE	Many organizations have a “no cell phones in this area” policy to comply with regulations. Ensuring that policies are maintained is key for security.
UNAPPROVED WIRELESS CAMERAS *(using Wi-Fi and other protocols)*	Inexpensive wireless cameras are great for security when your security department installs them. But if someone else installs them then they can be used to plan security breaches. Know every camera operating in your facility and whether it works for your security team or someone else.
VULNERABLE WIRELESS BUILDING CONTROLS *(e.g. default credentials)*	Many new pieces of equipment ship with two consoles: Ethernet and “Radio Ready” Consoles. You know about your Ethernet console but is there another console on your equipment set up with default configuration and broadcasting for instructions?
UNAPPROVED IoT EMITTERS	New thermostats and building sensors often have multiple data radios. Wi-Fi is the one you know about. But is your sensor also transmitting on other frequencies like ZigBee (short range) or LoRa (up to 1 mile range)? What data is beaming down the street that you don’t know about?
VULNERABLE BUILDING ALARM SYSTEMS	Many Window, Door and Motion detectors can be ordered to “pay no attention to the man climbing in the window” by someone carrying a $10 radio jammer, or $300 Software Defined Radio, which can also simulate any alarm event. Security professionals need to be alerted when someone attempts to jam any part of their alarm system.

800.530.3341 / info@bastille.net