Discussion-5 Preventing identifying and isolating wireless networks' rogue devices

Discussion Topic:

One known issue with wireless networks would be rogue devices (mostly access points). What strategies and tools would you utilize to prevent, identify, and isolate them?

My Post:

Hello Class,

Wireless networks are everywhere and have infiltrated every aspect of daily life as they provide convenience and flexibility at home and work. However, their convenient and flexible nature come with security risks, particularly through rogue devices. The Information Technology Laboratory (n.d.) defines rogue devices as “an unauthorized node on a network.” These devices can be smartphones, laptops, Internet of Things (IoT) devices, or any other device capable of connecting to a network (Nile, n.d.). Focusing on wireless networks, this post explores rogue device types, prevention, identification, and isolation; the post also provides an overview of wireless monitoring tools.

Wireless Types of Rogue Devices

In the context of wireless networks, rogue devices can range from wireless access points, laptops, and smartphones to software like network sniffers or compromised IoT devices. Here are some common types:

Table 1

Wireless Types of Rogue Devices

Device Type	Description	Threats	Examples
Rogue Access Points	Unauthorized wireless access points connect to a network without permission	Vulnerability to "wardriving": Attackers scan for unsecured Wi-Fi networks. Evil twin attacks: Fake Wi-Fi hotspots mimicking legitimate hotspots.	Intentionally malicious access points such as an employee-installed access point to improve Wi-Fi.
BYOD (Bring Your Own Device)	Personal devices (smartphones, laptops, tablets) connected to a business network.	May be used as rogue devices without the device owner's knowledge.	An employee connecting a personal, unsecured smartphone to the network.
IoT Devices	Internet-connected devices. IoTs usually have limited security features.	Can be exploited to gain access to a network.	Smart thermostats, security cameras, smart appliances.
Malicious Peripherals	Everyday USB and wireless devices like printers, drives, and keyboards that were modified or tampered with are used for malicious purposes.	- Data theft - Malware injection - Network disruption - Mimicry: mimics of legitimate peripherals,	- USB or wireless drives programmed to steal data. - USB or wireless Keyboards that record keystrokes.

		making them hard to detect.	- USB or wireless Printers that spread malware. USB or wireless devices mimicking keyboards or mice.

Note: Data from several sources (Gratas, 2024; Ciarlone, 2023; uCertify, 2019).

As shown in Table 1, rogue devices can be of various types, from unauthorized wireless access points to basic peripherals like modified wireless keyboards, with each type posing a unique set of security threats.

Preventing Identifying and Isolating Rogue Devises

With so many types of possible rogue devices, it is important for wireless network administrators to prevent, identify, and isolate them.

Preventing rogue devices can be done by disabling Service Set Identifier (SSID) broadcasts making the network less discoverable by wardriving scans (uCertify, 2019). Rogue devices can be also prevented by implementing network access controls "to ensure that only authorized devices and users can connect to your network" (Nile, n.d., p.1). This can be done by implementing Network Access Control (NAC) appliances and strong authentication methods, such as 802.1x with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) or PEAP (Protected Extensible Authentication Protocol). Other preventative measures are continuously monitoring the network for suspicious activity, identifying and categorizing devices on the network, and implementing a network segmentation policy such as dividing the network into smaller and isolated subnetworks, as well as implementing a guest Wi-Fi guest network for visitors and employees' personal devices.

Identifying and isolating rogue devices can be done by utilizing network scanning tools such as Nmap to scan for all devices connected to the network (Zamot, 2020). This allows a network administrator to identify unauthorized devices and isolate them. Intrusion Detection Systems (IDS) can also help to identify rogue devices by monitoring traffic and detecting suspicious activities (Solarwinds, n.d. a). Additionally, wireless rogue access points can be detected using a tool such as Firebox which measures the strength and characteristics of an access point and compares it to a list of trusted access points (watchguard, n.d.). The table below provides an overview of several tools used to detect wireless network anomalies.

Table 2

Wireless Monitoring Tools

Tool	Key Features	Pros	Cons
SolarWinds NPM WiFi Analyzer	Automatic device discovery, visual heatmaps, unauthorized user detection	Comprehensive features, intuitive console, simplifies troubleshooting	Potential issues with customer service and support, large file size and system requirements
Datadog Network Monitoring	Real-time metrics, customizable dashboards, alerting, anomaly monitoring, synthetic testing	Easy to use, comprehensive monitoring capabilities, customizable dashboards, cloud-based	Can be expensive, especially for smaller businesses, steep learning curve for some features

PRTG Network Monitor	Bandwidth monitoring, alerts, customizable dashboards, remote device management, vendor agnostic, preconfigured sensors, MIB translation	User-friendly interface, comprehensive feature set, good price-performance ratio, monitors various IT verticals	Initial setup can be overwhelming, shift to subscription model with increased costs
NetSpot	Wireless network visualization, Wi-Fi planning, troubleshooting, hidden network detection, supports various Wi-Fi standards	Easy to use, comprehensive features, generates professional reports quickly, cross-platform compatible, excellent customer service	Limited features in lower-priced editions
NetStumbler	Network verification, coverage analysis, interference detection, rogue access point detection, broadband availability mapping	Free, simple, effective for basic wireless network detection	Compatibility issues with some chipsets, cannot show hidden SSIDs
Kismet	Passive network detection, intrusion detection, packet logging, channel hopping, supports various protocols	Powerful and versatile, passive detection capabilities, intrusion detection features, open-source	Can be complex to use for beginners
AirMagnet	Site surveying, performance monitoring, security analysis, spectrum analysis, end-user experience measurement	Powerful and feature-rich, comprehensive wireless network management	Expensive, complex to use, potential licensing and support issues

Note: Data from several sources (Reddy, 2023; MetricFire Blogger 2023; Sharma, 2023; NetSpot, n.d.; Goodman, 2018; Kismet Wireless, 2016, Netscout, n.d.; Solarwinds, n.d. b)

To summarize the convenience and flexibility provided by wireless networks come with security risks, primarily from the threat of rogue devices. These devices can be unauthorized access points or peripherals such as printers and keyboards. Preventing, identifying, and isolating these rogue devices is crucial for network security. These security vulnerabilities can be mitigated by implementing network access controls, using monitoring tools, and implementing measures like network segmentation and dedicated guest networks.

-Alex

References:

Ciarlone, J. (2023, December 29). Spotting the most common wireless network vulnerabilities. Hummingbird Networks. https://services.hummingbirdnetworks.com/blog/most-common-wireless-network-vulnerabilities-to-watch-for

Goodman, D. (2018, November 18). Network Stumbler: A powerful broadband tool. Connected Nation. https://connectednation.org/press-releases/network-stumbler-a-powerful-broadband-tool

Gratas, B. (2024, September 9). Rogue device detection in 5 simple steps. Invgate Blog. https://blog.invgate.com/unauthorized-asset-detection

Information Technology Laboratory (n.d.). Rogue device. Glossary. NIST – U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/rogue_device

Kismet Wireless (2016). *Kismet*. Kismet Documentation. https://www.kismetwireless.net/static/documentation.shtml

MetricFire Blogger (2023, October 12). *10 best tools for monitoring wireless access points.* MetricFire https://www.metricfire.com/blog/10-best-tools-for-monitoring-wireless-access-points/

Netscout (n.d.). *AirMagnet Enterprise* [PDF]. AirMagnet. https://assets.tequipment.net/assets/1/26/Documents/AirMagnet_Enterprise_Datasheet.pdf

NetSpot (n.d.). *Your Wi-Fi planning and wireless site survey app* [Video]. NetSpot. https://www.netspotapp.com/features.html

Nile (n.d.). *What are rogue devices? How to detect and prevent them*. Nile. https://nilesecure.com/network-security/what-are-rogue-devices-how-to-detect-and-prevent-them

Reddy, M. (2023, July 7). Unlocking the power of datadog: Understanding its key features. Nitor. https://www.nitorinfotech.com/blog/unlocking-the-power-of-datadog-understanding-its-key-features/

Sharma, A. A. (2023, July 4). *PRTG Network Monitor: Why and how?* DEVOPS DONE RIGHT. https://opstree.com/blog/2023/07/04/prtg-network-monitor-why-and-how/

Solarwinds (n.d. a). Detecting and preventing rogue devices [PDF]. Solarwinds Whitepaper. https://www.solarwinds.com/assets/solarwinds/swdcv2/licensed-products/user-device-tracker/resources/whitepaper/udt_wp_detect_prevent_rogue_devices.pdf

Solarwinds (n.d. b). *Wi-Fi Network Analyzer.* Solarwinds. https://www.solarwinds.com/network-performance-monitor/use-cases/wifi-analyzer

uCertify. (2019). 8.3 Securing wireless LANs. *CompTIA Network+ Pearson N10-007* (*Course & Labs)* [Computer software]. uCertify LLC. ISBN: 9781616910327

Watchguard (n.d.) *Rogue access point detection – Fireware Help*. Watchguard. https://www.watchguard.com/help/docs/fireware/12/en-us/Content/en-US/wireless/wireless_rogue_ap_detection_c.html

Zamot, M. (2020, December 1). *Finding rogue devices in your network using Nmap*. Red Hat Blog. https://www.redhat.com/en/blog/finding-rogue-devices