EnGenius

White Paper

Protect Wireless Network with Security Access Points

Table of contents

Introduction

How Secure is your SASE Wireless Environment?

As SaaS becomes more widely adopted by enterprises and work-from-home options grow more popular, corporate IT managers need to consider how to make sure legitimate users with legitimate devices are able to access authorized corporate resources whether they are at the office, at home or on the road. So an SASE (secure access service edge) infrastructure with Zero Trust Network Access policy rules becomes necessary to ensure the same policy applies to every individual. However, the bottom line is legitimate users have to be able to access the wired and wireless network securely without worrying about their credentials or data being breached or hackers mimicking legitimate clients.

Unlike hardwired switch networks with client devices connected to a dedicated wired port, wireless local area networks (WLANs) transmit and receive data over the air, which makes WLANs vulnerable to interference, interception, eavesdropping, and all kinds of hacking. WFH (work-from-home) users also expose themselves to threats in an unsecured home Wi-Fi environment. Even if a VPN tunnel is enforced to secure the connection between the home gateway and HQ, it is still hard to secure a WLAN at an employee's workplace even if an authorized VPN tunneled device is provided by the company for home users.
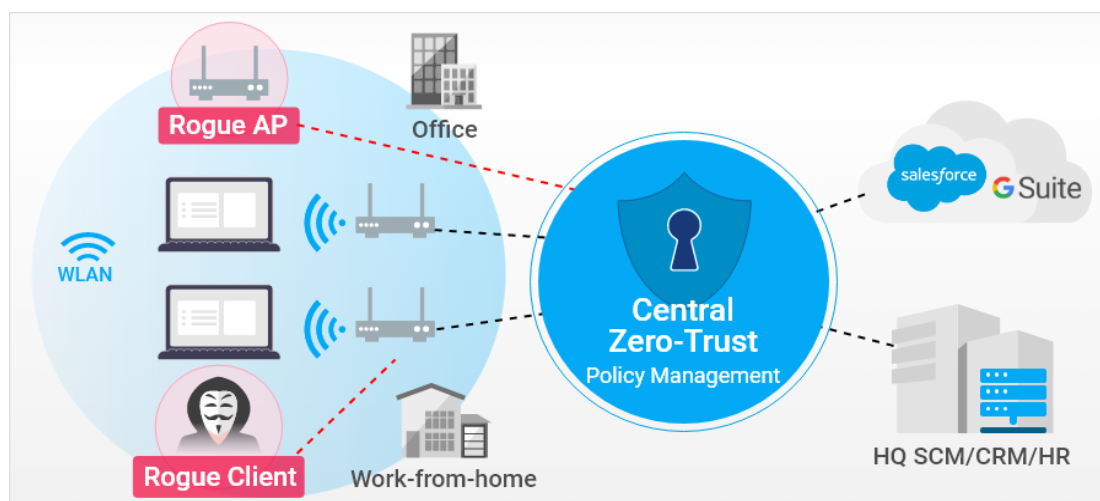
Figure01 -- SASE Infrastructure also requires wireless security protection

Besides the threats of WLAN, there are also many kinds of security issues happening including leaving the device credential at factory default, leaving the SSID open, exposing management frames without encryption. The EnGenius Cloud solution provides the essential features to help IT managers strengthen their infrastructure and protect corporate assets.

Wireless Network Security Issues

There are three common security threats in WLAN:

Denial of Service

A denial of service attack crowds the radio channel by sending out de-authentication or dis-association packets to prevent clients from connecting to the AP and accessing the network. An RF jammer is a tool typically used to jam the radio channel, so valid clients won't be able to access the network. Rogue clients can also spoof the SSID and AP to de-authenticate or dis-associate legitimate clients.

Passphrase or Password Cracking

Hackers can sniff or eavesdrop over-the-air traffic to crack the PSK passphrase of an SSID and access the network. They can also break user credentials to change settings as an admin or access un-authorized resources as authorized users.

Data Breach

By spoofing a legitimate SSID or AP, hackers can leverage the rogue spoofing AP to collect user data. Common threats are from man-in-the-middle or evil twin attacks.

Denial of Service and EnGenius Solution

Radio Interference

Users might experience strong Wi-Fi signal strength but have problems connecting to the AP or suffer an extremely low data rate. It's usually because the WiFi channel utilization rate is so high that there is no bandwidth for valid clients. The interference sources might come from your neighbors' Wi-Fi or from non-Wi-Fi appliances like microwave ovens.

Detection, Analysis, and Solution

Operating Channel Utilization Rate

EnGenius Cloud provides a real-time channel utilization analysis tool to view how many Wi-Fi and non-Wi-Fi radio signals utilize the operating channel, so users can know if the connectivity issue is because of high channel utilization or from non-Wi-Fi appliances nearby.
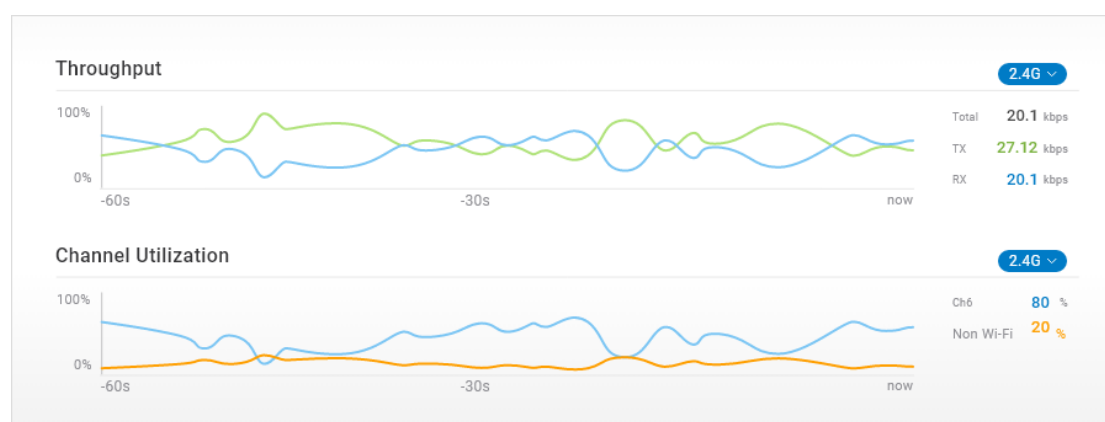
Figure02 -- Operating Channel Utilization Rate

Full Channel Utilization Tool

When the operating channel is crowded, the best remedy is to move to a clean channel. Besides the real-time channel utilization analysis to see the utilization status of the current operating channel, EnGenius Cloud provides an additional helpful tool to show full channel utilization and density analysis to help you identify which channel is cleaner.
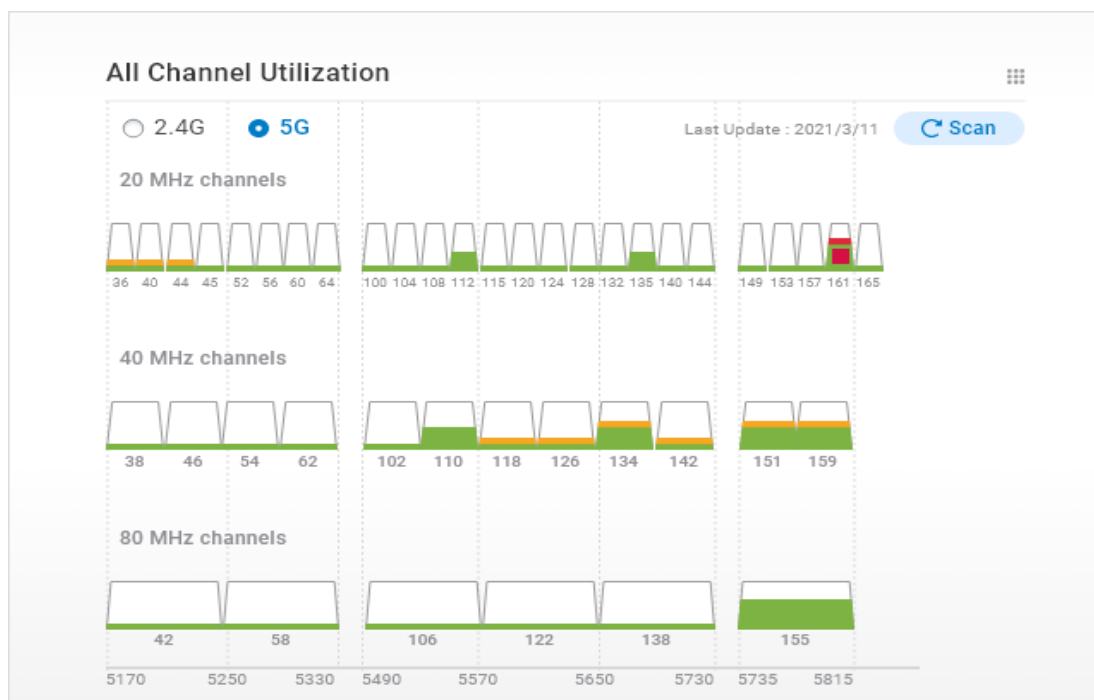
Figure03 -- Utilization Analysis of All Channels

Spectrum Waterfall Analysis

When analyzing channel utilization, the user will see how dense the usage is in a given moment. However, brief interference might mislead the user into thinking the interference is ongoing. The spectrum waterfall analysis tool helps users see the interference over time with the "waterfall" display, so users can know which channel is cleaner over time instead of one specific time.

Figure04 -- Spectrum Waterfall Analysis

ACS (Auto Channel Selection)

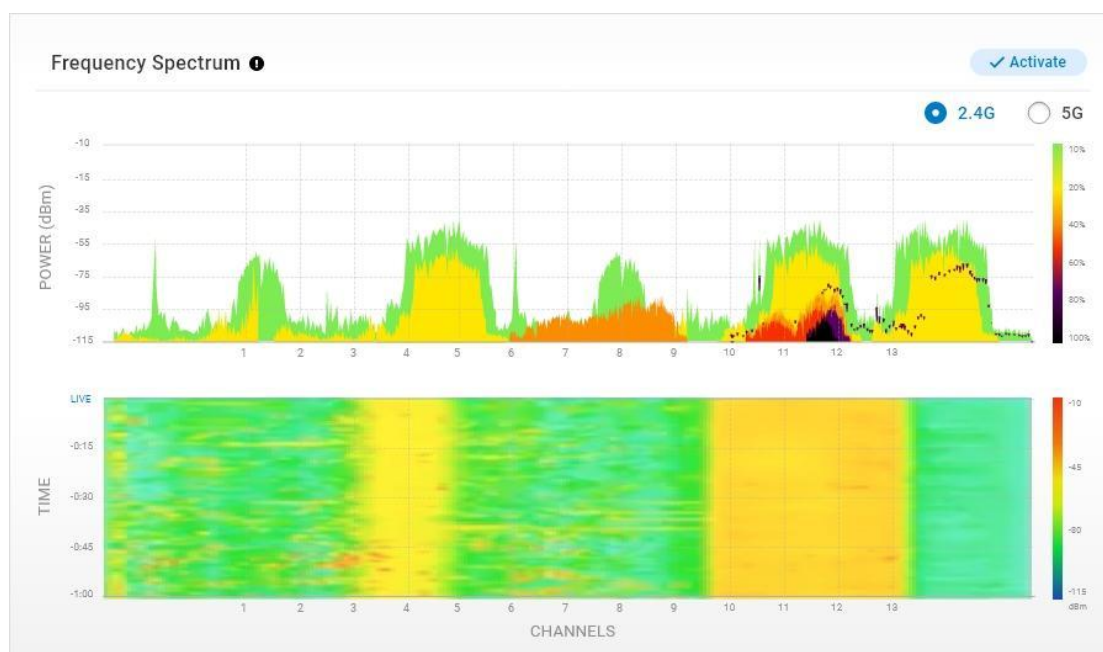Without manually selecting the channel from the full channel utilization graph or waterfall spectrum, users can run EnGenius auto channel selection (ACS) for an EnGenius AP to scan the environment and, based on the EnGenius algorithm, identify and move to a cleaner channel automatically.

Zero-Wait DFS for High-Density Environment

Under high density deployment, many non-overlapping Wi-Fi channels require that DFS channels be used to avoid channel interference. However, the AP will need to switch to another channel once protected radar is detected. Since non-DFS channels are highly dense, switching to another DFS channel is the best option. However it usually requires a >30 sec wait time to make sure the DFS channel can be used causing client session downtime. EnGenius zero-wait DFS technology in EnGenius "S" models (i.e., ECW220S, ECW230S) uses a dedicated scanning radio to keep listening for other available DFS channels that the AP can switch to immediately to keep client sessions connected.

RF Jamming

There are two kinds of RF jamming: radio jamming to simply block the radio channel and packet flooding to generate a massive number of Wi-Fi packets

on the channel so that there is no bandwidth for valid clients to connect to the network.

Detection, Analysis, and Solution

RF Jamming Detection and Classification

EnGenius AirGuard provides RF jamming attack detection and categorizes the attacks as radio jamming or packet flood. It then specifies which channel is attacked and detected by which EnGenius AP, so users can know approximately which detected APs might have an RF jammer around. When the channel is jammed, users can use EnGenius ACS (auto channel selection) to move the SSID to another channel without being attacked.

Figure05 -- RF Jamming Detection List

Abnormal De-authentication and Disassociation packets

Clients must be authenticated by the AP with the correct security protocol (i.e., WPA2-personal PSK key) before associating with the AP. Clients are typically disconnected when they receive deauthentication or disassociation frames from the AP. Since the auth/deauth, asso/disasso management frames are unprotected most of the time, hackers can easily mimic the client to keep sending deauth/disassociation requests to the AP or mimic the AP to send deauth/disassociation responses to all clients, preventing them from accessing the AP.

Detection, Analysis, and Solution

Malicious De-Authentication and Disassociation Detection and Classification

EnGenius AirGuard has an algorithm to detect frequent abnormal de-authentication and disassociation frames and to report the malicious attack into one of two categories: de-authentication and disassociation. AirGuard can also detect if the attack is directed to a specific client, then the attacked party will show the client's MAC address. Or if the attack is to mimic the AP to disconnect all clients, then the attacked party will show ff:ff:ff:ff:ff:ff instead.

Suspicious SSIDs 5	Other SSIDs	Evil Twins 1	Malicious Attacks 6		RF Jamming 5		
+ Add Filter							
Category	**SSID**	**Channel**	**Attacked Party**	**Connected to AP**	**Last Seen**	**First Seen**	**Network**
Dis-association attack	FAtest	2	All Clients (FF:FF:FF:FF:FF:FF)	- - -	34 sec ago	2 weeks ago	8F
Dis-association attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Connected	34 sec ago	2 weeks ago	8F
Dis-association attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Connected	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	All Clients (FF:FF:FF:FF:FF:FF)	- - -	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Unconnected	34 sec ago	2 weeks ago	8F
De-Auth attack	FAtest	2	James's NB (92:3E:DE:00:96:42)	Unconnected	34 sec ago	2 weeks ago	8F

Figure06 -- Malicious Attacks Detection List

802.11w Support to Protect the Management Frame

It's highly recommended to enable 802.11w (802.11w-2009 MFP-Management Frame Protection) to protect the management frames and make sure the management frame is from a legitimate AP. Both clients and APs need to support 802.11w to communicate.

Data Breach, Passcode Cracking, and the EnGenius Solution

Honey Pot (Rogue SSID) Attack

Almost everyone can easily purchase an access point or Wi-Fi router to generate a rogue SSID that looks exactly the same as the legitimate corporate SSID. It can be placed, for example, in the parking lot around the

corporate building as a honey pot to which a valid employee's notebook might inadvertently connect.

The rogue SSID attack is more likely to happen whenever more companies use cloud services like Google Suite, Salesforce.com, etc. The hacker doesn't need to hack the corporate network but simply put out a honey pot and sniff the traffic between valid users and cloud services.

It becomes even easier when new roaming technology is implemented in mobile phones and notebooks that will detect the stronger signal of the same SSID and roam to it. The hacker can then boost his rogue AP aside the corporate building whereas corporate Wi-Fi might have weaker coverage around the corners or border of the building.
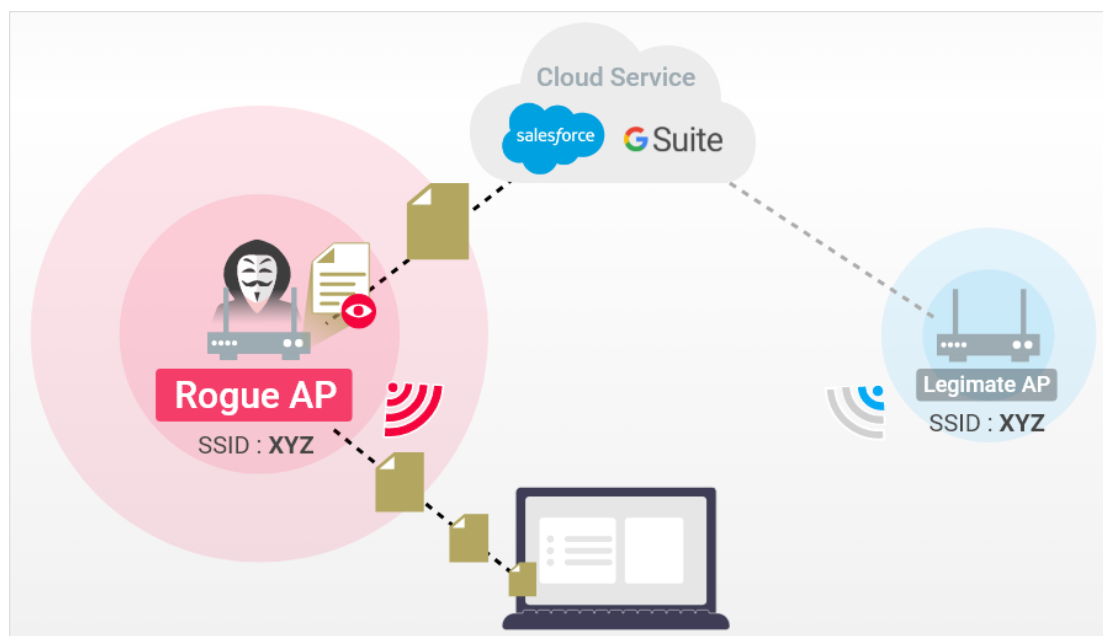

Figure07 -- Honey Pot (Rogue SSID) Attack

Detection, Analysis, and Solution

Rogue SSID Detection

EnGenius AirGuard can check the SSID name (ESSID) or AP radio MAC (BSSID) to automatically detect the rogue AP that mimics the legitimate SSID but is not listed among legitimate EnGenius managed APs in the same network.

EnGenius Rogue/Whitelisted Rules and Honey Pot to Lure Hackers

It is a good practice to set up a honeypot environment in a corporate network to lure and identify malicious attackers. Administrators can set up a network separate from corporate networks with a honeypot AP using an open SSID and some clients generating traffic. Malicious hackers will then find the "weak" SSID of the honey pot and attack.

AirGuard allows users to set rogue rules and whitelist rules by comparing the SSID name or BSSID MAC address. In the honeypot case, administrators can monitor which MAC sources mimic the honeypot SSID, observe how they are trying to attack the network, and take actions accordingly. In case there might be legitimate non-EnGenius APs deployed in the corporate network, administrators can whitelist the MAC address of the non-EnGenius APs and separate them from the rogue SSID list.

Figure08 -- Rogue Rules and Whitelist Rules of SSIDs

Man-In-The-Middle Attack

By luring valid users to connect to the rogue AP, hackers can connect a proxy to the rogue AP and redirect all traffic through the proxy. Hackers can then snoop through sensitive corporate information while the valid user is accessing corporate cloud services.

If the hacker can furthermore connect to a legitimate AP, then he can connect a rogue AP to a legitimate AP, and mimic the legitimate SSID. Everything looks the same from the client end when the client connects to the rogue SSID of a man-in-the-middle rogue AP.

There are three easy ways a hacker can connect to a legitimate AP:

- Factory Default Device Admin Credential

  This is the most common fraud that users might encounter accidentally. Using the factory default credential, hackers can hack into the device and change the configuration to allow a rogue AP to connect to a legitimate AP.

- When the SSID security type is set to "Open."

  When an SSID is "Open," everyone can connect to the legitimate AP and access corporate networks and assets. It's also quite common to set the SSID security type to Open when the captive portal splash page is set up for user authentication. The rogue AP can easily connect to the legitimate AP and pass overall traffic, including splash page authentication while sniffing all data.

- Exploit the vulnerability without updating the firmware

  There were some vulnerability issues found in WPA2, like the KRACK issue where hackers could leverage a four-way handshake sequence of WPA2 and hack the PSK to steal sensitive information like credentials, credit card info, and so on. The vulnerability was fixed but users had to upgrade to the most up-to-date version of their device firmware. Managing the device firmware across the corporate network is also a task for the administrator.
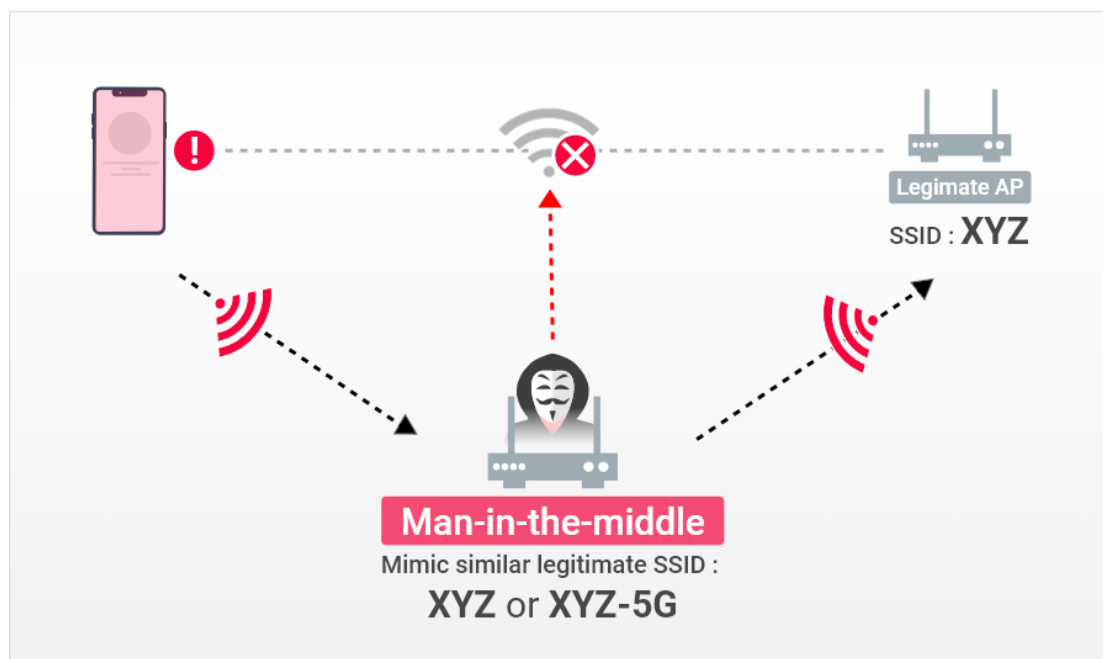
Figure09 -- Man-in-the-Middle Attack

For example, the hacker can start a DoS attack to break the connection between clients and a legitimate AP, so that the clients will have problems connecting to the legitimate SSID. For example, if a hacker finds a network called "XYZ," the hacker can create a look-alike SSID "XYZ-5G" to connect to. (The hacker can also use the exact same SSID name to simulate a legitimate SSID; however, this will be found through "rogue SSID" detection.) The hacker can then either redirect the traffic to a phishing web page to steal credentials or direct the traffic back to a legitimate AP and sniff all data transferred in between.

Detection, Analysis, and Solution

Rogue SSID Detection

AirGuard will monitor all SSID's with the same name as the legitimate SSID and check if the SSID is from legitimate AP's in the network. Users can also set whitelist rules by adding legitimate AP MAC lists which are not managed by EnGenius Cloud to exclude from the rogue SSID list.

myPSK to Protect Passphrase of WPA-personal SSID

It is common and easy to set the passphrase of the WPA PSK of the SSID to have basic security access control. However, once someone knows the passphrase he/she can access the SSID forever uninhibited. EnGenius myPSK allows the network administrator to set a unique PSK for each person and control the valid period and VLAN, so when the person is not eligible to access the network, the PSK will be invalid. This feature is especially suitable

for school dormitories where the students and teachers come and go with different levels of resource access. Dormitory administrators can base access on the full school year or certain semesters for students to be assigned a unique PSK and access a certain VLAN for a limited period of time.

All devices come with a default account and password for easy first-time configuration. If the administrator doesn't change the account/password, it's easy for someone to log in to the device and change the configuration. This is the most common oversight that puts corporate network security at risk.

EnGenius encourages users to set a unique network-wide local admin account and password immediately. When a new device is assigned to the network and a new network created, the local admin account and password to access the local GUI of the device must be changed accordingly. If the factory-default credential is not changed. EnGenius Cloud will mark the network as "insecure" by putting a warning icon on the network to indicate that the network devices are exposed to security fraud.

WPA3 Support to Have Higher Security

WPA3 enhances the security mechanism with OWE (Opportunistic Wireless Encryption) to replace the open security type. Clients don't need the passphrase to access the AP, because OWE will encrypt the transmission. In addition, WPA3-personal uses SAE technology to replace the WPA2 pre-shared key, a more secure way to do the key exchange and to prevent attacks like the four-way handshaking KRACK.

Secure Connection for Captive Portal Authentication

EnGenius provides an HTTPS option for users to encrypt the communication between the client and AP before the user gets authenticated through a captive portal. Without the encryption, a man-in-the-middle can easily sniff the credential during the captive portal login process.

Auto Firmware Upgrade

To make sure the firmware of devices on the corporate network is most up-to-date and vulnerabilities fixed as soon as possible, the EnGenius Cloud auto firmware upgrade feature allows users to set time slots each week to upgrade. Once set, administrators won't need to worry about firmware version management across the whole network.

Evil Twin Attack

Hackers use evil twin devices to hack into networks by seducing legitimate clients to connect. Since security detection checks to make sure frames are from legitimate access points, hackers will change the MAC address and even the SSID name of the evil twin to match the MAC address and SSID name of the legitimate AP.
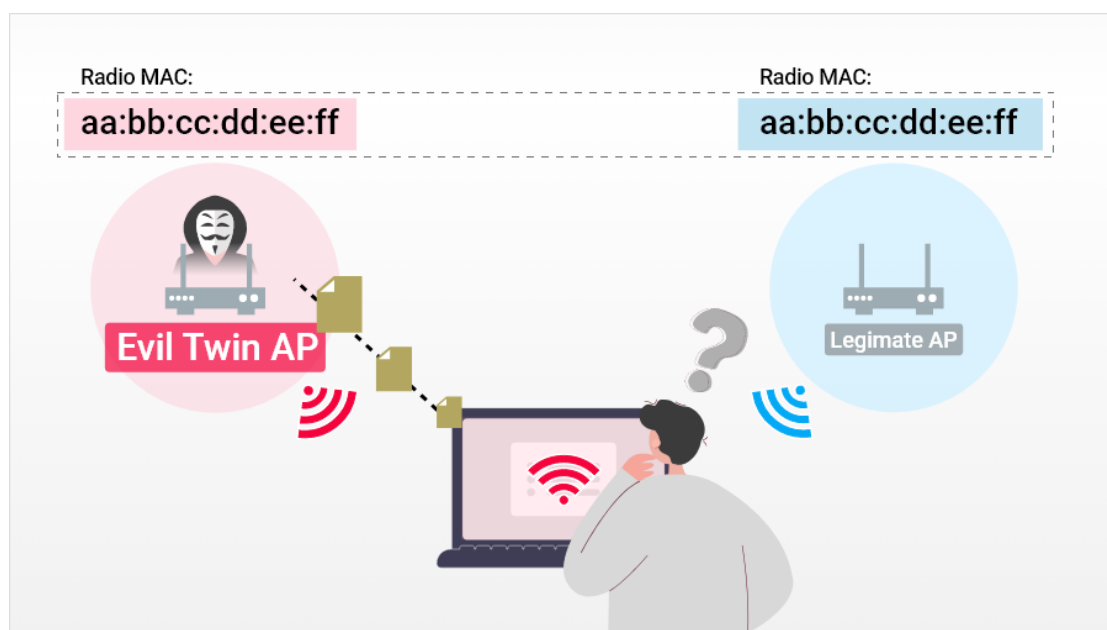
Figure10 -- Evil Twin Attack

Detection, Analysis, and Solution

Evil Twin Detection and Classification

AirGuard can detect the evil twin attack with an algorithm to distinguish if the frames are from a legitimate EnGenius AP or rogue AP mimicking the legitimate MAC address.

Two categories are classified:

- AP Spoofing

  The rogue AP will spoof the legitimate AP by sending frames with the same MAC address as the legitimate AP.

- AP impersonation

  The rogue AP not only mimics the MAC address of the legitimate AP but also its SSID name.

Enhanced Co-Defense Evil Twin Detection

Usually the way an AP can detect an evil twin is by leveraging the technique of "I know you are not me." So when "I," the detecting AP, detect frames with my MAC address, I know I didn't send the frame, so I know there is an evil twin around. However if an evil twin is outside the range of the victim AP, the victim AP won't be able to identify whether it's legitimate or fake.

EnGenius enhances the evil twin detection algorithm by letting all legitimate APs in the network know who my colleagues are and who the evil twin is.

Locate the Rogue Sources

With the EnGenius Cloud Map function, users can upload a floor plan and place an AP on the floor map to see the heat map of Wi-Fi coverage. Users can also add walls and doors to the floor plan to see how the obstacles affect the heat map.

For every rogue detected, AirGuard will list the detecting APs with signal strength (RSSI value) so users can leverage the floor plan to locate those detecting APs and discover if the rogue source might be nearby.
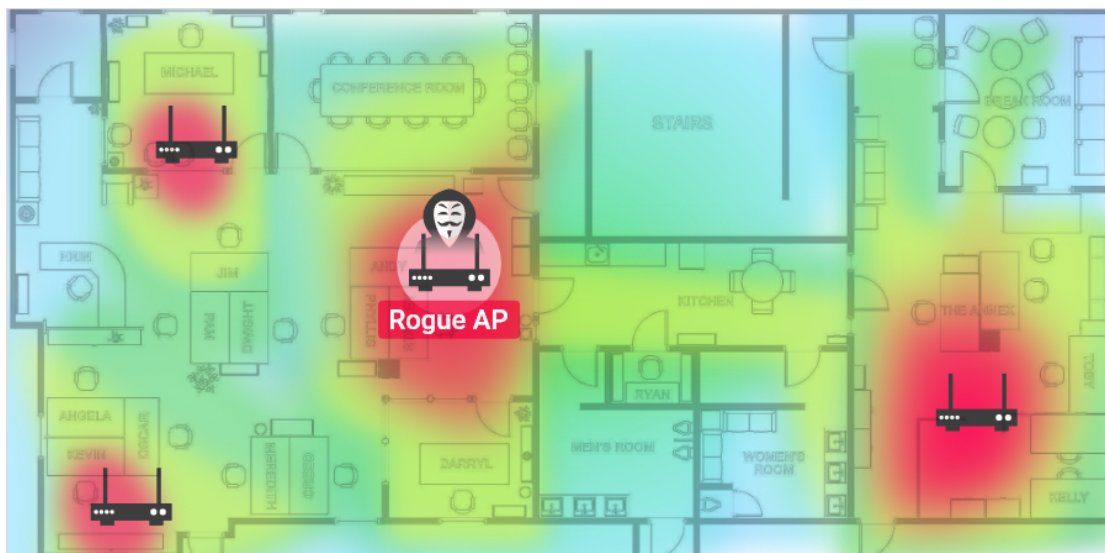

Figure11 -- Locate the Rogue Access Point with the Heat Map

Factory Built-In Certificate

Every EnGenius Cloud device has a built-in certificate installed at the factory, which is a mandatory component when communicating with EnGenius Cloud.

Therefore, an evil twin rogue AP can clone the same MAC as a legitimate AP. However, the rogue AP cannot connect to EnGenius Cloud without the built-in certificate to access the corporate network.

MFA for Device On-Boarding

To get the built-in certificate, the intruder might purchase an EnGenius AP from the market to function as an evil twin rogue AP; however, the AP needs to go through the MFA (multiple-factor authentication) process to be able to connect to the Cloud and join the network. First, EnGenius Cloud will check the certificate, MAC address, serial number, and key exchange process, and then check if the device is registered to an org or if the device is associated with the network.

No User Data and Secure Control Plane Protection

Only the control plane of device information and configuration goes to EnGenius Cloud. All other user data planes will not pass through the Cloud, so users don't need to worry if EnGenius Cloud will capture or store any user-sensitive data. EnGenius Cloud also encrypts the control plane information to prevent hackers from sniffing the management traffic.

EnGenius Solution and Benefits

AirGuard to Protect the WLAN

EnGenius AirGuard is the way EnGenius detects the attacks of RF jamming, de-authentication and dis-association abnormal frames, evil twins and identifies rogue SSID's from rogue APs. AirGuard also provides ways to set rogue rules and whitelist rules by identifying SSID names or radio MAC addresses.

Diagnostic Tools to Easily Find the Root Cause

EnGenius provides diagnostic tools for each AP to see the channel utilization of Wi-Fi and non-WiFi traffic, and waterfall spectrum to see what congestion of the channel looks like overtime. The tools also provide the capability to do ping, traceroute, and live client list.

Secured Cloud-connected Devices

Every EnGenius Cloud device has a built-in certificate from the factory and requires multiple authentication methods to be able to connect to EnGenius Cloud. Only management traffic will flow through EnGenius Cloud. All other user important data flows will not pass through EnGenius Cloud to protect user privacy.

Features for High Availability

EnGenius Cloud zero-wait DFS is perfectly suitable for a high density environment to leverage as many available channels as possible. Also, the auto-channel selection (ACS) algorithm allows the AP to find a clearer channel for best connection.

Security Compliance Features

The EnGenius Cloud AP supports myPSK by setting a unique PSK for each user to protect the passphrase from leakage. The Cloud AP also supports WPA3, 802.11w for more secure WLAN connection from breach over the air. EnGenius Cloud enforces the auto firmware upgrade to make sure all managed AP firmware versions are most up-to-date to amend any vulnerability issues. EnGenius Cloud also keeps checking if the default credential has changed and will keep warning users to change the default password. A sophisticated floor plan tool helps users to see heap maps of the floor and how walls, doors, and other obstacles affect coverage. Administrators can use the floor map combined with AirGuard to find the rogue source location by identifying the detected AP list on the floor map.

About EnGenius

EnGenius Technologies is a leading global manufacturer of pioneering wireless and voice communications. For more than 20 years, EnGenius has delivered best-in-class voice and data solutions that empower mobility, enhance productivity, and embrace simplicity. EnGenius prides itself on providing consumers with the best, most reliable, feature-rich, personalized network solutions to drive the success of their business.

Learn more about EnGenius Cloud: https://www.engenius.ai/cloud