Evil Twin Attacks: Vulnerabilities and Défense Mechanisms

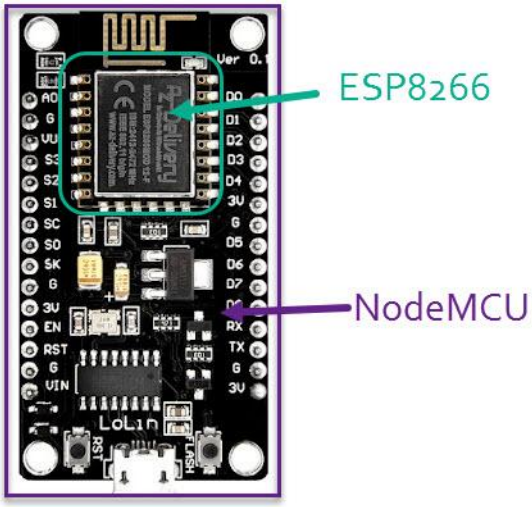
SAHIL HUSEN SHAIKH[1], PAWAR PRAJWAL ASHOK[2], PAWAR AMAR BHAU[3]
[1, 2, 3]Department of Computer Engineering, Navsahyadri Group of Institute, Pune

Abstract- The evolution of wireless communication technologies has greatly enhanced connectivity and digital engagement across the globe. However, this growth also exposes users to a range of sophisticated cybersecurity threats. Among these, the "Evil Twin Attack" stands out as one of the most deceptive, where attackers create rogue access points that impersonate legitimate Wi-Fi networks to intercept and manipulate user data. With the introduction of more secure and efficient protocols like Wi-Fi 6 and WPA3, there is an assumption of improved defense mechanisms. Despite these advancements, attackers continue to find loopholes and adapt their strategies. This paper presents a comprehensive study of Evil Twin Attacks, highlighting their operational framework, evolution, and implications in the context of modern wireless networks. It also explores the use of low-cost, readily available microcontrollers such as the ESP8266 and NodeMCU in executing these attacks. Furthermore, this study evaluates the effectiveness of existing defense mechanisms and proposes a multi-layered security strategy to mitigate potential threats.

Indexed Terms – NodeMCU, ESPTool, SSID Authentication Flaws, SSID Evil Twin Attack, Wi-Fi 6, WPA3, ESP8266, NodeMCU, Cybersecurity, Wireless Security, Rogue Access Point, IoT Security, Network Defense

I. INTRODUCTION

In an era driven by wireless connectivity, the reliance on Wi-Fi networks for both personal and professional communication has increased exponentially. Public Wi-Fi hotspots, while offering unmatched convenience, often become fertile grounds for cyber threats due to their open and unmonitored nature. The Evil Twin Attack is a particularly insidious type of cyberattack that exploits the trust users place in familiar network names (SSIDs). In this attack, a malicious actor sets up a counterfeit access point with the same SSID as a legitimate one. Unsuspecting users, upon connecting to the rogue access point, inadvertently expose their sensitive information such as login credentials, banking details, and personal communications. This paper delves into the mechanics of such attacks and evaluates whether current advancements like Wi-Fi 6 and WPA3 truly offer substantial protection. Through practical experimentation and a review of existing literature, this study aims to uncover the persistent gaps in wireless network security.



History:

The concept of Evil Twin Attacks emerged in the early 2000s, when wireless networking began to proliferate in public spaces. Back then, most wireless networks operated with minimal or no security, making them vulnerable to interception. Attackers exploited this by setting up rogue access points that mimicked legitimate networks. Tools like Aircrack-ng and BackTrack (later evolving into

Kali Linux) made it easier for even amateur hackers to conduct wireless attacks. The advent of inexpensive hardware like the ESP8266 and NodeMCU democratized access to technology that could be repurposed for malicious activities. While network security protocols evolved from WEP (Wired Equivalent Privacy) to WPA (Wi-Fi Protected Access) and eventually WPA2 and WPA3, each new iteration has had its own set of vulnerabilities. For example, WPA2 was compromised by the KRACK (Key Reinstallation Attack), illustrating that even advanced encryption methods can be exploited. This historical context underscores the importance of continuous vigilance and innovation in network defense.

Future Scope:

The threat landscape of Evil Twin Attacks is expected to evolve in parallel with the advancement of wireless technologies. As the world moves towards 6G networks, AI-powered IoT devices, and smart infrastructure, the attack surface for rogue access points will expand significantly. Future threats may involve AI-generated SSIDs, machine-learning-based impersonation techniques, and quantum computing-powered decryption methods. Consequently, the focus of future research should be on developing AI-driven intrusion detection systems, real-time network anomaly analysis, and quantum-resilient cryptographic protocols. Moreover, integrating Zero Trust Network Access (ZTNA) and Software-Defined Perimeter (SDP) models could offer robust frameworks for preemptive defense. Continuous user education and cybersecurity training will remain essential components of any long-term strategy against such attacks.

Objective:

- To comprehensively understand the technical workings and societal impact of Evil Twin attacks.
- To evaluate the robustness of modern wireless standards like Wi-Fi 6 and WPA3 against impersonation and spoofing attacks.
- To analyze the practicality and misuse of ESP8266/NodeMCU modules in real-world attack scenarios.
- To propose a comprehensive set of defense mechanisms, including technical, procedural, and educational approaches.
- To encourage the development of cybersecurity awareness programs aimed at end-users and network administrators.

Research Technology:

This study employs a combination of hardware and software tools to simulate and analyze Evil Twin Attack scenarios. The ESP8266 and NodeMCU microcontrollers, due to their low cost and high adaptability, serve as the primary platforms for constructing rogue access points. Software tools such as Wireshark, Bettercap, and WiFi-Pumpkin are utilized for network traffic monitoring, manipulation, and visualization. The security features of Wi-Fi 6—such as Orthogonal Frequency Division Multiple Access (OFDMA), Target Wake Time (TWT), and BSS Coloring—are studied to their role in minimizing interference and improving efficiency. WPA3's enhancements, including Protected Management Frames (PMF) and Simultaneous Authentication of Equals (SAE), are critically assessed for their effectiveness against rogue AP attacks. Comparative analysis is also conducted between WPA2 and WPA3 configurations to highlight security improvements and persistent vulnerabilities.

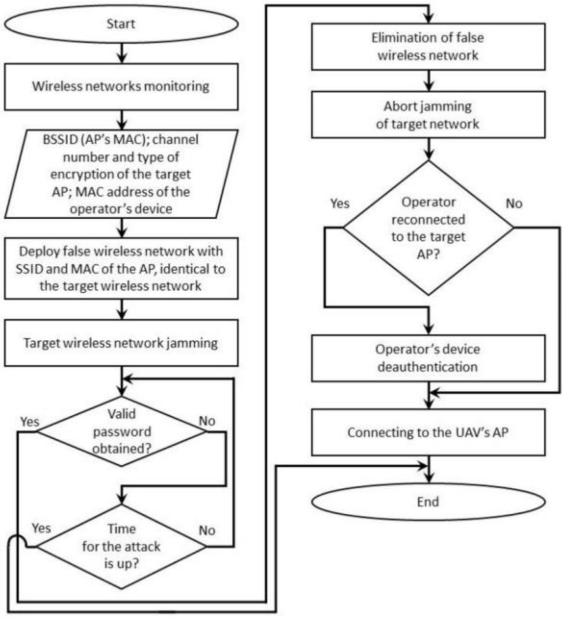
Attack Methodology: An Evil Twin attack typically proceeds in stepsokta.com:

- Setup fake AP: The attacker surveys the target area for a popular SSID (e.g. "CoffeeShop_WiFi") and configures a Wi-Fi device (like a laptop or microcontroller) to broadcast that SSID. Tools such as Hak5's WiFi Pineapple or free ESP8266-based firmware can turn a small device into a Wi-Fi hotspotokta.comgithub.com. The fake AP is usually placed physically closer to victims so its signal appears stronger, enticing clients to connectpeople.engr.tamu.eduokta.com.
- Force client disconnections: In many scenarios, the attacker sends deauthentication frames to clients on the legitimate AP (for example using an ESP8266 running "Deauther"

coderesearchgate.net). This forces devices off the real network. When devices automatically reconnect, they often pick the strongest matching SSID – the evil twin. Okta notes attackers can even launch a broad jamming (DoS) attack on the legitimate AP to kick off all users and lure them to the fake hotspotokta.com.

- Present captive portal or MITM proxy: Once victims connect to the evil twin, the attacker typically serves a malicious captive login page or proxy. For example, the attacker may replicate a login portal and capture credentials entered by usersokta.comokta.com. Alternatively, the attacker can transparently relay traffic while sniffing all unencrypted data. In either case, anything the user does online can be intercepted – e.g. usernames, passwords, session tokensokta.comresearchgate.net. If the user accesses non-HTTPS sites or services, the attacker can steal or alter sensitive data outright.

This process is deceptively simple and effective. As Song *et al.* observe, "many users will be tempted by the higher signal strength" of the evil twin; often the client's Wi-Fi logic automatically selects the strongest AP of a given SSIDpeople.engr.tamu.edu. In short, an Evil Twin attack exploits user trust in network names and device logic that is indifferent to which AP (real or fake) it is joiningresearchgate.netpeople.engr.tamu.edu.


Start
Wireless networks monitoring
BSSID (AP's MAC); channel number and type of encryption of the target AP; MAC address of the operator's device
Deploy false wireless network with SSID and MAC of the AP, identical to the target wireless network
Target wireless network jamming
Yes
Valid password obtained?
No
Yes
Time for the attack is up?
No
Elimination of false wireless network
Abort jamming of target network
Yes
Operator reconnected to the target AP?
No
Operator's device deauthentication
Connecting to the UAV's AP
End

Methodology:

Testbed Setup: A controlled environment was created using routers that support Wi-Fi 6 and WPA3, alongside legacy WPA2-compatible devices for comparative study.

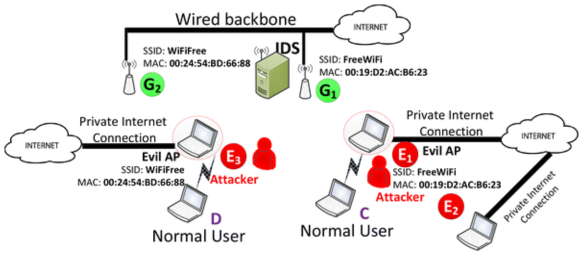
Rogue Access Point Deployment: Custom firmware was uploaded onto ESP8266 and NodeMCU boards to mimic the SSIDs and signal strength of legitimate access points.

User Simulation: Devices were made to automatically connect to the rogue AP to observe behavior and vulnerabilities.

Data Capture and Analysis: Wireshark and Bettercap were employed to capture and analyze packet data from victim devices to identify potential information leakage.

Security Feature Testing: Features like PMF enforcement, certificate validation prompts, and MAC address filtering were tested under various configurations.

Defense Evaluation: Deauthentication detection tools, user alerts, and network segmentation methods were tested to measure their effectiveness in mitigating attacks.



1. Low-Cost Evil Twin Deployments: ESP8266 and NodeMCU

Modern attackers often use tiny microcontroller boards to launch Evil Twin attacks. The ESP8266 (and its development board NodeMCU) is an inexpensive Wi-Fi–enabled microcontroller that has gained popularity in the IoT and security communitiesresearchgate.netgithub.com. For a few dollars, an attacker can obtain an ESP8266 and program it using Arduino or MicroPython to act as a Wi-Fi AP (using softAP mode). These boards are compact and can be battery-powered, making them easy to conceal.

Researchers have demonstrated complete Evil Twin toolkits on ESP8266 boards. For instance, one project ("EvilTwin-ESP8266") pairs a NodeMCU with a captive portal script to scan for networks, create a fake AP, deauthenticate clients, and perform a man-in-the-middle attackgithub.com. The GitHub "EvilTwinFramework" README succinctly defines the concept: the attacker *"creates a fake Wi-Fi hotspot with the same or similar name (SSID) as a trusted network, luring unsuspecting users to connect"*github.com. Similarly, an academic outline of an ESP8266-based attack flow notes that Evil Twin hotspots "mimic actual AP functions" and are used to carry out Wi-Fi phishingresearchgate.net.

In practical terms, an attacker might use one ESP8266 running deauthentication code to knock users off the real AP, and a second ESP8266 (or the same board reconfigured) to host the evil twin SSID. Devices like Stefan Kremser's "ESP8266 Deauther" and "Wi-Fi Pineapple" firmware make it possible to automate these steps. For example, a lab setup might involve programming two NodeMCUs: one continuously broadcasting a strong, fake SSID (with a login page), and the other repeatedly sending disassociation packets to force clients onto that fake APresearchgate.netresearchgate.net. Once victims connect, the attacker can see all transmitted data. These proofs-of-concept emphasize how ubiquitous and accessible the threat is — no specialized hardware is needed beyond a few dollars of microcontrollers and some open-source coderesearchgate.netgithub.com.

2. Vulnerabilities in Modern Wi-Fi Networks (Wi-Fi 6 and WPA3)

Even as Wi-Fi technology advances, networks remain vulnerable to Evil Twin–style attacks because fundamental design flaws and implementation bugs persist. Recent research has highlighted several notable weaknesses in the latest standards:

SSID Authentication Flaws: A May 2024 study (CVE-2023-52424) discovered that the IEEE 802.11 standard does *not* always tie the network's SSID into the cryptographic handshakethehackernews.com. This allows an attacker to trick a client into joining a malicious AP ("WrongNet") while the user interface still displays the original network name ("TrustedNet")thehackernews.com. In practice, a device may think it's on the secure enterprise network even as it is connected to an attacker's AP. This "SSID Confusion" attack also tricks some VPN clients to disable themselves (they see a "trusted" SSID) and thus leaves traffic exposedthehackernews.com. Crucially, this flaw affects *all* Wi-Fi generations (including WPA3 and 802.11ax), meaning even Wi-Fi 6 and WPA3 networks can be downgraded if they reuse SSIDs or credentials across bandsthehackernews.com. Network designers are advised to use unique passwords per SSID and distinct RADIUS identities to avoid confusionthehackernews.com.

WPA3 Dragonfly and Transition Mode: WPA3's Simultaneous Authentication of Equals (SAE) "Dragonfly" handshake is designed to be resistant to offline dictionary attacks. However, academic work (Dragonblood) exposed side-channel leaks in early WPA3 implementations. For example, timing and cache-based side channels on the Dragonfly handshake (especially with certain elliptic curves) could leak bits of the passwordwpa3.mathyvanhoef.com. Even more fundamentally, WPA3 devices must support a "transitional mode" to allow WPA2 connections.

Researchers have shown that this transition can be exploited: an attacker can force a WPA3-capable client into using a weaker WPA2 handshake (with a known SSID) and then mount a dictionary attack on that WPA2 connectionsecurityaffairs.com. In short, if an AP accepts both WPA3 and WPA2 (for legacy devices), an evil twin can pretend only to offer WPA2 and trick clients into a less secure exchangesecurityaffairs.com.

Wi-Fi 6 (802.11ax) Protocol Issues: Newer Wi-Fi standards add features but do not eliminate older attacks. For example, NIST notes a design issue (CVE-2022-47522) where an attacker can send crafted Power Save and authentication frames to remove a client's encryption context on an AP, allowing interception of otherwise-protected datanvd.nist.gov. More broadly, the FragAttacks research (2021) showed that nearly every Wi-Fi implementation (802.11a/b/g/n/ac/ax) was vulnerable to frame fragmentation/aggregation flaws. These allowed attackers to forge or replay frames regardless of the authentication protocol. (In practice, FragAttacks can be mitigated by patching firmware, but legacy and unpatched devices remain at risk.)

Legacy WPA2 and KRACK: Although WPA3 aims to replace WPA2, many networks still use WPA2, which had its own share of vulnerabilities. The 2017 KRACK attacks (key reinstallation attacks) exploited how WPA2 handled handshake replay and are a cautionary example of how even encrypted networks can be broken. WPA3 fixes the KRACK issues, but if the Evil Twin attack downgrades a client to WPA2, KRACK could be relevant again if keys are reused improperly.

General Factors: Other Wi-Fi features (WPS, SoftAP modes, public login portals) also introduce risk if misconfigured. For example, an Evil Twin could use an open SSID with a captive portal, or spoof a hidden SSID, etc. The bottom line is that even the latest Wi-Fi 6 and WPA3 protocols are not immune. Design-level issues like SSID confusion and transitional downgrade allow cunning attackers to circumvent improvements, so networks must rely on additional safeguards beyond protocol-level encryptionthehackernews.comnvd.nist.gov.

3. Example Evil Twin Setups (Safe Demonstrations)

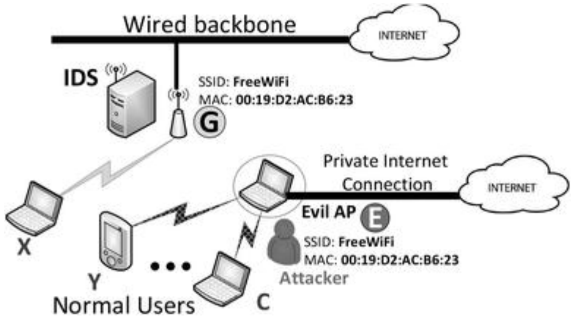
Although we strongly condemn malicious use, security researchers have demonstrated Evil Twin setups to highlight vulnerabilities. Common examples include:

NodeMCU "Evil Phone": A proof-of-concept called *Loki* assembled an ESP8266 NodeMCU with a small LCD, buttons, and battery to create a handheld "evil phone." This device could scan for nearby SSIDs and, at a button press, broadcast the chosen SSID as a fake AP, complete with LEDs and buzzers to indicate activitymedium.com. The project description lists all components (NodeMCU, OLED screen, antennas, etc.) used to build an Evil Twin tester.

ESPTool (Hackaday): The *ESPTool* project created a NodeMCU-based Wi-Fi security tester. Although it includes many attacks, it has an "evil twin hotspot" mode for demonstration. The device mimics a specific SSID, shows a web dashboard, and can capture credentials (for testing on the attacker's own network)hackaday.iohackaday.io. The author explicitly warns it is for education only, illustrating how simple it is to replicate such attacks with a few components.

Hak5 Wi-Fi Pineapple: While not a microcontroller board, the commercial Wi-Fi Pineapple is essentially a portable Evil Twin generator. It runs specialized firmware on embedded hardware to scan and clone SSIDs, deauth clients, and log all traffic. Demonstrations show that tools like the Pineapple can be used "out of the box" by even untrained users to launch Evil Twin attacks.

Moreover, dozens of online tutorials and GitHub repositories (e.g. *samphoerna/EvilTwin-ESP8266*github.com) provide step-by-step code to set up a rogue AP on an ESP8266. These resources illustrate that any modern computer or microcontroller can be a vector. Even smartphone apps exist that can tether in hotspot mode with a chosen SSID. The key lesson from these examples is that the barrier to entry is extremely low: a few lines of code and a cheap board allow one to mimic a Wi-Fi network and harvest data.



Defense Mechanisms

Combatting Evil Twin attacks requires layers of defense at the user, enterprise, and technological levels. Some key strategies include:

User Best Practices: Individuals should treat public Wi-Fi with caution. Simple measures can thwart attackers. For example, avoid auto-connecting to open networks; disable the “connect automatically” feature so that you must manually choose networks each timeokta.com. Always use a VPN on untrusted Wi-Fi. A VPN encrypts all traffic end-to-end, so even if an evil twin intercepts packets, it cannot decipher themokta.com. Be mindful of login forms: if a captive portal appears, verify its authenticity (e.g. ask staff to confirm the correct login URL or SSID). The FTC and security blogs advise users to turn off Wi-Fi when not needed, “forget” networks after use, and keep device software updated. Finally, favor HTTPS sites and apps (which encrypt data regardless of Wi-Fi). Okta explicitly recommends: *“The quickest and easiest way to stay safe is to avoid any public WiFi connection… If you must connect via public WiFi… Use VPN… Turn off autosaves… Be careful about the logins you use”*okta.com.

Enterprise Configuration: Organizations can greatly reduce the risk by enforcing strong Wi-Fi policies. This starts with 802.1X authentication and certificates (WPA2/WPA3-Enterprise with EAP-TLS) instead of preshared keys. Certificate-based Wi-Fi prevents users from logging into a fake AP unless the attacker can present a valid server certificate. Enterprises should also disable open or easily-duplicated SSIDs: do not reuse a single passphrase across multiple SSIDs or between 2.4/5 GHz bandsthehackernews.com. Segment the network: offer a separate guest SSID with its own password and encryption, isolated from the corporate LANcisa.gov.

Promote multi-factor authentication (MFA) for sensitive services so that even if a password is stolen, a second factor blocks accesscisa.gov.

4. Wireless Intrusion Detection/Prevention (WIDS/WIPS): Large organizations should deploy WIDS/WIPS tools that continuously scan the air for rogue APs and abnormal behavior. These systems use techniques like RF fingerprinting and motion detection to flag new APs with duplicate SSIDs or unusual MAC addresses. A WIPS can even automatically block or deauthenticate known rogue devices. CISA recommends “deploying a wireless intrusion detection system (WIDS) and a wireless intrusion prevention system (WIPS) on every network”cisa.gov. Commercial solutions (from Cisco, Aruba, etc.) integrate AP-side scanning or dedicated sensors to alert on Evil Twin attempts. In tandem, regular site surveys and wireless audits help verify only authorized APs are present.

AI/ML-Based Detection: Recent research has explored using machine learning to spot Evil Twins. For example, one approach trains a classifier (e.g. k-Nearest Neighbors or Random Forest) on beacon signal characteristics to distinguish a legitimate AP from a clonemdpi.com. Others use deep learning on Wi-Fi signal preambles: a CNN model can learn the unique “radio signature” of an AP’s hardware and flag when an unexpected AP claims the same identityresearchgate.net. These systems analyze anomalies like inconsistent PHY-layer features or sudden jumps in RSSI distributions. While such ML defenses are largely experimental today, they hold promise for client-side apps or AP firmware that can recognize impostor networks. In practice, they could alert a user if, say, the channel or signal pattern of “MyCoffeeShopNet” suddenly changes. (These AI methods achieved high accuracy in controlled testsmdpi.comresearchgate.net, though real-world variability remains challenging.)

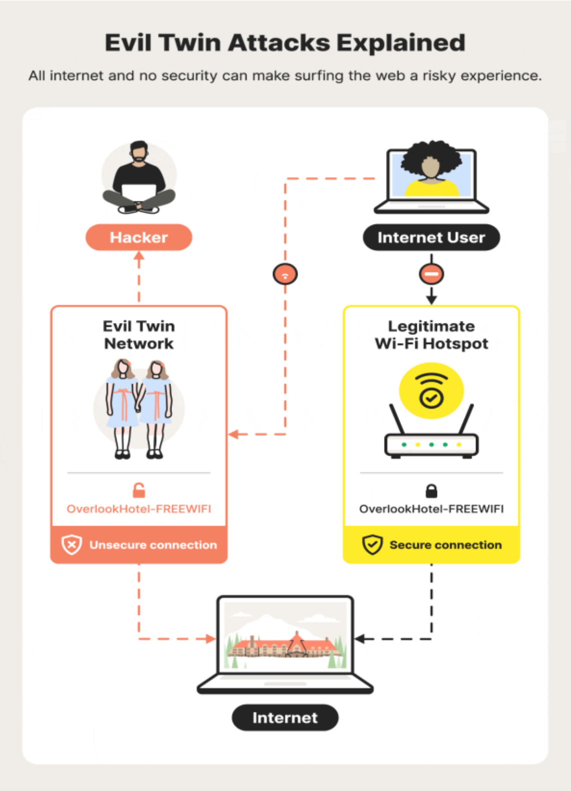
Additional Technical Protections: Whenever possible, use the latest encryption standards: WPA3 (especially Enterprise mode) offers stronger cryptography and mandatory Protected Management Frames (PMF) which can prevent deauthentication floods. Keep all network drivers and firmware updated to patch known flaws. Disable deprecated protocols (e.g. WEP, WPS) that could simplify attack setup. Some OSes and devices offer warning systems: for instance, Apple devices now can detect captive portals with untrusted SSL or warn when a Wi-Fi login page is suspicious. Encouraging user awareness (via training) is also crucial – if people know that "CoffeeShop Wi-Fi" might be risky, they are more likely to open the VPN or verify with an employee.

5. Recommendations by Environment

Home: Use a strong unique passphrase for your home Wi-Fi and WPA3 if available. Give your home SSID a hard-to-guess name (avoid common names). Enable client isolation on home routers to limit any one compromised device. Even at home, do not allow open (unencrypted) guest networks. Educate family members that any login page asking for personal credentials on home Wi-Fi should be treated with skepticism.

Public Wi-Fi Users: Treat all public networks as hostile. Consider disabling Wi-Fi completely except when needed, and always use cellular data or a VPN for sensitive transactions. Never assume that a network offered in a cafe or airport is legitimately provided by that venue – confirm the exact SSID with staff if in doubt. If you see multiple APs with the same name, avoid connecting until you can verify which is real.

Corporate/Enterprise: Follow CISA's guidance: enforce WPA3-Enterprise with 802.1X, roll out WIDS/WIPS, segment guest access, and use MFA everywherecisa.govcisa.gov. Have a centralized system to detect and respond to rogue APs. Rotate and isolate credentials across SSIDs so one AP compromise doesn't cascade. Implement network access control (NAC) so devices without current patch or certificate can't join. Finally, conduct regular penetration tests: ethical hackers should attempt Evil Twin attacks as a drill, verifying that the organization's defenses (e.g. VPN-only, certificate pinning, or AP alarms) do in fact alert and protect.



CONCLUSION

Evil Twin Attacks remain a persistent and potent threat in the cybersecurity landscape, even as wireless technology continues to evolve. Despite the improvements introduced with Wi-Fi 6 and WPA3, these standards are not invulnerable, particularly in the absence of proper implementation and user awareness. The accessibility of tools like ESP8266 and NodeMCU has significantly lowered the barrier for launching sophisticated attacks, making adopting a comprehensive defense strategy imperative. This strategy should encompass technical solutions such as anomaly detection systems, enforcement of modern security protocols, and regular firmware updates, as well as non-technical measures like user training and administrative vigilance. A multi-pronged, layered approach to network security will safeguard wireless ecosystems against future iterations of Evil Twin and other impersonation-based threats.

Evil Twin attacks exploit both human trust and technical design gaps to infiltrate wireless networks. As long as attackers can freely forge AP identities, merely increasing encryption levels (WPA3, Wi-Fi 6) is not a panacea. The modern Wi-Fi ecosystem, from devices to drivers, contains a variety of vulnerabilities – from Dragonfly side channels to SSID confusion flawsthehackernews.comnvd.nist.gov – that can aid an evil twin in its deception. Defending against Evil Twins therefore requires a multi-layered approach. Users must practice safe Wi-Fi habits (VPNs, verifying SSIDs), and organizations must deploy robust authentication, monitoring, and anomaly detection (including advanced AI methods) okta.comresearchgate.net. By combining vigilance, user education, and technical controls like WIPS/WIDS and certificate-based Wi-Fi, networks can greatly reduce the risk of falling prey to an evil twin.

Sources: This discussion is informed by recent cybersecurity articles and research. Definitions and attack descriptions are drawn from Okta's technical blogokta.comokta.com and authoritative studiespeople.engr.tamu.eduresearchgate.net. Modern vulnerabilities (e.g. SSID Confusion, Dragonblood) are documented in industry reportsthehackernews.comwpa3.mathyvanhoef.comsecurityaffairs.com. Examples of ESP8266-based attacks come from research and open-source projectsresearchgate.netgithub.com. Defense recommendations follow guidelines from CISA and cybersecurity expertscisa.govokta.com. All cited sources are reputable security publications and academic works.

REFERENCES

[1] IEEE 802.11ax (Wi-Fi 6) Specification

[2] WPA3 Security Enhancements - Wi-Fi Alliance

[3] ESP8266 Technical Reference Manual - Espressif Systems

[4] "WiFi-Pumpkin: Framework for Rogue Access Point Attacks" - GitHub

[5] Aircrack-ng Suite Documentation

[6] "Understanding Evil Twin Attacks" – Journal of Cybersecurity Research, 2023

[7] Bettercap Documentation – https://www.bettercap.org/docs/

[8] Wireshark Official Documentation – https://www.wireshark.org/

[9] Ali, S., & Khan, A. (2022). "A Comparative Study on Wi-Fi Security Protocols." International Journal of Computer Networks & Communications.

[10] Zhang, M. et al. (2021). "Security Challenges in Wireless Networks: A Case Study on Evil Twin Attacks." Journal of Information Security.