A Trusted Wireless Environment: The Cornerstone of Responsible Wi-Fi Deployment

Table of Contents

A **Trusted Wireless Environment** is a framework for building a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure. In this paper you will learn about the evolution of Wi-Fi and how it has spurred the growth of the six known Wi-Fi threat categories: (1) rogue access point, (2) rogue client, (3) neighbor access point, (4) ad-hoc network, (5) "evil twin" access point, and (6) misconfigured access point. The latest Miercom report clearly demonstrates which vendor's products protect from these six Wi-Fi threat categories, indicating the solutions that support the new **Trusted Wireless Environment** for defending your airspace and protecting your business 24/7.

The Evolution of Wi-Fi

With the rise of Internet-enabled devices, so did wireless security risks. In 2017, there were 8.4 billion connected devices and the volume is expected to hit 20.4 billion by 2020, according to analyst firm Gartner. When wireless devices are hacked, it can result in a wide range of issues, including denial of service, compromised personal data, and major infrastructure failures – all costing companies time and expense. Hackers prefer to go after the weak link in the security chain and it doesn't take much to hack into a Wi-Fi network using easily accessible tools and a plethora of online how-to videos. Even the most rookie hacker can intercept traffic flowing over Wi-Fi and steal valuable data from your smartphone, tablet, smartwatch, or laptop. What's worse – your business networks become compromised due to malware implanted and credentials stolen over Wi-Fi, and it can cost millions in fines and breach remediation expenses to fix.

Did you know?

1. **$600,000** = Cost of FCC fine issued to a hotel chain using a wireless security system in violation of regulations[1]
2. **$1 Billion** = Estimated cost of the 2005 TJ Maxx Wi-Fi breach[2]

The Six Known Wi-Fi Threat Categories

1. **Rogue access points** are connected to the authorized network, usually with an open SSID, allowing attackers to bypass perimeter security. They can be a physical access point (AP), or one created in software on a computer and bridged to the authorized network.

2. **Rogue clients** are defined as clients that previously connected to a rogue access point or other malicious access point within the range of a private network. This client could have been victimized by a plethora of man-in-the-middle (MitM) attacks that include loading ransomworms, malware, or backdoors onto the client.

3. **Neighbor access point** is an independent AP that is not under the control of network administrators. It provides access through a separate network and could be used to bypass internal security or content-filtering policies.

4. **Ad-hoc connection** is a peer-to-peer Wi-Fi connection between clients that can circumvent perimeter security and allow clients to evade firewalls, and content and security controls.

5. **Evil twin access point** is one that mimics a legitimate AP by spoofing its SSID and unique MAC address. Besides a commonly known physical access point, attackers can use software that utilizes Wi-Fi network adapters in standard laptops and tablets or certain native mobile devices to minimize their physical footprint and avoid drawing attention to large antennas, devices, or cables.

6. **Misconfigured access points** are connected to your private network with a configuration that does not conform to your security policies and allows insecure connections. For example, if your Wi-Fi security policy is configured in Wi-Fi Cloud to only allow SSIDs to broadcast on your authorized APs with WPA2 encryption and an admin accidentally misconfigures an authorized AP to broadcast an open, unencrypted SSID, that AP would be considered misconfigured.

1. http://www.networkcomputing.com/wireless/fcc-marriott-wifi-blocking-fine-opens-pandoras-box/2053001237
2. http://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

Pillars of a Trusted Wireless Environment

The Wi-Fi systems that you have been installing are no longer adequate. Your employees, vendors, and guests rely on you to keep them safe and it is your responsibility to be knowledgeable about Wi-Fi security risks and how they impact your organization. As you face the responsibility of evolving your Wi-Fi networks to include security, you're finding that many vendors, like Cisco Meraki, Aruba and Ruckus do not enable you with the right products.

Your organization needs technology and solutions that enable you to build a complete Trusted Wireless Environment – delivering on each of the three core pillars of market-leading performance, scalable management, and verified comprehensive security that protects from all six known Wi-Fi threat categories.

A Trusted Wireless Environment is a framework for building a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure. Businesses face the responsibility to build Trusted Wireless Environments protecting their employees and customers from hackers who easily exploit the weak or non-existent security of traditional Wi-Fi networks.

Companies that offer a Trusted Wireless Environment deliver on these three core pillars:

1. **Market-Leading Performance:** You should never be forced to compromise security to achieve adequate performance to support your environment with the speed, connections and client density that it needs.
2. **Scalable Management:** With easy set-up and management, you should be able control your entire wireless network, big or small, from a single interface and execute key processes to safeguard the environment and its users.
3. **Verified Comprehensive Security:** Many vendors rely on ambiguity when it comes to delivering secure Wi-Fi. You need proof that your security solution defends your business against Wi-Fi attacks and can deliver on the following benefits:
   - Provide automatic protection from the six known Wi-Fi threat categories
   - Allow legitimate external access points to operate in the same airspace
   - Restrict users from connecting to unsanctioned Wi-Fi access points

Miercom Test and Key Findings

Miercom – a widely recognized company that generates industry reports based on hands-on competitive testing – recently covered a ground-breaking, never-been-done series of tests, to determine how effectively an access point can support real-time applications such as voice, video, and data while simultaneously detecting and preventing the most common Wi-Fi security threats.

For each Wi-Fi threat, they recorded the time to detect and time to prevent using Wi-Fi equipment from WatchGuard, Aruba, Cisco Meraki, and Ruckus.

Test Details

Access points, firmware and management platforms used in all tests:

Vendor	Access Point Model	Management Platform	Firmware
WatchGuard	AP420	Wi-Fi Cloud	8.5.0-658
Aruba	AP335	Aruba Central / Aruba Instant	8.3.0.0_64659
Cisco Meraki	MR53	Meraki Cloud Controller	MR 25.11
Ruckus	R710	Zone Director 1200	10.1.1.0

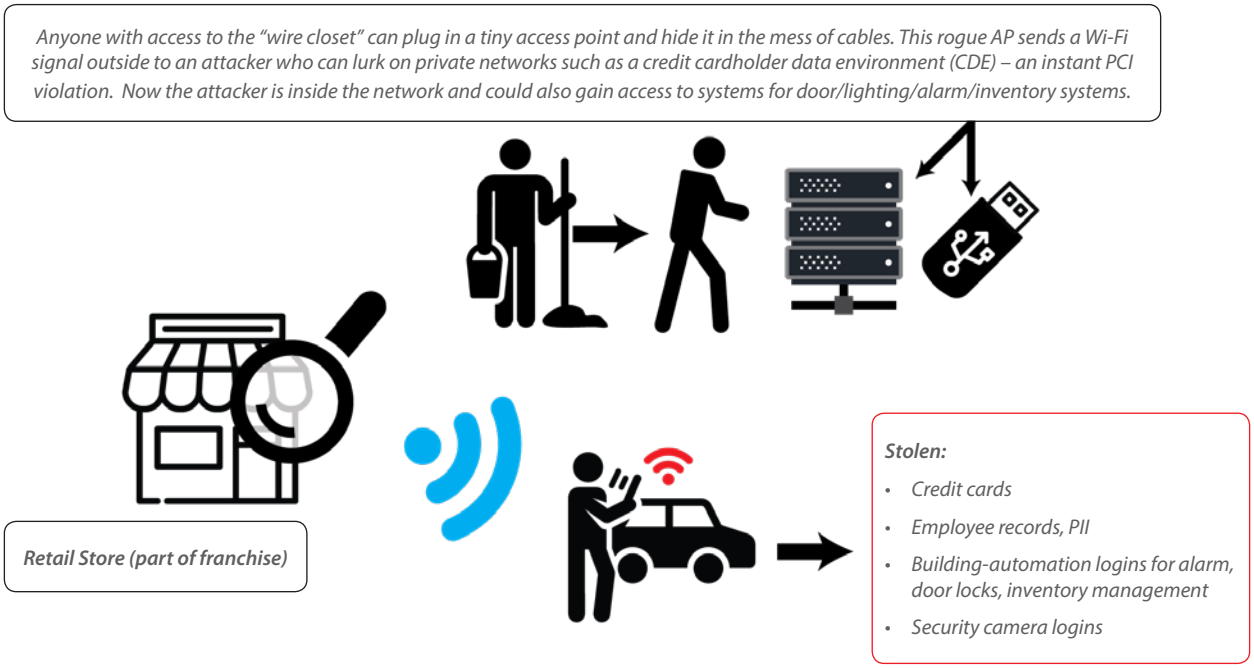
In every Wi-Fi threat test case, IP multi-cast traffic was generated to keep the access points busy. In a real environment, APs need to be able to serve clients as well as provide security protection without impacting the quality of user experience. Multi-cast to unicast conversion was utilized in all APs and served to a total of 18 clients, with 6 on 2.4 GHz and 12 on 5 GHz. Spectrum analysis was performed continuously to confirm that no other APs nearby were utilizing channel 1 or 149-153 during the testing. Channel utilization did not exceed 60% for 2.4 GHz or 40% for 5 GHz during the tests.

Client devices used for continuous traffic generation during all Wi-Fi threat tests:

- 18 - Acer Laptops with Qualcomm Atheros 1x1 Wave 2 WLAN capability and Windows 10 OS

Rogue AP Test Details

Rogue APs are a dangerous Wi-Fi security threat where an AP is plugged into a private network by a nefarious person often broadcasting hidden SSID(s) so that attackers within range can gain access to internal network resources over the air. Common targets include credit card data (CDE or cardholder data environment), which is a serious PCI compliance risk, and building-automation controls for alarms, door locks, and video cameras.



Clients used in Rogue AP test:

- 1 - OnePlus2 QCA 1x1 Wave Android
- 1 - Samsung S2 Tab BCM 2x2 Wave 1 Android

AP used as the Rogue AP:

- Apple Airport Express*

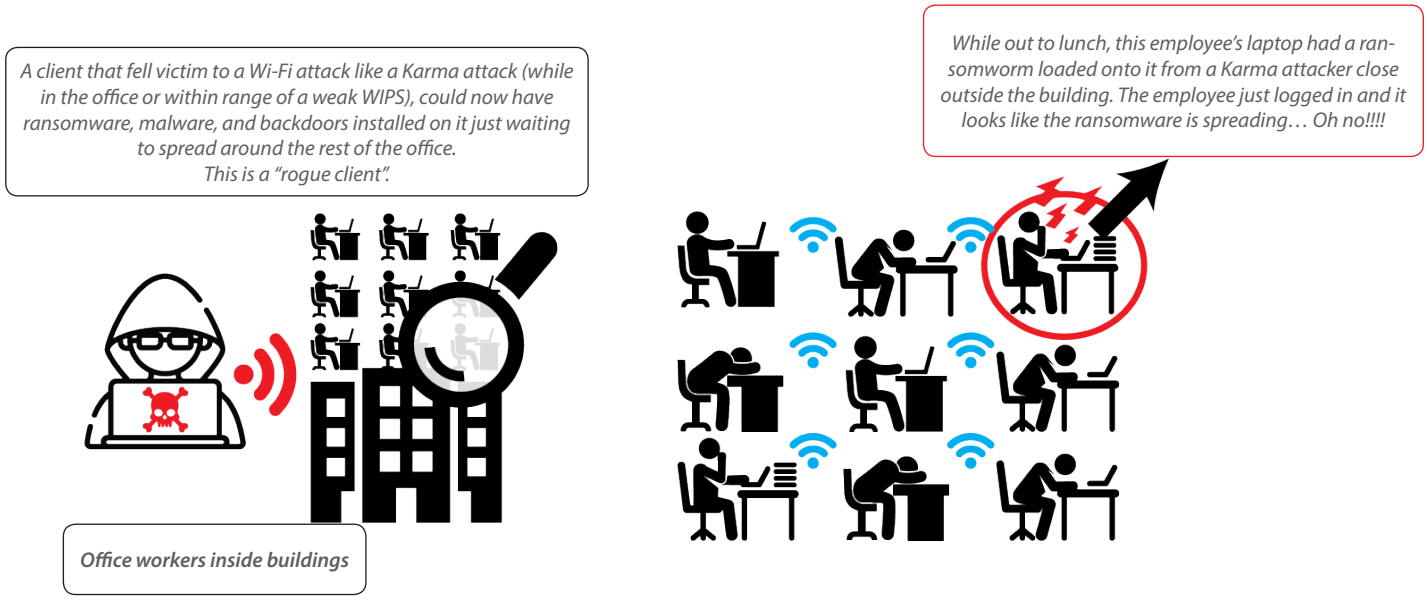
** Many Wi-Fi security solutions utilize MAC address correlation to identify devices on the same network. The Apple AirPort AP used as the Rogue AP in this test has a differential of more than 5 bits between the wired and wireless interfaces. This variance could potentially cause a correlation algorithm to fail, making the AP undetectable on the wire and therefore undetectable as a rogue AP.*

Test Method:

1. Configure Apple AirPort Open/NAT mode
2. Connect Apple AirPort to same network as DUT
3. Enable auto prevention
4. Start timer when Apple AirPort SSIDs are detected by NetSpot or inSSIDer
5. Connect clients to Apple AirPort (1 Client to 2.4 GHz and 1 Client to 5 GHz)
6. From clients connected to Rogue AP, ping wired host continuously
7. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Rogue Client Test Details

Any client previously connected to a rogue AP or other malicious AP within range of a private WLAN network is considered a rogue client. This client could have been victimized by a plethora of man-in-the-middle (MitM) attacks that include loading ransomworms, malware, or backdoors onto the client.



Clients used in Rogue Client test:

- 1 - Samsung S2 Tab BCM 2x2 Wave 1 Android

Test Method:

1. Start with an Uncategorized Client
2. Bring up a Rogue AP (e.g. Apple-Rogue and/or AP discoverable by MAC adjacency for DUT that is unable to detect the Apple AirPort as "Rogue")
3. Connect Uncategorized Client to Rogue AP
4. Confirm Rogue AP is seen by DUT as "Rogue"
5. Verify Uncategorized Client is now recognized as Rogue Client
6. Disconnect Rogue Client from Rogue AP
7. Enable auto prevention in DUT
8. Connect client to Authorized AP and ping wired host continuously
9. Start timer as soon as Rogue Client connects to Authorized AP
10. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Neighbor AP (Misbehaving Client) Test Details

Environments such as offices, airports, healthcare locations, retail, and restaurants often contain a mixture of company-managed Wi-Fi client devices that are only intended to connect to company-managed SSIDs so that network security controls, encryption, and traffic visibility can be maintained, while public guest clients are not company-managed. In these environments, company-managed Wi-Fi clients should never be allowed to connect to nearby 3rd party, or neighbor, SSIDs. Doing so bypasses all important network security controls and traffic visibility for network administrators. For example, a point of sale (POS) handheld card reader that operates over Wi-Fi should only be allowed to connect to the private company-managed SSID within the restaurant and not nearby public hotspots or mobile/LTE Wi-Fi hotspots that are likely not encrypted and could expose sensitive information to attackers looking to intercept the data over the air. Another common example is in corporate offices where clever employees figure out they can connect their company-managed smartphones, laptops and tablets to nearby public Wi-Fi hotspots or internal guest Wi-Fi SSIDs to bypass web content-filtering controls.

Employees frustrated by their corporate firewall blocking websites have cleverly figured out easy ways to bypass this important network security control: by using their smartphones' hotspot feature and tethering their corporate laptops to them or by connecting to guest Wi-Fi either inside the office or nearby from neighbors.

Clients used in the Neighbor AP test:

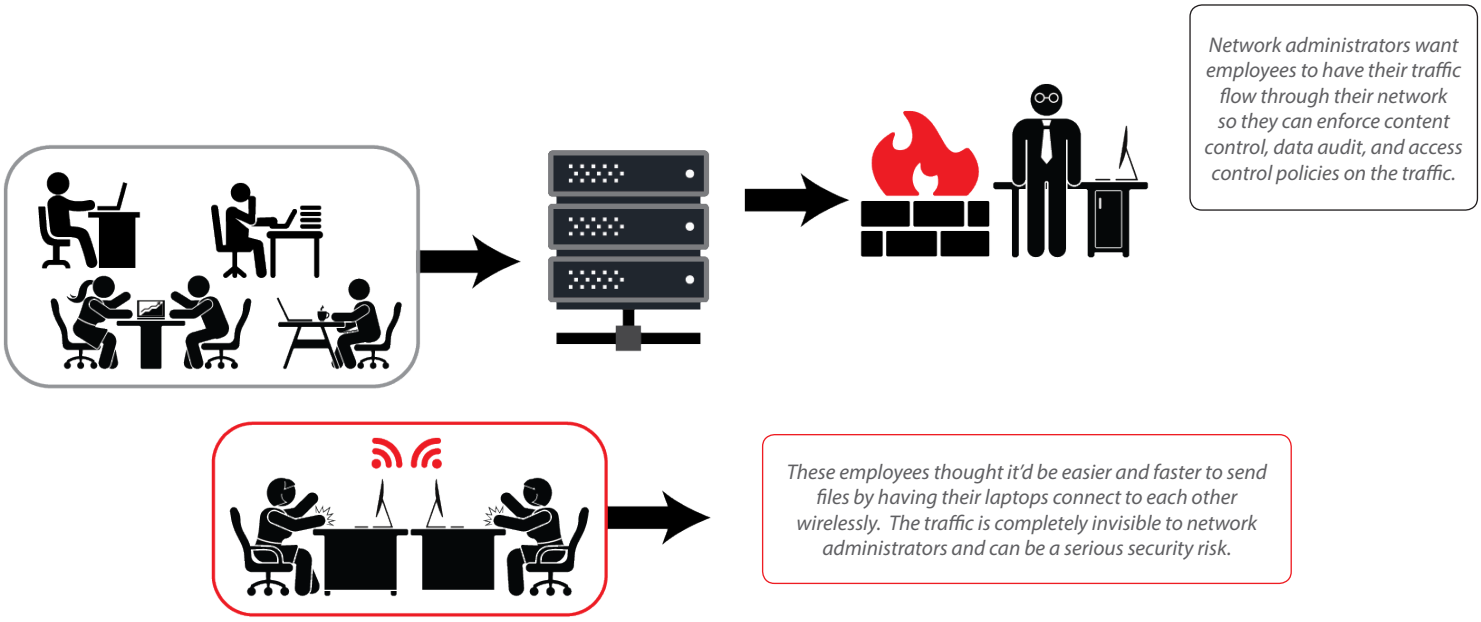
2 - Samsung S2 Tab BCM 2x2 Wave 1 Android

Test Method

1. Add authorized SSID
2. Verify AP as listed as Authorized AP in user interface
3. Connect client to Authorized AP
4. Verify client is listed as Authorized Client in user interface
5. Bring up Neighbor AP (e.g. Mobile HotSpot)
6. Enable auto prevention in DUT
7. Connect a neighbor client to Neighbor AP and ping local wired host continuously
8. Connect Authorized Client to Neighbor AP and ping local wired host continuously
9. Start timer as soon as Authorized Client connects to Neighbor AP
10. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Ad-Hoc Network Test Details

It can be a security risk in certain environments when Wi-Fi clients connect directly to each other, as the traffic generated in this peer-to-peer session is invisible to network administrators.



Network administrators want employees to have their traffic flow through their network so they can enforce content control, data audit, and access control policies on the traffic.

These employees thought it'd be easier and faster to send files by having their laptops connect to each other wirelessly. The traffic is completely invisible to network administrators and can be a serious security risk.

Devices used in the Ad-Hoc Network test:

1 - MacBook Air BCM 2x2 Wave 1 MacOS (as Ad-Hoc AP)

1 - Acer Laptop with Qualcomm Atheros 1x1 Wave 2 and Windows 10 OS (as client)

Test Method:

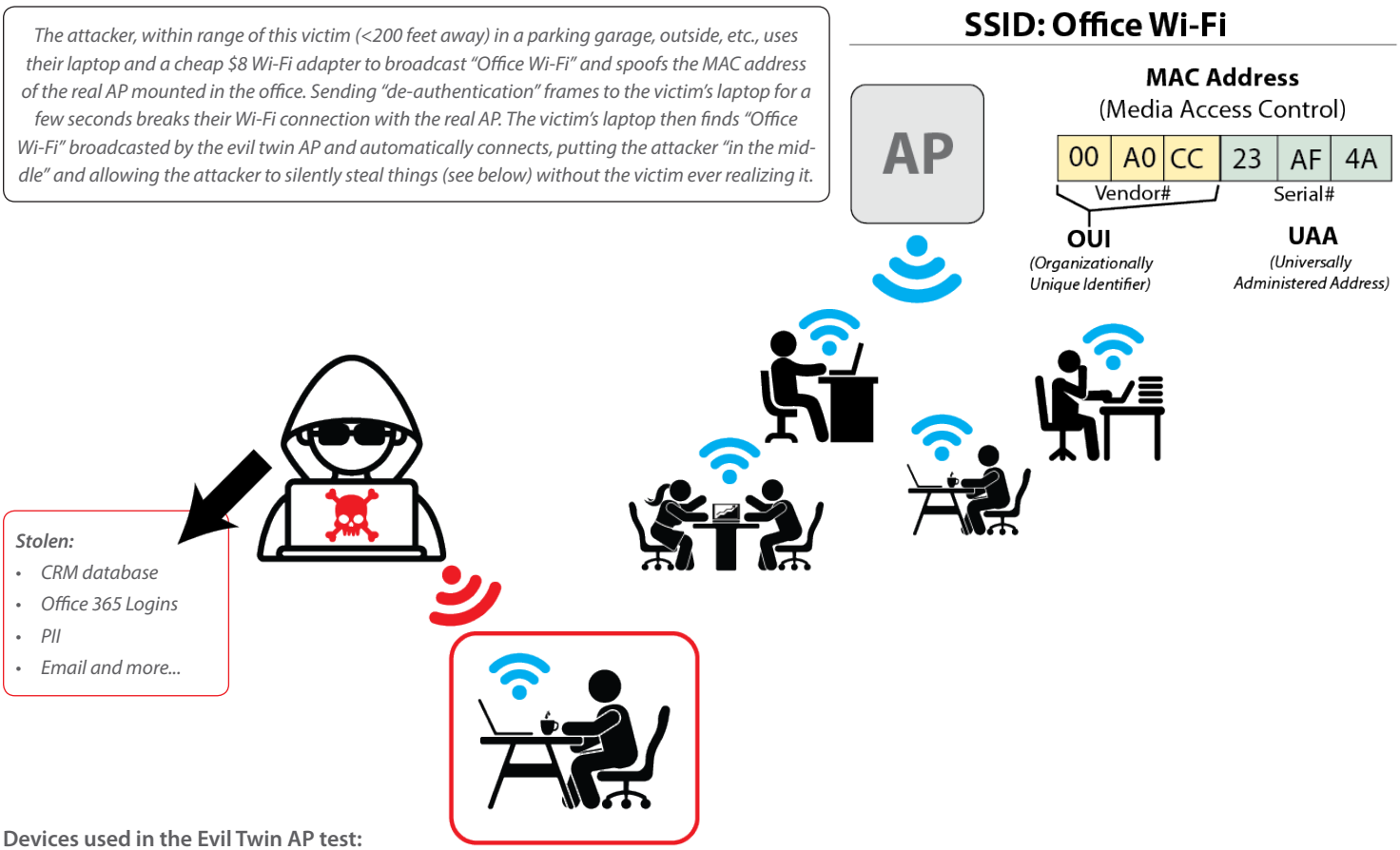
1. Create Ad-Hoc AP
2. Enable auto-prevention
3. Associate Authorized Client to Ad-Hoc AP and ping wired host continuously
4. Start timer when the ad-hoc SSID is detected by NetSpot or inSSIDer
5. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Evil Twin AP Test Details

Evil twin APs are very dangerous, as victims typically have no idea that everything they are sending over Wi-Fi is being intercepted by an attacker and typically the traffic is invisible to any network security controls. This makes the attack a very safe one for an attacker as usually there are no tracks left behind of the attack that could pinpoint the culprit. An evil twin is an AP where the attacker has copied and broadcasted the same SSID name as a legitimate AP within range and often spoofs the legitimate AP's MAC address, thus creating an "evil" copy of the real AP. Victims' Wi-Fi clients will auto-connect to evil twin APs as there is no apparent difference between the real AP and the evil AP. Once connected to an evil twin AP, the traffic a victim generates travels through a "man-in-the-middle," allowing the attacker to intercept sensitive information and inject packets into the data stream to alter communications.

These office workers are all diligently working their fingers to the bone from their Wi-Fi connected laptops. Their laptops are all connected to the access point (AP) mounted above their heads in their office to the SSID "Office Wi-Fi"

The attacker, within range of this victim (<200 feet away) in a parking garage, outside, etc., uses their laptop and a cheap $8 Wi-Fi adapter to broadcast "Office Wi-Fi" and spoofs the MAC address of the real AP mounted in the office. Sending "de-authentication" frames to the victim's laptop for a few seconds breaks their Wi-Fi connection with the real AP. The victim's laptop then finds "Office Wi-Fi" broadcasted by the evil twin AP and automatically connects, putting the attacker "in the middle" and allowing the attacker to silently steal things (see below) without the victim ever realizing it.



Devices used in the Evil Twin AP test:

1 - Samsung S2 Tab BCM 2x2 Wave 1 Android (client)

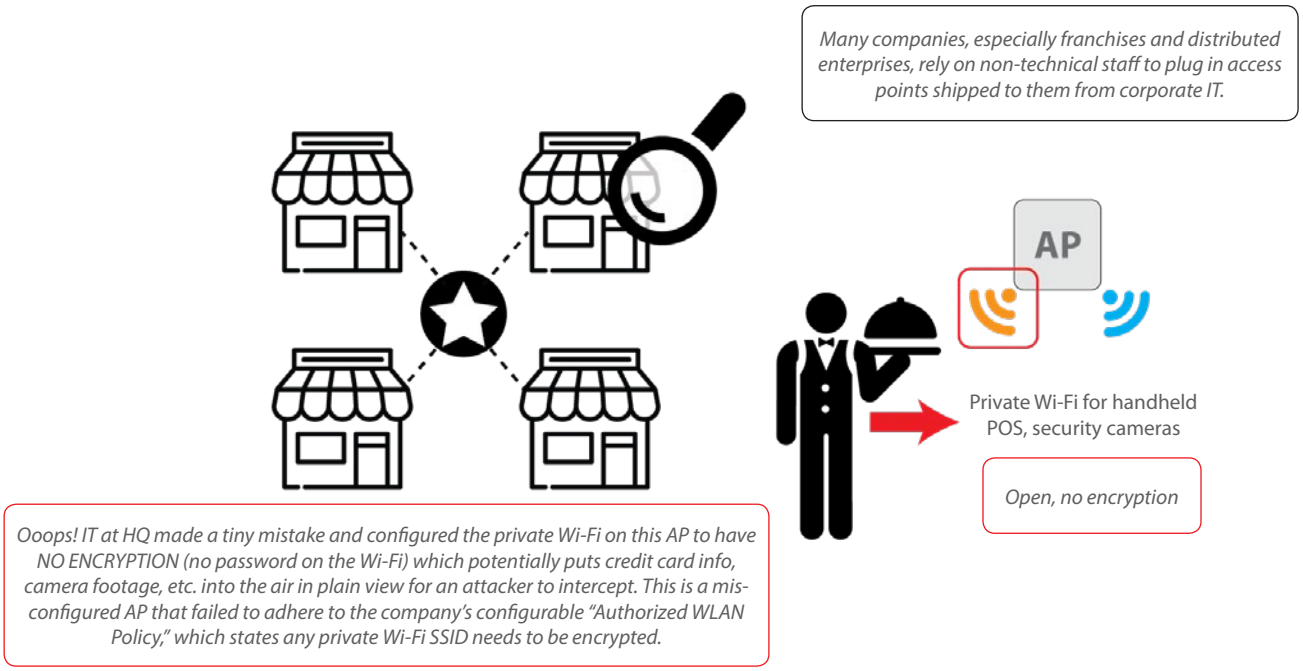
1- Wi-Fi Pineapple Tetra by Hak5 (Evil Twin AP spoofing SSID and MAC)

Test Method:

1. Add an SSID to Evil Twin AP
2. Ensure SSID is enabled only in 5 GHz band
3. Verify non-malicious instance of Evil Twin AP is seen as Authorized in the user interface
4. Enable auto prevention in DUT
5. Enable Wi-Fi Pineapple AP spoofer on 2.4 GHz band (SSID only)
6. Start timer as soon as Evil Twin AP is detected by NetSpot or inSSIDer
7. Associate a client to non-malicious instance of Evil Twin AP to be spoofed and ping wired host continuously
8. Associate a client to the spoofed Evil Twin AP and ping wired host continuously
9. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Misconfigured AP Test Details

In busy networks where new APs are being deployed, it can be too easy for network administrators to accidentally make a configuration mistake such as making a private SSID open with no encryption, potentially exposing sensitive information to interception over the air.
A misconfigured AP is one that has a configuration, such as one with encryption requirements, that do not adhere to network security policy.



Clients used in the Misconfigured AP test:

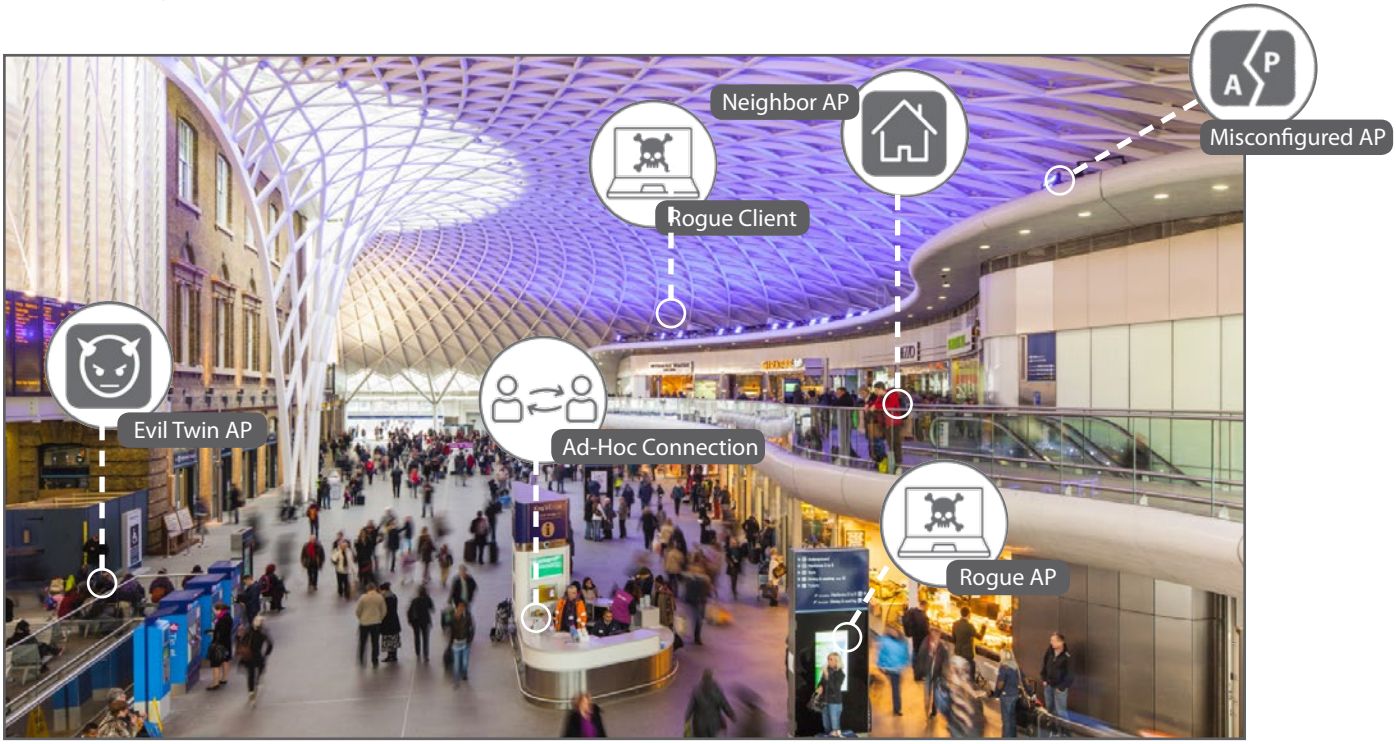
1 - Samsung S2 Tab BCM 2x2 Wave 1 Android

Test Method:

1. Add an SSID with open security using the same SSID name as an Authorized SSID with WPA2/PSK security
2. Enable auto prevention
3. Associate a client to the properly configured AP (WIPS-Test/WPA2PSK) and ping wired host continuously
4. Associate a client to the Misconfigured AP (WIPS-Test/Open) and ping wired host continuously
5. Start time as soon as client connects to Misconfigured AP
6. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Concurrent Threats Test Details

Crowded places like conference centers, train stations, airports, and concerts are perfect places for a hacker to take advantage of any and all Wi-Fi attack vectors. These busy environments are prime hunting grounds for attackers as they know people are usually under time pressure and distracted by their surroundings.



Devices used in the Concurrent Threats test:

- 1 - OnePlus2 QCA 1x1 Wave Android
- 6 - Samsung S2 Tab BCM 2x2 Wave 1 Android
- 1 - MacBook Air BCM 2x2 Wave 1 MacOS (as Ad-Hoc AP)
- 1 - Acer Laptop with Qualcomm Atheros 1x1 Wave 2 and Windows 10 OS (as client)
- Wi-Fi Pineapple Tetra by Hak5 (Evil Twin AP spoofing SSID and MAC)
- Apple Airport Express (as Rogue AP)

Test Method:

1. Disable auto prevention
2. Enable all six threats concurrently
3. Associate all clients and initiate pings to host continuously
4. Enable auto prevention
5. Record approximate time to detect and prevent by WIPS (10-minute maxi-mum allowed)

Test Results

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

View the full Miercom report at: **www.watchguard.com/wifi-security-report**

P = Pass
F = Fail
MP = Marginal Pass
N/A = Feature Not Supported

Key Findings for WatchGuard

- The ONLY vendor to automatically detect and prevent the six known Wi-Fi threat categories simultaneously while maintaining performance
- The ONLY vendor to support automatic detection and prevention of rogue APs and rogue clients
- The ONLY vendor to automatically detect and prevent endpoints from communications over ad-hoc Wi-Fi connection
- The ONLY vendor to automatically prevent connections to evil twin APs and dangerous connections to misconfigured APs such as private SSIDs without encryption

Download Miercom report at: **www.watchguard.com/wifi-security-report**

Miercom CERTIFIED SECURE

Learn More: Visit www.trustedwirelessenvironment.com

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com