

ATTACKS ON CORPORATE WI-FI NETWORKS

2017

Information Security Analytics Team

Wireless networks are a key part of corporate infrastructure for most modern businesses. Wi-Fi is convenient for employees, who can connect from anywhere in an office using a variety of devices, and for customers, who enjoy the convenience of high-speed Internet access. It is also a major cost-saver for companies: networks can be quickly and easily deployed without laying cable.

But administration flaws and insecure use of these networks pose a security threat. An intruder can hack a Wi-Fi network to intercept sensitive information, attack wireless network users, and gain access to a company's internal network. Attacks against wireless networks are diverse. Creating rogue access points, accessing internal resources from a guest wireless network, and exploiting vulnerabilities in authentication protocols are a mere sliver of the possibilities. Since these networks are so popular with businesses, such attacks can cause enormous damage to businesses and individual users.

This article provides an overview of the most common vulnerabilities detected during security testing of wireless networks carried out by

Positive Technologies in 2016. Our clients represented many industries, but we found that regardless of industry, Wi-Fi security was low or extremely low across the board in our 2016 testing.

In addition to describing popular attack scenarios involving Wi-Fi networks, security recommendations are provided. The demonstrated scenarios are far from being the only possible ones, but they enable tracing the main thrust of an attacker's activities. Note also that the scenarios are not mutually exclusive and may occur simultaneously on the same system: an open guest wireless network can be "supplemented" by a rogue access point, and passwords are often bruteforced on networks whose signal is accessible outside of restricted areas.

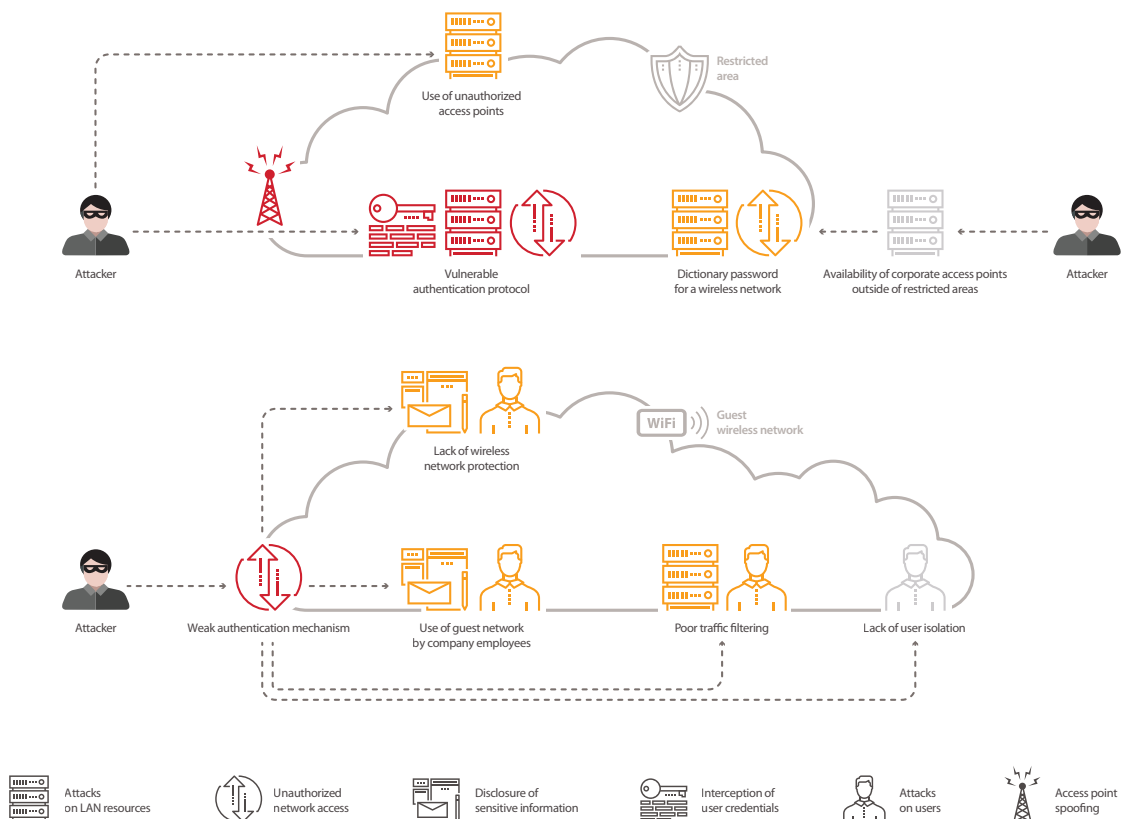


Figure 1. Basic security flaws



EXCESSIVE NETWORK COVERAGE

Attackers targeting corporate infrastructure require both skill and specialized tools. Their toolkits may include powerful Wi-Fi adapters supporting various frequency ranges, omnidirectional antennas, microcomputers to create a rogue access point, equipment to perform stealthy reconnaissance of wireless networks, and software of all kinds for active security analysis.

At the initial stage, the attacker's focus will go to information about the encryption algorithms and security/authentication mechanisms in use. This information is useful for subsequent attacks on corporate infrastructure. But these attempts are successful only if there has been a failure to contain the Wi-Fi signal within a restricted area.

Secure use of Wi-Fi networks requires that a network can be seen only by employees who are within the restricted area (such as the client's office). If there are no restrictions on the router's signal strength, access to wireless networks can be achieved from a neighboring building or public parking lot. During security testing, Positive Technologies experts regularly detect corporate wireless access points whose signal reaches far outside of client buildings.

Attackers can then conduct various attacks on the LAN from outside the restricted area, taking the opportunity to perform time-consuming attacks such as brute forcing network passwords at a distance, without having to worry about being discovered. They also can use a rogue access point that pretends to be part of the network: since the attacker's router has a stronger signal, staff devices will switch to it (access point spoofing attacks are detailed in the following section).

To prevent such situations, restrict the availability of corporate wireless networks from outside the restricted area. We recommend adjusting the router settings to reduce the signal strength accordingly. If current routers do not support this ability, consider purchasing routers that do. Alternatively, adjust the placement of routers so that their signal does not go outside the restricted area.

ROGUE ACCESS POINT

Cell phones, tablets, and laptops automatically remember the names of the networks they connect to (in technical parlance, this is called the network's SSID). Users often enable the insecure option to automatically connect to known Wi-Fi networks. But the problem is that this option relies on the SSID. Any time the device is within the coverage area of another Wi-Fi network that has the same SSID, the device will attempt to connect.

Attackers can create a rogue access point with the same SSID so that employee devices near the rogue access point will automatically send requests for authentication. Use of the PEAPv0/EAP-MSCHAPv2 protocol, combined with non-existent or faulty validation of the access point certificate, allows attackers to obtain the Challenge-Response values used in authentication. Armed with this data, the attacker can brute-force the password hash for the legitimate network bearing the same SSID. Employees may not even suspect that they have been attacked.

Despite the seeming complexity and effort involved, such attacks occur regularly in the real world. In 75 percent of Wi-Fi security tests, Positive Technologies was able to intercept authentication data using similar attacks.

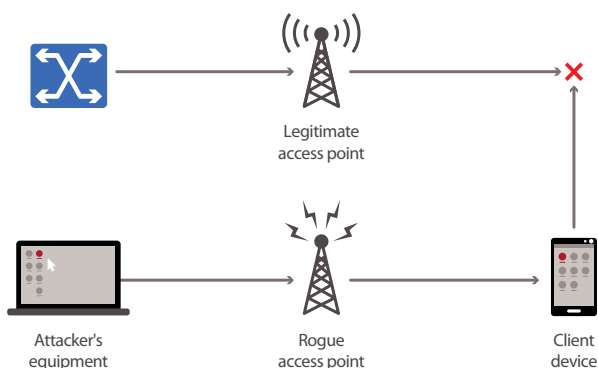


Figure 2. Access point spoofing

One way to leverage this technique is to perform a "watering hole" attack targeting places where staff of the target company are likely to congregate. This could be the entrance of a business center, restaurant, or the nearest bus stop: an employee's device will try to connect to an attacker's network as soon as it sees a familiar SSID. This is both simple and effective, since an attacker can obtain authentication data with little effort from a large number of devices without ever setting foot in the client's building.

```

wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (Identifier 140)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: received EAP packet (code=2 id=140 len=43) from STA: EAP Response-PEAP (25)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (Identifier 141)
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: received EAP packet (code=2 id=141 len=123) from STA: EAP Response-PEAP (25)
wlan1: EAP-FAST : Challenge
wlan1: EAP-FAST : 56:d1:3e:a6:d8:f0:db:c5
wlan1: EAP-FAST : Response
wlan1: EAP-FAST : b:9f:bb:e3:a9:f6:b4:6d:ef:a4:63:d5:73:5d:2f:28:89:f6:63:81:8d:54:2a:70
wlan1: STA 6c:71:d9:b6:13:51 IEEE 802.1X: Sending EAP Packet (Identifier 142)

```

Figure 3. Interception of the Challenge–Response pair

After intercepting the Challenge–Response pair, an attacker can use a supercomputer to bruteforce 2^{56} keys based on the DES and SHA1 algorithms, and get a hash of the password (which is enough for logging in to the wireless network). This brute-force method has a 100-percent chance of success. In addition, attackers can use third-party decryption services (costing about \$200 online) or else conduct a head-on brute-force attack themselves using the power of modern graphics cards, although success cannot be guaranteed.

If the wireless network is connected to the LAN and a domain account is used for access, then a successful brute-force attack means that an attack on the internal network is possible and attackers can get access to critical resources such as email accounts.

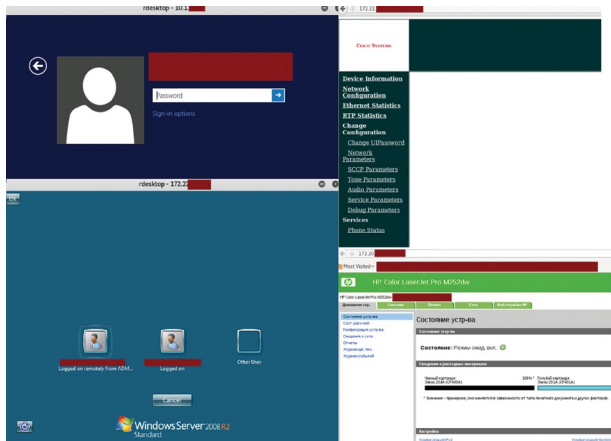


Figure 4. Access to LAN resources from a guest wireless network

What can security-conscious companies do? Use secure authentication methods, such as EAP-TLS, featuring a client certificate and mandatory validation of the server certificate. The EAP-TLS protocol requires installation of a client certificate on each wireless device. In case of an access point spoofing attack, certificate validation will fail and attackers will not receive any authentication data.

FROM A GUEST NETWORK TO CORPORATE

At most companies, guest Wi-Fi access is simple to obtain. Customer convenience is often priority #1, but this convenience may come at the expense of security. As security analysis shows, access to other network segments, including LAN resources, can often be obtained after connecting to a guest network. Our testers have succeeded in accessing Windows log-in prompts, printer administration consoles, and router settings from the guest wireless network at target companies, as seen above (Figure 4).

What's more, company employees themselves may regularly use the guest network. But guest networks are not always encrypted. So, if the access point does not isolate users from each other, an attacker who has access to an unencrypted guest network can attack company employees, listen in to their traffic, and intercept sensitive information, including access credentials. Attackers can combine this flaw with use of a rogue access point as described previously.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
33:33:33:33	-19	100	1128	11 0 1	54	OPN				quest
C9:43:9E:DC	-81	100	1820	0 0 1	54a	WPA2	CCMP	PSK		
C8:43:9E:DC	-81	100	1820	0 0 1	54a	WPA2	CCMP	MGT		
C6:4F:CF:23	-85	87	766	0 0 1	54a	WPA2	CCMP	MGT		
C6:4F:CF:20	-84	78	753	0 0 1	54a	OPN				
C6:4F:CF:25	-84	80	809	0 0 1	54a	WPA2	CCMP	PSK		
C6:4F:CF:22	-84	67	819	0 0 1	54a	WPA2	CCMP	MGT		
52:8A:3A:5A	-87	0	6	0 0 1	54a	OPN				
A3:F9:FF:CD	-87	2	44	1 0 1	54a	OPN				
CE:1A:1A:1A	-87	2	44	1 0 1	54a	WPA2	CCMP	PSK		

Figure 5. An unencrypted guest network

```

wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.1.1.1 netmask 255.255.254.0 broadcast 10.1.1.1
inet6 ::::: prefixlen 64 scopeid 0x20<link>
ether ::::: txqueuelen 1000 (Ethernet)
RX packets 1985 bytes 246216 (240.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2158 bytes 163770 (159.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@android:/home/positive# ^C
root@android:/home/positive# nc -lvp 1337
listening on [any] 1337 ...
10.1.1.1: inverse host lookup failed: Unknown host
connect to [10.1.1.1] from (UNKNOWN) [10.1.1.1] 46326
hello neo

```

Figure 6. Demonstration of support for direct data transfers between clients on a guest network

To improve the security of the guest network, we recommend configuring the access point to isolate users from each other, using strong encryption (WPA2), and prohibiting use of guest networks by company employees.



UNAUTHORIZED ACCESS POINTS

The human factor is important when securing any infrastructure, including Wi-Fi networks. Many employees access the Internet for personal purposes (social networks, email, and chat). But some companies restrict access or even have a total ban on Internet use. So, what are employees to do? Often they go online using their smartphones or, for greater convenience, use tethering to create their own mobile hotspot that connects to their workstation and access the Internet via this unauthorized connection.

Wi-Fi security testing revealed an average of three unauthorized access points per site in 2016. At one company, we found seven unauthorized access points running simultaneously.

If successful, attacks on such Wi-Fi networks can provide access to LAN resources and enable attacks on users of these hotspots. During one test, our experts detected a wireless network that did not belong to the client company.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:00:00:00:00:00	0	0	0	0	6	54	WPA2	CCMP	PSK	
00:00:00:00:00:00	0	0	0	0	6	54	WPA2	CCMP	PSK	
	PWR	Rate	Lost	Frames	Probe					
:C2:A8:DE	-73	0	1	0	1					
:B4:44:15	0	0	1	0	44					
:E2:ED:6A	-64	0	1	4	4					
:B5:19:05	-65	0	1	11	2					
:B7:1E:4E	-65	0	1	85	7					
:64:42:D5	-67	0	1	0	1					
:4F:89:50	-71	0	1	0	2					
:3A:29:7A	-72	0	1	0	1					
:0A:32:34	-73	0	1	0	1					
:6A:34:2D	-18	0	1	140	115					
:68:53:FD	-67	0	1	88	124					

Figure 7. Information on a detected secure wireless network

Our experts then captured a handshake between the client and hotspot, which allowed them to conduct local brute-force attacks to obtain the hotspot password. Dictionary attacks and information about the network environment helped us to find out that the external IP address of the device belonged to the network of a mobile operator. As a result, we made a successful attempt to log in to the account page of the employee on the mobile operator's website without entering a password. It turned out that this was a corporate account. With our access to the account page, we could have set up call forwarding, sent text messages, and read incoming text messages.

To stay safe, we recommend regularly sweeping for and disconnecting unauthorized access points within the restricted area. Employees must be familiar with security rules and procedures. An awareness program covering all employees should concentrate on the practical aspects of information security. Training should be periodic, with follow-up to ensure the program's effectiveness.

DICTIONARY PASSWORDS

Dictionary passwords are disturbingly common on almost all infrastructures (see our report with vulnerability statistics for corporate information systems¹). Wi-Fi networks are no exception. Passwords are often short and/or simple, making them quick for attackers to brute-force. As mentioned previously, attackers can intercept a handshake for an access point in order to conduct a brute-force attack locally (on the attacker's own computer, without requiring a network connection) to find the password. Passwords consisting of dictionary words or simple combinations can be bruteforced in mere seconds.

¹ www.ptsecurity.com/upload/corporate/ww-en/analitics/Corporate-Vulnerability-2016-eng.pdf

At some companies, the Wi-Fi password is based on the company's name or similar information. This makes it child's play for attackers to discover the password. They can conduct a personalized brute-force attack using special software (for example, CeWL and RSMangler). The dictionary of possible passwords tried by the attacker will be specially created for the targeted company. During one test, our experts accessed LAN resources by first brute forcing a password similar in spelling to the name of the client company.

```
Aircrack-ng 1.2 rc4
[00:00:00] 8/9822768 keys tested (102.97 k/s)
Time left: 1 day, 2 hours, 45 minutes, 1 second      0.00%
KEY FOUND! [ 12345678 ]

Master Key      : 9B E0 20 EF 21 4F 5D 7D 1C 7A 06 93 F1 85 86 6F
                  4B D9 D1 F1 5A 70 2F 16 05 F9 2E 71 9C 81 DF 88

Transient Key   : EB B3 2E 39 CE F2 F3 65 6A A3 D6 54 85 73 93 E2
                  29 0F 9E CE BA 66 2D 83 37 3B 76 49 86 D7 1A AF
                  1D 8F 9A DA 61 08 96 9A 20 6C A5 07 FD 29 1A E4
                  6E 49 A1 C3 E0 AB 63 7F 79 0F A1 F4 B1 DC 52 BD

EAPOL HMAC     : 6E 6C 38 2C 89 D3 C5 BE 79 55 D5 B5 5C 8B FE 2D
```

Figure 8. Bruteforcing a Wi-Fi password with Aircrack

The recommendation here is unsurprising but important: enforce a strict password policy requiring the use of hard-to-guess passwords.

WPS WEAKNESSES

WPS (Wi-Fi Protected Setup) is another case when convenience comes at the cost of security. WPS is enabled by default on most routers and is designed to simplify setup of Wi-Fi networks, by automatically setting the network name and type of encryption. No configuration is necessary—all that is necessary for connecting is a PIN code. This sequence of numbers is often written on the outside of the router itself, visible to anyone able to approach the device for a few seconds. Even worse, these PINs are weak. An attacker can easily bruteforce the PIN and connect to the network. There is even special free software targeting WPS, enabling an unskilled attacker to identify access points with WPS turned on and crack their PIN codes.

WPS has been widely criticized by security researchers, but our experts still frequently encounter WPS-enabled wireless access points in the wild. In some cases, this has allowed them to gain access to LAN resources.

```
[*] Sending M2 message
[*] E-Hash1: b1:98:e4:a3:15:55:01:1b:29:ca:47:16:23:de:b9:8e:cd:9c:a5:7e:92:f9:40:bb:f2:b3:2f:93:cf:b5:b5
[*] E-Hash2: b9:53:d3:a9:5d:bb:d4:e4:9d:b0:a5:c1:1a:0f:be:03:83:9a:d9:a5:92:54:c0:5e:1a:a7:00:ca:72:95:d5:04
[*] Received M3 message
[*] Sending M4 message
[*] Received M5 message
[*] Sending M6 message
[*] Received M7 message
[*] Sending WSC NACK
[*] Sending WSC NACK
[*] Pin cracked in 60 seconds
[*] WPS PIN: '24301626'
[*] WPA PSK: '0090641373'
[*] AP SSID: '0090641373'
```

Figure 9. Successful brute-force of a WPS PIN

Protection against this type of attack is simple: disable WPS in the settings of all access points.



INSECURE AUTHENTICATION

In some cases, a wireless network may use a list of authorized MAC addresses (whitelist) to authenticate devices. This approach is insecure because MAC addresses can be easily faked by intruders conducting man-in-the-middle (MITM) attacks.

Our testers discovered a wireless network for which access is implemented through an HTTPS website. After successful authentication, the MAC address of the connected device is used to identify packets on the network. Future connection attempts are authenticated based on the user's MAC address.

To demonstrate the threat, our experts installed a rogue access point and their own equipment, which forwarded user requests to the legitimate access point. A tablet of an employee connected to the rogue access point; the employee entered credentials in a fake authentication form. From that point onward, all of user's network traffic was transmitted to the access point by way of our equipment, which allowed listening in and adding the MAC address of our "malicious" workstation to the whitelist. And with Wi-Fi access, our testers could access other, even more sensitive segments of the network.



Figure 12. Authentication form on the rogue access point

To prevent such situations, use secure authentication methods (see the "Rogue access point" section).



Figure 10. Wi-Fi network authentication form

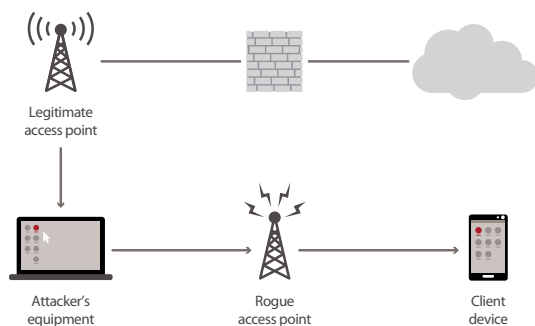


Figure 11. Man-in-the-middle (MITM) attack

CONCLUSIONS

As our experience shows, the majority of companies using Wi-Fi networks do not take sufficient security measures. All security tests carried out by Positive Technologies uncovered various security flaws, and even more concerning is the fact that in every test, we could use our foothold on wireless networks to conduct attacks on LAN resources.

In practice, a single flaw frequently leads to the compromise of the whole system. For example, one client used domain authentication for the company's wireless networks. One of these accounts was found on the company's official website as cleartext. At the same time, connections to Wi-Fi networks could be made from outside the restricted area. Therefore, any attacker able to perform a Google search could have obtained network access without entering the target's building.

So is it worth doing away with Wi-Fi networks entirely? Not necessarily. These problems remain manageable with the help of a comprehensive layered approach to security. Acceptable security can be ensured if administrators use secure configuration, segment wireless networks, implement secure authentication methods with certificate validation, restrict access of guest clients to the LAN, regularly test wireless network security, and identify and disconnect unauthorized access points. Of course, this approach also requires education of employees to improve security awareness and ensure ongoing vigilance.

POSITIVE TECHNOLOGIES

ptsecurity.com

info@ptsecurity.com

