wandera

Mobile **Wi-Fi** Security Report

People tend to favor Wi-Fi over cellular for obvious reasons - it's usually faster, it doesn't tax your data plan and it's widely available. However, there are a number of inherent risks in allowing your devices to connect to Wi-Fi networks. This report is designed to inform you of the many dangers of Wi-Fi, and how to deal with them.

TABLE OF CONTENTS

Introduction

Modern organizations that are enabling mobility for their workforce are achieving powerful productivity benefits. With this new reality of mobile working also comes the need for countless wireless networks that can support an increasing number of devices and the data they access.

According to Statcounter, mobile traffic surpassed desktop for the first time in November 2016, representing a marked shift in how people access the web. Similarly, the number of mobile devices in the workplace has also exploded in recent years.

As a result, it is vital for organizations to provide mobile-friendly connectivity, both for employees and partners who need remote access to corporate facilities. That means setting up a robust broadband connection to handle the significant increase in data consumption, and multiple Wi-Fi access points for those users or situations where cellular is not appropriate.

Although it is less relevant for businesses today, the primary advantage of having a wired infrastructure is the control it provides. Unauthorized visitors can be kept out of your corporate network and it won't be overloaded with non-work related traffic.

Conversely, as a mobile enterprise, your network extends beyond the physical walls of the office giving attackers a potential route into the business, without ever having to compromise a single part of the corporate infrastructure.

Once those work-assigned devices leave the confines of the office walls, it's harder to see and control how they are connecting to the internet. Many businesses, especially those in the service industries, are also offering wireless connectivity for customers, passengers, guests and general public. But how is a user to know whether these hotspots use encryption? And how can they ensure no one around them can see their data in transit?

"Mobile data is more secure than Wi-Fi due to the encryption automatically applied to CDMA/LTE and HSDPA/3G-based connections by mobile operators."

PAUL LEYBOURNE, HEAD OF SALES AT VODAT INTERNATIONAL.

In this report, we will provide an overview of Wi-Fi network growth and the variety of hotspots available. We'll then introduce you to Wi-Fi threats in the context of the wider mobile threat landscape. And finally, we will work our way through the layers of Wi-Fi risks ranging from incidental privacy exposures to motivated attacks before providing you with advice for managing these risks.

Mobile Connectivity Overview

Wireless internet: Cellular vs Wi-Fi

The two major categories of wireless internet access are cellular and Wi-Fi. The key, obvious difference being that cellular is available almost everywhere, while Wi-Fi is only available within range of a Wi-Fi hotspot. Typically, hotspots have a range of approximately 50 to 200 feet from the access point (AP).

For some time now, the advantages of Wi-Fi have meant that Wi-Fi traffic has exceeded cellular traffic, and the disparity isn't expected to change significantly. Cisco predicts by 2021, 63% of total mobile data will be on Wi-Fi, compared to 60% in 2016*.

Within Wandera's global footprint of protected devices, the ratio of Wi-Fi to cellular data usage for the average employee is 3:1, suggesting employees use Wi-Fi more often with work phones. This may be for a number of different reasons, the fact they are often used within office spaces, airports or hotels with a Wi-Fi connection available. Good news from a cost perspective for the business, but potentially bad news from a security perspective.

THE SPLIT OF WIRELESS DATA USAGE ON THE AVERAGE EMPLOYEE DEVICE

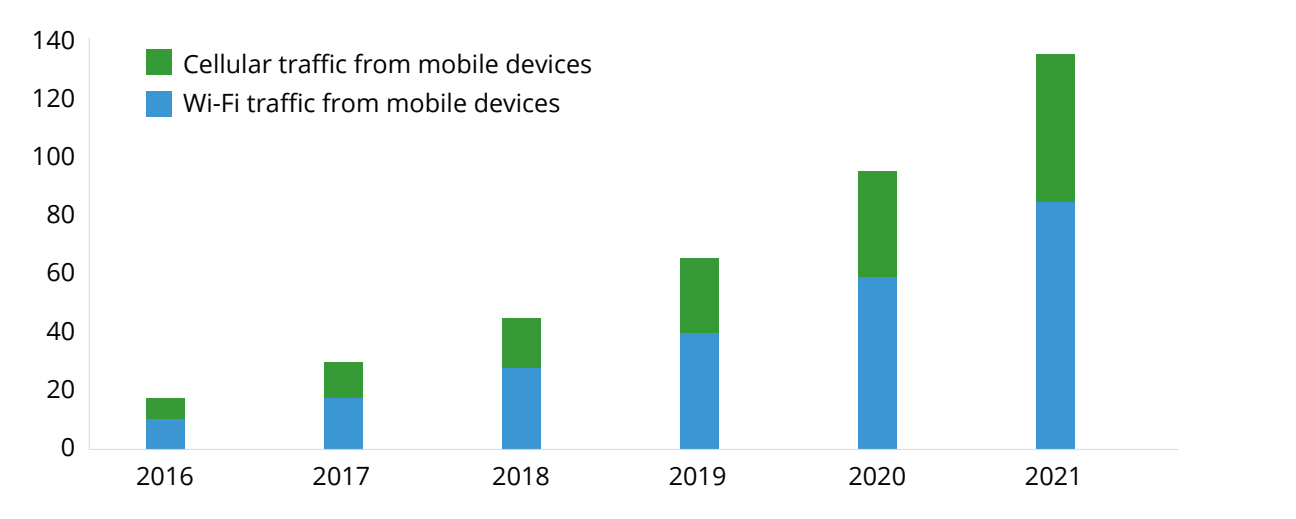
WI-FI
74%

CELLULAR
26%

12
AVERAGE NUMBER OF DAILY WI-FI CONNECTIONS ON A CORPORATE DEVICE

To support this increase in Wi-Fi traffic, the number of hotspots is also trending upwards. According to Cisco, the number of Wi-Fi hotspots will grow six-fold from 94 million in 2016, to 541.6 million in 2021*.

BY 2021, 63% OF TOTAL MOBILE DATA TRAFFIC WILL BE ON WI-FI



Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper

Wi-Fi hotspots are unavoidable in the modern employee's world. According to the data in our network of enterprise mobile devices, the average number of Wi-Fi connections a device makes a day is 12.

As an attack vector, these hotspots are the perfect vehicle to intercept a user's traffic. Using relatively cheap and readily available tools, minimally skilled hackers can easily eavesdrop and monitor your online traffic to capture valuable information, such as login credentials and credit card details.

The next part of this report will explain different types of Wi-Fi connections as well as the spectrum of Wi-Fi risks ranging from digital exhaust and open Wi-Fi snooping, to more severe attacks that compromise the device trust model.

Types of Wi-Fi connections

Wi-Fi hotspots can be created by a wireless broadband router commonly used at home or in a small office. Free Wi-Fi hotspots are available in public areas such as coffee shops, airports and lounges. However, some providers charge for access. When Wi-Fi isn't on offer, there are other ways to create a Wi-Fi hotspot yourself. It's easy to see how Wi-Fi has become hard to avoid. Here are some examples of common hotspots.

1. STATIONARY HOTSPOTS (MOBILE BROADBAND ROUTER)

Typically called a "mobile broadband router," stationary units include a Wi-Fi base station that supports multiple devices over a wide range such as a home or office. They include a slot for a SIM card and can also include LAN ports for connecting wired devices.

2. SMARTPHONE HOTSPOTS (TETHERING)

Smartphones have both cellular and Wi-Fi radios built in, and most phones can be made to connect the two and turn the device into a portable hotspot for tablets and laptops. This is commonly known as "tethering."

3. PORTABLE HOTSPOTS (MIFI)

Portable hotspots are dedicated units that leverage 3G or 4G mobile phone networks and use this connection to create a mini wireless broadband hotspot for multiple devices to connect to. Also known as a "mobile wireless router" or "travel router," these units are available from most mobile carriers. The cellular fee is either added to the user's existing data plan, or a new plan must be activated. A popular trademark for these devices is MiFi.

4. USB WI-FI DONGLES

Cellular service can be added to laptops by plugging in a small USB 'dongle'. Mobile broadband dongles are offered on a fixed-term contract, or pay-as-you-go.

5. VEHICLE HOTSPOTS

Built-in units provide a Wi-Fi hotspot within the cabin of a vehicle for multiple passengers. In-vehicle cellular hotspots are offered by many manufacturers, and third-party devices are also made that plug into the On-Board Diagnostics (OBD) board, the vehicle's electronic troubleshooting system.

6. HOTSPOTS ON PUBLIC TRANSPORT

Everywhere you go, there are different types of hotspots available. On certain train lines and buses, Wi-Fi is offered using a similar technology to vehicles. Some train networks also offer Wi-Fi in stations via broadband routers. For example the London Underground network hosts almost 300 different Wi-Fi hotspots across its many stations. Many airlines offer inflight Wi-Fi via ground-based mobile broadband towers or satellite technology - sometimes payment is required.

Mobile threat landscape

Before we detail the security risks inherent to mobile networks, let's take a step back and look at the broader issue of security for the mobile-equipped enterprise.

A recent investigation by Harvard Business Review revealed 45% of IT executives saw mobile devices as the weak spot in their company's defenses. While 37% also cited employee data, and 34% cited wireless access of networks as their weak spots.

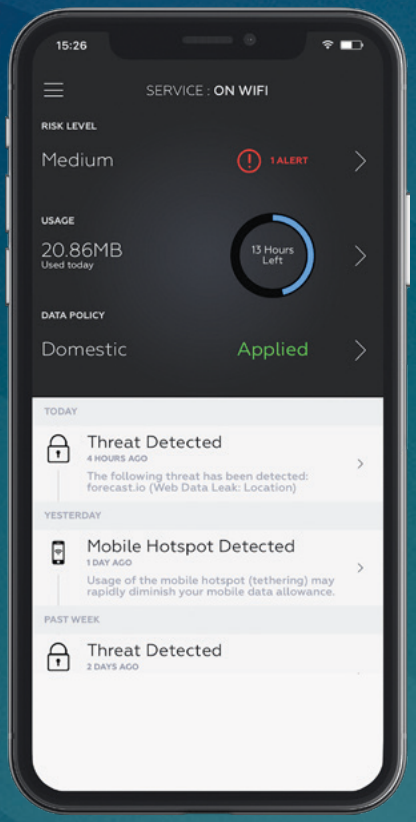
To understand the sophistication of mobile threats, it is helpful to categorize them by what technology is involved. There are four broad threat categories in the mobile ecosystem - device threats, app threats, network threats and web-based threats.

MOBILE DEVICE SECURITY

Mobile devices present a unique challenge to IT departments. In addition to a form-factor that makes devices more susceptible to loss/ theft, the OS puts ease-of-use ahead of security. EMMs help configure devices, but organizations are still concerned with configuration vulnerabilities and physical attacks on the device such as jailbreaking or rooting the OS.

MOBILE NETWORK RISKS

The Wi-Fi access points that mobile devices utilize are full of risk, and they're not the only network infrastructure being targeted by attackers. These network connections expose mobile devices to malicious threats, such as man-in-the-middle attacks, and the risk of data loss on a public channel. Do you trust the Wi-Fi networks that your users are attaching to?



MOBILE APPLICATION RISK

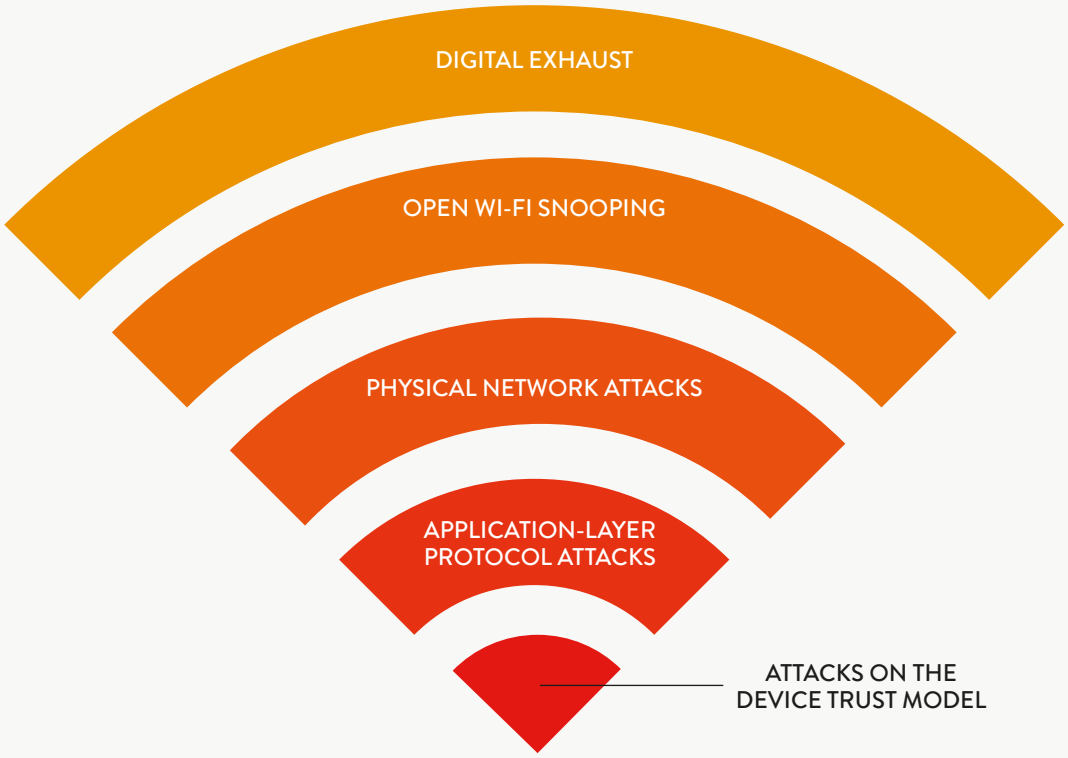
Apps are the cornerstone of every mobile ecosystem, and also a primary attack vector. Malware from third party app stores and apps that leak sensitive data are among the issues in this category that organizations must control. Security-conscious organizations know to not overlook the browser in their app assessments, as it is a popular entry point for the attackers.

WEB CONTENT RISKS

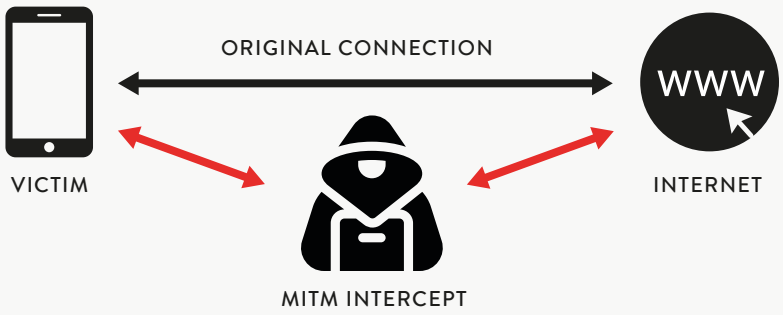
The Internet is full of risk, but the web is particularly dangerous for mobile users. Phishing attacks that can appear in any messaging or social media app, sites that host malware and malvertising attacks that are hidden within the pervasive ad networks are just a few examples of what mobile users face every minute they are connected.

Wi-Fi risks

The accessibility and popularity of Wi-Fi makes it the ideal avenue for hackers to intercept and manipulate traffic. The layers of Wi-Fi risk are varied - in some cases the attacker needs to be in the immediate vicinity of the victim(s) and in others they attack the device rather than the network. As we explore each layer, we'll identify the prevalence of the risk in terms of the number of devices exposed, and the severity in terms of attack consequences.



Many of these attacks occurring over Wi-Fi involve a "man-in-the-middle". Man-in-the-middle (MitM) attacks happen when communication between two systems is intercepted. The intention is usually to eavesdrop on communication, obtain data from the victim's device or to manipulate the data in transit. As you will see in the following sections, a MitM can occur in different ways, at times the malicious actor will attack the network, and sometimes they will compromise device trust model.



Digital exhaust

When an attacker picks up the cookie crumbs your mobile device leaves as it connects to different hotspots.

PREVALENCE: WIDESPREAD

SEVERITY: LOW

NOTES: AFFECTS ALL USERS WITH WI-FI ENABLED BUT IS ONLY A SHALLOW PRIVACY RISK, NO PERSONAL DATA IS LOST

Laptops spend time listening for beacons from Wi-Fi access points, which contain the network name along with other information. While this discovery method generally works well, the laptop sometimes has to 'listen' for a long period of time before it can be sure it's gathered all the nearby Wi-Fi networks.

This drawn-out 'listening' on a smartphone would be a major drain on battery consumption. As a result, the majority of smartphones use a different method for Wi-Fi network discovery: a 'probe request'.

Every once in awhile, a smartphone will broadcast a probe, seeking a response from every Wi-Fi network that it has ever joined. On iPhones, this is known as a Preferred Network Offload (PNO). This means that every minute an employee's smartphone's Wi-Fi is enabled (but not connected), it is broadcasting the name of every Wi-Fi network that it has ever joined to the nearby vicinity. These particular smartphone emissions can be described as 'digital exhaust'.

And this information is alarmingly easy to access. A small script that works on most Macs can listen to probes sent out by any smartphone in a certain vicinity. When you consider how many Wi-Fi networks a typical employee's smartphone has joined in the previous two years, that is an awful lot of information to broadcast to the public.

For a number of years, users' concerns regarding security and privacy has led them to turning off Wi-Fi and Bluetooth radios when not in use. For iPhone users, this is conducted using the Control Center in iOS, but since the latest major upgrade iOS 11 was released, this doesn't permanently turn-off the radio; it only disconnects from any active networks. Wi-Fi and Bluetooth radios can still be permanently disabled within the Settings app. Android has exhibited the same behavior since 4.4.2.

Aside from proactively disabling Wi-Fi, another way to avoid digital exhaust is to regularly reset network settings, allowing the smartphone to 'forget' its learned networks so it's not broadcasting them to potential eavesdroppers.

"With a cheap Wi-Fi adapter and some free software anyone can listen in on all conversations your phone or laptop is having with the outside world."

GLENN WILKINSON, SENIOR SECURITY ANALYST AT SENSEPOST

Wi-Fi snooping

When an attacker eavesdrops on your online activity while you're both connected to the same network.

PREVALENCE: WIDESPREAD

SEVERITY: LOW-HIGH*

NOTES: AFFECTS ALL DEVICES CONNECTING TO OPEN WI-FI, BUT ONLY A RISK WHEN USING WEB SERVICES THAT DO NOT ENCRYPT TRAFFIC.

Insecure networks make all data traffic visible to a malicious actor that wants to see any online communication of the people physically nearby.

Insecure networks are all around us and our mobile devices are likely connecting to these networks every week. Almost every coffee shop, hotel, airport, train, hospital, etc., offers a service of open Wi-Fi connectivity to their customers with zero security, encryption or privacy. Why is this the case? Convenience.

In Wandera's global footprint of protected devices, we can see that 12% of the hotspots that employees are connecting to are open. According to Secure List, approximately 24.7% of Wi-Fi hotspots in the world do not use any encryption at all. This means employees are likely being more conscientious with their corporate devices perhaps due to the fact that security solutions implemented by IT management are flagging the risk of open Wi-Fi.

For a Wi-Fi network connection to be encrypted, a Pre-Shared-Key (or certificate) must be provided by the client, and so it is no surprise that a minority of public networks follow this approach.

It seems that users don't have any reservations about connecting to open Wi-Fi hotspots and typically favor convenience over security, with a quarter (24%) of devices in our network using open hotspots.

What are the implications of having your traffic 'snooped'? Well, this shouldn't normally be too much of a problem. There is one significant exception, however. When insecure apps and sites are accessed on the connection, your data suddenly becomes at huge risk of a data leakage event.

12%

OF THE HOTSPOTS THAT EMPLOYEES ARE CONNECTING TO ARE OPEN

24%

OF DEVICES IN OUR NETWORK USE OPEN HOTSPOTS

"Any device that is connected to hotel Wi-Fi is effectively sending all data in clear-text, allowing a remote attacker to identify and extract information."

ADAM TYLER, CHIEF INNOVATION OFFICER OF CSID

When a leaking site or app is being used on an open Wi-Fi network, the unencrypted information can be harvested by a malicious actor or "man-in-the-middle". Depending on what is being leaked it could involve credit card theft, identity theft, or even the reuse of login credentials to access a corporate network.

Research in our Mobile Leak Report found over 200 sites and apps leaking users' PII. Alarmingly, some of those leaks came from reputable companies including Fox Sports Australia, Royal Mail, AMC Cinema, and Deezer. Worryingly, 59% of all the leaks identified were from just three categories: news & sports, business & industry and shopping. A further 28% were from another four: travel, entertainment, lifestyle and technology. All categories which would normally be considered safe and allowed by IT administrators.

Authentication systems on open Wi-Fi networks are also lacking. If any authentication is provided it is often in the form of a captive portal. Despite the fact that Apple, Windows and Android operating systems provide automatic HTTP detection for captive portal pages, a large number of Wi-Fi networks spoof HTTPS certificates for the purpose of redirecting traffic to their portal.

On modern operating systems and browsers this leads to certificate mismatch warnings that, if a user bypasses, could lead to sensitive information (such as email passwords) being exposed to the captive portal page host.

Even with a secure captive portal system, the device is only tied to the access point by its MAC (Media Access Layer) address. Any hacker not wishing to pay for Wi-Fi on a flight for example, can easily spoof the MAC address of a nearby connected device via ARP (Address Resolution Protocol) spoofing. Which brings us to the next layer.

Physical/network layer attacks

When an attacker has physically compromised a wireless infrastructure or has the ability to tamper with signaling on the local network.

SSID SPOOFING

PREVALENCE: WIDESPREAD
SEVERITY: MEDIUM
NOTES: AFFECTS ONLY OPEN WI-FI SSIDS THAT ARE LEARNT BY THE USER'S DEVICE

SSID spoofing is when a hacker advertises the same network name as a legitimate hotspot or business WLAN, causing nearby devices to connect to their malicious hotspot.

These malicious hotspots are called 'Evil Twins'. In order to set one up, hackers can use tools to 'listen' to the probe requests coming from nearby devices (aka digital exhaust), discover SSIDs they're connecting to, and automatically start advertising those SSID names.

Once clients connect and traffic is routed through the malicious network, then there are any number of things a hacker can do with that traffic such as intercepting credentials and obtaining valuable PII and corporate communications.

HOTELS

WESTIN-GUEST
SHANGRI-LA
HOTELWIFI
PREMIER INN FREE WI-FI
MARRIOTT_GUEST
@HYATT-WIFI
RADISSON_GUEST

AIRPORTS

BALOUNGEWIFI
_HEATHROW WI-FI
AIRPORT_FREE_WIFI_AENA
*WIFI-AIRPORT
AIRPORT
AIRPORT-FRANKFURT
DBX FREE WIFI

RETAIL

WALMARTWIFI
MCDONALD'S FREE WIFI
MCDONALDS
GOOGLE STARBUCKS
BTWIFI-STARBUCKS
..STARBUCKS..
LEGOLAND-GUEST

CARRIERS

O2 WIFI
BT OPENZONE
BTOPENZONE-B
ATTWIFI
ATT-WIFI
BTWIFI
_BTWI-FI

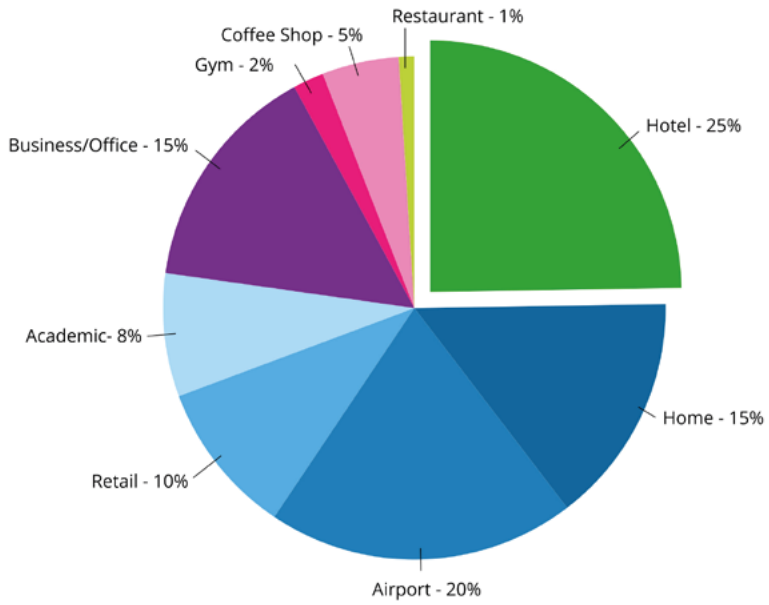
GENERIC

GUEST
GUEST
_THE CLOUD
NETGEAR
WIFIPASS
CABLEWIFI
FREE WIFI

Looking at the vast list of frequently used hotpots in our network shows there are some common themes. It appears many of the most heavily used hotspots belong to hotels, airports, retailers and mobile carriers. There are also many generic SSID names such as "Guest" or "Free WiFi". It's also apparent that there are very similar names with small differences such as "Attwifi" and "att-wifi". If two similar SSIDs are displayed on an end user device at the same time, it could be that one is an Evil Twin.

"Hackers set up a fake network to mirror the real, freely available one, users unwittingly connect to the fake network, and then a hacker can steal account names and passwords, redirect victims to malware sites, and intercept files."

STEVE FALLIN, SENIOR PRODUCT MANAGER AT NETMOTION WIRELESS



The vast majority of open hotspots that employees connect to are at hotels, airports, offices and homes.

The only effective defense against Evil Twins is server authentication, but unfortunately, today there is no standard for authentication to open Wi-Fi networks.

Your first defense is a solution that can alert the user before connecting to an open hotspot so they have a chance to think twice before connecting. However, this is only effective if end users are aware of the risks of open Wi-Fi. For deeper security, a solution that can detect and block a man-in-the-middle is your only defense.

APR SPOOFING

PREVALENCE: LIMITED
SEVERITY: MEDIUM
NOTES: AFFECTS ALL DEVICES CONNECTED TO WI-FI NETWORKS RUNNING IN PROMISCUOUS MODE

Also known as ARP Cache Poisoning, ARP spoofing is very simple to execute and is difficult to detect and defend against. ARP spoofing takes advantage of the unsecured nature of ARP (Address Resolution Protocol) requests. These are the requests that allow a device to request the MAC (Media Access Layer) address of another device on a given IP address so the devices can establish a connection and the traffic can reach its intended destination. IP address can be explained as the street and MAC as the house number.

Any device can send an ARP reply packet to another host, without authentication required, and force that host to update its ARP cache with the new value.

An attacker connected to the same hotspot as a victim can fool two devices into thinking they are communicating with each other by associating the attacker's MAC address with the IP address of the victim so that any traffic meant for the target will be sent to the attacker instead. As a man-in-the-middle, the attacker can inspect traffic and forward on to the intended destination to avoid detection.

Wi-Fi networks can defend against ARP attacks by operating their Access Points in a closed manner and using an IDS (Intrusion Detection System) to detect duplicate ARP responses.

KRACK

PREVALENCE: WIDESPREAD
SEVERITY: LOW-MEDIUM
NOTES: AFFECTS ONLY OPEN WPA2 ON UNPATCHED OPERATING SYSTEMS

In October 2017, researchers discovered a serious weakness in WPA2, the security protocol that protects most modern Wi-Fi networks.

The weakness allows anyone to break the security layer that is established between a wireless device and the targeted Wi-Fi network, essentially exposing network traffic, including passwords, chat messages and photos to the attackers.

The practise of exploiting this vulnerability was named KRACK, an acronym for Key Reinstallation AttaCK.

The reasoning behind the name comes from the fact that this type of attack tricks a victim into installing an already in-use key to their device (a piece of code that allows an attacker to decrypt encrypted network traffic).

In theory, every key on every device should be unique, but this vulnerability in WPA2 allows hackers to manipulate communications between routers and devices so that the keys can be reused. This can lead to the decryption of traffic on an affected network.

This WPA2 weakness is present in the Wi-Fi standard itself; it is not a vulnerability in an individual product or a specific implementation. This means that every instance of WPA2 contains the weakness, thus impacting a wide range of devices and operating systems, from Android and Apple to Linux and Windows.

As a result, any attack that attempts to exploit the WPA2 weakness must do so within range of the wireless signal between the device and the Wi-Fi network. From a defensive perspective, this is a good thing, as it prevents the attack from being launched remotely.

Furthermore, industry best practices call for sensitive data being transferred on the network to be protected using Secure Socket Layer (SSL) encryption, which sits above the network-layer WPA2 protections.

In summary, for the WPA2 weakness to be exploited, the attacker must be physically co-located near the wireless signal he or she is trying to compromise. Even if the attacker is successful in compromising the Wi-Fi signal via the WPA2 weakness, sensitive data being sent over that channel would likely be encrypted using SSL, ensuring it is still protected from the attacker. The risk becomes more serious when users are accessing sites and apps that don't use encryption, allowing sensitive information to be sent across the internet in the clear. The best defense in this case is a solution that detects and blocks access to leaking services.

Higher-layer protocol attacks

When an attacker tampers with the connection that is established between a client application and the Internet.

SSL STRIP

PREVALENCE: LIMITED

SEVERITY: HIGH

NOTES: AFFECTS ONLY CERTAIN APPS AND WEBSITES THAT DON'T ENFORCE HSTS MEANING AN UNENCRYPTED VERSION OF THE WEBSITE WILL BE SERVED IF THE ENCRYPTED VERSION IS NOT SUPPORTED

The most common form of security protocol compromise is SSL stripping, also known as HTTP-downgrading attacks. HTTPS uses a secure tunnel, commonly called SSL (Secure Socket Layer), to transfer and receive data. In SSL Strip, all the traffic from the victim's machine is routed via a proxy that is created by the attacker which forces a victim's browser to communicate with a server in plain-text.

The attack only affects certain websites and apps that don't enforce HSTS (HTTP Strict Transport Security). HSTS ensures that a website will only load securely or it will not load at all. Websites and apps that don't enforce HSTS can load via HTTP if requested or if HTTPS is not supported or compatible.

SESSION HIJACKING

PREVALENCE: LIMITED

SEVERITY: HIGH

NOTES: AFFECTS ONLY CERTAIN APPS AND WEBSITES THAT DON'T ENFORCE HSTS OR USE TLS

Another form of application layer protocol attack is browser session hijacking. Session hijacking through cookie stealing involves HTTP sessions. Websites that require login credentials are a good example of session-oriented connections. You must be authenticated by the website with your username and password to formally set up the session. The website maintains some form of session tracking to ensure you are still logged in and are allowed to access resources. The credentials are cleared when the session ends.

As we have seen in previous attacks, nothing that goes across an unencrypted connection is safe and HTTP session data is no different. The principle behind most forms of session hijacking is that if certain portions of the session establishment can be intercepted, then that data can be used to impersonate a user to access session information. This means that if a hacker captured the cookie that is used to maintain the session between your browser and the website you are logged into, they could present that cookie to the web server and impersonate your connection on another website.

DNS SPOOFING

PREVALENCE: LIMITED

SEVERITY: HIGH

NOTES: ONLY AFFECTS DEVICES THAT CONNECT TO APPS AND WEBSITES THAT DON'T ENFORCE HSTS OR USE TLS

The Domain Naming System (DNS) is a protocol that maps user-friendly domain names to unique IP addresses. DNS spoofing is a MitM technique used to supply a false IP address in response to a request for a domain made in the browser.

For example, when you type a web address such as www.mybank.com into the browser, a DNS request with a unique identification number is made to a DNS server. The attacker could use an ARP spoof or other inline method to intercept the DNS request. From there the attacker can respond to the DNS request with their own malicious website's IP address using the same identification number so that it is accepted by the victim's computer. This type of MitM attack does not provide the attacker with any visibility into cryptographically secured content unless combined with other techniques.

BROADPWN

PREVALENCE: WIDESPREAD
SEVERITY: LOW
AFFECTS ONLY UNPATCHED OPERATING SYSTEMS AND ISOLATED TO A PARTICULAR WI-FI CHIP

Broadpwn is the name given to a recently discovered bug in a Wi-Fi chipset that would allow an attacker to remotely hack into devices using a vulnerable Broadcom chipset. According to Wired, this threat has the potential to impact more than a billion devices worldwide. Broadpwn is a particularly interesting type of attack because it is only present in certain hardware configurations, but is exploited through a higher-layer protocol attack.

The vulnerability, which was quickly patched, allowed a hacker not only to compromise a victim's phone remotely, but also turn it into a rogue access point. The attacker was able to accomplish this by tampering with the "handshake" process that occurs between a device and Wi-Fi access point.

Nitay Artenstein, a researcher for the security firm Exodus Intelligence, who was credited with the discovery, describes it as the first Wi-Fi worm because the compromised device, acting as a rogue access point, could then infect nearby devices within Wi-Fi range.

Optimizations in modern mobile devices aimed at maximizing battery life actually allowed this vulnerability to have a broader impact. Ultimately, this Broadpwn created a new attack paradigm within the infrastructure that mobile devices inherently trust. With Apple and Google tightening security of their Operating Systems, more and more security researchers have started focusing on the security of peripheral components that will allow complete compromise of a device.

This type of attack can be mitigated at the OS level through Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP). Unfortunately, these two techniques mainly apply to the application process and have not been widely adopted on peripherals.

Attacks on the device trust model

When the attacker tampers with a user's device configuration, forcing it to implicitly trust the attacker and their malicious services.

PREVALENCE: WIDESPREAD

SEVERITY: HIGH

NOTES: REQUIRES AN INDIVIDUAL DEVICE TO BE HACKED AND IS OFTEN INITIATED VIA A PHISHING ATTACK OR PERSONALIZED MESSAGE

By far the most serious form of man-in-the-middle attack is those that involve tampering with certificates and profiles to make the device implicitly trust the attacker.

SSL certificates are a way of digitally certifying the identity of a website. They inform the user that their personal information has been encrypted into an undecipherable format that can only be returned with the proper decryption key.

Each device ships with a trust model of root certificate authorities that are trusted. In this manner a device will automatically trust certificates signed by these trusted authorities who vet applications for certificates.

If a malicious 3rd-party root certificate authority (CA) is installed and trusted on the device, a malicious actor can craft a certificate to any resource and the end-user will not be prompted for any error.

Our research shows that 4% of corporate mobile devices have come into contact with a man-in-the-middle attack in the past month. These range from intercepting data leaks to motivated attacks that compromise the device trust model.

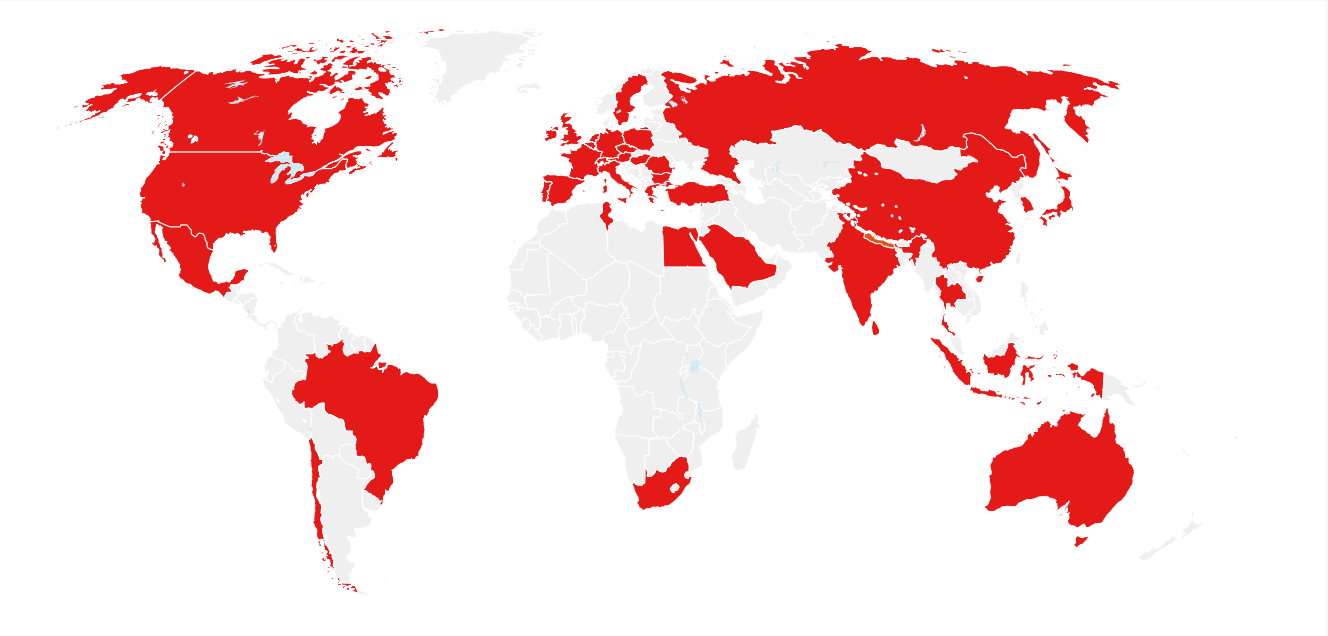
Certain applications work around comprised trust stores by certificate-pinning but web browsers have no such protection nor are they protected by other SSL-pinning methods today.

The below heatmaps show the prevalence of high severity man-in-the-middle attacks. This means the hacker has tampered with SSL certificates to execute the attack. The first map suggests these serious attacks are taking place in the world's developed regions. It might be tempting to think of Wi-Fi threats as only issues to be concerned about in notoriously dangerous places like China or Ukraine. However, the data shows that even more privacy and security-conscious locations, such as those in Western Europe and North America, are vulnerable to Wi-Fi attacks. As is the case with many other kinds of threats, attackers are targeting the places they believe they can get the biggest gains - and that means aiming at US and European businesses. This is a global issue that must be taken seriously.

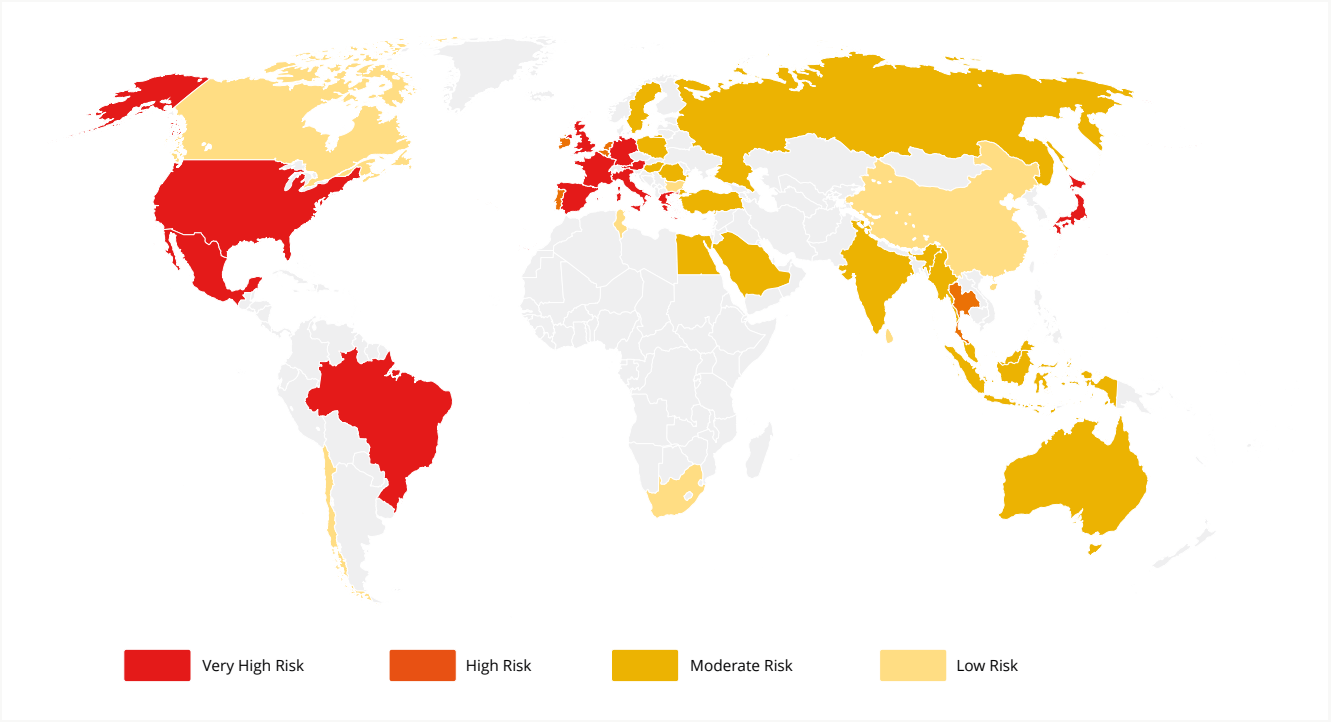
4%

PERCENTAGE OF CORPORATE MOBILE DEVICES THAT CAME INTO CONTACT WITH A MITM ATTACK IN NOVEMBER 2017

GLOBAL DISTRIBUTION OF HIGH SEVERITY MAN-IN-THE-MIDDLE ATTACKS ON CORPORATE MOBILE DEVICES*



HIGHEST CONCENTRATION OF HIGH SEVERITY MAN-IN-THE-MIDDLE ATTACKS ON CORPORATE MOBILE DEVICES.*



** This data was taken from a sample of the Wandera customer dataset, comprised of more than 500 global enterprises. While most organizations included in the sample set have physical offices headquartered in Western locations, the sample set included a large number of frequent travelers.*

Attackers are targeting the places they believe they can get the biggest gains.

HIGHEST CONCENTRATION OF HIGH SEVERITY MAN-IN-THE-MIDDLE ATTACKS ON CORPORATE MOBILE DEVICES.*

1. GERMANY
2. MEXICO
3. UNITED KINGDOM
4. FRANCE
5. SPAIN
6. ITALY
7. UNITED STATES

8. HONG KONG
9. AUSTRIA
10. PORTUGAL
11. LUXEMBOURG
12. JAPAN
13. BRAZIL
14. SWEDEN

15. GREECE
16. SAUDI ARABIA
17. SWITZERLAND
18. BELGIUM
19. SINGAPORE
20. POLAND

Protecting your business

Wi-Fi technologies, products, and attacks will continue to emerge. Security admins still need to be aware of new threats, assess their security posture, and take appropriate action to protect their networks and their corporate devices. The state of Wi-Fi security has significantly improved over the years. However, enabling Wi-Fi encryption will not make applications running over wireless networks safe. We recommend the following precautions:

- Avoid using open Wi-Fi networks to access sensitive information. Users should turn off Wi-Fi when trying to pay bills or make online purchases.
- If using public Wi-Fi is unavoidable, consider offering a VPN to your users. VPNs create a private network for your data in transit, adding an extra layer of security to your connection. You should ensure the VPN is routed securely and processed according to their standards (e.g., routing all of the traffic back through the HQ for processing).
- Have a security product that can detect insecure web services and block data leaks to dramatically reduce the risk that Wi-Fi threats pose.
- Configure your device settings to disable automatic connection to available Wi-Fi hotspots. This will prevent you from unknowingly connecting to public networks. It will also limit your digital exhaust. Enterprise Mobility Management (EMM) services can assist in managing device configuration centrally, eliminating the need to rely on end user action.
- Implement a security solution that can identify insecure hotspots and alert admins during suspected MitM attacks

Ultimately, as with much of information security, employee education plays an important part in Wi-Fi security at the device level. Employees need to be aware of how their smartphones are connecting to the internet, with or without permission, and what information is being shared.

The best way to protect your entire mobile fleet from malware is to have a security solution monitoring device traffic at all times and ensuring man-in-the-middle activity and communication with leaking apps and sites can be detected and blocked in real-time.

For more information or to request a free demonstration, visit

wandera.com/demo

ABOUT THE AUTHOR

Dan Cuddeford is Director of Sales Engineering at Wandera, the leading global provider of security and management for mobile data. Prior to this, Dan served as Enterprise Solutions Architect for Amazon Web Services, where he shaped and delivered customer strategy on all AWS products. An experienced engineer in network and cloud security, Dan has worked with start-ups through to global enterprises.

Earlier in his career, Dan served as Technical Solutions Manager at ScanSafe before it was acquired by Cisco. Here he was part of a team that grew from 25 to over 100, where he led pre-sales efforts and technical training in new markets. For the three years that following the acquisition, Dan served as Consulting Systems Engineer at Cisco, leading high value security projects for global enterprises.