Briefing Note

Public Wi-Fi: Stealing Secrets in the Sky

Introduction

'Free Wi-Fi' – a phrase so commonly heard today that we have come to expect it in most public places. The vast majority of hotels, restaurants, coffee shops and transport systems today offer some form of Wi-Fi network for its guests and customers. In recent years, exploits using equipment such as a Wi-Fi Pineapple have captured the attention of IT Professionals and have raised awareness of the vulnerability of public Wi-Fi networks to Man-in-the-Middle attacks. However, in reality such attacks are quite rare. A much more significant issue is the ease with which anyone can quietly view unencrypted internet traffic transmitted on any network to which they can attach.

Man-in-the-Middle attacks

A Man-in-the-Middle attack is initiated when an unsuspecting victim connects to a public Wi-Fi network but is tricked into connecting to a rogue access point. Once connected, they browse the internet as normal and may login to an online account. However, depending on the attacker's motives fake sites can be shown in place of real ones. This means that if the victim browses towards a site like Amazon.com and places an order, the Man-in-the-Middle will be able to read the login and financial details inputted and promptly steal them. These attacks can target both HTTP and HTTPS websites, however any communication with a website running HTTP is especially vulnerable as all data communicated is sent in plain text.

What may be most troubling about MitM attacks is that they are astonishingly quick and easy to set up. Wi-Fi Pineapples are freely available online and cost as little as $100. Following simple instructions on YouTube and manufacturer's forums, the device can be set up and a new network established in minutes. The Pineapple then reads 'probe requests' from nearby devices and pretends to be a legitimate network allowing the hackers complete overview of connected device browsing activity. However, attacks such as these using dedicated technology like Wi-Fi Pineapples are actually quite rare. There are much simpler ways to sniff Wi-Fi traffic.

Open Wi-Fi Networks

Most businesses and public places that offer free Wi-Fi do so with an open Wi-Fi network, allowing users to connect to an access point without the need for a password. Customers in the

vicinity simply select the network they wish to use from the list detected by their device and connect. However, what most users are unaware of is how easy it is for anyone nearby to gain access to the traffic or any information sent over this network. With basic IT skills and simple utilities (most of which are built into Macbooks) in the right location, anyone can sniff packets and perform a packet trace on a Wi-Fi network with unsecured traffic. This means that when using the network, both the content of the users' unencrypted traffic, i.e. their searches, messages, usernames and passwords, and their browsing destinations regardless of encryption, are made visible to the third party. This becomes especially dangerous when the content or destination of the user's traffic is sensitive or confidential in nature.

Closed Wi-Fi Networks

Unlike open networks, some public Wi-Fi connections do require a password to access the internet. However, despite their seemingly more secure systems, these too can be intercepted relatively easily. In reality, most public places that require a password to access their free Wi-Fi do not do so to provide extra security for the network but rather to limit access to paying customers only. Because of this, password protection actually does very little to prevent third parties attaching to closed networks and sniffing the same traffic that is visible on an open Wi-Fi network.

Even when the hacker does not know the password due to the limitations of Wi-Fi, widely available tools such as 'Wifite' or 'airodumping-ng' can be used to connect to a router, capture packets, and decrypt the password. WAP2 passwords in particular, if poorly configured, can be ascertained relatively easily in this way allowing anyone to attach to a network once they are in close proximity to the AP. Once access is gained to the network, all unencrypted traffic passing through is then made visible to the hacker, including the websites visited and users' login credentials.

Wired Network Connections

Wired networks provide some security for public internet access as, given the need for a physical connection, they are fundamentally more difficult to hack. Malicious actors need to find a cable point to plug into and presumably these are only available in particular physical locations making it harder to covertly hack or access a network. However, hacking wired networks is not impossible and once accessed, the same information can be made visible to an attacker as on an open wireless network.

Key takeaways:

- 44% of organizations' mobile workers connect to a non-corporate owned network more than half the time that they are working. As well as this, in 2018 87% of workers admitted to potentially putting company data at risk by accessing email, bank accounts, and financial information while using public Wi-Fi.

- So what can be done to protect sensitive data? In the case of public Wi-Fi the best protection is prevention. Employees need to be trained to avoid sending any sensitive information unencrypted over any network and to be aware that on any Wi-Fi or wired network, other than one to which access is controlled by themselves or an organization they trust, where they go online and any data accessed, received or sent can be made visible to anyone.

Want to find out more about how to protect your mobile devices from public Wi-Fi and other mobile threats?
Contact Corrata today