Securing your Wired and Wireless Networks

Navigating the Challenges with Wireless Security

White Paper

WatchGuard Technologies, Inc.
Published: January 2016

What could possibly supersede our basic needs for food, water, shelter and warmth? The answer is four letters: **Wi-Fi**! As we wait for all the psychology textbooks to be updated with Fig. 1, let's explore four drivers of Wi-Fi usage that are behind this explosion of wireless connectivity and the security implications we must not forget.

Figure 1

Wi-Fi Driver #1: Mobility

Overview

In the early days of Wi-Fi, the 1990s and early 2000s, we had a tempered view of Wi-Fi and its capabilities. For example, we didn't receive more than 54mbps until 2007 when 802.11n was introduced. During these times, Wi-Fi was mainly used in coffee shops, restaurants, and as corporate guest networks where no one was going to lose their job for "slow Wi-Fi." However, with the introduction of 802.11ac, for the first time in history, Wi-Fi speeds can match wire speeds. Providing gigabit speeds and beyond to Wi-Fi clients has smashed the door down for empowering businesses to utilize Wi-Fi for employee mobility. Users can seamlessly roam around their buildings and campuses at work while maintaining constant connectivity, allowing for a truly mobile workforce.

Security Threats

Employees are not always accessing the corporate Wi-Fi network using company-issued and securely-protected mobile devices. The Bring Your Own Device (BYOD) movement is in full swing which means that more smartphones and tablets are being introduced to corporate Wi-Fi networks and that these devices could also be compromised with malware looking to replicate itself.

Wi-Fi Driver #2: Hotspots

Overview

iPass is predicting the number of public "Wi-Fi hotspots" to grow from 22.7 million in 2014 to 289.3 million in 2018. The reason behind this explosive growth? Wi-Fi hotspots are excellent value-additions to a business, particularly those in the retail and hospitality industries. By offering Wi-Fi service to their guests and customers, businesses can increase customer loyalty, repeat business, and have a positive impact on their top lines.

There are many kinds of hotspots that we have all been exposed to: some that require no password to log in, others that do, and those that ask us to log in using our social network accounts. The hotspots

 Copyright ©2016

that require no passwords are open, using no encryption and should be joined with extreme caution as anyone with a simple packet sniffer can potentially pick up your login credentials to sensitive websites and applications if not using an encrypted authentication system; more on this later. The hotspots that require a "password of the day" are encrypted, but watch out, a sophisticated Wi-Fi attacker can exploit this and decrypt the traffic with ease with today's advanced Wi-Fi hacking toolkits.

Lastly, the hotspots that invite us to log in using our social network credentials are on the rise. This type of social Wi-Fi experience is popular to businesses, as through your social profiles, the business can now place demographic information with IP and MAC addresses such as age, gender and occupation. Through this data, powerful analytic software solutions can craft the placement of ads, unique to the individual, and have substantial impact on the businesses sales.

Security Threats

The devices that connect to hotspots are typically unmanaged and unknown to the business offering the hotspot. This means that protections like Mobile Device Management (MDM) to enforce security policies on smartphones are out the window. Although it's very common for hotspot network traffic to be completely isolated from the main corporate/backend network, there is significant brand tarnishing that could occur if a business offering free Wi-Fi access were to obtain a reputation for allowing people that join the hotspot to become victims of data theft. Wi-Fi hacking toolkits continue to progress in capability and are easy ways that even the most junior script kiddie hacker can successfully intercept data on public hotspots.

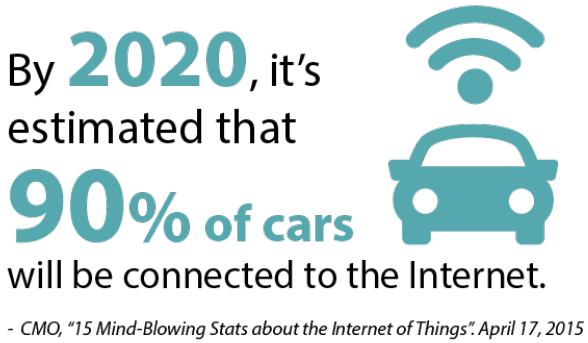
Wi-Fi Driver #3: IoT

Overview

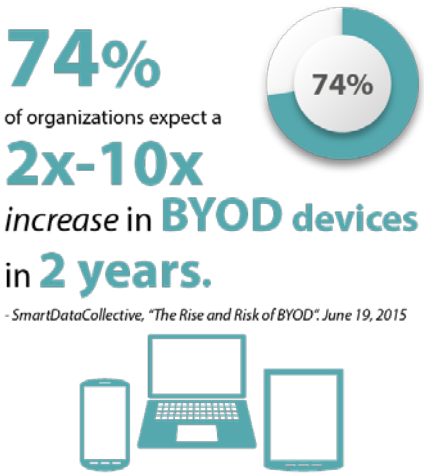
You probably knew this one was coming. The "Internet of Things" or IoT can take on many definitions, but for the purpose of this reading, let's assume we are talking about any Wi-Fi connected device that does not have a full-featured, GUI-rich operating system. Common examples include multi-function printers, IP security cameras, medical devices, and Point of Sale (POS) embedded systems. The IoT movement not only includes new products designed with wireless connectivity in mind such as smart watches, but also existing products that are being "IoT'd" by having Wi-Fi modules added to them.

Security Threats

The security threats posed to businesses and consumers coming from IoT devices are monumental. The consumer-grade devices such as smart watches are under immense pressure to be delivered to market as fast as possible for companies participating in this quickly evolving market to remain competitive.



A trade-off to a very fast time to market schedule is that security is typically not baked into the original product design. Additionally, the existing products that



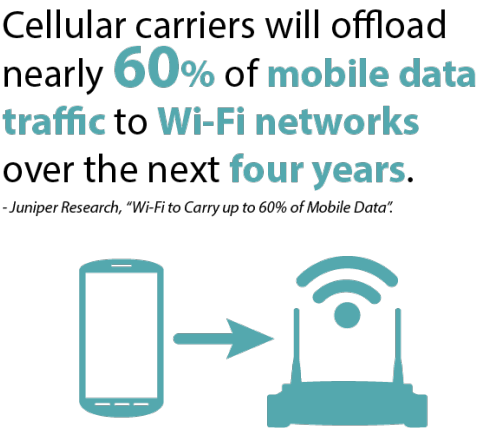
are being "IoT'd" are having Wi-Fi modules added into them. These Wi-Fi modules are the easiest, fastest way for a product design team to add Wi-Fi connectivity to their products and are considered bolt-on additions to the products. As bolt-ons, again, security is not a common priority among product teams.

Both types of IoT devices often run embedded or hardened computer operating systems designed for very specific operations such as monitoring a patient's blood pressure or the temperature in your conference room. These embedded operating systems often include well-known vulnerabilities that attackers can exploit to gain a foothold into a network and once inside, move laterally and pivot from the compromised IoT device. The IoT'd devices are particularly at risk and a report from TrapX security reveals how these IoT backdoors may exist for long periods of time without notice (http://deceive.trapx.com/rs/trapxcompany/images/AOA_Report_TrapX_AnatomyOfAttack-InternetOfThings.pdf).

Wi-Fi Driver #4: Cellular Offload onto Wi-Fi

Overview

If you haven't heard about this yet, you will soon enough. Essentially, the world's cellular carriers are running out of licensed spectrum to serve their customers. As more consumers buy smartphones, (which according to the FCC, use 24 times more data than a traditional cell phone) the need for more spectrum is greater than ever. The problem is, much of the spectrum for mobile signal transmission has already been licensed to wireless carriers, or is being used by TV broadcasters or government agencies, resulting in a declaration of spectrum shortage by the industry and the FCC[1]. Given that the explosive cellular market shows no signs of slowing anytime soon, cell carriers are implementing vast Wi-Fi hotspot networks throughout the world to offload a portion of the traffic they serve to give them some breathing room.



Security Threats

The security threats are very similar to offering a Wi-Fi hotspot, however cyber-attacks are a numbers game, and cellular offload to Wi-Fi means a much greater number of unknown devices connecting to the same Wi-Fi network as you. Security concerns are increased.

[1] CNET, "Wireless spectrum: What it is, and why you should care." August 13, 2012

Specific common wireless network security threats

Besides the aforementioned drivers behind the explosive growth in Wi-Fi and the security threats posed to connected clients, the following are specific threats that exist across any Wi-Fi network:

- **Wi-Fi Password Cracking:** Wireless access points that still use older security protocols, like WEP, are easy targets because those passwords are notoriously easy to crack.
- **Rogue Hotspots:** Nothing physically prevents a cyber-criminal from enabling a foreign access point near a hotspot with a matching SSID, which invites customers to log in. Users that fall victim to the rogue AP are susceptible to malicious code, which often goes unnoticed.
- **Planting Malware:** Customers that join a guest wireless network are susceptible to unknowingly walking out with unwanted malware, delivered from bad-intentioned neighboring users. A common tactic used by hackers is to plant a backdoor on the network, which allows them to return at a later date to steal sensitive data.
- **Eavesdropping:** Guests run the risk of having their private communications intercepted, or packet sniffed, by cyber snoops while on an unprotected wireless network.
- **Data Theft:** Joining a wireless network puts users at risk of losing private documents that may contain highly sensitive information to cyber thieves who opportunistically intercept data being sent through the network.
- **Inappropriate and Illegal Usage:** Businesses offering guest Wi-Fi risk playing host to a wide variety of illegal and potentially harmful communications. Adult or extremist content can be offensive to neighboring customers, and illegal downloads can leave the business susceptible to lawsuits.
- **Bad Neighbors:** As the number of wireless users on the network grows, so does the risk of a pre-infected device entering the network. Mobile attacks, such as Android's Stagefright, can spread from guest to guest, even if "victim zero" is oblivious to the outbreak.

What are the hackers after exactly?

The goal of hackers that target Wi-Fi networks varies depending on the environment. For example, in retail environments, attackers focus their efforts on extracting payment transaction details such as credit card numbers, customer identities, and mailing addresses. This information, although valuable, is only one-tenth as valuable on the market as medical personally identifiable information (PII) according to a report from Reuters[2]. Such medical PII is often targeted on healthcare Wi-Fi networks around the globe by hackers looking to extract more value for their efforts.

If not seeking specific valuable data, often attackers have longer-term goals such as finding a weakness in the Wi-Fi network and installing a backdoor from which they can gain access to the network remotely. There are common hacking toolkits to scan a Wi-Fi network for known vulnerabilities and exploit them in various ways. In the hotel industry, cyber security firm, Cylance reported such a vulnerability existing in many hotel Wi-Fi routers: (http://www.wired.com/2015/03/big-vulnerability-hotel-wi-fi-router-puts-guests-risk/).

Other goals of Wi-Fi hackers would fall under the category of opportunistically browsing the wireless LAN (WLAN) for weaknesses. These kinds of attacks, although not very targeted, are still incredibly malicious and can result in data theft, malware drops, and a generally poor quality of experience for everyone on the WLAN.

[2] Reuters, "Your medical record is worth more to hackers than your credit card," Sept. 24, 2014

How to avoid these Wi-Fi security threats

The world has decided that Wi-Fi is here to stay and demands that more and more client devices include Wi-Fi connectivity. As a business looking to embrace Wi-Fi as a means for employee and/or customer connectivity, the number of security threats and attack surfaces introduced to a network by adding Wi-Fi may seem daunting. However, there are several best practices to follow which will ensure your Wi-Fi network is not going to be on the front page news as the source of the next big hacking story:

- **Implement WPA2 Enterprise (802.1x) wherever possible**. It's one of the hardest encryption methods to crack and will provide the extra security your employee WLAN deserves.
- **All Wi-Fi traffic should at a minimum be inspected for:**
    - Viruses
    - Malware, including zero day threats and advanced persistent threats
    - Intrusion attempts
- **Implement application ID and control** for monitoring and optionally blocking certain risky traffic
- **Enable web content filtering** to prevent unsuspecting Wi-Fi clients from accidentally clicking a hyperlink that invites exploitation, malware, and backdoors to be loaded into your network

Summary

Although to the end-user of Wi-Fi service (which all of us are nowadays) all Wi-Fi service may seem to be created equal, the back-end Wi-Fi access points (APs) and their management systems are definitely not. There are the APs and corresponding management systems that were created along with the invention of Wi-Fi which focus purely on getting clients to connect wireless while passing any and all traffic, and there are those that do this with strong security safeguards. In the evolution of Wi-Fi, we are presently at a stage where the world now requires a secure Wi-Fi solution to serve our wireless needs.