WI-FI NETWORK THREATS AND ITS CHALLENGES MEASURES

Mr.Prakash Chandra Behera

Asst.prof, Dept.Of Computer Science, St.Claret College, Bangalore, India
prakasbehera@gmail.com,ph.No-9632145895

Abstract

In the recent years we have huge development of wireless technology. We are presently getting more subject to wireless technology. As we know wireless networks have broadcast nature so there are different security issues in the wireless communication. The security conventions intended for the wired systems can't be extrapolated to wireless systems. Hackers and intruders can make utilization of the loopholes of the wireless communication. Users must update to better security measures while connecting to open Wi-Fi hot-spots as they turn out to be more risky than useful. It would come across as a cause of concern to know that 42% of wireless 802.11 access points come with no security mechanisms. By this we mean they are not even protected by WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access).

This research paper lighted some common issues of Wi-Fi security threats, challenges and how to measure such challenges.

Keyword*: Wi-Fi, Eavesdropping, Security threats, Hotspots, WPA*

INTRODUCTION

Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter. The most well-known wireless technologies use electromagnetic wireless telecommunications, for example, radio. With radio waves distances could be short, for example, a couple of meters for TV remote control, or the extent that thousands or even a huge number of kilometres for profound space radio communications. It includes different sorts of fixed, mobile and portable applications, including two-way radios, cell phones, individual PDAs, and wireless networking.

Figure 1 shows an example of wireless communication. The various available wireless technologies differ in local availability, coverage range and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them. Supporting technologies include:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a/b/g/n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become normal standard for access in private homes, within offices, and at public hotspots.

Cellular Data Service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

Wireless Technology permits services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in **Telecommunications Industry** to refer to telecommunications systems (*e.g.*, radio transmitters and receivers, remote controls, computer networks, network terminals, *etc.*,) which use some form of energy (*e.g.*, radio frequency (RF), infrared light, laser light, visible light, acoustic energy, *etc.*,) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

The following situations justify the use of wireless technology:

1. To span a distance beyond the capabilities of typical cabling,
2. To provide a backup communications link in case of normal network failure,
3. To link portable or temporary workstations,
4. To overcome situations where normal cabling is difficult or financially impractical, or
5. To remotely connect mobile users or networks.

Wireless technology is becoming more and more popular due to so many advantages.

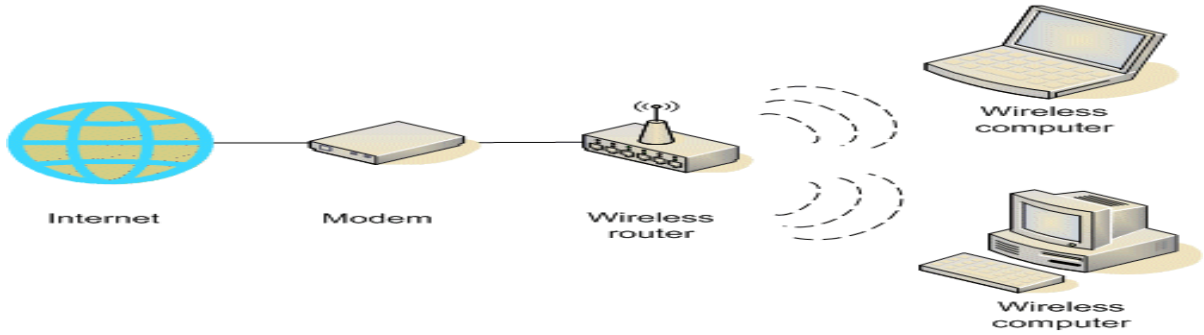

Figure 1. Wireless Communication

SECURITY GOALS

1) **Authentication:** This means that before sending and receiving data using the system the receiver and sender identify should be verified.

2) **Confidentiality:** Usually this function is how much people identify a secure system it means that only the authenticated people are able to interpret the message content and one else.

3) **Helvetica:** Integrity means that the content of the communicated data is be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

4) **Non–Repudiation:** This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

5) **Service reliability and availability:** Since secure systems usually get attached by intruders, which may affect their availability and type of service to their users. Such system should provide a way to grant their users the quality of service they expect.

SECURITY REQUIREMENTS

While any organization wants to protect its sensitive data, to detect tampering of data and to limit access to authorized individuals, various industries must also comply with an array of regulatory and industry requirements and guidelines [4]. One common requirement is that sensitive data that is stored or communicated over public networks must be encrypted using certified algorithms. Another common requirement is for users to authenticate themselves using two-authentication, generally achieved by a combination of something the user possesses such as a security token (*e.g.*, USB dongle or security smart card), and something the user knows (*e.g.*, password). Biometric approaches can also be used as one of the authentication factors. Regulations are becoming more stringent, both at the state and federal level. Organizations designing new mobile-access solutions need to plan accordingly to ensure they comply with both current and future requirements.

The WEP was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication. The working of the WEP can be understood with the help of sender side encryption and receiver side decryption.

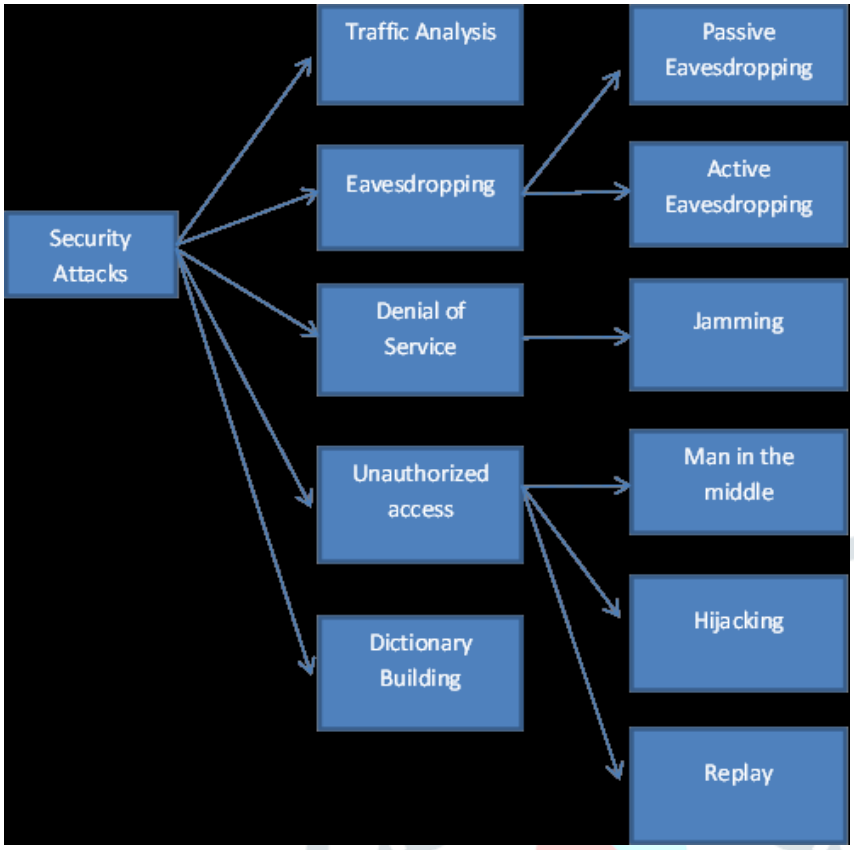

Figure 2. Different Types of Security Attacks

SITUATION TO HANDLE SECURITY THREAT

WI-FI: 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 : 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 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.

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- 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.

WI-FI : 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 FCC1. 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.

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 neighbouring 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 neighbouring customers, and illegal downloads can leave the business susceptible to lawsuits.

• **Bad Neighbours:** 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 Stage fright, can spread from guest to guest, even if "victim zero" is oblivious to the outbreak.

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
  1. Malware, including zero day threats and advanced persistent threats
  2. 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

CONCLUSION

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.

REFERENCES

1. Srilasak, S., Wongthavarawat, K.,andPhonphoem A, Integrated Wireless Rogue Access Point Detection and Counterattack System, IEEE April 2008.
2. "Ten Tips for Public Wi-Fi Hotspot Security" http://www.pcmag.com/slideshow_viewer/0,3253,l=254315&a=254312&po=3,00.asp , PC Magazine, (accessed October 16, 2014)
3. Public Wireless Network, http://www.microsoft.com/security/online-privacy/public-wireless.aspx (accessed November 13, 2014)
4. Sachin R. Sonawane, Sandeep Vanjale, Dr.P.B.Mane, a survey on evil twin detection methods for wirelesslocal area network, international journal of computer engineering& technology (ijcet)Volume 4, Issue 2, March – April (2013), pp. 493-499
5. IEEE Std. 802.11b, Supplement to part 11: Wireless LAn Medium AccesssControl (MAC) and Physical Layer (PHY) Specification: Higher Speed Physical Layer Extension in the 2.4 GHz band. 1999
6. S. Capkun,L.Buttyan, and J. HUBAUX,'Sector: secure Tracking of Node Encounters in Multi-hop Wireless Networks.proc.ofAcm Workshop on Security of Ad Hoc and Sensor Networks,' 2003
7. Deng,,W. Li,Agrawal,D P.,'Routing Security in Wireless Ad Hoc Networks,' Cincimmati Uni.,OH,USA;IEEE Communication Magazine,Oct. 2002, vol. 40,pp.70-75,ISSn :0163-6804
8. J. P. HuBaux ,L.Buttyam and S. Capkun., ,The Quest for Security Immobile Ad Hoc Network, , In Proc. ACM MOBICOM, Oct.2001
9. H. Hsieh and R Sivakumar, ,Transport over Wireless networks, , Handbook of wireless Networks and mobile computing
10. Y. Hu, A. Perrig, and D Johnson ,packet Leashes: A defence Against WormHole Attacks in Wireless Ad Hoc networks,'Proc. Of IEEE INFORCOM. 2002
11. J. Kong et al.,'Providing Robust and Ubiquitous Security Support for Mobile AdHocNetworks,'Prentice Hall PTR, A Division of Pearson Education Inc 2002
12. Kyasanur , and N. Vaidya, ,Detection and handling of MAC layer Misbehaviour in Wireless Networks,' DCC,2003
13. P. Michiardi. R. Molva, 'Ad Hoc Networks Security,' IEEE press Wiley, New York, 2003 *14+ IEEE Std. 802.11 i/D30, ,Wireless Medium Access Control(MAC) and physical Layer(PHY)Specification for enhanced Security,' 2002

14. Black, U., Internet Security Protocol: Protecting Traffic, Upper Saddle River, NJ: Prentice Hall 2000
15. Stalling, W., Cryptography and Network Security: Principles and Practice ,Upper Saddle River, NJ: Prentice Hall 2000
16. E. Ferro and F. Potorti, ,Bluetooth and Wi-Fi Wireless protocol: A survey and a Comparison ', IEEE Wireless Commmun., Vol 12, No 1, pp, 12-16, Feb 2005