Wi-fi network for an office building reports example

Law, Security

ABSTRACT

The rapid growth in information and communication has made people interconnected than ever before. Online activities are increasingly demanded on a daily basis whether in the office, in conference halls or while on the move. The activities range from information search, file sharing or report delivery and online purchases. Wireless network connection provides an option for people to be interconnected wherever they are even in rural settings. The appropriate wireless network for an office infrastructure is Wireless Local Area Network. This network type allows employees to interact seamlessly in the office setting while on stationary locations and on the move. This flexibility offered by wireless networks means that internet connection is not only restricted to office locations alone. People can now interact while in the cafeteria, on the corridors and even parking bays. It raises the issue of information security and privacy as data shared and transferred can be intercepted by attackers and third parties who are not authorized to. In this paper, we explore a Wi-Fi network for an office building. A Wireless LAN is preferred in the office setting. The paper explores the security vulnerabilities that are associated with Wi-Fi and how they can be mitigated. A review of the classic attacks in WLAN including identity theft, malicious association, network injection and denial of service among others is considered. Ways of increasing network security are also explored in the paper. Finally, a recommendation on the future of Wi-Fi network will be drawn considering future directions and an understanding of the underlying issue and expected changes.

BACKGROUND: WIRELESS TECHNOLOGY IN WIFI

Wi-Fi is a short range wireless transmission technology spanning hundreds of feet to support internet access using radio signals. There are two distinctive devices in a WIFI, wireless clients comprising of PCs with a wireless network card and access point acting as a bridge between the wired and wireless networks. A wireless access point is made up of a wireless and wired network interface. Access point is a wireless base station that aggregates multiple wireless access points in the cable network.

Wireless networks provide high speed wireless Internet connection. They are classified as Wireless Local Area Network, Wireless Metropolitan Area Network and Wireless Wide Area Network.

Wireless Local Area Network is made up of several components including access points, clients, routers and antennas. WLAN utilizes radio frequency signals as a transmission medium in the 2. 4GHz and 5. 0GHz medium. WLAN is defined by IEEE 802. 11 standard. There are different protocols defined in the 802. 11 family of standards with respect to various operating frequencies and maximum throughputs.

The appropriate network in this case is a WLAN because it will provide office employees the flexibility of conducting their operations without being restricted to the office space. With proliferation of mobile devices such as Smartphone, tablets and iPads, and the recently emerging Corporate Owned Personally Enabled phenomenon. There is increasing need for flexibility in the working environment that can only be offered by WLAN.

Wireless LAN is typically used in office and home premises. However, the

issue of security of data shared via these networks and privacy of users emerges as the top concerns.

SECURITY ASPECTS IN WLAN

Despite the productivity, cost advantage and convenience provided by WLAN, the radio waves utilized in wireless networks are at increased risk of being hacked. Security issues in wireless networks are broadly classified based on assets, perpetrators, vulnerabilities and threats. The assets that facilitate communication via wireless networks vary in their usefulness and priority. For instance, an asset for military communication is more prioritized in terms of security than one for commercial purpose.

With respect to vulnerabilities, systems failures, weak encryptions, failure of thrusters, power failures, signal distortion schemes, and signal strength determined by physical sizes of antennas all determine the security of a communication.

Finally, there are the perpetrators and of insecurity and threats. Perpetrators range from government players, to criminals to technology enthusiasts to business competitors to malicious employees, to eavesdroppers and thieves among others. The perpetrators impose threats on the communication system of an office either for malicious or unintended purpose. For instance, hackers may be after crucial trade secrets to be sold to competitors, while denial of service attacks may be as a result of rogue employees.

Attacks in 802. 11b protocol as well as other wireless solutions are set to increase significantly in terms of number and the complexity as time goes. The risks can be put into the following seven categories:

- Insertion attacks

- Jamming

- Encryption attacks

- Brute force attacks against access point passwords

- Mis-configurations

- Interception and unauthorized traffic monitoring

MAJOR SECURITY ISSUES

The three major security issues in WLANs are denial of service, spoofing and eavesdropping.

Denial of service

It is the kind of attack where an intruder floods the network with valid or invalid messages to affect the availability of the network resources. The nature of radio transmission in WLAN makes it increasingly vulnerable to a denial of service attacks. This is because bit rates in WLAN are low and can easily be overwhelmed and left open for denial of service attacks. A powerful transceiver, for instance, causes radio interference that would unable WLAN from communicating effectively using radio path.

Spoofing and session hacking

It is the most serious security issue with respect to privacy. An attacker can gain access to privileged data and resources in the network by assuming the identity of a valid user. It is the cause because 802. 11 protocols do not authenticate the Medium Access Control address of the frames. Attackers in this way spoof the MAC addresses and hijack sessions. 802. 11 protocols do

not require an access point to prove it is an AP. Thus, attackers who masquerade as AP have a chance of attacking the network.

Eavesdropping

It is an attack on the confidentiality of data that is traversing the networks. By their nature, Wi-Fi intentionally radiates network traffic into the space. It makes it increasingly difficult to control who receive the signals in a wireless LAN installation. Eavesdropping of the third parties is the most common threat in wireless networks. An attacker intercepts the transmission over the air distance from the office premises, compromising the confidentiality of data. In this case, an attacker located at the premises packing lot can comfortably eavesdrop the data transmitted by the employees.

HOW DRAMATIC THE SECURITY ISSUES ARE

In the case of insert attacks, unauthorized devices are deployed or new networks which are administered in a wireless medium are created without thorough review of the security aspect of the network. An attacker can try to make a connection to a client with a wireless access point without authorization. Where access points are configured not to need any password, an attacker will connect to internal network resources and cause damages. In the corporate network, an organization might not know of the fact that internal employees are creating wireless features on the devices. This situation where there is no awareness could be the source of insertion attacks with unauthorized employees gaining entry to resources which are at corporate levels by means of rogue access points.

Wireless traffic can be intercepted and monitored as long as the attacker is

within the range of the access point. The installation of an internal antenna determines signal access in corporate premises. Attacks such as wireless packet analysis and broadcast monitoring are common. For wireless packet analysis, the attacker captures the traffic using techniques and tools such as Wireshark on the first part of the connection session. The attacker then masquerades as a legitimate user and hijacks the user session or issue unauthorized commands.

If an access point is connected to a hub instead of a switch, any traffic across the hub can be broadcasted over the wireless network and monitored. It is even more sensitive data not intended for wireless clients is revealed.

An attacker with proper tools (most of which are readily available from the internet) can flood the 2. 4GHz frequency, corrupting the signal and disrupting communication completely. The source of the attacks can be external to the network or inadvertently come from 802. 11 devices installed on the network.

WAYS OF IMPROVING SECURITY

Securing wireless networks varies according to the security requirements of an organization. Existing security safeguards include authorization, authentication, encryption, firewalls physical controls and reducing visibility to traffic flows. Other additional controls are intended to increase safety of the corporate network and spans from employee education, antivirus applications, penetration testing hierarchical access controls to redundant systems and surveillance.

Security of the corporate resources can be achieved in a number of ways.

There are technical controls, logical controls and physical controls aspects. An internal network that is properly configured to handle wireless traffic will have firewalls, intrusion detection and prevention systems to monitor traffic on the wireless segments data encryption capabilities.

In the figure below, two firewalls are used, one to control access to and from the internet and the other to control access to and from wireless access point. The access point comprises of dedicated IP addresses for remote management through SNMP while the wireless clients may also employ SNMP agents for remote management. The network comprises of sensors that ensure that each unit is correctly configured and guard against alteration. The wireless network is frequently monitored to identify access points in use and ensure that they are authorized and properly configured.

The first IEEE 802. 11 standard utilized for protecting WLAN is the Wired Equivalent Privacy WEP. WEP mandates all clients and access points to share up to four different symmetric keys. This provision makes it difficult to implement large installations. Apart from this, there are other drawbacks that include: simple encryption algorithms, simplicity in cracking keys, complex key management, and the requirement for an external key management control system among others.

WPA protocol was proposed to solve WEP issues such as inability to prevent forgery of packets, improper use of RC4 and brute forcing on standard computers. Enterprise WAP uses an authentication server 802. 1x to guarantee user security. It combines 802. 1x server and EAP for authentication and TKIP encryption.

WPA2 protocol is an advanced WPA protocol that is based on AES national

standard cipher mixed with sophisticated cryptographic techniques. AES-CCMP is a standard developed for wireless networks for [personal or enterprise security. The enterprise security protocol is founded on 802. 1x EAP authentication framework and secure key distribution.

802. 11i wireless protocols allow secure and flexible wireless network suitable for corporate functions. It allows client authentication, key distribution, and the essential for roaming pre-authentication.

CONCLUSION

The preference of wireless LANs for corporate use is attributed to the cost and the support it offers employees in a corporate network to connecting to same resources in multiple office locations. The 802. 11b standard shares unlicensed frequencies with other devices including Bluetooth and PAN. Though the technologies can interfere with each other, it also fails to delineate roaming strategies leaving each vendor to implement a different solution. Thus, future proposals should consider these shortcomings in 802. 11.

For the foreseeable future, wireless technologies will continue to be preferred the choice over wired networking. Wireless LAN is a perfect way to improve data connectivity in an existing building without installation expenses. In corporate settings, it accords the flexibility to users and makes it easy to connect. However, security considerations should come first owing to the importance of securing data in corporate organizations.

References

Feng, P. (2012). Wireless LAN security issues and solutions. Robotics and Applications (ISRA), , IEEE.

Gonzalez, D. (2010). Home Wireless Security ands Privacy. Sixth Advabced International Conference on Telecommunications.

Hamid, R. A. (2012). Wireless LAN: security issues and solutions. GIAC Security Essential Certification .

Mavridis . I. P., H. P. (2011). Real life paradigm of wireless network security attacks. 2011 Panhellenic Conference on Informatics.

P., H. (2012). WiFi network information security analysis research. 2012 Conference on computer and information science.