Good example of wireless network security research paper

Sociology, Violence

Pedro J. Gonzalez

ISSC456

American Military University

I. Introduction.

The use of wireless network has increased due to its low cost and accessibility. Many businesses have switched to the use of wireless networks because of convenience and the ability of their employees having access to data while on the road. Although it is convenient, it does have some vulnerabilities. There are several modes of unauthorized access to wireless networks such as man-in-the-middle attacks, Denial of Service (DoS), identity theft (MAC spoofing), network injection, etc. With an increase of unauthorized access to networks, there are several security measures administrators can implement to prevent any of the aforementioned intrusions. With strong security measures, businesses can continue production without the loss of money or assets.

II. Threats and Vulnerabilities

Wired and wireless networks differ by one of the essential features of networks – the existence of uncontrolled areas between the end points of the wireless network. This allows the attacker or intruder in the immediate vicinity of the wireless structures, producing a series of attacks that are not possible in the wired world.

Radio-beacon monitor station broadcasting. The access point turns on a radio beacon with a specific frequency in order to inform the neighboring wireless nodes of its presence. These broadcast signals contain basic information about a wireless access point, including, generally, SSID and the

wireless nodes are offered to register in the given network. Thus, radio-beacon monitor station broadcasting is a congenital defect of wireless networks. A variety of models allow disabling a SSID containing part of such a broadcasting to complicate the wireless eavesdropping, but, SSID, however, is sent upon connection, so there is still an area of vulnerability.

WLAN detection. The NetStumber utility together with a satellite navigation of the global positioning system (GPS) is usually operated to detect WLAN. The given utility identifies the SSID of a certain WLAN and specifies whether the network is using WEP encryption system. Application of the external antenna on a laptop enables WLAN detecting while bypassing the desired area or traveling through the city. A reliable method of WLAN detecting is surveying the office building with laptop computer.

Audio interception and eavesdropping. These processes are carried out in order to gather required information in the network which is planned to be attacked later. The interceptor can use the data obtained in order to gain access to network resources. The equipment used for network eavesdropping can be even no complex than the usual network access point equipment. Wireless networks inherently allow the connection to the physical network to computers that are at slight distance and in case if the computer is directly online. For instance, to connect to a wireless network, located in the building, the one does not need to be located too close or too far from the access point – the intruder can even be located in a car parked next to the office. Passive eavesdropping attack is almost impossible to detect.

Invalid access points. An experienced attacker can organize an invalid

access point with simulated network resources. Subscribers, suspecting nothing, turn to this false access point and provide it with important details, such as authentication information. This type of attack is sometimes used in combination with a direct network access “ jamming” of the true access point.

Denial of service. Complete network paralysis can cause such attacks as DoS (Denial of Service). It is aimed to create the interference with access to network resources. Wireless systems are especially susceptible to such kinds of attacks. The physical layer of a wireless network is an abstract space around the access point. An attacker can turn the device on, filling the entire range of the operating frequency interference and illegal traffic – such a process is none of any difficulties. The DoS-attacks fact on the wireless network physical level is difficult to prove.

Man-in-the-middle attacks. Such attacks are executed on wireless networks which is much easier than wire attacks since in the case of a wired network a certain type of access is required to implement such an intrusion. Usually man-in-the-middle attacks are used to destroy the confidentiality and integrity of the communication. MITM attacks are more sophisticated than the other attacks because their implementation requires detailed information on the network. An attacker usually substitutes the identification of one of the network resources. This provides the opportunity to eavesdrop and illegally seizure the data streams in order to change its content required to meet some of their goals, such as spoofing IP-addresses, MAC address changes for simulating another host, etc.

Anonymous Internet access. Unprotected wireless LANs provide hackers with

the best anonymous access for Internet attacks. Hackers can use an unprotected wireless LAN of a company to access the Internet to carry out illegal activities without leaving any traces. An organization with an unsecured LAN formally becomes a source of attacking traffic aimed at another computer system that is connected to the potential risk of liability for damages to the victim of hackers' attack.

III. Modes of Unauthorized Access

Man-in-the-middle Attacks

A man-in-the-middle attack is one in which the intruder covertly blocks and transfers messages between two sides who accept they are corresponding specifically with one another. This is actually a type of eavesdropping when the whole communication between two parties is controlled by attacker who is even able to adjust the substance of every message send. Regularly abridged to MITM, MitM, or MITMA, is now and again alluded to as a session of seizing assault; it has an in number possibility of achievement if the aggressor can mimic every gathered message as per the general inclination of the other. MITM assaults represent a genuine risk to online security in light of the fact that they give the aggressor the capacity to catch and progressively control sensitive data while acting like a trusted gathering amid exchanges, discussions, and the exchange of information.

An adequate system for executing MITM assault includes malware distributing for receiving the access to the client's browser and the information it operates. Malware can likewise be utilized for adding passages to the Hosts file located on the user's computer as well as the DNS cache. It

allows diverting the user to the site he/she desires to reach which looks just the same. The assailant then makes an association with the genuine site and goes about as an intermediary, having the capacity to peruse, embed and alter the movement between the client and the real site before sending them on. The targets of such attacks are usually relates to e-banking systems since the intruders can easily capture the login data and other required information even in case of webpage encryption by the means of SSL/TLS communications.

An aggressor can likewise misuse vulnerabilities in a remote switch's security design, for example, a feeble secret key to dispatch a MITM assault and capture data being sent through the switch. A malevolent switch can likewise be setup in an open spot like a bistro or inn for the same reason. Different ways that assailants can do while MITM attack include spoofing ARP, DNS, STP redirection, disfiguring the switch and tunneling the traffic sent through the switch.

Most of the protocols providing the cryptographic security incorporate some type of endpoint validation particularly in order to anticipate MITM assaults. Thus, TLS verifies the client’s equipment utilizing a commonly trusted certification. On the other hand, unless clients take into account the notices when a suspect endorsement is introduced, MITM assaults can even now succeed with false or forged declarations.

Denial of Service (DoS)

Denial of service assaults are described by an express endeavor by aggressors to forestall clients of an administration from utilizing that administration. The typical examples are:

In the way of attempts of flooding a network the intruder averts real system activity;

Attempts to keep a certain individual from getting to an administration or receiving a certain service;

Attempts to disturb associations between two equipments, accordingly averting access to an administration

Service denial to a certain client or user.

It is noteworthy that not all the services blackout, even those that outcome from vindictive activities, are essentially for such assaults. Different kinds of assault may incorporate a dissent of certain service as a part, yet the disavowal of the service may be a piece of a bigger assault on the network. Illegitimate utilization of assets or sources may additionally bring about dissent of service. For example, a gatecrasher may use your unknown ftp range as a spot to store unlawful or illegal duplicates of business programming, devouring circle space and creating system traffic activity. Dissent of-service can basically impair both PC and network system. Contingent upon the way of your endeavor, this can viably cripple the organization.

Some DoS attacks can be executed with restricted assets against a vast, refined site. This kind of assault is once in a while called a “ lopsided assault” or “ asymmetric attack”. The example of such an attack is when an assailant

with an old equipped PC and a slow connection may have the capacity to cripple much quicker and more modern machines or systems.

DoS attacks are usually targeted on services and cause harm due to destruction of non-renewable sources of the client, configuration abolition and network components physical extermination.

Network Injection

These assaults are in view of a solitary issue that holds on in numerous advancements: to be specific, no strict division exists between instructions of program and the client information. This issue is considers by hackers to sneak system directions into spots where the designer expected just considerate information. By sneaking in program instructions, the intruder educates the system to perform activities of the assailant's desires. The hacker attempts the location information in order to perform a successful intrusion. There are three components of a successful network injection. Since the network injection process is heavily dependent on the language the program was developed as well as the injured hardware equipment. Thus, a key point to successful attack lies through identification of running programs and application requiring Internet access. This is possible due to having access to the footers, pages errors, etc. also, such tools as THC-Amap, Nmap and Nessus are commonly used to provide the above possibility.

The second key point lies in the necessarily to define user inputs. Sure, some of them are rather evident, like commonly used cookie and other HTML headers providing the hacker with the required data. Thus, to manipulate the

hidden information on inputs (since lots of scripts are not seen even by the end users), the attackers often utilize such applications as WebScarab and Burp. They provide proxy of web pages.

IV. Security Measures

SSID Hiding

Considering the SSID hiding, it includes 32 alphanumeric characters, thus it is sensitive to case. Each kind of identifier is connected to the header of bundles sent through the wireless network. In such a case it is a password for devices trying to access the basic service set. This is a component of 802. 11 IEEE protocol of WLAN architecture which is actually a connection to the wireless adapter. Wireless stations are BSS in cases when at least one access point is connected to the wired network.

Also, the SSID plays the role of separator of different WLANs. This is why all the devices and all access points which try to access a certain wireless network must use the same SSID. This, in its turn, provides for effective roaming. In addition, network interference card will not be permitted to receive the access to the available basic service set in case if the above mentioned asset has a different SSID. In this case access point denies the network access. The router by default broadcasts the SSID and lets the clients within the network range connect their devices to the available network.

We can conclude that the SSID is a rather weak security measure. Most access point transmit the SSID even by several times per second, so a hacker using means of 802. 11 analysis to identify the SSID. Sometime when

SSID broadcasting is enabled, it still can be reached from the frames used by stations for access point associating.

MAC ID Filtering

MAC addresses' filtering is supported by modern access points and wireless switches. However, it is not included in 802. 11 standards, but this feature is planning to be improved in terms of safety in future. This feature is implemented by creating a table of MAC-addresses of the wireless adapter which is authorized to operate the network. Then, there are tree available ways of implementing a filtration. Stations with any MAC-addresses can have access by the means of access point; the devices which have trusted MAC-addresses can access the network; the network access is denied to those devices which have MAC-addresses listed in the black list. The second way is the most reliable from the perspective of security, but the drawback of this method is the absence of MAC-address substitution, which allows the intruder to easily carry out the network attack.

802. 11 Security

Thanks to the efforts of Wi-Fi equipment providers deploying a wireless network can be carried out even by an untrained user. The majority of devices come out pre-configured by the default settings, which allow to immediately starting working with equipment even without looking thought system settings. Most of them are rather cheap, and this is amount of money costing you for intentional or unintentional hacking your network from own employees who have established without the consent of its own access point and did not take care of ensuring proper security measures. Another great

bigger problem is that wireless users are mobile by definition. Users may appear and disappear, change their location, and are not tied to fixed entry points, as with wire networks, so they can be anywhere in the network coverage area. All this greatly complicates the task of holding intruders beyond the threshold and tracking sources of wireless attack. Because the radio signals are broadcast by their nature, they are not limited to the walls of buildings and available to all receivers, the location of which is difficult or impossible to fix - attackers are particularly easy and convenient to attack the wireless network.

Conclusions

Modern wireless networks generate new classes of risks and threats, from which it is impossible to protect the network by traditional wired means. Even if the organization is formally banned by Wi-Fi it does not mean that someone from the users does not set a stranger, and it will bring down all the investments in networks safety to zero. In addition, due to the wireless features, it is important to monitor not only the security of access infrastructure, but also to monitor the users who may be subject to malicious attacks or simply can accidentally or deliberately go to the corporate network on an insecure connection. However, most of these risks can be minimized or even nullified

References

Cannings, R., Dwivedi, H., Lackey, Z. (n. d.) Common injection attacks. Retrieved from http://searchitchannel. techtarget. com/tip/Common-injection-attacks

CERT (1997). Denial of Service Attacks. Retrieved from https://www. cert. org/information-for/denial_of_service. cfm?

Kan, M. (2015). Microsoft's Outlook. com faces brief man-in-the-middle attack in China http://www. pcworld. com/article/2872392/microsofts-outlookcom-faces-brief-maninthemiddle-attack-in-china. html

Kennedy, S. (2003). Best Practices for Wireless Network Security. Retrieved from http://www. computerworld. com/article/2573986/mobile-wireless/best-practices-for-wireless-network-security. html

Rouse, M. (n. d.). Man in the middle attack (fire brigade attack). Retrieved from http://searchsecurity. techtarget. com/definition/man-in-the-middle-attack

Stewart, J. (2014). Firewall Fundamentals. In Network security, firewalls, and VPNs (2nd ed.). Burlington, Mass.: Jones & Bartlett Learning

http://www. sans. edu/research/security-laboratory/article/wireless-security-1

http://www. pcworld. com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now. html