RESEARCH PAPER | Computer Science | Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

Wireless Lan Vulnerabilities, Threats and Countermeasures

KEYWORDS: Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding

Sridevi

Assistant Professor, Department of Computer Science, Karnatak University,Dharwad,State:Karnataka.India 580003.

ABSTRACT *Implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities; wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. In recent years, wireless LANs are widely deployed in places such as Business- organizations, government bodies, hospitals, schools and even home Environment. Mobility, flexibility, scalability, cost-effectiveness and rapid deployment are some of the factors driving the proliferation of this technology. However, the architecture of this technology made it insecure as WLANs broadcast radio-frequency (RF) data for the client stations to hear. The main aim of this research paper is to encourage network and security administrators to carry out risk assessment so as to identify the risks and threats relating to their information system, and then deploy adequate control measures to reduce or eliminate possible risk.*

1. Introduction

Wireless communication has broken the constraint users used to have with wired technology. The liberty to gain access to corporate network without being bonded, mobility while accessing the Internet, increased reliability and flexibility are some of the factors driving the wireless local area network technology[1]. Other factors that contribute to tremendous growth of Wireless Local Area Networks (WLANs) are reduced installation time, long-term cost savings, and installation in difficult-to-wire areas. Today, Wireless Local Area Network (WLAN) is a choice to reckon in various sectors, including business, education, and government, public and individual. IEEE 802.11 dominates the wireless networking technology. This can be attributed to the low cost of the hardware and high data rates that support current applications (from 1 to 54 Mbps) as well as promising future extensions (possibly exceeding 100 Mbps with 802.11n). Increasingly, portable devices (Laptops, PDAs, and Tablet PCs) are being sold with wireless LAN as a standard feature.

2. Types of Wireless LANS

The part of success behind the popularity of WLANs is due to the availability of the 802.11 standard from IEEE. The standard specifies operation of WLANs in three ways:

2.1.1 Infrastructure Mode

An infrastructure mode consists of a group of 802.11 devices communicating with each other through a specialized station known as the access point (AP). The client stations do not communicate directly with each other, rather they do with the access point which forwards the frames to the designated station. The access point (also often referred to as a base station) is connected to the wired network infrastructure. If only one access point is involved, then we have a basic configuration referred to as a BSS topology in the 802.11 standard. Communication between wireless nodes, wireless computers and the wired network will be via the AP. For communication of data to take place, wireless clients and AP's must establish a relationship, or an association. It is only after an association is established can the two wireless stations exchange data [2].

2.1.2 AD HOC Mode

This consists of a group of 802.11 stations that communicate directly with one another within a limited range. It is essentially a simple peer-to-peer WLAN, and it is sometimes referred to as IBSS topology. Here, there is no need for access point and the networks do not require any pre-planning or site survey. So, the network is usually a small one and only last long enough for the communication of whatever information that needs to be shared.

2.1.3 Mixed Network Mode:

Every WS can work in the above two modes simultaneously. This is also called the Extended Basic Service Set (EBSS) [3].

3. Wireless LAN Vulnerabilities, Threats and Countermeasures

To prevent unauthorized use risk posed by unsecured wireless access points, Wired Equivalent Privacy (WEP) - a low-level data encryption system – was invented for wireless security purposes. WEP protocol protects link level data during wireless transmission between clients and access points. It does not provide end-to-end security, but only for the wireless portion of the connection. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. The encryption keys must match on both the client and the access point for frame exchanges to succeed. A successor to WEP is Wi-Fi Protected Access (WPA). Introduced in 2005 as an intermediate measure to take the place of WEP while 802.11i was prepared, WPA avoids most of WEP's vulnerabilities by making heavier use of dynamic/temporal keys, using the Temporal Key Integrity Protocol (TKIP) [5].

Ratified on 24 June 2009, Wi-Fi Protected Access 2 (WPA2) is the follow-on security method to WPA. WPA2 uses the Advanced Encryption Standard (AES). There is virtually no known wireless attack against AES. CCMP is the security standard used by AES. CCMP computes a Message Integrity Check (MIC) using a proven Cipher Block Chaining (CBC) technique. Messages are encrypted using a 128-bit secret key and a 128- bit block of data. The result is an encryption scheme that is very secure.

3.1 WLAN Security Attacks

Attacks on wireless LANs are aimed at the confidentiality and integrity of an information, and network availability. These security attacks can be passive or active [4]. Figure 1 shows a general taxonomy of WLAN security attacks.

2.0.1 Passive Attacks

Consist of unauthorized access to an asset or network for

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

the purpose of eavesdropping or traffic analysis, but not to modify its content. This is tricky to detect because data is unaffected. Consequently, emphasis is on prevention (encryption) not detection. There are two phases to an attack. The first phase is referred to as the reconnaissance phase, this is a passive attack. During the reconnaissance phase, the goal of an attacker is to discover a target network, and then gather information about the network. The attacker does this in a way that is unnoticeable. However, some of the means of reconnaissance can be detected by an intrusion detection system There are two methods used in executing undetectable passive attack: eavesdropping, and traffic analysis.

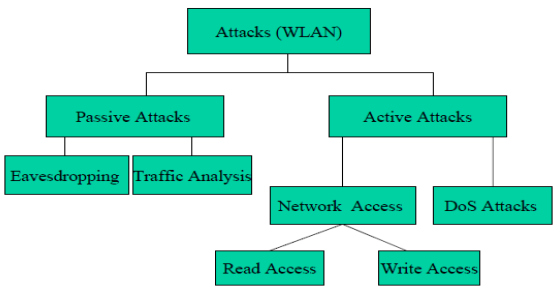

Figure 1: General Taxonomy of WLAN security attacks

Eavesdropping: Is the capability to monitor transmissions for message content. An attacker listens and intercepts wireless signals between the AP and wireless client.

Traffic analysis: Is the capability to gain intelligence by monitoring transmission for patterns of communications, or perform packet analysis. This can be carried out even when the messages are encrypted and cannot be decrypted.

3.1.2 Active Attacks

An active attack is one whereby an unauthorised change of the system is attempted. This could include, for example, the modification of transmitted or stored data, the creation of new data streams or limiting an organization's network availability. Active attacks may take the form of one of four types (or combination): masquerading, replay, message modification, and denial-of-service (DoS).

Masquerading: An active attack in which the attacker impersonates an authorized user and thereby gains certain unauthorized privileges. It could be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt could come from an insider, an employee for example, or an outsider through the public network. Once entry is made and the right access to the organization's critical data is gained, the attacker may be able to modify and delete software and data, and make changes to network configuration and routing information.

Replay: Also known as Man-in-the-Middle attack, a replay attack is one whereby the attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction.

Message modification: The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

Denial-of-service: The attacker prevents or prohibits the normal use or management of communications facilities. DoS attacks can range from physical destruction of equipment, disruption of certain network services to a specific person or system, prevention of a particular individual from accessing a service to flooding a network, thereby preventing legitimate network traffic. Below are some common practices for accomplishing DoS:

- Deploy radio-jamming equipment
- Saturate a network' bandwidth by continually broadcasting frames
- Conduct disassociation/de-authentication attacks
- Conduct transmit duration attacks by configuring the transmit duration field to a maximum of 30-packets-per-second rate

Access control attacks: These attacks attempt to penetrate a network by circumventing filters and firewalls to obtain unauthorized access. MAC spoofing (also known as identity theft) and Rogue Access Points are more common among these.

Integrity attacks: These attacks send forged/modified control, management or data frames over wireless to mislead the recipient or facilitate another type of attack. Denial-of-service attacks are the most common of the attacks that can be facilitated by this.

Confidentiality attacks : These attacks attempt to intercept private or sensitive information sent over wireless associations - whether sent in the clear or encrypted by 802.11 or higher layer protocols .Eavesdropping, WEP Key Cracking, Evil Twin AP (poorly-understood attack) and Man-in-the-Middle (a form of active eavesdropping) are the most common attacks in this Category.

Authentication attacks : Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services. Dictionary attack and brute force attack are the two most common techniques employ here by the attackers to achieve their objectives.

Availability attacks : These attacks attempt to inhibit or prevent legitimate use of wireless LAN services. The most common type of availability attack is the denial-of-service (DoS) attack, known as RF Jamming in the wireless world.

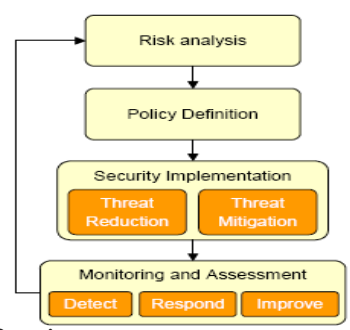

Figure 2: Security as a process

3.2 Risk Analysis

Risk is chances of threats in getting benefits from defects or weaknesses which are causes of losses and/or damages to assets or groups of assets, effecting an organization directly or indirectly. Risk analysis is an effective tool in WLAN threat management. With this a good security policy can be derived and implemented to defend the WLAN against possible attacks [5]. On-going monitoring and periodic testing can then be used to verify that a deployed WLAN meets defined objectives. Vulnerabilities discovered in the process are then (re)analyzed so as to refine the policies and/or apply fixes. This iterative process is illustrated in the figure2. It's extremely important to understand the attacks that might affect a network. However, it should be noted that some attacks are less likely or more damaging than others. More also, it should be noted that it is not practical or possible to defend any network against all possible attacks. A more realistic goal is to reduce associated risk to an acceptable level. Risks are

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

put into perspective by identifying one's own WLAN's vulnerabilities -the probability that attacker will exploit them - and business impact would occur.

The following points are necessary in performing risk analysis

- Define business needs
- Document who needs WLAN access, and where?
- Identify users or groups permitted to use 802.11 at the office, on the road, and at home.
- Determine resources reached over wireless
- Which applications, databases, and shares must be opened to wireless users, and When?
- Next, quantify new business risks caused by adding wireless.
- What information do those services and databases contain?
- Consider data that resides on wireless stations and flows over wireless links
- For each asset, estimate the likelihood of compromise and potential cost to business, using quantifiable metrics like downtime, recovery expenses, etc.

Completion of this process provides a prioritized list of at-risk assets. Base on this, a security policy that defends important assets from wireless-borne attack, balancing cost/benefit and residual risk can be written. Next step is to select, install, and configure countermeasures that implement and enforce the security policy.

3.3 Conducting a Vulnerability Assessment

A vulnerability assessment is an explicit study that uses penetration testing and observation to identify security weaknesses that could be exploited, and the risks. The results obtained are then evaluated to determine severity and steps to reduce or eliminate the threats. To be truly effective, assessments should be carried out regularly to spot out newly-introduced vulnerabilities and verify that installed security measures are working as intended. Assessments may be performed by in-house or third-party staff, with full, partial, or no knowledge of the organization network and security implementation.

3.3.1 Vulnerability/Penetration Testing

The overall objective of penetration testing is to discover areas of the enterprise network where intruders can exploit security vulnerabilities. These tests are typically performed using automated tools that look for specific weaknesses, technical flaws or vulnerabilities to exploit, with the results presented to the system owner with an assessment of their risk to the networked environment and a remediation plan highlighting the steps needed to eliminate the exposures. Various types of penetration testing are necessary for different types of network devices. For example, a penetration test of a firewall is different from a penetration test of a typical user's machine. Even a penetration test of devices in the DMZ (demilitarized zone) is different from performing a scan to see whether network penetration is possible. The type of penetration test should be weighed against the value of the data on the machine being tested and the need for connectivity to a given service [3].

3.3.2 Using Wireless Intrusion Protection System (WISP) To Monitor Activity

WIPS is a network monitoring tool that runs round the clock and pinpoints attacks or attempted attacks on wireless network. It is an extension of the advanced protection found in wired firewall and virtual private network security systems. WIPS can be extremely useful during a WLAN vulnerability assessment, as WIPS can triangulate a discovered device's location on a floor plan, making searches more efficient .WIPS helps to spot misconfigured devices, actual attacks that may have occurred recently, problem-prone locations and devices that may warrant additional scrutiny and on-going risky user behaviour by generating policy-based alerts. Also during penetration testing, WIPS can confirm that tests are working as expected. It can teach how to recognize signs of attack. It can record information needed for incident investigation or understanding of its impact, long after the attack ends. WIPS can even combine current and past observations to suggest how to mitigate threats. Penetration test results can, in the other hand, help to fine-tune WIPS.

3.4 Countermeasure

If there are vulnerabilities, then there are their countermeasures also, which cannot overcome them fully but can protect to a great extent. Here are few countermeasures, which can help a lot in retaining security of WLAN.

- Change the Access Point default Admin password, always update the Access Point firmware and drivers for the wireless Adapter(s)
- Do not trust WLAN and work under the coverage of a VPN (Virtual Private Networks).
- Maintain a good key management system, which changes the key before the sufficient no of packets required for cracking the key are transmitted.
- Increasing the bit length of IV and secret key is also a partial solution.
- Use of strong algorithm like AES
- Making the checksum of the message a keyed function, using algorithms like HMAC: Keyed Hashing.
- Configuring AP for allowing only few MAC addresses, which are there in his Access Control Lists (ACLs).
- Define the ACL depending upon Signal strength.
- One must take care of the physical security also. You should take care that no unauthorized person gets access of your laptop or any Work Station, which is in the Network because he can just copy the secret key.
- Enable RADIUS or Kerberos authentication for workstation to Access Point.
- Enable IPSec or Application level encryption for secure data communications
- Requires strong authentication of management and control frames.
- Use of Wireless Intrusion Prevention System (WIPS);

4. Conclusion

The following conclusions were drawn:

1. WLAN technology has inbuilt security problems in its architecture, as the APs and the clients must advertise their existence through beacon frames, thereby exposing the signals to attackers.
2. There exist a wide range of attacks - from passive to active- on wireless LANs, and are aimed at the confidentiality and integrity of an information, and network availability as shown in table 7. Some of the attacks are less likely or more damaging than others, and some are more common than others.
3. The flaws detected in WEP have been fixed with the ratification of the IEEE 802.11i standard, and the rollout of WPA and WPA2. However, a combination of security measures is required to further increase the security offered by WLAN technologies as explained in section 4.4.
4. Security risk assessment is necessary so as to produce a list of threats a network is prone to and the severity each has on the network. Base on this a good security policy is made to defend the network. It is not practical or possible to defend any network against all possible attacks. The goal, however, is to reduce associated risk to an acceptable level.
5. There exist a number of countermeasures to mitigate a network against a particular risk. Some of these countermeasures are simple, some are complicated. A combination of countermeasures, however, ensures that a network is robust and more secured against an attack.

It is essential that organisations put in place suitable protective measures for their wireless network. Though wireless group of standards IEEE 802.11 provide basic security, it is

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

not foolproof enough to give the level of protection required for organizations network infrastructure. Vulnerability assessment is necessary to determine the combination of measures that should be implemented to mitigate the risks associated with the use of wireless technologies.

REFERENCE

[1] W. Stallings, Wireless Communications and Networks. Pearson Education, India, 2006, pp 448-492. | [2] R. Pejman, & L.Jonathan, 802.11 Wireless LAN fundamentals: A Practical Guide to understanding, designing and operating 802.11WLANs. Cisco Press, Indiana,pp 21-34. | [3] C. Doru, 'Telecommunication System: Wireless Local Area Network', Blekinge Institute of Technology, Nov. 2005, pp 1-54 | [4] Y. Jui-Hung, C. Jyh-Cheng & L. Chi-Chen, 'WLAN Standards: In Particular, The IEEE 802.11 Family,' Potentials, IEEE, Vol. 22, Issue 4, Oct.-Nov. 2003, pp 16 –22. | [5] C. Jyh-Cheng, J. Ming-Chia, & L. Yi-wen, 'Wireless LAN security and IEEE 802.11i' Wireless Communications, IEEE, Vol. 12, Issue 1, Feb. 2005, pp 27 –36. | [6] K. Sankar, Cisco Wireless LAN Security: Expert Guidance for Securing Your 802.11 Networks, Cisco Press, Indianapolis, 2004, pp 125-155. | [7] J.Koziol, Intrusion Detection with Snort, Sams Publishing, Indianapolis, 2003. | [8] E. Sithirasenan, S. Zafar, & V. Muthukkumarasamy, 'Formal Verification of the IEEE 802.11i WLAN Security Protocol', J. IEEE Computer Society, Issue 18-21, April 2006, pp 181-190. | [9] D. Welch, & S. Lathrop, 'Wireless Security Threat Taxonomy', J. IEEE Systems, Issue 18-20, June 2003, pp 76 – 83.