WIRELESS LAN SECURITY ATTACKS AND CCM PROTOCOL WITH SOME BEST PRACTICES IN DEPLOYMENT OF SERVICES

Abhijit Bodhe
Asst.Prof.SRES COE,
Kopargaon .

Mayur Masuti
Asst.Prof.SRES COE,
Kopargaon.

Dr. A.S.Umesh
Reseaech Guide,
VTU, Karnataka

---***---

Abstract- ***Wireless local area Networks (WLANs) are unit cost effective and fascinating gateways to mobile computing which allows computers or laptops to be mobile and cable less including communicate with speeds near the speeds of wired LANs. These options came with high-ticket worth to pay in areas of security of the network. This paper identifies and summarizes these security considerations and their solutions, the paper overviews each physical and logical WLANs security issues followed by a review of the most technologies would not to overcome those. The paper also addresses logical security attacks like man in- the-middle attack(MIM) and Denial of Service(DoS) attacks furthermore as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the primary logical answer to secure WLANs. However, WEP suffered several issues that were partly resolved by IEEE802.1x protocols. Towards perfection in securing our personal WLANs, IEEE802.11i emerged as a replacement waterproof layer normal that for good fixes most of the safety issues found in WEP and alternative temporary WLANs security solutions. This paper discusses the safety threats and risks related to wireless networks. With some best practices in company readying for WLAN***

Key words:*WLAN, wireless LAN, security attacks, WEP, IEEE802.11i, CCMP.*

I. INTRODUCTION

A Wireless local area Network (WLAN) is a variety of native space network that uses high frequency radio waves instead of wires to speak between network-enabled devices. A wireless access purpose (AP) could be a hardware device that permits wireless communication devices, like PDAs and mobile computers, to attach to a wireless network. Usually, associate degree AP connects to a wired network, and provides a bridge for digital communication between wireless and wired devices. A Service Set symbol (SSID) could be a configurable identification that permits wireless purchasers to speak with associate degree applicable access purpose. With correct configuration, solely purchasers with correct SSID will communicate with the access points. In effect, SSID acts as one shared positive identification between access points and purchasers.

- Open System Authentication

Open System Authentication is that the default authentication protocol for the 802.11 commonplace. It consists of a straightforward authentication request containing the station ID associate degreed an authentication response containing success or failure information. Upon undefeated authentication, each stations square measure thought of reciprocally genuine . It is used with WEP (Wired Equivalent Privacy) protocol to supply higher communication security, but it's vital to notice that the authentication management frames square measure still sent in clear text throughout authentication method. WEP is employed just for encrypting information once the consumer is genuine and associated. Any consumer will send its station ID in an endeavor to go with the AP. In effect, no authentication is truly done.

- Shared Key Authentication

Shared Key Authentication could be a commonplace challenge and response mechanism that creates use of WEP and a shared secret key to supply authentication. Upon encrypting the challenge text with WEP mistreatment the shared secret key, the authenticating consumer can come the encrypted challenge text to the access purpose for verification. Authentication succeeds if the access purpose decrypts an equivalent challenge text. Infrastructure mode is another networking topology within the 802.11 commonplace, additionally to ad-hoc mode. It consists of variety of wireless stations and access points. The access points sometimes hook up with a bigger wired network. This topology will scale to create large-scale networks with arbitrary coverage and complexness.

- Wired Equivalent Privacy Protocol

Wired Equivalent Privacy (WEP) Protocol could be a basic security feature within the IEEE 802.11 commonplace, meant to supply confidentiality over a wireless network by encrypting data sent over the network. A key-scheduling flaw has been discovered in WEP, therefore it's currently thought of as unsecured as a result of a WEP key is cracked in an exceedingly jiffy with the help of machine-driven tools. Therefore, WEP shouldn't be used unless a safer methodology isn't on the market

- Wi-Fi Protected Access And Wi-Fi Protected Access two

Wi-Fi Protected Access (WPA) could be a wireless security protocol designed to deal with and fix the this protocol to enhance user authentication. Wi-Fi Protected Access two (WPA2), supported IEEE 802.11i, could be a new wireless security protocol within which solely approved users will access a wireless device, with options supporting stronger cryptography (e.g. Advanced cryptography commonplace or AES), stronger authentication management (e.g. protractible Authentication Protocol or EAP), key management, replay attack protection and information integrity.

In July 2010, a security trafficker claimed they found vulnerability on WPA2 protocol, named "Hole 196". By exploiting the vulnerability, an enclosed genuine Wi-Fi user will rewrite non-public information of others and inject malicious traffic into the wireless network. once investigation1, such attack cannot truly recover, break or crack any WPA2 cryptography keys (AES or TKIP). Attackers will solely masquerade as AP and launch a man-in-the-middle attack once purchasers hooked up to them. Moreover, such attack wouldn't be succeeded in an exceedingly correct organized atmosphere. If consumer isolation feature is enabled in access points, wireless purchasers aren't allowed to speak with one another once they square measure attaching to an equivalent access purpose. during this affiliation, assaulter is unable to launch man-in-the-middle attack to different wireless users.

TKIP was designed to use with WPA whereas the stronger rule AES was designed to use with WPA2. Some devices might enable WPA to figure with AES whereas some others might enable WPA2 to figure with TKIP. however since Gregorian calendar month 2008, vulnerability in TKIP was uncovered wherever assaulter could also be able to rewrite tiny packets and inject arbitrary information into wireless network. Thus, TKIP cryptography isn't any longer thought of as a secure implementation. New deployments ought to think about using the stronger combination of WPA2 with AES cryptography.

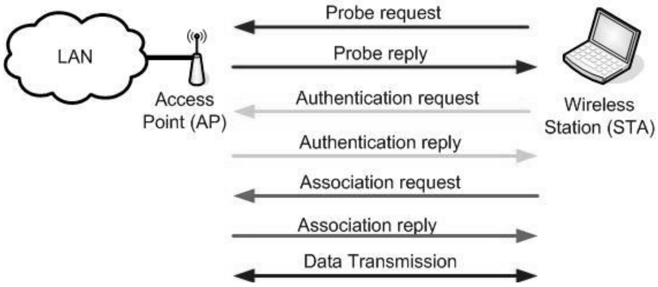


Fig. The three phases undergone through WLAN for the establishment of connections between STAs and AP.

familiar security problems in WEP. WPA provides users with a better level of assurance that their information can stay protected by mistreatment Temporal Key Integrity Protocol (TKIP) for encryption. 802.1 x authentications has been introduced during

These square measure searching, authentication and association Wireless native space Networks (WLANs) succeeded in providing wireless network access at acceptable knowledge rates. The Institute of Electrical and physics Engineering (IEEE) have set standards and specifications for knowledge communications in wireless setting, IEEE802.11i is that the driving technology customary for

WLANs [1]. WLANs square measure deployed as associate extension to the present fixed/wired LANs and attributable to the very fact that the character of WLANs square measure totally different from their wired counterparts, it's vital to boost the protection of WLANs to levels nearer or up to the wired LANs. normally IEEE802.11i will operate in 2 topology modes, impromptu and Infrastructure modes. This paper discusses WLANs in infrastructure mode. within the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access purpose (AP) that is connected to the wired network, this setup forms a LAN. The institution of connections

between STAs and AP goes through 3 phases; searching, authentication and association [1]. In searching section, the STA will either listen passively to AP signals associated mechanically tries to affix the AP or will actively request to affix an AP. Next is that the authentication section,

the STA here is echt by the AP victimisation some authentication mechanisms delineated later. once with success authenticating, the STA can send associate association request to the AP, once approved, the AP adds the STA to its table of associated wireless devices. The AP will associate several STAs however associate STA are often associated to at least one AP solely at a time. Figure one shows the 3 phases in WLANs

II. SECURITY ATTACKS AND RISKS

There square measure several security threats and attacks that may harm the protection of WLANs. Those attacks are often classified into logical attacks and physical attacks followed by general attacks.

- **LOGICAL ATTACKS**

1. Attacks on WEP

Wired Equivalent Privacy (WEP) may be a security protocol supported encoding algorithmic program known as "RC4" that aims to produce security to the LAN kind of like the protection provided within the wired computer network [2]. WEP has several drawbacks just like the usage of little initialisation Vector (IV) and short

RC4 encoding key further as victimisation XOR operation to cipher the key with the plain text to get cipher text. causing the mack addresses and also the IV within the clear additionally to the frequent use of one IV and also the indisputable fact that secret keys are literally shared between communications parties square measure WEPs major security issues

2. mack Address Spoofing

info of legitimate wireless stations and their mack addresses. The wrongdoer will simply spoof the mack address of a legitimate wireless station and use that mack address to achieve access to the LAN. Stealing STAs with mack addresses licensed by the AP is additionally potential. this will cause a serious security violation. The network security administrator has got to be notified of any purloined or lost STA to get rid of it from the list of STAs allowed to access the AP thence the LAN.

3. Denial of Service attack

Denial of Service attacks or DoS may be a serious threat on each wired and wireless networks. This attack aims to disable the provision of the network and also the services it provides [5]. In WLANs, DoS is conducted in many ways that like intrusive the frequency spectrum by external RF sources thence denying access to the LAN or, in best cases, granting access with lower knowledge rates [3]. in a different way is causing unsuccessful association messages to AP and overloads the AP with connections until it collapses that, as a result, can deny alternative STAs from associating with the AP.

4. Man-in-the-middle attack

This is a illustrious attack in each wired and wireless networks. a bootleg STA intercepts the communication between legitimate STAs and also the AP. The contraband STA fools the AP and pretends to be a legitimate STA; on the opposite hand, it additionally fools the opposite finish STA and pretends to be sure AP. victimisation techniques like IEEE802.1x to attain mutual authentications between APs associated STAs further as adopting an intelligent wireless Intrusion Detection System will facilitate in preventing such attacks.

5. dangerous network style

WLANs operate as associate extension to the wired computer network thence the protection of the computer network depends extremely on the protection of the LAN. The vulnerability of WLANs means the wired computer network is directly on risk.

6. Default AP configurations

Most APs square measure shipped with minimum or no security configuration by default. this is often true as a result of shipping them with all safety features enabled can build usage and operation tough for traditional users. The aim of AP suppliers is to deliver high rate, out of the box MAC addresses square measure sent within the clear once a communication between STAs and AP takes place. some way to secure access to APs and thence to the network is to filter accesses supported mack addresses of the STAs making an attempt to access the network [7]. Since mack addresses square measure sent within the clear, associate wrongdoer will acquire the mack address of licensed station by sniffing airwaves victimisation tools like ethereal [12] or fate [11] to get a installation APs with- out sincere commitment to security. Network security directors ought to put together these AP in keeping with the organizations security policy [8]. a number of the default unsecured setting in APs shipped nowadays square measure default passwords that happens to be weak or blank

PHYSICAL ATTACKS

1. Rouge Access Points (RAP)

In traditional things, AP authenticates STAs to grant access to the LAN. The AP isn't asked for authentication, this raises a security concern, what if the AP is put in while not IT center's awareness? These APs square measure known as "Rogue APs" and that they type a security hole within the network [8]. associate wrongdoer will install a rascal AP with safety features disabled inflicting a mass security threat. there's a desire for mutual authentication between STAs and APs to confirm that each parties square measure legitimate. Technologies like IEEE802.1x are often wont to overcome this drawback [7]. Network security directors will discover rascal APs by victimisation wireless analyzing tools to look and audit the network.

2. Physical placement of AP

The installation location of APs is another security issue as a result of inserting APs not suitably can expose it to physical attacks. Attackers will simply reset the APs once found inflicting the AP to modify to its default settings that is completely insecure. it's important for network Security directors to fastidiously select applicable places to mount APs

GENERAL ATTACKS

Low readying prices build wireless networks engaging to users. However, the simple convenience of cheap instrumentation additionally provides attackers the tools to launch attacks on the network. the planning flaws within the security mechanisms of the 802.11 customary additionally bring about to variety of potential attacks, each passive and active. These attacks alter intruders to pay attention to, or tamper with, wireless transmissions

1.Parking Lot Attack

Access points emit radio signals in a very circular pattern, and also the signals nearly always extend on the far side the physical boundaries of the realm they will cowl. Signals are often intercepted outside buildings, or perhaps through the floors in multi-storey buildings. As a result, attackers will implement a "parking lot" attack, wherever they really sit within the organisation's parking zone and take a look at to access internal hosts via the wireless network.

2.Shared Key Authentication Flaw

Shared key authentication will simply be exploited through a passive attack by eavesdropping on each the challenge and also the response between the access purpose and also the authenticating consumer. Such associate attack is feasible as a result of the wrongdoer will capture each the plaintext (the challenge) and also the ciphertext (the response).

3.Service Set symbol Flaw

Access points go with default SSIDs. If the default SSID isn't modified, it's relatively attract additional attacks from attackers since these units square measure thought to be poorly designed devices. Besides, SSIDs square measure embedded in management frames that may be broadcasted in clear text regardless access purpose is IEEE802.11 defines 2 styles of authentication ways accustomed access WLANs, open-system and shared key [1]. within the open-system methodology all communications between the STA and also the AP square measure within the clear (i.e. visible and not hidden). during this methodology it doesn't matter if the WEP keys (section three.3) accustomed access the wlan wireless local square measure a network WLAN WiFi local area network are correct, the AP can permit accessing the wlan wireless local square measure a network WLAN wireless fidelity WiFi local area network notwithstanding the keys used are invalid, the sole demand here is that the network SSID (section three.2). However, APs broadcast their SSID by default thus exploitation open-system authentication is completely insecure. within the shared key methodology, the AP sends a challenge text to the STA; this challenge is encrypted by WEP keys then it's came back back to the AP to either grant access to the WLAN or not.

2.Service Set symbol (SSID)

SSID could be a network symbol range broadcasted by APs [4]. while not knowing the SSID range, STAs cannot access the network. This looks fine however the matter with SSID is that it's really broadcasted by the AP. Unauthorized stations will capture the SSID of a WLAN and use it to achieve access. it's helpful to prevent SSID broadcast, this suggests that wireless stations have to be compelled to actively look for the SSID correspondent to the WLAN they need to access to. it's conjointly counseled to vary the worth of the SSID oft however that may overload network directors if several APs exist during a WLAN with the absence of central management theme to regulate all of them directly. SSID isn't a really economical access management technique; but, it's one hurdle that might be tuned to form it tough for non-skilled attackers to access the WLAN.

3.Wired Equivalent Privacy (WEP)

designed to disable SSID broadcasting or enabled encoding. By conducting analysis on the captured network traffic from the air, wrongdoer is in a position to get the network SSID and performs additional attacks.

III. WLAN SECURITY TECHNOLOGIES

There square measure many security technologies introduced to unravel the authentication drawback and to preserve the privacy and integrity of knowledge transmitted on air. IEEE802.11 fixed 3 basic security technologies to evidence access to the WLAN and to preserve the privacy of knowledge transmitted, they're open system authentication, shared key authentication and WEP [1]. owing to the disadvantage of security technologies in IEEE802.11, Wi-Fi Alliance free a brand new security commonplace for the trade known as "Wi-Fi Protected Access" (WPA)

1. Authentication techniques

WEP is that the security protocol in use since the first IEEE802.11 commonplace [1]. it's accustomed secure communications between APs and STAs and to produce secured authentication schemes; the aim was to produce security to the WLAN kind of like the protection provided within the wired LAN. it's supported a stream cipher coding rule known as "RC4". WEP is employed to regulate access to the WLAN and to write in code hint. it had been tried in theory and much that WEP failing as a security protocol owing to several issues.

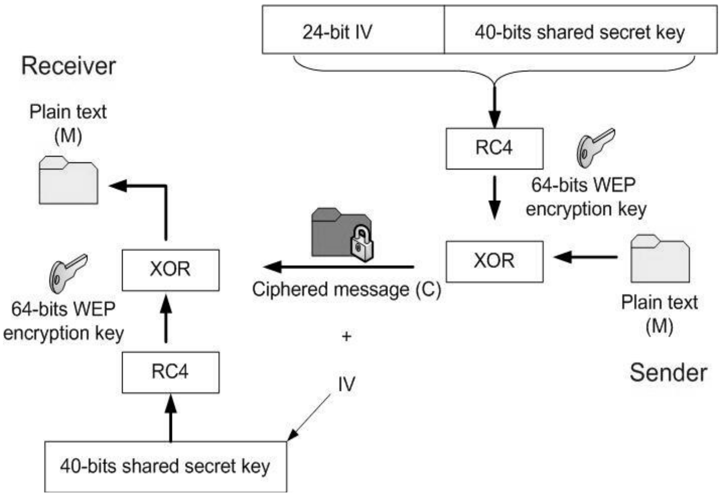

24-bit IV
40-bits shared secret key
Receiver
Plain text (M)
RC4
64-bits WEP encryption key
XOR
XOR
Ciphered message (C)
Plain text (M)
64-bits WEP encryption key
+
RC4
IV
Sender
40-bits shared secret key

Fig. Schematics of the Wired Equivalent Privacy (WEP) protocol used to control access to the WLAN and to encrypt confidential information**.**

III. LAN SECURITY TECHNOLOGIES

There unit several security technologies introduced to unravel the authentication downside and to preserve the privacy and integrity of data transmitted on air. IEEE802.11 fastened three basic security technologies to proof access to the LAN and to preserve the privacy of data transmitted, they are open system authentication, shared key authentication and WEP [1]. attributable to the disadvantage of security technologies in IEEE802.11, Wi-Fi Alliance free a novel security commonplace for the trade called "Wi-Fi Protected Access" (WPA)

1. Authentication techniques

IEEE802.11 defines a pair of forms of authentication ways in which accustomed access WLANs, open-system and shared key [1]. inside the open-system methodology all communications between the STA and conjointly the AP unit inside the clear (i.e. visible and not hidden). throughout this system it does not matter if the WEP keys (section 3.3) accustomed access the wireless {local sq. measurea network|WLAN|wireless fidelity|WiFi|local space network|LAN} ar correct, the AP will allow accessing the wireless {local sq. measurea network|WLAN|wireless fidelity|WiFi|local space network|LAN} however the keys used ar invalid, the only demand here is that the network SSID (section 3.2). However, APs broadcast their SSID by default therefore exploitation open-system authentication is totally insecure. inside the shared key methodology, the AP

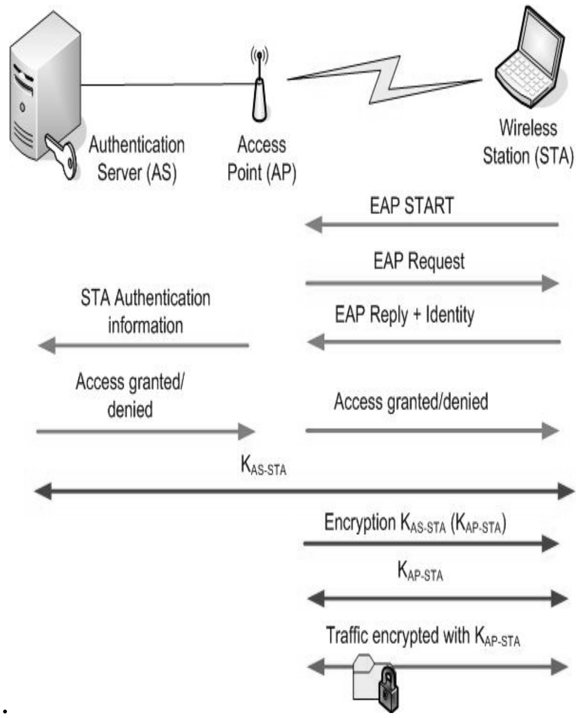
3.Wired Equivalent Privacy (WEP)

WEP is that the protection protocol in use since the primary IEEE802.11 commonplace [1]. it's accustomed secure communications between APs and STAs and to supply secured authentication schemes; the aim was to supply security to the LAN reasonably just like the protection provided inside the wired computer network. it's supported a stream cipher writing rule called "RC4". WEP is utilized to manage access to the LAN and to put in writing in code hint. it had been tried in theory and far that WEP failing as a security protocol attributable to many problems

sends a challenge text to the STA; this challenge is encrypted by WEP keys then it's came back back to the AP to either grant access to the LAN or not.

2.Service Set image (SSID)

SSID can be a network image vary broadcasted by APs [4]. whereas not knowing the SSID vary, STAs cannot access the network. This appearance fine but the matter with SSID is that it's extremely broadcasted by the AP. Unauthorized stations can capture the SSID of a LAN and use it to realize access. it's useful to stop SSID broadcast, this implies that wireless stations have to be compelled to be compelled to actively seek for the SSID correspondent to the LAN they have to access to. it's put together endorsed to vary the price of the SSID oftentimes but that will overload network administrators if many APs exist throughout a LAN with the absence of central management theme to manage all of them directly. SSID is not a extremely economical access management technique; however, it's one hurdle that may be tuned to make it powerful for non-skilled attackers to access the LAN.



.
Fig. Illustration of IEEE802.1x network access control for efficient key exchange mechanism between clients and servers in wired and wireless LANs.

V. IEEE802.11i

To solve the roots of the issues in WEP and TKIP, IEEE nominative a brand new normal that has increased security moreover as support to bequest protocols for backward compatibility. IEEE802.11i [3] is predicated on IEEE802.11 with security sweetening within the mack layer; it had been approved in Gregorian calendar month 2004. IEEE802.11i elevates the extent of security shipped with local area network merchandise like APs and wireless network interface cards. a particular task cluster within the IEEE referred to as "Task cluster I (TGi)" developed and still change this normal, the cluster tried to specify a regular that may bring home the bacon most significant security goals, authentication, confidentiality and integrity.

- CBC-MAC Protocol (CCMP)

IEEE802.11i mandates the employment of a protocol to guard confidentiality and integrity of information transferred, named Counter mode with CBC-MAC Protocol (CCMP). CCMP provides confidentiality and integrity of the information transferred and credibleness of the sender. it's supported the Advanced secret writing normal (AES) block cipher. AES is that the most reliable block cipher thus far, it uses a minimum of 128-bit key length and text blocks of 128- bits moreover [4]. this can be a good advancement over ancient WEP protocol that is predicated on weak RC4 stream cipher. CCMP consists of 2 vital protocols, Counter Mode AES secret writing (CTR-AES) and Cipher Block Chaining – Massage Authentication Code (CBC-MAC) supported AES. CTR-AES encrypts knowledge transferred (i.e. achieves confidentiality) and CBCMAC provides integrity of information and authentication of the sender by hard the Message Integrity Code (MIC) of the message shows MIC is calculated exploitation CBC-MAC supported AES block cipher.

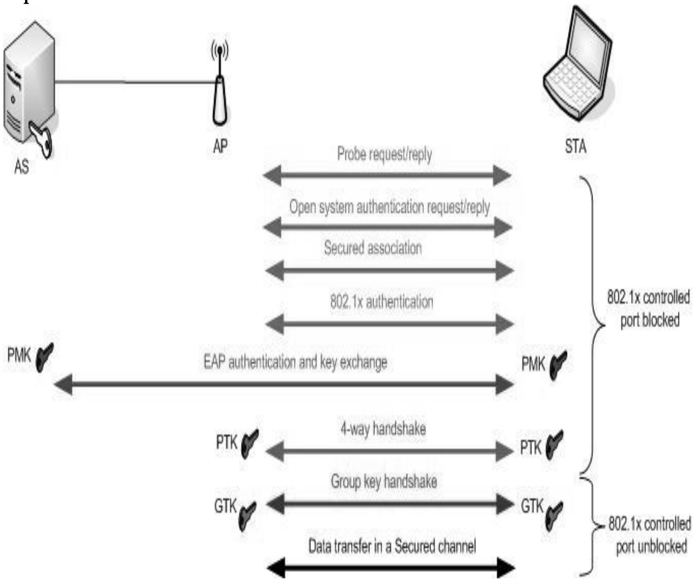

AS
AP
STA
Probe request/reply
Open system authentication request/reply
Secured association
802.1x authentication
802.1x controlled port blocked
PMK
EAP authentication and key exchange
PMK
PTK
4-way handshake
PTK
GTK
Group key handshake
GTK
Data transfer in a Secured channel
802.1x controlled port unblocked

Fig. Key management structure in IEEE802.11i protocol.

VI. BEST PRACTICES IN company readying FOR local area network

1. Define a Wireless Security Policy

The organization ought to develop a robust wireless security policy to deal with all the usage choices of wireless networks and therefore the styles of info that may be transmitted. The policy ought to define a framework for the event of installation, protection, management and usage procedures. Security and operation pointers, standards and personnel roles ought to even be clearly outlined.

2. Keep Track of Development for Wi-Fi Standards

Since the 802.11 customary was initial introduced, enhancements have incessantly been created to strengthen knowledge rates, signal vary, and security of wireless networks. Therefore, it's an honest plan to stay track of the event of recent standards as they seem, particularly once procuring new instrumentation or deed new wireless network services.

3.Perform web site Surveys

Due to the character of frequency (RF) propagation, radio radiation emissions cannot usually be contained among a selected building or location. Excessive coverage by the wireless signal may cause important threat to the organisation, gap it to automobile parking space attacks on the network.

4.Apply a Defence-in-Depth Approach
The conception of "defence-in-depth" has been wide used within the secure style of wired networks. an equivalent conception can even be applied to wireless networks. By implementing multiple layers of security, the chance of intrusion via a wireless network is greatly reduced. If associate degree assaulter breaches one live, extra measures and layers of security stay in situ to guard the network.

5.Separate Wireless Networks from Wired Networks
Due to the character of wireless technology, wireless networks area unit comparatively exhausting to contain among a building associate degreed it's usually thought of to be an un-trusted network. As a best observe, wireless networks and wired networks shouldn't be directly connected to every different. it's common to deploy firewalls to separate and management the traffic between totally different networks.

6.Implement sturdy Physical Security Controls
The loss or thieving of network instrumentation could cause a major threat to a wireless network as a result of configuration of the network will be retrieved from a lost access purpose or wireless interface card. By firmly mounting network instrumentation, like access points, in less accessible locations at the side of sturdy physical security controls, the chance of thieving will be minimised.

7.Avoid Excessive Coverage of Wireless Networks
Using the data collected throughout the location survey, correct placement of access points will be designed to avoid excessive coverage by the wireless network and thence limit the chance of intrusion. additionally to correct placement of the access points, adjusting the frequency (RF) power transmission or mistreatment directional antennas can even management the propagation of the RF signal and thence management coverage of a wireless network

8.Secure Access Points
Access points area unit the core of a wireless network. Their security clearly has associate degree overall result on the protection of the wireless network. Properly securing access points is that the initiative in protective a wireless network.

9.Keep Security Patches Up-to-date
Newly discovered security vulnerabilities in vender merchandise ought to be patched to forestall accidental and malicious exploits. Patches ought to even be tested before readying therefore on guarantee they work properly.

10.Educate Users concerning the Risks of Wireless Technology
User awareness is often a important success consider effective info security. an honest policy isn't enough. it's conjointly vital to coach all users in following the policy. Best practices or security pointers ought to be developed that end-users perceive and cling to.

11.Review Audit Logs often
Regular checking of log records should be performed, to make sure the completeness and integrity of all logs. Any irregularities noticed should be reportable and a close investigation ought to be dole out if necessary.

CONCLUSION

IEEE802.11i was ab initio designed to interconnect wireless devices to wired networks; the aim was to attain networking with minimum or no security. Security wasn't a very important issue at that stage, however, with the winning of WLANs and therefore the quick adoption of this technology, security became vital and achieving security became a primary concern. Wired Equivalent Privacy (WEP) security protocols was the primary to be adopted in a trial to satisfy the necessity for securing wireless networks, shortly WEP became vulnerable and there was a requirement for an improved security protocol. Industries already invested with in wireless devices therefore any new protocol ought to contemplate the hardware capabilities of such devices

REFERENCES

[1] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) andPhysical Layer Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[3] Wang Shunman, TaoRan, WmgYue and ZhangJi, "Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.

[4] Matthew S. Gast, 802.11 Wireless Networks, O'REILLY, 2002.

[5] William Stallings, Cryptography and Network Security, Principles and Practices, 3rd Edition, Prentice Hall 2003.

[6] Matija Sorman, Tomislav Kovac and Damir Maurovic, "Implementing Improved WLAN security", 46th International Symposium Electronics in Marine. ELMAR-2004, Zadar. Croatia, 16-18 June 2004.

[7] Joon S.Park and Derrick Dicoi, "WLAN Security: Current and Future". IEEE Computer Society, October 2003

[8] AirSnort Software, http://airsnort.shmoo.com

[9] Ethereal Software, http://www.ethereal.com

[10] KISMET Software, http://www.kismetwireless.net

[11] Brown, B. "802.11: the security differences between b and I", IEEE Potentials, October/November 2003.

[12] Joel W. Branch, Nick L.Petroni JR, Leendert Van Doorn and David Safford, "Autonomic 802.11 Wireless LAN

Security Auditing". IEEE Security & Privacy, 2004.
[13] War driving website, http://www.wardriving.com/
[14] NetStumbler Software, http://www.netstumbler.com
[15] Cisco Systems. "Wireless LAN Security". February 2001, (online) [Available: http://mithras.itworld.com/WhitePapers/Cisco/WLAN_WP_BW7012.pdf].
[16] WEPCRACK, Software, http://www.sourceforge.net/projects/wepcrack .