Security in Wireless LAN

Rajendra Kumar Sharma[1]
Sr. Tech. Asst. (CS)
Vivekananda Institute of Technology
Jaipur, India

Akash Jaiman[2]
Assistant Professor (ECE)
Vivekananda Institute of Technology
Jaipur, India

***Abstract*:-Wireless LAN (WLAN) has been widely used in many fields.The WLAN securityis necessary because WLANtransmission has no physical boundary, and is prone to unlawful access over network resources, resulting in the penetrability of private, confidential and important data. Network operations and availability can also be negotiated in case of a WLAN security breech. To resolve these issues, encryption, various authentications, in-visibility and other administrative controlling methods are used in WLANs. Corporateand businessWLANs in particular require suitable security measures to detect, prevent and block greedybenefactors, eavesdroppers and other burglars.**

Keywords- Network, Throughput, Encryption,

INTRODUCTION

This section gives brief information on the WLAN components and its architecture in order to observe the WLAN security threats. A Wireless local area networks (WLANs) based on the Wi-Fi standards are one of today's fastest growing technologies in schools, businesses and homes, for good reasons. They offer mobile access to the Internet and to organizational networks so users can remain connected away from their desks. This type of networks can be start and running quickly when there is no available wired Ethernet infrastructure. These can be prepared to work makingminimum efforts without relying on specialized corporate installers. A WLAN is a flexible data communications system which can use either infrared or radio frequency technology to transmit and receive information over (WEP) that is supported in the IEEE 802.11 wireless LAN standards. WLANis a wireless distribution method for two or more than two devices which use high-frequency radio waves and often include an access point to the Internet. InWLAN users can move from place to placein the coverage area, often a home or small office, while maintaining a network connection. A WLAN is also calledLocal area wireless network (LAWN).

A WLAN is a communications system that uses either radio frequencyor infrared technology to transmitting as well as receiving information over the air. 802.11 were implemented as the 1st WLAN standard in 1997. It is based on radio technology operating on 2.4 GHz frequency and it has a maximum throughput of 1 Mbps to 2 Mbps. The presently most spread and deployed standard, IEEE 802.11b, was introduced late in 1999. It is also operates in the same frequency range, but its maximum speed is 11 Mbps. WLAN has been mostly used in many sectors ranging from corporate, manufacture,retail, education, healthcare,finance and warehousing.

It has progressively becoming a key technology to fulfill the needs for connection flexibility, mobility, reduced cost-of-ownership, and scalability.

WLAN SECURITY:-

Security has been animportant concern in WLANs around the world. While wireless networks provide flexibility and convenience, they also increase network vulnerability. Security threats such as unauthorized accessing, session hijacking, denial of service attacks, IP and MAC spoofing, and eavesdropping can all be problems for WLAN. To counter these threats, multiple standard authentication and encryption techniques are mixed with other access control mechanisms. These devices, protocols and techniques collectively secure the WLAN a level that equals and even better than wired LAN security.

The following table denotes some of the technologies which are employed in WLAN security:

Wireless security cheat sheet

Encryption standard	Fast facts	How it works?	Should you use it?
WIRED EQUIVALENT PRIVACY (WEP)	First 802.11 security standard; easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64-or 128-bit keys. Static master key must be manu-ally entered into each device.	No
WI-FI PROTECTED ACCESS (WPA)	An interim standard to address major WEP flaws. Back-wards compatible with WEP devices. It has two modes: personal and enterprise.	Retains use of RC4, but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authen-tication via 802.1x and EAP.	Only if WPA2 is not available
WPA2	Current standard. Newer hardware ensures advanced encryption doesn't affect performance. Also has personal and enterprise modes.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authen-tication and en-cryption.	Yes

WIRED EQUIVALENT PRIVACY (WEP):-

It is an old encryption standard used to overcome security threats. WEP provides security to WLAN by encrypting the data transmitted over the air so that only the receivers with the correct encryption key can decrypt the data. It is a data encryption and user authentication system from IEEE 802.11 used to overcome the security threats. Basically, WEP provides security to WLAN by encrypting the data transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the data. The further section explains the technical functionality of WEP as the core security protocol for WLAN.

WORKING OF WEP:-

When deploying WLAN, it is important to understand the ability of WEP to get better security. This section describes how WEP functions achieve the level of privacy as in a wired LAN. WEP uses a pre-established shared secret key known as the base key, the RC4 encryption algorithm and the CRC-32 (Cyclic Redundancy Code)algorithm as its basic building blocks. WEP supports up to four different base keys, identified by KeyIDs. Each of base keys is a group key called a default key, meaning that the base keys are shared among the associates of a specific wireless network. Some implementations also support a set of nameless per-link keys called key-mapping keys. However, it is less common in first generation products, because it implies the existence of a key management facility, which is not defined by WEP. The WEP specification does not permit the use of both key-mapping keys and default keys concurrently and most deployments share a single default key across all of the 802.11 devices. WEP tries to achieve security goal in a simple way. It operates on MAC Protocol Data Units (MPDUs), the 802.11 packet fragments. For protecting the data in an MPDU, WEP first computes anreliability check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP attaches the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to notice if data has been corrupted in flight or the packet is an outright forgery. Next, WEP picks a base key and an initialization vector (IV), that is a 24-bit value. WEP constructs a per-packet RC4 key by concatenate the IV value and the certain shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and KeyID identifying the selected key are encoded as a four-byte string and pre-pended to the encrypted data.

The IEEE 802.11 standard defines the WEP base key size as comprising of 40 bits, so the per-packet key consists of 64 bits when it is combined with the IV. Many in the 802.11 community once believed that small key size was a security problem, so some professionals modified their products to support a 104-bit base key as well. This difference in key length does not create any different in the overall security. An attacker can co-operate its privacy goals with comparable effort regardless of the used key size. This is due to the vulnerability of the WEP construction which will be discussed in the further section.

WI-FI PROTECTED ACCESS (WPA):-

WPA is a security standard for computing devices equipped for users with wireless internet connections, or Wi-Fi. It improved upon and replaced the original Wi-Fi security standard, WEP. WPA provides more complex data encryption than WEP, and it also provides user authentication - WEP's user authentication was considered insufficient.

Its encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP includes a perpacket mixing function, a message integrity check, an extended initialization vector and a re-keying mechanism. WPA offersrobust user authentication based on 802.1x and the Extensible Authentication Protocol (EAP). WPA depends on a central authentication server:like as RADIUS, to authenticate each user.

Software updates that allow both server and client computers to realize WPA became widely available during 2003. Access points can work in mixed WEP/WPA mode to support both WEP and WPA clients. However, mixed mode efficiently provides only WEP-level security for all users. Home users of access points that use only WPA can operate in a particular home mode in which the user needs only enter a password to be connected to the access point. The password will prompt authentication and TKIP encryption.

WPA2:-

WPA2 is the security standard that old-fashioned it in 2004. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It is based on the compulsory Advanced Encryption Standard algorithm, which provides message authenticity and integrity verification, and it is stronger and more reliable than the original TKIP protocol for WPA.

WPA2 still has vulnerabilities;most important among those is unauthorized access to the enterprise wireless network, where there is anraid of attack vector of certain Wi-Fi Protected Setup (WPS) access points. This can take the invader several hours of intensive effort with state-of-the-art computer technology, but the threat of system compromise should not be discounted. It is suggested that WPS be disabled for each attack vector access point in WPA2 to deject such threats.

CONCLUSION

When implementing wireless technologies for a secure network, some key points need to be taken into concern. Some risks are involved in contribution in wireless connections in your organization. This paper covered the various WLAN structures and how WLANs work. The SAFE WLAN design techniques can be used to respond to the risks of open wireless.

REFERENCES

1. Cisco website www.cisco.com
2. Dlink website www.dlink-india.com
3. www.docsslide.us
4. www.sans.org
5. www.ijsret.org
6. www.assignmentpoint.com