ABSTRACT

Wireless Local Area Networks (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. The protocol standard for WLAN is IEEE 802.11.

The 802.11 standard has several methods of encryption and authentication that provide varying levels of security for wireless networks. Due to the rapid growth of wireless networking, the fallible security issues of the 802.11 standard have come under close scrutiny. There are serious security issues that need to be sorted out before everyone is willing to transmit valuable corporate information on a wireless network.

This research focuses on inherent flaws in Wired Equivalent Privacy protocol (WEP) used by the 802.11 standard, Temporal Key Integrity Protocol (TKIP) which is considered an interim solution to legacy 802.11 equipment.

Many organizations choose not to change WEP keys regularly, which provides attackers with the opportunity to capture enough data to compute the WEP key and use it to gain unauthorized access to data or perform other attacks such as eavesdropping, replay, and message modification. Passive eavesdropping on legacy IEEE 802.11 WLAN communications may cause significant risk to an organization. An adversary can capture data traversing the wireless medium. Sensitive information, including proprietary information, network IDs and passwords, and configuration data, are some examples of data that may be captured. In addition, attackers with high-gain
antennas can capture data from wireless networks beyond a network’s normal operating range, again making confidentiality a critical security measure.

The Key management is probably the most critical aspect of any wireless network. Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing and destroying the key material is left to those deploying WLAN. There are many vulnerabilities available in WLAN environment because the key management was not part of the original 802.11 specification.

Key management for 802.11 is not considered as part of network specification. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys. The flaws in WEP data encryption might have been ameliorated if static WEP has included a method to automatically update the encryption keys regularly.

Temporal Key Integrity Protocol (TKIP) is developed to address the vulnerabilities associated with WEP and developed to provide backwards compatibility with WEP to prevent the need to replace all hardware that only supported WEP. TKIP supports a re keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. It creates a new key for each packet significantly reducing the possibility of guessing a key.

The physical layer is the first layer in the ISO/OSI reference model. It consists of two sub-layers, called Physical Layer Convergence
Procedure/Protocol (PLCP) and Physical Medium Dependent (PMD), respectively. The Physical Layer (PHY) layer is responsible for the actual Radio Frequency (RF) transmission and defines the frequencies and the modulation methods used. The PHYs provide multiple transmission rates by employing different modulation and channel coding schemes. The PHYs have multiple data transfer rate capabilities that allow implementations to perform dynamic rate switching with the objective of improving performance.

This research’s main objective is to enhance key mixing mechanisms in TKIP through transmission rate from Physical Layer Convergence Protocol to generate various pattern of key streams in order to avoid key reuse which is vital security flaw amongst various security flaws.

This research reveals an enhanced re keying mechanisms, to provide fresh encryption keys, undoing the threat of attacks stemming from key reuse and shows enhanced pattern of key streams generated from TKIP during the time of encryption and decryption of payload.

The new per-packet key construction, TKIP key mixing function, substitutes the Signal Rate value from PLCP frame for the WEP base key and constructs per-packet key to generate dynamic key streams for each transmission. Every mobile station will generate different set of per-packet encryption keys which eliminate key reuse problems in WEP. This mechanism breaks one-to-one relation between TKIP per-packet encryption keys and WEP initial vector (IV) and it can be completely implemented on software to save the investment done in hardware.
This research also suggests enhancement to nonce of Cipher Block Chaining – Message Authentication Code (CCMP) because the nonce is constructed from the Packet Number (PN), Media Access Control (MAC) layer, Address field (A2) and MAC layer priority field. The reconstruction of nonce is possible by an adversary.