CHAPTER 6

CONCLUSION

Passive eavesdropping on legacy IEEE 802.11 WLAN communications may cause significant risk to an organization. Since key management was not part of the original 802.11 specification. Key management for 802.11 is left largely as an exercise for the users of the 802.11 network. 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 (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original 802.11 specification, with the key distribution unresolved, WEP-secured WLANs do not scale well. If an enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment.

The reuse of a single key by many users also helps make the attacks more practical, since it increases chances of IV collision. The chance of random collisions increases proportionally to the number of users; even worse, PCMCIA cards that reset the IV to 0 each time they are reinitialized will all reuse keystreams. Also, the fact that many users share the same key means that it is difficult to replace compromised key material. Since changing a key requires every single user to reconfigure their wireless network drivers, such updates will be infrequent.
The 802.11 devices are comprised of hardware and software, like most modern communication equipment. WLAN hardware has been designed as a commodity, so it is cost effective to add or swap out particular hardware chips in a WLAN device. Millions of WEP-based devices, however, have already shipped and deployed. It is also not cheaper to replace the hardware as an entire unit. This implies that WEP patches operating on already-deployed 802.11 hardware will, of necessity, rely entirely on software upgrade.

TKIP is developed to provide backwards compatibility with WEP to prevent the need to replace all hardware that only supported WEP. TKIP supports re keying mechanism and per-packet key mixing function. This research work enhances TKIP key mixing mechanisms to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse in TKIP through transmission rate to generate various pattern of key streams. In order to make a stream cipher more difficult to crack, this methodology uses transmission rate from PLCP as crypto key which varies in time. This would help to avoid any discernible patterns in the resulting ciphertext.

In fact, by randomly changing the crypto key used on each bit of data, one can produce ciphertext that is mathematically impossible to crack. This is because using different random keys would not generate any repeating patterns. Due to Key value differences, every station will generate different set of WEP per packet encryption keys which eliminates key reuse problem in WEP. Once the base WEP key is changed, new IV/base WEP key pairs are used, and unique packet keys will be generated. The mechanism breaks any one to one relation between TKIP per-packet encryption keys and WEP IV, and the mechanism can
be completely implemented on software to save the investment done in hardware.

For every frame, the TKIP algorithm is initialized with the key value prior to the start of the pseudorandom key stream generation. But if the keys were to remain fixed, the algorithm would be initialized to the same state every time. Therefore the key stream produced would be the same sequence of bytes for every frame. This is disastrous because, if the attacker can figure out the key stream. This research work reveals that new key streams are created by initializing PLCP signal field with S-boxes. The simulated system uses key update mechanism using special re-key enhancement from PLCP signal bit rates which forces the encryption mechanism to generate different key streams for every frame. This proposal is more suitable to existing legacy 802.11 equipments based on 802.11 b/g.

802.11i includes standard known as Advanced Encryption Standard –Counter Mode Cipher Block Chaining –Message Authentication Code (AES-CCMP)

AES-CCMP requires a hardware coprocessor to operate. Therefore, extra hardware is needed in the implementation of AES-CCMP. AES-CCMP will not work on many of the current shipping standard. TKIP is software-oriented whereas CCMP is hardware-oriented. CCMP is based on advanced encryption standard which requires new 802.11 hardware with great processing power.

This research work ensures that Encryption Key Stream is not repeated at any time, which means, the cipher text generated by this key
stream is never breakable which leads to maintain one of the security measures, confidentiality in WLAN. Passive attacks such as eavesdropping and traffic analysis can be avoided. Every mobile station uses the dynamic keys, amount of traffic may not be available to an eavesdropper for analytic attacks. Active attacks such as replay, message modifications, denial of service can also be avoided.