**Brief history**

Wireless security has been developing rapidly in the recent past. There has been constant increase and improvement of features associated with wireless security. Initially, wireless communication outlined two forms of authentication described by the 802.11 standards. These two forms were the open system association and shared key authentication. Actually, open system authentication was not authentication per se. it was just that open and free for all to access the network resources without any form of verification. Shared key, on the other hand, employed the use of WEP key. This was a shared key hat was used for all platforms connecting wireless networks across different networks. There are disadvantages associated with the use of shared key in authentication process. WEP allowed per packet master key reuse also allowing group use of same PSK and sharing of keys across APs. It lacked proper network authentication to clients and as such allowed vulnerabilities associated with confidentiality and integrity (Allen 142).

As the numerous vulnerabilities of WEP were exposed, there was need to improve the security of wireless networks. 802.11i group of standards were created by the IEEE to solve the problem. WPA was created which gave a transition towards creation of very well developed secure networks. WPA was just meant to curb the vulnerabilities of WEP. The same hardware that supported WEP was used in the development and implementation of WPA. In the mean time, stronger mechanisms were created to curb the security vulnerabilities (Allen 142). These mechanisms included Wi-Fi. A platform with interoperability between major vendors and developers was created. The groups that came together in the development of this platform were the alliances of Wi-Fi, TKIP and WPA. Temporal key integrity protocol was specified by WPA to support authentication. Other features were included in the WPA to enhance security these included:

**Increase in the secure key space by advancement of 8 bits which were aimed at excluding the weak keys**

PTKs were also implemented in order to increase effective key space for each session

There was a specification of IV rotation which was meant to prevent key re-use

There was also the advancement of non linear algorithm for integrity

A standard 802.1X was developed meant to be used for network authentication.

For now, the standard 802.1X is deemed the most secure protocol for use in the wireless security. It allows for effective key exchange as well as key rotation. 802.1X also employs a master key protection mechanism and AES encryption (Layton 211).

**Common concepts in wireless security**

The common concepts in wireless security currently are WEP, VPN, WPA and IDS.

WEP

WEP stands for the Wired Equivalent Protocol. It is the most widely used protocol in the wireless field. It actually was the first protocol established in the security of wireless networks sector. Though this method is widely used in the in wireless industry, it is prone to many problems. The first problem has to do with the fact that the system is based on alphanumeric keys. It becomes easier for a hacker to uncover private and public key by use of hacking methods such as dictionary or brute force approach. Another problem associated with these methods of authentication in wireless security is the length of the keys. The keys used are short in length hence giving a hacker easy time in guessing the possible combinations of the same. Moreover, the same keys are static. It means that the same do not change unless done so manually. Static keys are easier to guess or hack into; however, the server can change dynamic keys frequently. In static key approach offered by the WEP technology, an administrator has to change the keys of every device in each location.

**WAPs**

Wireless access points are radio devices, which have low frequency and can transmit over short distances. The distances covered by the broad cast could be as short as ten meters or a few blocks away. WAP cards can be used in PCs at home to connect to WAP cable modem, which is cheaply available. There is a disadvantage, however, associated with the WAP. Just like any radio device, the WAP is subject to interferences or attenuation. Buildings or walls can block or reduce the signal receive. Mountains and long distances also affect the same. High-tension electrical signals cannot be forgotten as another source of problem to WAP. The same can jam the signals.

WAP offers the potential of responding to the strongest radio frequency signal. The same, however, can be a disadvantage since any one can eavesdrop on someone’s WAP by just going or moving closer to it and setting its device to default. The most important advantage that WAP allows is the ability to implement dynamic WEP.

**Wireless VPNs**

VPN stands for Virtual Private Network. Wired VPNs are currently in use in the industry. The advantage that this private network offers is the improved security features. Data can be sent over ten networks by encapsulating them within a specified protocol and sending the same via a TCP/IP protocol (Dhillon 89). VPN offers a good secure platform for dial-up connections. VPNs are however complex to configure and are mostly affected by traffic networks. VPN provide an opportunity to clients working in hotspots to access company’s wireless LAN easily and securely.

**IDS (Wireless Intruder Detection Systems)**

Wireless Intruder Detection Systems are used to identify or detect intrusions in the system network. They are either sniffer devices or network software applications that analyze gathered data concerning the network in order to identify any potential threat to the system. This can be achieved by studying the expected patterns or methodology of a particular attack and as well identify abnormal network activity. Some IDSs are developed in a way that network rules and policy violations can be identified and reports generated for the administration to use (White 74). Traffic anomalies can also form the basis for anomaly detection in a wireless system by signature analysis. IDSs offer many advantages in the wireless systems therefore the need for its implementation. It is also able to detect spoofing and attack source by triangulating an attacker’s signal source. However, since IDS is new technology there is a worry that the same might affect the normal functioning of WLAN or reduce traffic.

**Future of wireless security**

There is ever increasing need for development of secure networks that cover long distances. From the development of the first protocols for wireless security, there has been rapid improvement in the field to increase the capacity of data that can be transmitted in the networks as well as increase the distance coverage. It is expected that in the future, at least every two years, the hardware capability of the wireless networks will be improving greatly. Software applications are also expected to be developed that will be able to monitor the networks effectively without the need for human intervention. The problems associated with attenuation of signals will be the thing of the past and there will be a variety of technologies to choose from, whichever one feels economical. The options would include Wi-Fi, WiMax, 3G cellular and many are some other new technologies that will come up.

**Threats to wireless security**

Just like any other system, wireless security is prone to threats. Threats can be caused by poor management of the system or intentional violations of the system functionality.

**Rogue access points**

This becomes a threat to the network if the same is not carefully managed. Unmanaged devices in the network provide easy backdoor and route of entry for attackers (Dhillon 301). This problem can be solved by ensuring strict policies and follow-ups on all the access points. An attacker can use WAPs to influence the wireless systems transmissions, which he can then monitor closely.

**Denial of service**

Denial of service is another threat to wireless networks. WAP suffer mostly from this because walls and obtrusive objects can block it. Attackers can also employ Radio frequency devices to jam network signals.

**Conclusion**

With the emergence of new devices and technologies, there is bound to be sophisticated wireless technologies. Every new technology will always have a fault in it and the developers of these technologies will always come up with better technologies. Overall, wireless technologies have simplified communications between devices getting rid of wired networking technologies. There is need to secure wireless networks to avoid unwarranted intrusion. They are the source of attacks to company networks. It is because of these that standards have been developed to ensure that the networks are set according to the standards.

Read more at: https://www.wowessays.com/free-samples/wireless-security-research-paper/