Wi-Fi Security Threats which can't be ignored.

1. **Data Interception:** In today's world data sent over Wi-Fi can be intercepted easily within few hundred feet's, and all Wi-Fi which are certified support AES CCMP data encryption. Unfortunately, there are still legacy products what use only TKIP and many are configured to accept both CCMP and TKIP, but TKIP is vulnerable to message integrity check (MIC) attack that allow a limited set of spoofed framework to be injected.

2. **Denial of Service:** Wi-Fi are vulnerable to DOS attack, almost everyone share unlicensed frequencies which make competition inevitable in populated areas, For an enterprise WLAN migrate to 802.11n, they can use channels in large less crowded 5 GHz which reduces the accidental DOS, Moreover contemporary AP (Access Point) can auto adjust channels to circumvent interference. That still leaves for the DOS attack. A phony message sent to the disconnected users, consume AP resources and keep the channel busy. To neutralize the attacks like DE authentication flood have the newer devices which support 802.11w management frame protection.

3. **Rogue APs:** A Rouge access point is an Access point installed on a wired enterprise network without authorization from the network administrator, A Rouge access point is installed by a legitimate user who is unware of its security implications or could be deliberately installed as an insider attack.

Most enterprise WIFI now use legitimate access point to scan channels for possible rogue AP's in the spare time. Unfortunately, verifying "true rogues" by tracing their wired network connectivity is a skill that ordinary WLAN gear has yet to perfect. Without accurate classification, automated rogue blocking is a risky proposition. To not only detect, but also effectively mitigate rogue Access point, deploy a