Summary of Wi-Fi Security Techniques

-Atharva Biwalkar(111508016)
-Yashashree Kolhe(111508041)
-Abhishek Kuvalekar(111508043)

Wireless technology provides us many benefits like portability and flexibility, increased productivity, and lower installation costs. Wi-Fi is the name of the popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connection. Wireless networks changed completely the way of sharing the information but still there are lot of challenges which are the hurdles in the wide adaptation of wireless network technology. This summary discusses about the wireless network challenges and the protocols like WEP and WPA/WPA2 which come under IEEE 802.11 standards.

The main problem that a Wi-Fi network faces is the security of the information which is shared through wireless communication. This security must provide following three important options:
Confidentiality (Encryption of messages), Integrity (Error detection), Authentication.

IEEE helped in securing the wireless networks by providing CIA factors through **SSID**, the use of **MAC address filtering**. Since, the networks using these security measures were vulnerable to attacks, **WEP**(Wired Equivalent Privacy) protocol was introduced with the introduction of IEEE 802.11 standard. Due to vulnerabilities of WEP to attacks, **WPA/WPA2** came into picture with IEEE 802.11g.

SSID: SSID is an acronym for Service Set Identifier. Each client under an Access Point needs to have same SSID. SSID works similar to that of password.

MAC Address Filtering: MAC (Media Access Control) address is unique for each client in a world. Access Point has a list of MAC addresses of client under its service set. SSID with MAC Address Filtering provides good security.

WEP: WEP was introduced in 1997 and was the first cryptographic protocol to enable privacy and authentication for Wi-Fi. WEP uses RC4 Stream Cipher Algorithm to encrypt wireless communication. The main problem of WEP was – it uses static encryption keys.

WPA/WPA2: WPA and WPA2 were developed with a purpose of solving problems in WEP cryptographic method. It was developed in 2003. They use cryptographic hash function for data integrity and provides key management and replay detection.

There are many protocols or standards for wireless network security but every protocol has its demerits, until now there is no protocol which can provide 100% security or near about it.