UNIVERSAL COLLEGE OF ENGINEERING,VASAI

WI-FI SECURITY

VEDANT VANKHEDE
JASH VEKARIYA

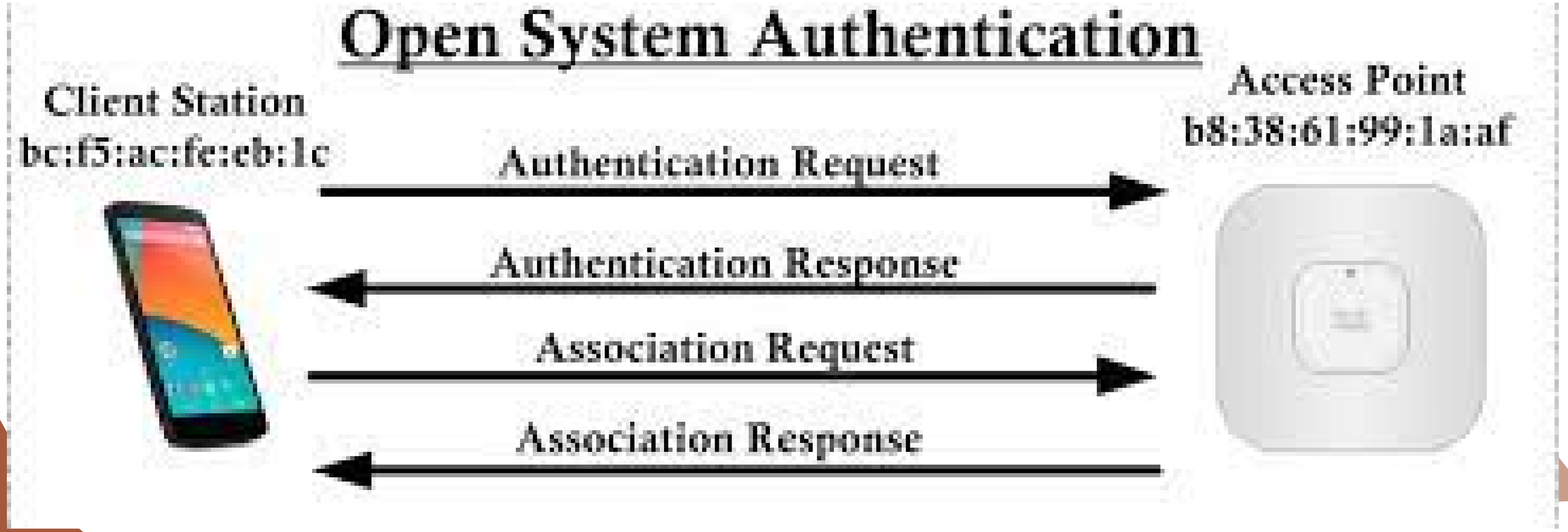
Introduction

- wireless networks transmit data over radio waves, it is easy to intercept data or "eavesdrop" on wireless data transmissions.
- Several Wi-Fi security algorithms have been developed since the inception of Wi-Fi.
- The wireless security protocols prevent unwanted parties from connecting to your wireless network and also encrypt your private data sent over the airwaves.

WEP-Wired Equivalent Privacy

- WEP is specified by IEEE 802.11 for encryption and authentication of Wi-Fi networks.
- It operates at physical and data link layer.
- The goal of WEP is to make wireless networks as secure as wired networks.
- WEP is having two main parts. Authentication and Encryption.

WEP Authentication



WPA-Wi-Fi Protected Access

- WPA stands for "Wi-Fi Protected Access".
- WPA was developed by the Wi-Fi Alliance to provide better user authentication than Wired Equivalent Privacy(WEP).
- One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically change keys as the system is used.

- WPA uses a solution called Michael, which is a Message Integrity Check (MIC), to the checksum being corrupted issue.
- WPA uses a 32 bit Integrity Check Value (ICV). This is inserted after payload and before IV.
- The MIC includes a frame counter, which helps to prevent replay attacks.
- It uses RC4 stream cipher with a 128 bit key and a 48 bit IV. the longer key and IV together defeat the key recovery attacks on WEP.

WPA supports two modes of operation.

1. Pre-Shared Key Mode or Personal Mode

- This mode is used for personal use. The preshared mode does not require authentication server. It utilizes a shared key that is communicated to both sides (AP and client) before establishing a wireless connection, this key is then used to secure the traffic.

2. Enterprise Mode

- Enterprise Mode requires an authentication server. It uses more stringent 802.1x authentication with the Extensible Authentication Protocol (EAP). It Uses RADIUS protocols for authentication and key distribution. In this mode, the user credentials are managed centrally.

	WEP	WPA
Release Year	1999	2003
Encryption Method	Rivest Clipher 4 (RC4)	Temporal Key Integrity Protocol(TKIP) with RC4
Session Key Size	40-bit	128-bit
Clipher Type	Stream	Stream
Data Integrity	CRC-32	Message Integrity Code
Key Management	Not provided	4-way handshaking mechanism
Authentication	WPE-Open WPE-Shared	Pre-Shared Key(PSK)& 802.1x with EAP variant

Thank You!

Do you have any questions for me before we go?