Wireless Security

Security is important in wireless network, because wireless signals are not contained within a wire, any device within the range of the signal can receive the traffic, in wired networks, traffic is only encrypted when sent over an untrusted network as the internet.
Authentication: only trusted devices should be given access to network, also clients should also authenticate the AP to avoid associating with a malicious AP, ways of authentication can be : password, username/password, certificates.
Encryption: all devices on the WLAN usually use the same protocol, however each client will use a unique key.
A group key is used by the Ap to encrypt traffic that it wants to send to all of its clients, all clients keep a copy of that key.
Integrity: to ensure that a message is not modified by a third party, by using MIC (Message Integrity Check): to help protect the messages integrity, if a calculated MIC value is different the message is discarded.

Open Authentication: the client sends an authentication request and AP accepts it, not secure, after the client is authenticated and associated with the AP, it's possible to require the user to authenticate via other methods before access to the network is granted (StarBuck's WiFi).
WEP (Wired Equivalent Privacy): WEP is used to provide authentication and encryption of wireless traffic, uses RC4 algorithm, a shared key protocol, key can be 40 bits or 104 bits in length combined with 24 bits initialization vector, not secure and can be easily cracked, the ap sends a challenge phrase to the client that encrypts it and sends it back to the AP.
EAP (Extensible Authentication Protocol): a framework that defines a set of authentication functions that are used by various EAP methods, integrated with 802.1x to provide port-based network access control.
802.1x is used to limit network access for clients connected to a LAN or a WLAN until they authenticate, has 3 main entities : supplicant → the device that wants to connect to the network , authenticator :AP or WLC that provides access to the network, the authentication server that receives the client credentials and permits/denies access (RADIUS server).
LEAP : Lightweight EAP: developed by Cisco as an improvement over WEP, clients must provide a username and password to authenticate, mutual authentication is provided by both client and server sending a challenge phrase to each other, dynamic WEP keys that are changed frequently are used, considered vulnerable.
EAP-FAST (EAP Flexible Authentication via Secure Tunneling): three phases → 1- a PAC (Protected Access Credential): is generated and passed from server to client, a secure TLS tunnel is established between client and authentication server, inside the secure TLS tunnel, the client and server communicate further to authenticate the client.
PEAP (Protected EAP): involves establishing a secure tunnel between the client and the server that has a digital certificate that the client uses to authenticate the server and establish a TLS tunnel, the client is authenticated within the secure tunnel for example using MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol).
EAP-TLS: requires a certificate on the AS and on every single client, the most secure method but more difficult to implement than PEAP, TLS tunnel is used to exchange encryption key information.

TKIP: (Temporal key Integrity Protocol): based on WEP, but adds: MIC to protect the integrity of messages, a key mixing algorithm to create a unique WEP for every frame, the initialization vector is doubled in length to harden brute force attacks, MIC includes the sender MAC address, a timestamp to prevent replay attacks, a TKIP sequence number to keep track of frames sent from each source MAC address and also protect against replay attacks, used in WPA 1.
CCMP (Counter/CBC-MAC Protocol): more secure, must be supported by the device's hardware, uses AES counter mode for encryption, CBC-MAC (Cipher Block Chaining Message Authentication Code) as a MIC to ensure the integrity of messages, used in WPA2.
GCMP (Galois/Counter Mode Protocol): more secure and efficient, increased efficiency allows higher throughput than CCMP, used in WPA3, uses AES counter mode or encryption, GMAC (Galois Message Authentication Code) for MIC, used in WPA3.
WPA (WIFI Protected Access): support two authentication modes: 1- personal mode: a pre-shared key is used for authentication, as password in home network (PSK is used to generate encryption key in a four way handshake.
Enterprise mode: 802.1x is used with an authentication server (RADIUS server), supports all EAP.
WPA: includes TKIP for encryption/MIC, 802.1X authentication (enterprise or PSK).
WPA2: CCMP provides encryption/MIC, 802.1X authentication (enterprise) or PSK.
WPA3: GCMP for encryption/MIC, 802.1X authentication (enterprise) or PSK, has additional security features as PMF (Protected Management Frames): protects 802.11 management frames from eavesdropping/forging.

PMF is optional in WPA2 and mandatory in WPA3.
SAE (Simultaneous Authentication of Equals): protects the 4 way handshake when using the personal mode authentication.
Forward Secrecy: prevent data from being decrypted after it has been transmitted over the air.