# CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-3-wireless_security
Title: Wireless Security
Subtitle: CompTIA Security+ (SY0-501)

## 6.3 Wireless Security

- 6.3 Given a scenario, install and configure wireless security settings.
    - Cryptographic protocols
        - WPA
            - An improvement over the weaker WEP protocol
            - Introduces TKIP
                - Generates a new key for each packet
            - Introduced Message Authentication Code that replaces the vulnerable CRC
            - Implemented in PSK or Enterprise
            - PSK
                - Good for home networks
                - Uses 256 bit key derived from the password for authentication
                - Single preshared key for tranmission between all clients on the network
                - Lacks centralized management
                    - When the PSK is changed on the AP, every STA has to be manually configured with the new PSK
                    - The PSK is stored on the client
            - Enterprise
                - Used in businesses
                - Adds 802.1X, RADIUS
                - Users log in with their business credientials
                - Every user essentially has their own key
                - Setup is more complex but allows for centralized administration
        - WPA2
            - June 24th 2004
            - Called 802.11i by the IEEE
            - Implemented as WPA2
            - Uses AES for encryption
            - CCMP replaces TKIP
            - Counter Mode Cipher Block Chaining Message Authentication Code Protocol
        - CCMP
        - TKIP
    - Authentication protocols
        - EAP
            - EAP is a framework that transports authentication information
            - EAP does is not and does not specify an authentication method
            - Can use multiple authentication mechanisms call EAP-types
            - Frequently used in wireles and point-to-point connections
            - When a user wants to connect to a wireless network, the AP will ask for the users ID info, then transfer that ID info to an authentication server(Could be RADIUS)
            - The authentication server will ask for validation of the ID, the AP will ask for the validation info from the user, then when received, forward that info to the authentication server.
            - If authentication is successful then the connection is approved, if the authentication fails, the connection is rejected
        - PEAP
            - EAP allows for authentication flexbility the whole process could be unencrypted
            - A malicious user could inject packets into the conversation or capture data for offline analysis
            - PEAP adds an TLS tunnel to encrypt the authentication information and maintain it's integrity
            - Then a second EAP method is used within the encrypted tunnel
            - PEAP is used to protect authentication information
            - Examples
                - PEAP-MSCHAPv2
                - PEAP-EAP-TLS
        - EAP-FAST
            - Flexible Authentication via Securing Tunnel (FAST)
            - Cisco propriatary session authentication in wireless networks and point-to-point
            - Developed as a replacement for Cisco's propriatary LEAP
            - Requires a Cisco software module, but is supported be Windows Vista and up/macOS 10.4.8/
        - EAP-TLS
            - Considered one of the strongest EAP types/methods available
            - Used in certificate-based authentication
            - Allow for mutual authentication
        - EAP-TTLS
            - Increases security over EAP-TLS
            - Creates an encrypted tunnel by TLS handshake

    - Allows for legacy authentication authentication protocols to be used against existing authentication databases while protecting the security of the legacy protocols
  - Scenarios
    - Dialup remote access: EAP-TLS
    - VPN remote access: EAP-TLS, PEAP-MSCHAPv2, PEAP-TLS
    - 802.1x: PEAP-MSCHAPv2, EAP-TLS, PEAP-TLS
  - IEEE 802.1x
    - Authentication mechanism for 802, 802.3 and 802.11 networks
    - Port-based authentication
    - Layer 2 technology
    - Coupled typically with RADIUS
    - 802.11 networks implement as part of WPA/WPA2-Enterprise
    - Components
      - Supplicant (client device)
      - Authenticator (Ethernet switch/Wireless AP)
      - Authentication Server (RADIUS)
  - RADIUS Federation
- Methods
  - PSK vs. Enterprise vs. Open
  - WPS
    - Introduced in 2006
    - Modes
      - PIN mode
      - Push button mode
      - NFC
      - USB (deprecated)
    - WPS PIN implemenation can be compromised with in a few hours
    - If disabled, ensure that the protocol is truly turned off
  - Captive portals
    - Used in public networks requiring the user to read and interact such as a password, EULA, AUP
    - Locations
      - Airports
      - Coffee Shops
      - Hotels
      - Convention Centers