Introduction to Connecting to the Internet

POTS and Dial-up

Broadband Connections

WANs

Wireless Networking

- **Video:** Introduction to Wireless Networking Technologies
  5 min
- **Reading:** Wi-Fi 6
  10 min
- **Reading:** Supplemental Reading for Alphabet Soup
  10 min
- **Reading:** Supplemental Reading for IoT Data Transfer Protocols
  10 min
- **Video:** Wireless Network Configurations
  2 min
- **Video:** Wireless Channels
  4 min
- **Video:** Wireless Security
  2 min
- **Reading:** Protocols & Encryption
  10 min
- **Video:** Cellular Networking
  1 min
- **Video:** Mobile Device Networks
  3 min
- **Reading:** Supplemental Reading for Mobile Device Networks
  10 min
- **Discussion Prompt:** Your Daily Connection
  10 min
- **Practice Quiz:** Wireless Networking
  5 questions

Graded Assessments

Protocols & Encryption

WPA3 Protocols & Encryption

Protocols and encryption are vital components in cybersecurity. Network security continues to evolve along with technological innovations and ever-increasing computing power. You have learned about WPA2 and how it improved the security of the Wi-Fi Protected Access (WPA) protocol. In this reading, you will explore WPA3, the third iteration of WPA wireless security. You will also learn about various internet connectivity technologies, as well as the basics of wireless and cellular networking.

WPA3 is built upon the WPA2 protocol and is intended to replace WPA2. The WPA3 protocol introduces new features and methods to repair the security weaknesses of WPA2. The benefits of this advancement in Wi-Fi security include:

- Simplified wireless security
- Stronger authentication
- Powerful encryption
- Stable business continuity
- Enhanced security methods
- Replacement for legacy protocols
- Protected Management Frames (PMF) requirement for enterprise networks

WPA3 offers two versions, a personal and an enterprise version.

WPA3-Personal

WPA3-Personal is intended for individual users and personal/home Wi-Fi networks. This protocol addresses common cybersecurity weaknesses that affect consumers' wireless devices. It also simplifies Wi-Fi security for users. The improvements to WPA3-Personal include:

- **Natural password selection:** Gives users the ability to set passwords that are easier for the user to remember.
- **Increased ease of use:** Users do not need to change the way they connect to Wi-Fi to benefit from WPA3's improved security.
- **Forward secrecy:** If a password is stolen, WPA3 can continue to protect data that is transmitted.
- **Simultaneous Authentication of Equals (SAE)**: WPA3-Personal improves upon the WPA2-Personal Pre-Shared Key (PSK) handshake protocol. SAE uses PSK to generate a Pairwise Master Key (PMK). The PMK uses password-based authentication and is shared between a Wi-Fi access point and a wireless device. The pair use a complex, multi-stage process for proving to one another that they each possess the PMK. This complex handshake makes it extremely difficult for cybercriminals to intercept packets in order to extract an identifiable authentication key. If the SAE transaction is successful, the wireless device will pass the authentication stage and gain access to the secured Wi-Fi network.

The SAE authentication also reduces the probability of successful dictionary and brute force attacks, in which cybercriminals try to crack short, weak, and commonly used passwords. Additionally, SAE corrects a weakness exploited by cybercriminals who could perform key reinstallation attacks (KRACKs) when in close proximity to a Wi-Fi user. This type of attack could decrypt data and expose passwords, credit card information, photos, chats, emails, and more.

WPA3-Enterprise

WPA3-Enterprise is intended for business networks with multiple users. This protocol addresses the WPA2-Enterprise weaknesses that cybercriminals have been able to exploit. In addition to the WPA3-Personal SAE improvements, the WPA3-Enterprise security improvements and options include:

- **Galois/Counter Mode Protocol (GCMP-256):** The Advanced Encryption Standard (AES) with GCMP-256-bit encryption replaces the WPA2 128-bit AES-Counter Mode Protocol (CCMP) Cipher Block Chaining Message Authentication Code (CBC-MAC). GCMP for data integrity. The GCMP-256-bit encryption strength takes significantly more computing power for cybercriminals to crack than 128-bit encryption. The average person would not have access to that level of computing power. GCMP-256-bit encryption provides a stronger security protocol and makes it harder for cybercriminals to perform Meddler-in-the-Middle attacks.
- **Opportunistic Wireless Encryption (OWE):** OWE improves upon the WPA2 wireless encryption standard of 802.1x Open Authentication and Extensible Authentication Protocol (EAP). In WPA2, EAP required additional support to help it encrypt and authenticate login credentials. In the WPA3 protocol, OWE replaces EAP with a solution that encrypts and authenticates all wireless traffic. It also replaces Wi-Fi passwords by assigning a unique key to each device that has permission to access the network. This technology repairs a weakness Wi-Fi users experience in open networks, which are often found in restaurants, coffee shops, hotels, airports, malls, and more.
- **Wi-Fi Device Provisioning Protocol (DPP):** DPP improves upon the WPA2 Wi-Fi Protected Setup (WPS) encryption technology between wireless devices and routers. WPA3's DPP uses QR codes or NFC tags to grant passwordless Wi-Fi access to wireless devices.
- **384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA):** HMAC creates hash code from a secret key. This hash code is sent with each message passed between a Wi-Fi access point and a user's device. The hash code from the origin of the message is compared to the hash code from the receiver of the message to determine if the hash codes match. A discrepancy between the two hashes would indicate that the message was compromised or corrupted during transmission.
- **Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA):** In WPA3, key management and authentication use the ECDHE protocol and ECDSA encryption for faster performance. The protocol is supported by most browsers. This key management technology replaces the WPA2 4-way handshake.

Key takeaways

As the tech industry develops more powerful computers, cybercriminals will use them to crack older encryption standards. The need to create more complex encryption algorithms will always be present in order to stay ahead of the evolving tools used by cybercriminals.

For **WPA3-Personal**, some of the new features include:

- Natural password selection
- Increased ease of use
- Forward secrecy
- Simultaneous Authentication of Equals (SAE)

For **WPA3-Enterprise**, some of the new features include:

- Galois/Counter Mode Protocol (GCMP-256)
- Opportunistic Wireless Encryption (OWE)
- Wi-Fi Device Provisioning Protocol (DPP)
- 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
- Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA)

Mark as completed

Like **Dislike** **Report an issue**