**Chapter 12: Secure Communications and Network Attacks**

The Point-to-Point Protocol (PPP) is an obsolete encapsulation protocol designed to support the transmission of IP traffic over dial-up or point-to-point links. It is the foundation of communication authentication. PPP supports automatic connection configuration, error detection, full-duplex communications, and options for authentication. The original PPP options for authentication were PAP, CHAP, and EAP.

Password Authentication Protocol (PAP) transmits usernames and passwords in cleartext. It offers no form of encryption.

Challenge Handshake Authentication Protocol (CHAP) performs authentication using a challenge-response dialogue that cannot be replayed. However, since CHAP is based on MD5, it is no longer considered secure.

Extensible Authentication Protocol (EAP) is a framework for authentication instead of an actual protocol. EAP allows customized authentication security solutions, such as supporting smartcards, tokens, and biometrics. Some EAP methods use encryption, but others do not. More than 40 EAP methods have been defined, including LEAP, PEAP, EAP-SIM, EAP-FAST, EAP-MD5, EAP-POTP, EAP-TLS, and EAP-TTLS.

Voice over Internet Protocol (VoIP) is a technology that encapsulates audio into IP packets to support telephone calls over TCP/IP network connections. VoIP security is often achieved through general network security practices and using Secure Real-time Transport Protocol (SRTP).

VoIP-originated voice-based social engineering attacks are known as vishing, which stands for voice-based phishing.

Phreaking (the “ph” represents “phone”) is a specific type of attack directed toward the telephone system and voice services in general.

PBX terminology is related to VoIP. Private branch exchange (PBX) is a telephone switching or exchange system deployed in private organizations in order to enable multistation use of a small number of external PSTN lines.

Changing default passwords on PBX systems provides the most effective increase in security. PBX systems typically do not support encryption, although some VoIP PBX systems may support encryption in specific conditions.

Persistence in relation to load balancing is also known as affinity. Subsequent communications from the same client are sent to the same server.

SMTP, POP, IMAP are natively plaintext protocols and do not provide any security to the eavesdropping and other MitM attacks.

STARTTLS (aka explicit TLS or opportunistic TLS for SMTP) will attempt to set up an encrypted connection with the target email server in the event that it is supported. STARTTLS is not a protocol but instead an SMTP command.

Secure Multipurpose Internet Mail Extensions (S/MIME) is an email security standard that offers authentication and confidentiality to email.

Two types of messages can be formed using S/MIME: signed messages and secured enveloped messages. A signed message provides integrity, sender authentication, and

nonrepudiation. An enveloped message provides recipient authentication and confidentiality.

Sender Policy Framework (SPF) can be configured to protect against spam and email spoofing.

Tunneling, or encapsulation, is a means by which messages in one protocol can be transported over another network or communications system using a second protocol.

A split tunnel is a VPN configuration that allows a VPN-connected client system (i.e., remote node) to access both the organizational network over the VPN and the internet directly at the same time.

A full tunnel is a VPN configuration in which all of the client’s traffic is sent to the organizational network over the VPN link, and then any internet-destined traffic is routed out of the organizational network’s proxy or firewall interface to the internet.

IPsec isn’t a single protocol but rather a collection of protocols, including AH, ESP, HMAC, IPComp, and IKE.

Authentication Header (AH) provides assurances of message integrity and nonrepudiation.

Encapsulating Security Payload (ESP) provides confidentiality and integrity of payload contents. ESP can operate in either transport mode or tunnel mode.

Hash-based Message Authentication Code (HMAC) is the primary hashing or integrity

mechanism used by IPsec.

IP Payload Compression (IPComp) is a compression tool used by IPsec to compress data prior to ESP encrypting it in order to attempt to keep up with wire speed transmission.

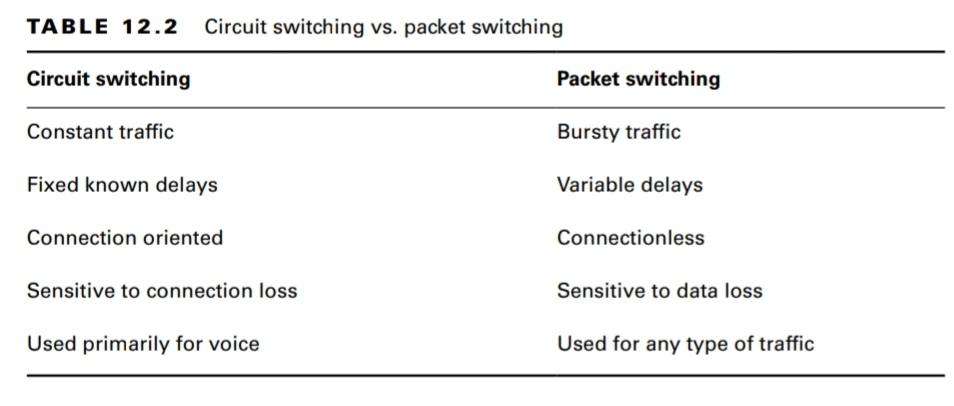
Internet Key Exchange (IKE) is a mechanism of IPsec that manages cryptography keys.

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

MAC flooding is accomplished by flooding the content addressable memory (CAM) table of a switch with Ethernet frames with randomized source MAC addresses. Once the CAM table is filled with false MAC addresses only, the switch is unable to properly forward traffic. Then It acts like a hub or a multiport repeater and sends each received Ethernet frame out of every port.

In Circuit Switching, the links between the two parties remain the same throughout the conversation. Circuit switching provides for fixed or known transmission times, a uniform level of quality, and little or no loss of signal or communication interruptions.

Packet switching occurs when the message or communication is broken up into small segments and sent across the intermediary networks to the destination. Each segment of data has its own header that contains source and destination information.



Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET) are

fiber-optic high-speed networking standards.

A permanent virtual circuit (PVC) can be described as a logical circuit that always exists and is waiting for the customer to send data.

A switched virtual circuit (SVC) has to be created each time it is needed using the best paths currently available before it can be used and then disassembled after the transmission is complete.

Software-defined networking (SDN) is a unique approach to network operation, design, and management. SDN aims at separating the infrastructure layer (hardware and hardware-based settings) from the control layer (network services of data transmission management).