CWSP Guide to Wireless Security

Secure Wireless Transmissions

Objectives

- Explain how documents to be transmitted wirelessly can be encrypted
- List and describe the secure management interfaces for encryption
- Tell the features of a virtual private network and how they are used to secure wireless transmissions

Encryption for Transmitting Documents

- Can be accomplished in one of two ways
  - Using private key cryptography
  - Using public key cryptography

Private Key Cryptography

- Private key (symmetric) cryptography
  - Basis of PSK in WPA and WPA2
  - Uses a single key to both encrypt and decrypt the document
  - Provides a weak degree of protection
    - Because of the problems associated with managing the keys

Private Key Cryptography (continued)

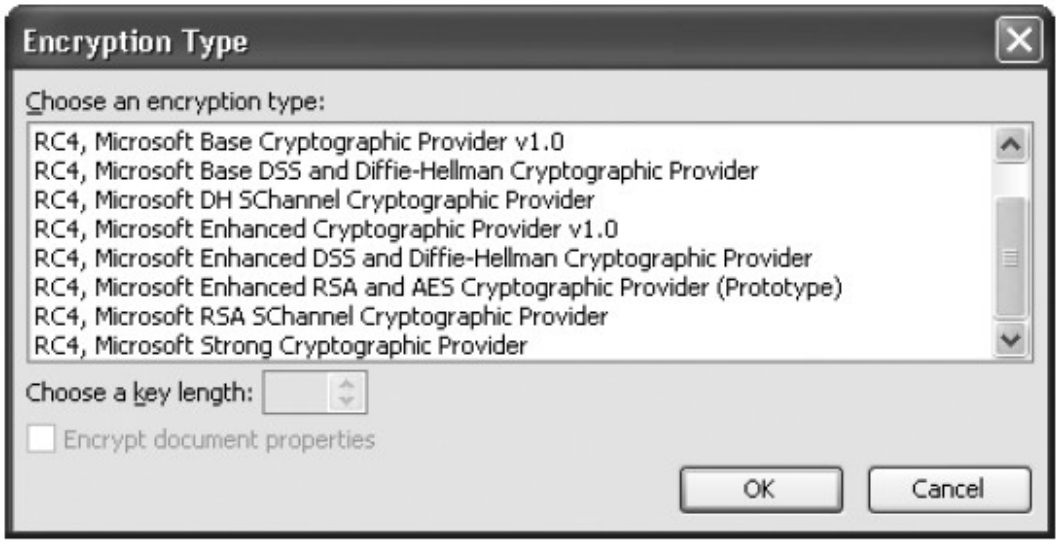

Figure 9-1 Microsoft Word encryption options

Public Key Cryptography

- Asymmetric encryption, or public key cryptography
  - Solves the key management problem
  - Two mathematically related keys are used instead of just one
    - One private and one public
  - Public key can be freely distributed
- Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG)
  - PGP is the most widely used public cryptography system for Windows
  - GNU is an operating system that offers free software
  - The GNU Privacy Guard (GnuPG) is a complete implementation of the OpenPGP , used for digital encryption and signing of data and mainly useful for offline communication (email) and data storage.

Public Key Cryptography (continued)

- Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG) also known as GnuPG (continued)
  - GPG is similar to PGP, but runs on Windows, UNIX, and Linux
  - PGP/GPG generates a random private (symmetric) key
    - And uses it to encrypt the message
  - Private key is then encrypted using the receiver's public key and sent along with the message
  - Receiver recovers the private key and decrypts the message

Public Key Cryptography (continued)

- Linux Cryptographic File System (CFS)
  - Can encrypt all files or selected directories and files on a Linux system: https://www.youtube.com/watch?v=wMGy11ydzKc
- Secure File Transfer Protocol (SFTP)
  - File Transfer Protocol (FTP)
    - Used to connect to an FTP server
    - Frequently used by both wireless and wired users for transmitting files

Public Key Cryptography (continued)

- Secure File Transfer Protocol (SFTP) (continued)
  - User can connect to an FTP server
    - Through a Web browser
    - Using an FTP client
    - From the command line
  - Vulnerabilities associated with FTP
    - FTP does not use encryption
    - Vulnerable to man-in-the-middle attacks
    - Binary files are converted to cleartext before they are transmitted

Public Key Cryptography (continued)

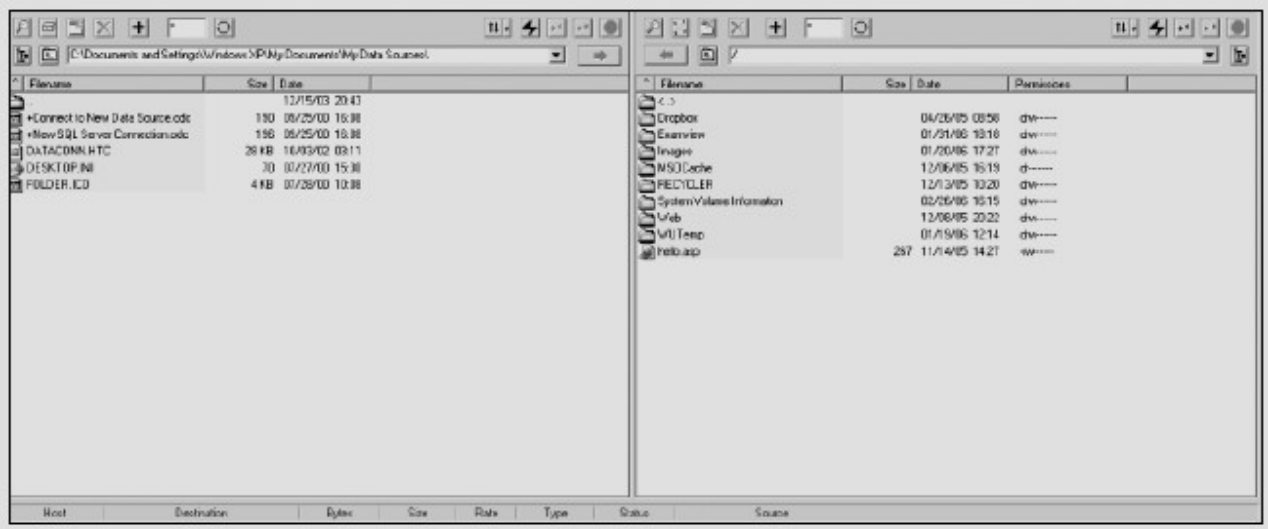

Figure 9-2 FTP client

Public Key Cryptography (continued)

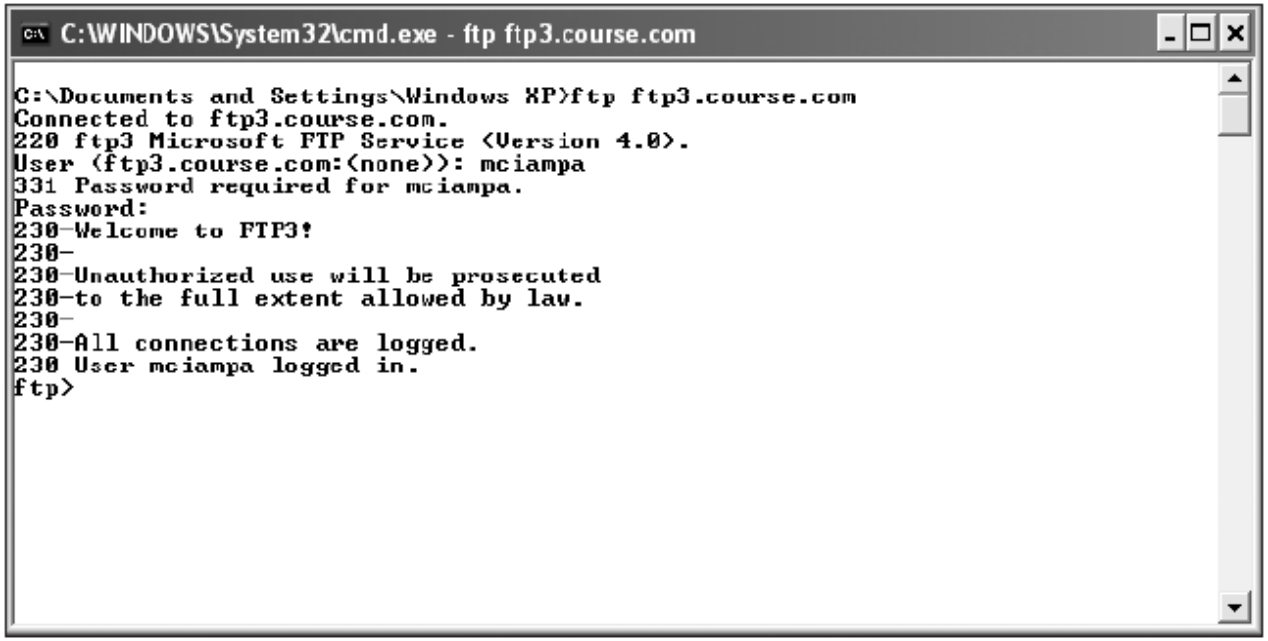

Figure 9-3 Command-line FTP

Public Key Cryptography (continued)

- Secure File Transfer Protocol (SFTP) (continued)
  - SFTP reduces the risk of attack
  - SFTP can be based on one of two protocols
    - Secure Sockets Layer (SSL)
    - Secure Shell
  - SSL was developed by Netscape for securely transmitting documents over the Internet
  - Transport Layer Security (TLS)
    - Guarantees privacy and data integrity between applications communicating over the Internet
    - Extension of SSL
    - https://www.youtube.com/watch?v=33xENGhjorg

Public Key Cryptography (continued)

- Secure File Transfer Protocol (SFTP) (continued)
  - Using SSL/TLS, SFTP provides:
    - Protection from man-in-the-middle attacks
    - Protection against packet sniffing during transmission
  - SSL/TLS is also used for securing e-mail transmissions

Public Key Cryptography (continued)

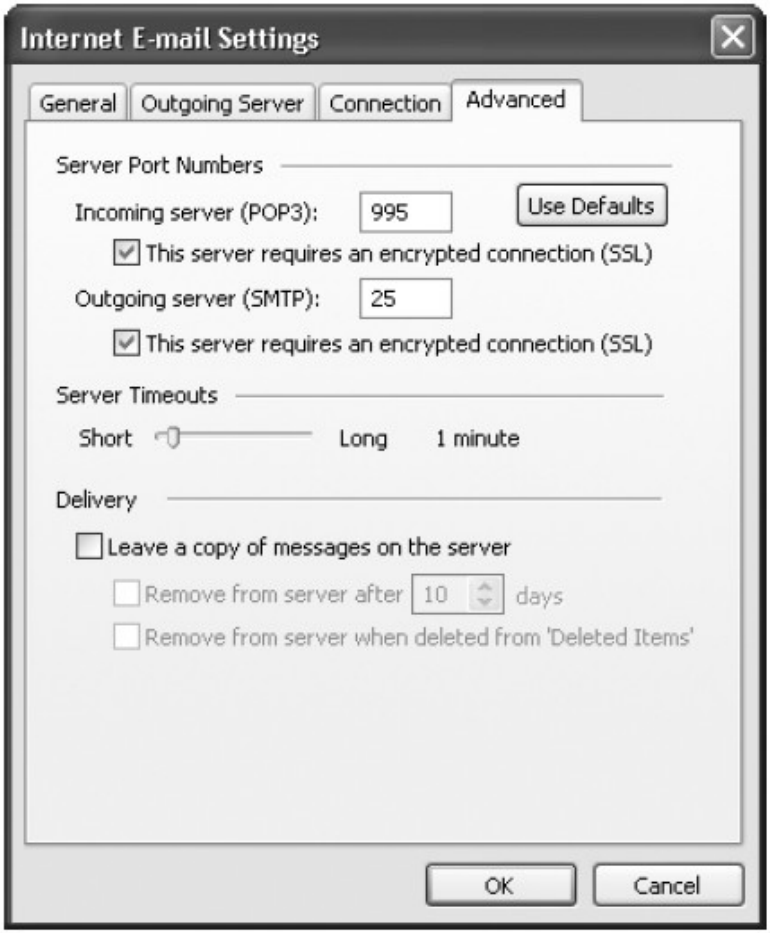

Figure 9-4 E-mail using SSL/TLS

Public Key Cryptography (continued)

- Secure File Transfer Protocol (SFTP) (continued)
  - Secure Shell (SSH)
    - UNIX-based command interface and protocol for securely accessing a remote computer
    - Suite of three utilities: slogin, ssh, and scp
    - Client and server ends are authenticated using a digital certificate
    - Passwords are protected by being encrypted
    - Can even be used as a tool for secure network backups

Public Key Cryptography (continued)

Table 9-1 UNIX commands for remote security

UNIX Command Name	Description	Syntax	Secure Command Replacement
rlogin	Log on to remote computer	rlogin *remotecomputer*	Slogin
rcp	Copy files between remote computers	rcp [*options*] *localfile remotecomputer:filename*	Scp
rsh	Executing commands on a remote host without logging on	rsh *remotecomputer command*	Ssh

Public Key Cryptography (continued)

- Secure Copy (SCP)
  - Facility for transferring files securely
  - Encrypts data during transfer
  - Does not perform authentication or other security
    - Relies upon the underlying SSH protocol
  - Command-line program scp
    - Most widely used SCP client
    - Provided in many implementations of SSH
  - GUI-based clients are typically not “pure” SCP clients

Encryption for Secure Management Interfaces

- Important to use encryption with wireless devices
- Technologies used for encryption include:
  - SSH port forwarding
  - HTTPS
  - SNMPv3

SSH Port Forwarding

- Also called tunneling
- Used to provide secure access to other services that do not normally encrypt data during transmission
  - TCP/IP connection to an external application that is not secure can be redirected to the SSH program
    - Which then forwards it to the other SSH party
  - SSH party forwards the connection to the desired destination host

Secure Hypertext Transfer Protocol (HTTPS)

- HTTPS
  - “Plain” HTTP sent over SSL/TLS
  - Designed to transmit individual messages securely
- Most wireless devices are managed through a Web interface
  - Devices typically provide several different HTTPS options

Secure Hypertext Transfer Protocol (HTTPS)

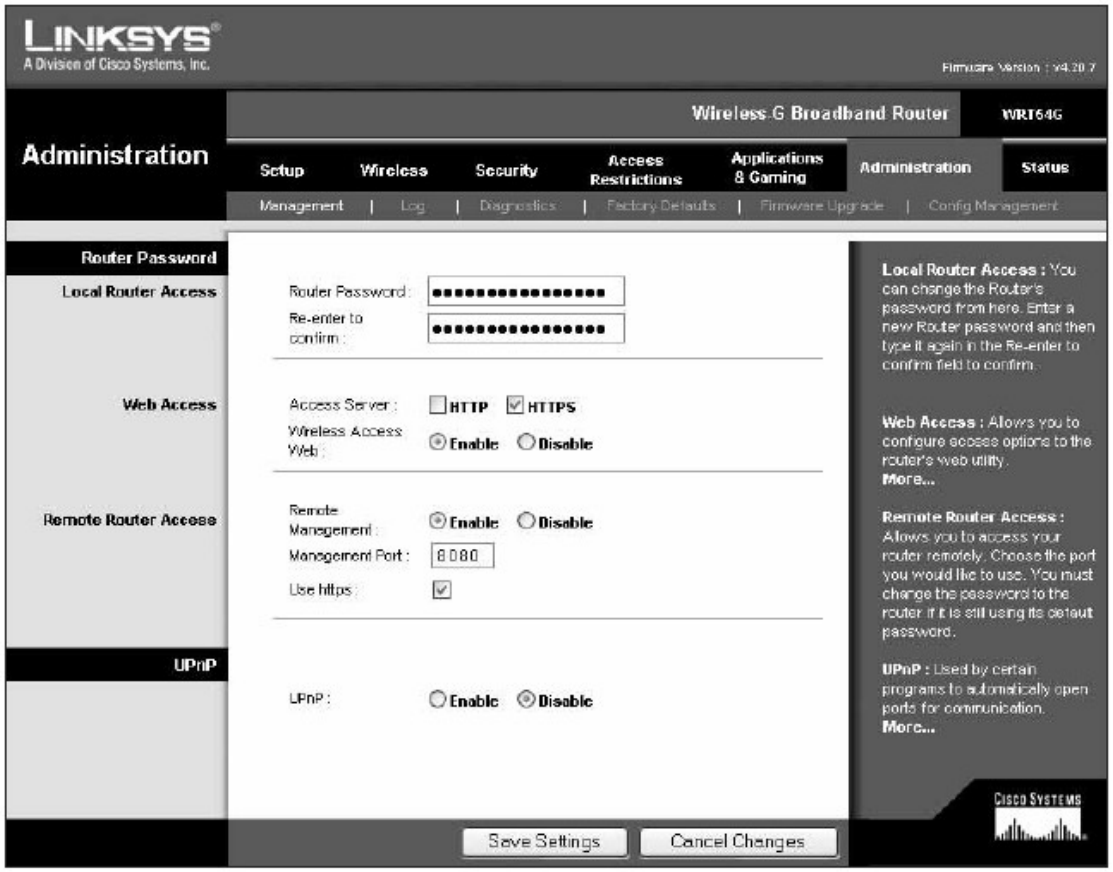

Figure 9-5 Web interface options

Secure Hypertext Transfer Protocol (HTTPS) (continued)

- SNMPv3
  - Simple Network Management Protocol (SNMP)
    - Protocol used to manage networked equipment
  - SNMP-managed device has an agent or a service
    - That "listens" for commands and then executes them
  - Agents are protected with a password known as a *community string*
  - Use of community strings in SNMPv1 and SNMPv2 had several vulnerabilities
  - SNMPv3 replaced community strings with usernames and passwords along with an encryption key

Encryption for Virtual Private Networks (VPNs)

- Drawbacks of public and private cryptography
  - User must consciously perform a separate action
    - Or use specific software
  - These actions only protect *documents* that are transmitted
    - Other communications performed over a wireless LAN are not secure
- VPNs
  - Solves all these problems
  - Essential tools for corporate “road warriors”

What is a Virtual Private Network?

- Virtual Private Network (VPN)
- https://www.youtube.com/watch?v=YPH5v6kGXbo
  - Uses an unsecured public network as if it were a secure private network
- VPN types
  - Remote-access VPN or virtual private dial-up network (VPDN)
    - User-to-LAN connection used by remote users
  - Site-to-site VPN
    - Multiple sites can connect to other sites over the Internet
- AVPN is roughly equivalent to an SSH session

VPN Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP)
  - Most widely deployed tunneling protocol
  - Allows IP traffic to be encrypted and then encapsulated in an IP header
    - To be sent across a wireless or public IP network
  - Based on the Point-to-Point Protocol (PPP)
  - Link Control Protocol (LCP)
    - Extension of PPTP
    - Establishes, configures, and automatically tests the connection

VPN Tunneling Protocols (continued)

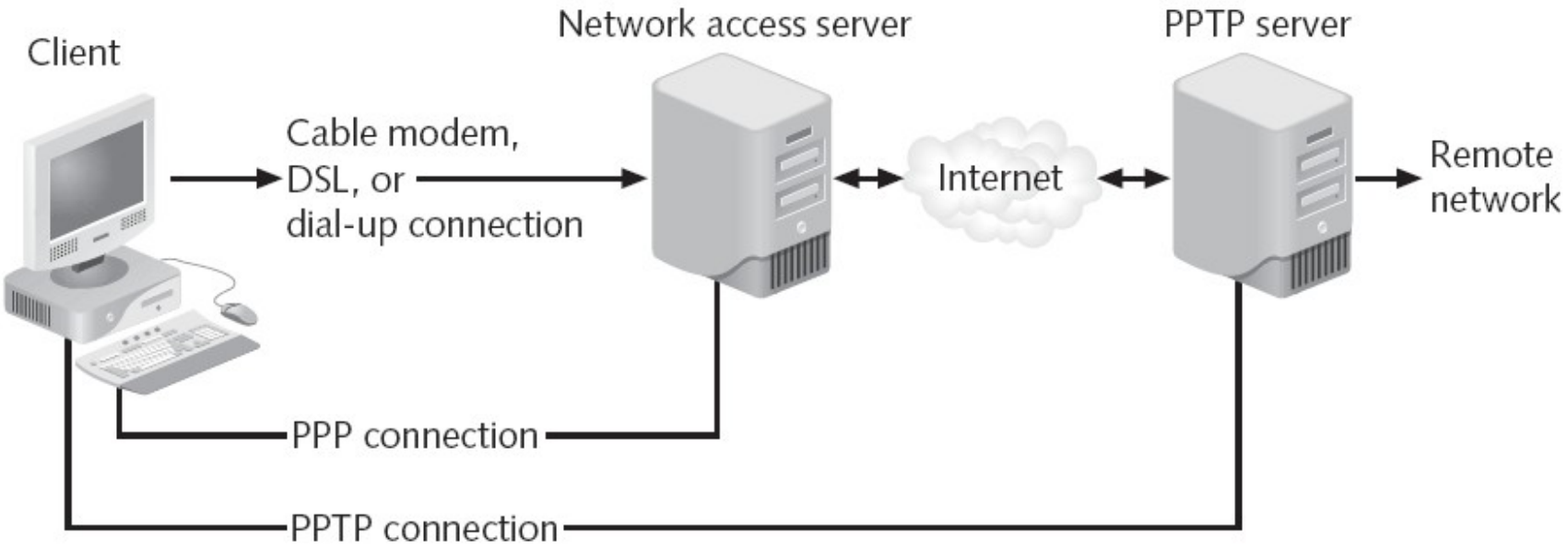

Figure 9-6 Point-to-Point Tunneling Protocol (PPTP)

VPN Tunneling Protocols (continued)

- Point-to-Point Tunneling Protocol (PPTP) (continued)
  - Point-to-Point Protocol over Ethernet (PPPoE)
    - Variation of PPP
    - Simulates a dial-up session and can assign IP addresses as necessary
- Layer 2 Tunneling Protocol (L2TP)
  - Represents a merging of the features of PPTP with Cisco's Layer 2 Forwarding Protocol (L2F)
  - Allows IP traffic to be encrypted and then transmitted over any medium that supports point-to-point delivery

VPN Tunneling Protocols (continued)

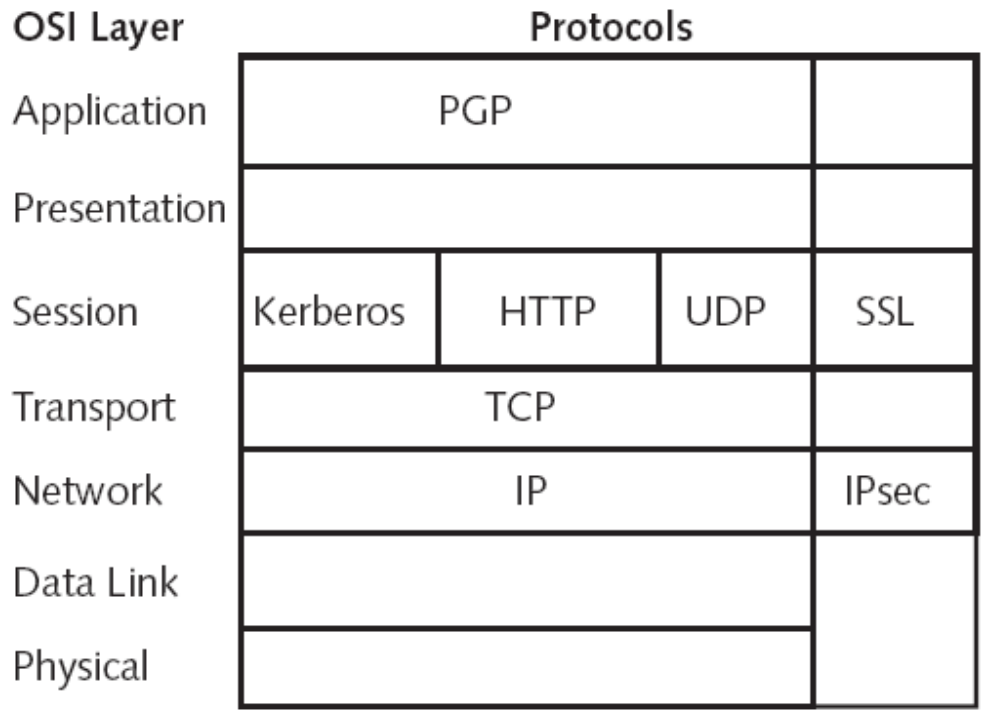

Figure 9-7 Security tools and the OSI model

VPN Tunneling Protocols (continued)

- IP Security (IPsec)
  - Different security tools function at different layers of the Open System Interconnection (OSI) model
    - Protecting at higher layers may require multiple security tools
  - IPsec is a set of protocols developed to support the secure exchange of packets
  - Transparent to applications, users, and software
  - Located in the operating system or the communication hardware

VPN Tunneling Protocols (continued)

- IP Security (IPsec) (continued)
  - Areas of protection
    - Authentication, accomplished by the Authentication Header (AH) protocol
    - Confidentiality, achieved through the Encapsulating Security Payload (ESP) protocol
    - Key management, accomplished through the Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley) protocol

VPN Tunneling Protocols (continued)

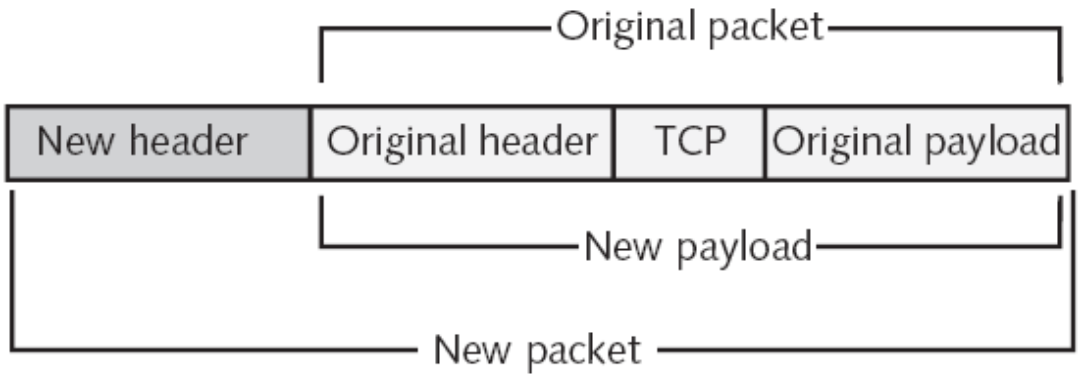

Figure 9-8 New IPsec packet

VPN Tunneling Protocols (continued)

- IP Security (IPsec) (continued)
  - Encryption modes
    - Transport mode, encrypts only the data portion (payload)
    - Tunnel mode, encrypts both the header and the data portion

VPN Tunneling Protocols (continued)

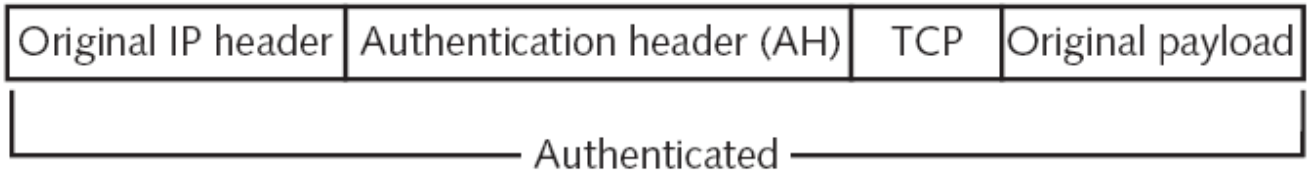

Figure 9-9 AH in transport mode

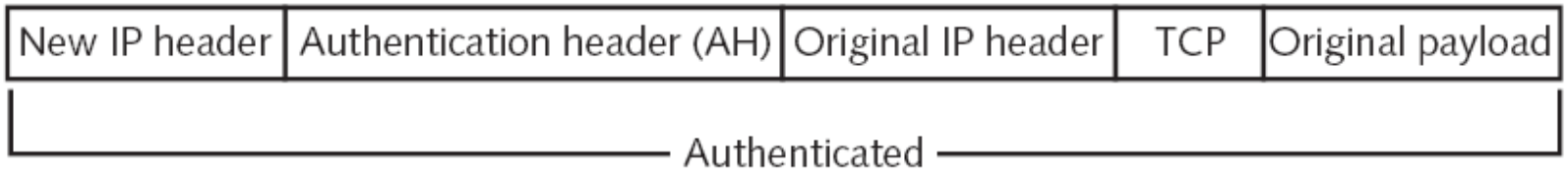

Figure 9-10 AH in tunnel mode

VPN Tunneling Protocols (continued)

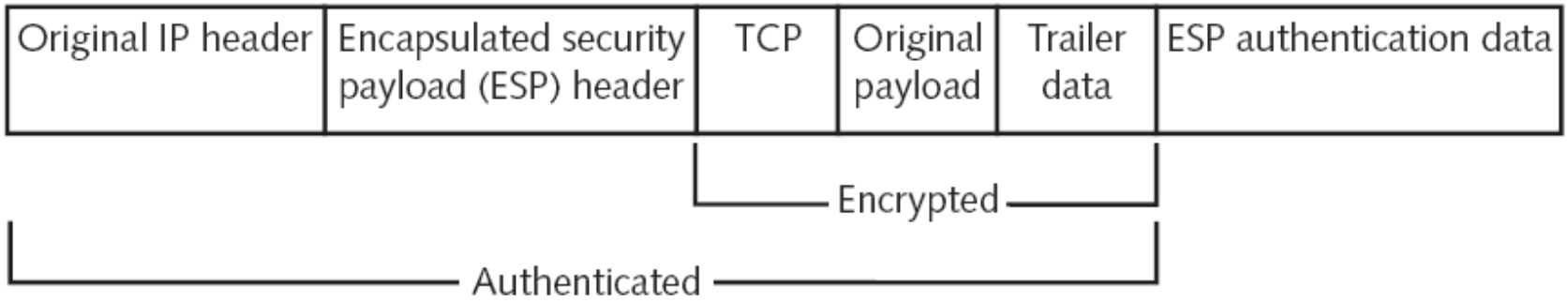

Figure 9-11 ESP in transport mode

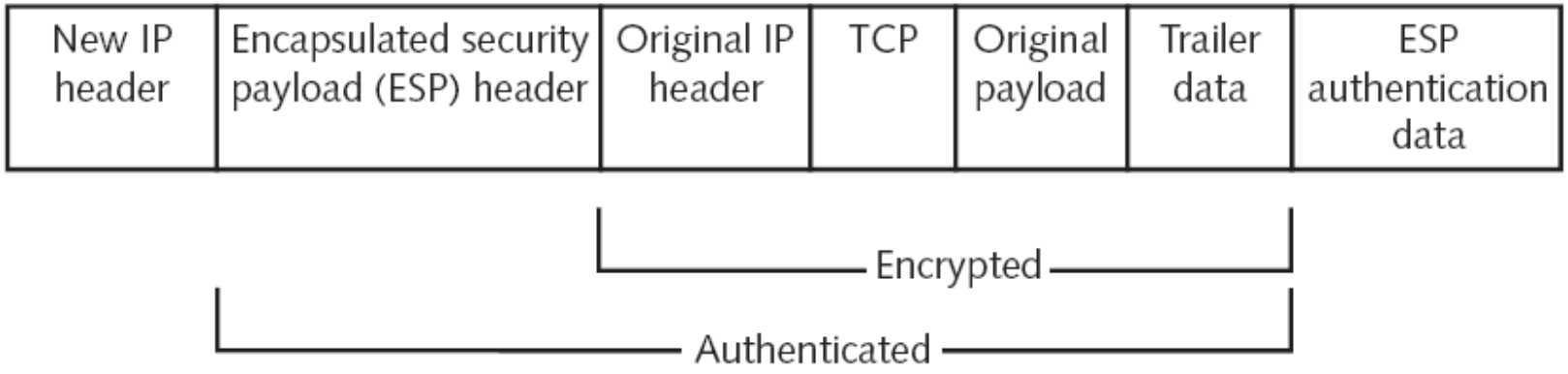

Figure 9-12 ESP in tunnel mode

VPN Tunneling Protocols (continued)

Table 9-2 Tunneling protocol comparisons

Protocol	Security Level	When It Should Be Used
PPTP	Moderate	Connecting to Windows server
L2TP	High	Connecting to Windows server
IPsec	High	Connecting to non-Windows server

VPN Hardware and Software

- VPN transmissions are achieved through communicating with endpoints
- Endpoint
  - End of the tunnel between VPN devices
  - Can be software or hardware
- VPN concentrator
  - Aggregates hundreds or thousands of multiple connections together

Client Software (continued)



Figure 9-13 Microsoft Windows VPN client

Client Software

- Endpoints that provide passthrough VPN capability
  - Require that a separate VPN client application be installed on each device
    - That connects to a VPN server
- Client application
  - Handles setting up the connection with the remote VPN server
  - Takes care of the special data handling required to send and receive data through the VPN tunnel

Client Software (continued)

- Built-in VPN endpoint
  - Handles all the VPN tunnel setup, encapsulation, and encryption in the endpoint
- Types of VPN clients
  - Operating system
  - Freeware
  - VPN vendors

Software-Based VPNs

- VPN endpoint is actually software running on the wireless device itself
- Preferred when both endpoints are not controlled by the same organization
- Advantages
  - Offer the most flexibility in how the network traffic is managed
  - More desirable for “road warriors”
  - Good options where performance requirements are modest

Software-Based VPNs (continued)

- Disadvantages
  - Do not have as good performance or security as a hardware-based VPN
  - Considered harder to manage than hardware endpoints
  - Software VPN products require changes to routing tables and network addressing schemes
  - Not all Internet routers allow for software-based VPN tunnels

Hardware-Based VPNs (continued)

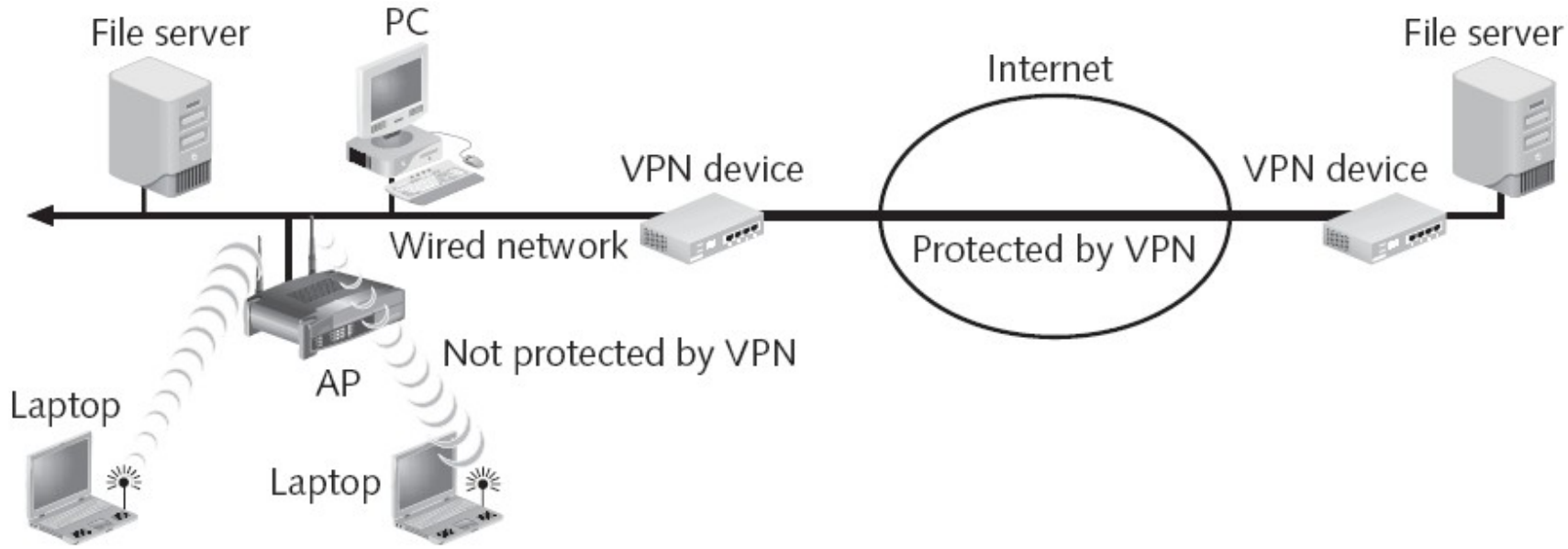

Figure 9-14 VPN protection

Hardware-Based VPNs

- More secure, have better performance, and can offer more flexibility than software-based VPNs
- Only the network devices, serving as passthrough VPNs, manage the VPN functions
  - Relieve the wireless device from performing any VPN activities
- Can protect all wireless devices behind it
- Disadvantages
  - Enterprise hardware-based VPNs can be expensive
  - It is necessary to match vendor VPN endpoints

Hardware-Based VPNs (continued)

- Support for hardware-based WLANVPN may be:
  - A separate VPN appliance
  - Integrated into existing networking equipment
- Enterprise-level access points may have built-in VPN functionality
  - To fully protect wireless transmissions from devices
- SOHO and home wireless gateways usually support passthrough VPN
  - For devices that are using software-based VPNs

Hardware-Based VPNs (continued)



Figure 9-15 Access point passthrough VPN

Hardware-Based VPNs (continued)

- VPN encryption functions at Layers 2 and 3 of the OSI model
  - Support IPsec, PPTP, or L2TP
- Traditional routing based on connection-level information at Layers 2 and 3
  - Often cannot keep pace with the data volumes
- Layer 4-7 devices
  - Can provide intelligent traffic and bandwidth management based on the content of a session

VPN Advantages and Disadvantages

- Advantages
  - Cost savings
  - Scalability
  - Full protection
  - Speed
  - Authentication
  - Industry standards

VPN Advantages and Disadvantages (continued)

- Disadvantages
  - Interoperability
  - Additional protocols

Summary

- Wireless encryption at an open hotspot and for secure management interfaces
  - Considered critically important to protect the content of transmissions
- Tools for encrypting secure management interfaces in WLANs
  - SSH port forwarding
  - HTTPS
  - SNMPv3

Summary (continued)

- A VPN uses an unsecured public network to send and receive private messages by using encryption
- VPN transmissions are achieved through communicating with endpoints
  - Which are the end of the tunnel between VPN devices