

# Telecommunication Remote Access

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: telecommunication\_remote\_access.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ Introduction

- **Involves the security of data and administrative information**
- **That is traveling on public and private networks**
- **Generally concerned with the privacy & Integrity**
- **Addressed by use of standardized authentication and authorization**
- **Such as RADIUS, TACACS+ or a VPN's**

## ❖ 802.1x

- **Provide authentication mechanism over physical media**
- **Used to improve the privacy of wireless LAN**
- **To get authentication functionality**
  - You must choose a particular flavor of EAP
  - Install it on your authentication server.
  - Transport Layer Security (EAP-TLS)
  - EAP Tunneled Transport Layer Security (EAP-TTLS) Built into XP, Win CE
  - RADIUS (FRC 2138,2139)
  - LEAP84, by Cisco
- **IEEE - 802.11 Standards**
  - Interface between clients and base station
  - The physical layer PHY can use:
    - DSSS - Direct Sequence Spread Spectrum
    - FH - Frequency Hoping Spread Spectrum
    - IR - Infrared pulse modulation
  - MAC Layer - Medium Access Control
  - Specifies CSMA/CA Carrier Sense Multiple Access Collision Avoidance
  - Provides:
    - Data Transfer
    - Association
    - Re-association
    - Authentication - WEP
    - Privacy - WEP
    - Power Management
  - 802.11b works at 2.4 GHz and provides data rates up to 11 Mbps
  - 802.11b standard uses the Wireless Application Protocol (WAP)

## ❖ VPN

- **Introduction**
  - VPN's usually perform user authentication and traffic encryption

- **Building a secure communication link between**
- **This link is called "Secure Encrypted Tunnel"**
- **On a VPN, traffic is decrypted at every endpoint.**
- **VPN - Private data network that makes use of the public teleco infrastructure**
- **VPN - use tunneling protocol to provide a secure network link**
- **Tunneling is used by an extranet to connect multiple intranets via the Internet.**
- **Common VPN protocols include: PPTP, L2TP, SSH and IPSec.**
- **Encapsulation tunnel Created using methods such**
  - Installing software or hardware agents on the client
  - Implementing various user or node authentication systems
  - Implementing key and certificate exchange systems
- **NAT**
  - Translation of an Internet Protocol address (IP address) to a different IP
  - NAT is an important part of VPN
  - Private addresses are not easily routable. This is the reason of using NAT
  - One network is designated the inside
  - One network is designated the outside
  - NAT is included as part of a router/firewall
  - NAT reduces the need for a large amount of publicly known IP
  - NAT use these reserved IP's
    - ♦ 10.0.0.0 - 10.255.255.255
    - ♦ 172.16.0.0 - 172.31.255.255
    - ♦ 192.168.0.0 - 192.168.255.255

## ➤ **VPN Protocol Standards**

- **PPTP**
  - Point To Point Tunneling Protocol
  - Work at the Data Link Layer
  - Enable ONLY one single point-to-point connection per session
  - Use PPP authentication and encryption services
  - Use PAP or CHAP
  - It is asynchronous
  - Microsoft supports the PPTP and IPSec standards for use in extranets.
- **L2TP**
  - Combination of PPTP and earlier Layer 2 forwarding Protocol
  - Dial-up VPN use this standard
  - Designed for Single Point-To-Point client to server Like PPTP
  - Multiple protocol can be encapsulated within L2TP tunnel
  - Work on Data Link Layer
- **IPSec**
  - Work at the Network Layer
  - They are installed on a network perimeter and encrypt traffic by creating a secure tunnel
  - They work only with IP they are NOT multi-protocol
  - Enable multiple and simultaneous tunnels
  - IPSec has 2 modes
    - ♦ Tunnel mode - encrypt payload and header information
    - ♦ Transport mode - Encrypt only the payload
  - Ensures confidentiality and integrity to IP packets
  - Authenticate and encrypt IP data

- Focus more on Network-To-Network connectivity
- **VPN Devices**
  - **Non-IPSec Compatible**
    - Socks
      - ◆ Socks based systems contain Authentication and Encryption similar to VPN
      - ◆ Socks Work on Application Layer 7
    - PTP
      - ◆ Multiprotocol used in Win9x and NT
      - ◆ Use PAP or CHAP for End-To-End Encryption
      - ◆ Commonly used by ISP's
    - SSH
      - ◆ Secure Shell SSH-2 is not a VPN product but it can be used as such
      - ◆ SSH open a secure encrypted shell session from the internet through a firewall
  - **Firewall based VPN**
    - Frequently available on Thrid generation of firewall (Statful Inspection)
    - Use VPN that integrate to the firewall and often it is proprietary and non-standard
    - Work on Application Layer 7 in tunnel mode

## ❖ RADIUS

- **Remote Access Dial-In User Service**
- **It provides a centralized server for single point of authentication**
- **Client/server protocol that authenticates users connecting to a network**
- **A protocol for carrying authentication, authorization, and configuration information**
- **Transactions between client and server use a shared secret**
- **Is a handshaking protocol**
- **Distributed RADIUS” are connected together and “forward authentication”**
- **Provide better authentication security than TACACS+**

## ❖ L2TP/PPTP

- **L2TP**
  - **Combination of PPTP and earlier Layer 2 forwarding Protocol**
  - **Dial-up VPN use this standard**
  - **Designed for Single Point-To-Point client to server Like PPTP**
  - **Multiple protocol can be encapsulated within L2TP tunnel**
  - **L2TP was intended as a replacement for PPTP**
  - **L2TP supports PAP, CHAP, MS-CHAP and other**
  - **L2TP and L2F use UDP port 1701.**
  - **Work on Data Link Layer (2)**
- **PPTP**
  - **Point To Point Tunneling Protocol**
  - **Supports PAP, CHAP and MS-CHAP authentication**
  - **Usually used to implement security over a PPP connection.**
  - **Use PPP authentication and encryption services**
  - **It implements tunneling over a PPP**
  - **PPTP uses TCP port 1723.**
  - **Enable ONLY one single point-to-point connection per session**

- It is asynchronous
- MS PPTP uses RSA RC4 encryption and a 40-bit or 128-bit key.
- The most popular tunneling protocol today.
- Work at the Data Link Layer (2)

## ❖ IPSEC

- Internet Protocol Security
- Uses Diffie-Hellman key exchange to communicate key
- Public key cryptography to sign the key exchange
- Method of setting up a secure channel for protected data exchange between two devices
- IPsec - is more flexible and less expensive than application and Link-Layer encryption
- Widely accepted standard for secure network layer transport
- Have strong encryption and authentication methods
- Useful for VPN and for remote user access through dial-up connection
- Is an open modular FRAMEWORK that provides a lot of flexibility
- Bi-directional communication requires two Security Associations
- A big advantage of IPsec does not require changes to individual user computers
- IPsec uses TCP port 1293 and UDP port 1293.
- ISAKMP uses UDP port 500 (UDP port 4500 when NAT is used)
- Provides
- Use Two Main Protocols
- Security Association (SA)
- IPsec - work in two modes
- IKE
- IKMP
- ISAKMP
- Encryption technologies used by IPsec