Virtual Private Networks

ECE 4886 - Internetwork Security
Dr. Henry Owen
Definition

- Virtual Private Network – VPN
  - *Virtual* – separation in protocol provides a “virtual” network using no new hardware
  - *Private* – communication over VPN is encrypted
  - *Network* – infrastructure over which computers communicate
VPN Elements

• Encrypted Tunnel
  - Privacy of Information – Important!
  - Internet is a public network <- need for secure communications
  - Data is encrypted upon transmission and decrypted upon arrival at the destination
  - Two hosts effectively communicate directly
  - Data is “tunneled” from one to the other
VPN Elements

- Authenticated Endpoints
  - Messages are authenticated
  - Possible replay attack to reveal crypto key
  - VPN hashing algorithm
    - If the packet has been changed by one bit, VPN will drop the packet
    - Hackers are reduced to guessing the key
    - Replay attack ineffective
VPN Elements

- Underlying Transport
  - Uses existing network connection
  - TCP/IP Protocol
    - VPN & Internet

- VPNs can be placed anywhere
  - Personal network
  - Internet
VPN Advantages

- Improved Security
- Consolidation of Scattered Resources
- Transparency to Users
- Reduced Cost
- Ease of Administration
VPN Disadvantages

- Time Consuming Setup
- Troubleshooting
- Internet Availability
- Interoperability with other Networks
Implementing VPNs

- SSH over PPP
- SSL over PPP
- IPSec
- PPTP
VPN via SSH & PPP

- Point-to-Point Protocol over a Secure Shell connection
- Establishing a Network Connection
  - Establish an SSH connection
    - VPN Client → VPN Server
  - Each have PPP daemons that will communicate through the SSH connection
  - Viola! A VPN CONNECTION!
VPN via SSL & PPP

- Point-to-Point Protocol over a Secure Socket Layer connection
- Secure Socket Layer
  - Built-in support for Host Authentication
  - Certificates
VPN via SSL & PPP

• Establishing a Network Connection
  ▪ Initial Handshake for secure communication
  ▪ “Hello” messages establish:
    – SSL Version, support for Cipher suites, and some random data
  ▪ Key is determined separately from handshake
  ▪ SSL Connection Complete!
  ▪ Data transferred over the link
VPN via IPSec

- Internet Protocol Security – IPSec
- Security at the IP layer
- Two Modes
  - Transport
    - Modifies only upper levels by adding headers and protection between upper level and original IP header
    - Designed for hosts to protect IP traffic between each other
VPN via IPSec

• Two Modes (Cont’d)
  ▪ Tunnel
    – Treats entire packet as a block
    – Encapsulates the packet into an encrypted payload
    – Designed to “tunnel” traffic between gateways

• Relies on sets of rules that specify the type of protection needed for certain packets – similar to firewall rules
VPN via PPTP

- Point-to-Point Tunneling Protocol
  - Microsoft’s Implementation of VPN
  - Data is first encapsulated inside PPP packets
  - PPP packets are then encapsulated in GRE packets and sent over the link
- PPTP uses two connections
  - One for the data being sent
  - Another for a control channel
VPN via PPTP

- PPTP Not Usually Used on Linux
  - Only for interoperability with Windows machines
- PPTP VPN can be established without encryption! Possible security issue here
- Not recommended for Linux systems, since there are easier and more secure VPN implementations
Resources

• Books:
  ▪ Building Linux Virtual Private Networks
    – Oleg Kolesnikov, Brian Hatch
  ▪ Linux Server Hacks
    – Rob Flickenger

• Websites:
  ▪ http://vpn.shmoo.com/
  ▪ http://www.tldp.org/HOWTO/VPN-HOWTO/