Distributed Systems
28. Virtual Private Networks

Paul Krzyzanowski
Rutgers University
Fall 2015

Private networks
Connect multiple geographically-separated private subnetworks together

What's a tunnel?
Tunnel = Packet encapsulation
Treat an entire IP datagram as payload on the public network

Tunnel mode vs. transport mode
• Tunnel mode
  – Communication between gateways
  – Or a host-to-gateway
  – Entire datagram is encapsulated

  • Transport mode
  – Communication between hosts
  – IP header is not modified

IPsec
• Internet Protocol Security
• End-to-end solution at the IP layer
• Two protocols:
  – IPsec Authentication Header Protocol (AH)
  – IPsec Encapsulating Security Payload (ESP)

IPsec Authentication Header (AH)
• Ensures the integrity & authenticity of IP packets
  – Digital signature for the contents of the entire IP packet
  – Over unchangeable IP datagram fields (e.g., not TTL or fragmentation)

  • Protects
    – Tampering
    – Forging addresses
    – Replay attacks (signed sequence number in AH)
  • Directly on top of IP (protocol 51) – not UDP or TCP
**IPsec Encapsulating Security Payload (ESP)**

- Encrypts entire payload
  - Optional authentication of payload + IP header (everything AH does)

- Directly on top of IP (protocol 51) - not UDP or TCP

**TLS/SSL**

- Designed to operate at the transport layer
  - Application-to-application VPN
  - Public key authentication & key exchange; symmetric encryption
  - Provides applications with a socket interface

- SSL VPN
  - Can create host-host, host-to-network, or network-network connections

- SSL-based VPNs (e.g., OpenVPN)
  - authentication: pre-shared keys, certificates
  - Transport: UDP or TCP
  - Multiplex communication stream onto a single TCP or UDP port
  - Transport layer, so works through proxy servers and NAT environments

---

**The End**