CN414
Computer Network Security

Week 11:- IP Security (IPSEC), VPN

By

Dr. Piya Techateerawat

IPSEC & VPN

- **VPN**
- VPN Types
  - PPTP
  - L2TP
  - IPSec
  - SOCKS
- VPN Application

IPSEC & VPN

- Virtual Private Network
  - An implementation of encryption to secure connections on an untrusted network

IPSEC & VPN

- Encryption among the network
  - Node-to-Node Encryption
    - Referred as Link-to-Link encryption
    - Encrypted at Data link Layer
    - Decrypted before passing to network layer
    - Require decrypt and encrypt among network node
    - Require key management and compatible

IPSEC & VPN

- End-to-End Encryption
  - Encrypt at higher layer
  - Data can be encrypted along the transmission without concern the network requirement
  - Revealed more information
  - E.g. Encryption at transport layer (layer 4)
    - Intruder can trap sender receiver and protocol
    - Plus port number which can specify the nature of data
    - Port 25 should be SMTP email

IPSEC & VPN

- VPN
  - Creating secure connection on untrusted network
  - It can be called as “Tunneling”
  - It encapsulating or embedding one network protocol to be carried within the packets of a second network.
  - There are several VPN protocols
    - PPTP
    - L2TP
    - IPSEC
    - SOCKS

IPSEC & VPN

- VPN
- VPN Types
  - **PPTP**
  - L2TP
  - IPSec
  - SOCKS
- VPN Application

IPSEC & VPN

- PPTP (Point-to-Point Tunneling Protocol)
  - Using in Microsoft Windows NT
  - One of world wide early implemented
  - PPTP operates at the data link layer (layer 2)
  - Operating among windows machine
  - PPTP is the extension of PPP (Point-to-Point Protocol)
  - PPTP uses Microsoft's Point-to-Point encryption
    - E.g. CHAP (Microsoft Challenge Handshake Authentication Protocol) :- RSA's MD4

IPSEC & VPN

- To establish connection,
  - CHAP server sends a random challenge to client
  - client to encrypt the client's password
  - The password is return to the server to login the client
- Currently MD4 is claimed that can be broken
- So, it apply that protocol may not be secured.

IPSEC & VPN

- VPN
- VPN Types
  - PPTP
  - **L2TP**
  - IPSec
  - SOCKS
- VPN Application

IPSEC & VPN

- L2TP
  - Combined L2F (Cisco layer two forwarding) and PPTP.
  - It operates at layer 2 or data link layer
  - Therefore, all nodes must be L2TP compliant.

IPSEC & VPN

- **VPN**
- VPN Types
  - PPTP
  - L2TP
  - **IPSec**
  - SOCKS
- VPN Application

IPSEC & VPN

- IPSec
  - Secure exchange of packets at IP layer
  - IPSec operates at layer 3 and support 2 modes
    - Transport Mode
    - Tunnel Mode

IPSEC & VPN

- IPSec Transport Mode
  - Encrypts only the data of information portion of each IP Packet
  - Header is untouched
  - No Special set up is required
  - Sniffer cannot catch the payload but still able to observe the header

IPSEC & VPN

- IPSec Tunnel Mode
  - To encrypt the entire network for both header and payload
  - Receiving device must be IPSec-compliant
  - Tunnel mode is safeguards.
  - Sending and Receiving devices exchange a public key information.
  - This assist to authenticate and also using sender's digital certificate.
  - This Tunnel mode is considered more secure.

IPSEC & VPN

- VPN
- VPN Types
  - PPTP
  - L2TP
  - IPSec
  - **SOCKS**
- VPN Application

IPSEC & VPN

- SOCKS
  - IETF Protocol is designed for handling TCP traffic through proxy server.
    - SOCK4
    - SOCK5 - add security to authentication

IPSEC & VPN

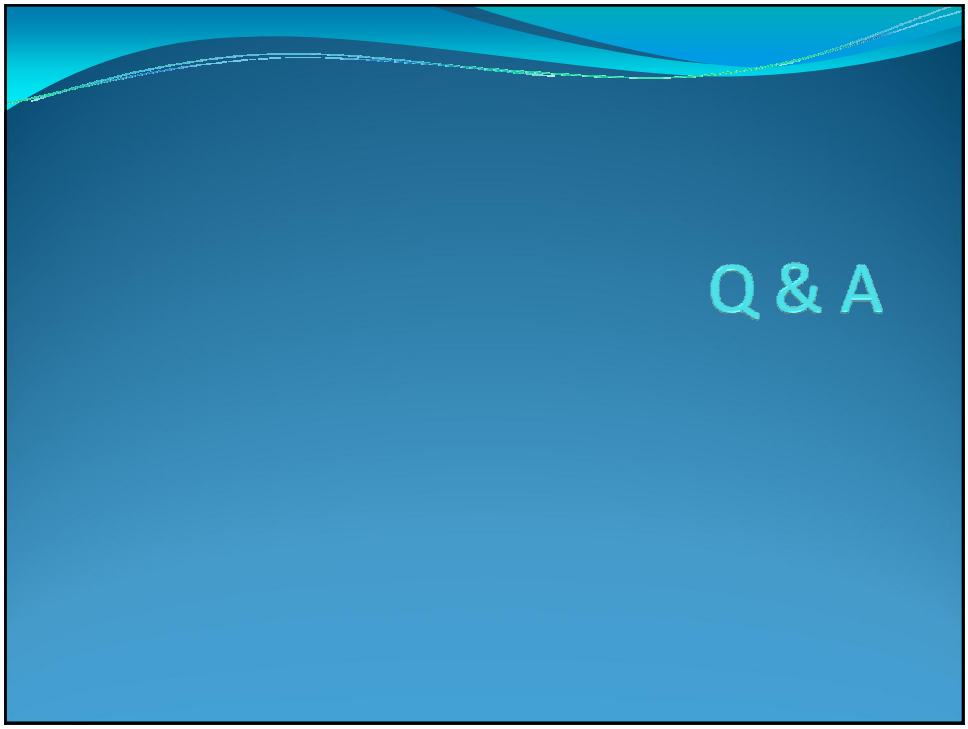
- VPN
- VPN Types
  - PPTP
  - L2TP
  - IPSec
  - SOCKS
- **VPN Application**

IPSEC & VPN

- Implementation & Example

Reference

- http://www.cisco.com/en/US/products/ps5743/Products_Sub_Category_Home.html


Q & A