Virtual Private Networks

Raj Jain

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/
Overview

- Types of VPNs
- When and why VPN?
- VPN Design Issues
- Security Issues
- VPN Examples: PPTP, L2TP, IPSec
What is a VPN?

- Private Network: Uses leased lines

- Virtual Private Network: Uses public Internet
Types of VPNs

- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers

Raj Jain
When to VPN?

- More Locations, Longer Distances, Less Bandwidth/site, QoS less critical
  \[\Rightarrow\] VPN more justifiable

- Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  \[\Rightarrow\] VPN less justifiable
VPN Design Issues

1. Security
2. Address Translation
3. Performance: Throughput, Load balancing (round-robin DNS), fragmentation
4. Bandwidth Management: RSVP
5. Availability: Good performance at all times
6. Scalability: Number of locations/Users
7. Interoperability: Among vendors, ISPs, customers (for extranets) ⇒ Standards Compatibility, With firewall
Design Issues (Cont)

8. Compression: Reduces bandwidth requirements
9. Manageability: SNMP, Browser based, Java based, centralized/distributed
10. Accounting, Auditing, and Alarming
11. Protocol Support: IP, non-IP (IPX)
12. Platform and O/S support: Windows, UNIX, MacOS, HP/Sun/Intel
13. Installation: Changes to desktop or backbone only
14. Legal: Exportability, Foreign Govt Restrictions, Key Management Infrastructure (KMI) initiative

⇒ Need key recovery
Security 101

- Integrity: Received = sent?
- Availability: Legal users should be able to use.
  Ping continuously ⇒ No useful work gets done.
- Confidentiality and Privacy:
  No snooping or wiretapping
- Authentication: You are who you say you are.
  A student at Dartmouth posing as a professor canceled the exam.
- Authorization = Access Control
  Only authorized users get to the data
Secret Key Encryption

- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)
Public Key Encryption

- Invented in 1975 by Diffie and Hellman
- Encrypted Message = Encrypt(Key1, Message)
- Message = Decrypt(Key2, Encrypted Message)
Public Key Encryption

- RSA: Encrypted_Message = m^3 \mod 187
- Message = Encrypted_Message^{107} \mod 187
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = 5^3 = 125
- Message = 125^{107} \mod 187
  = 125^{(64+32+8+2+1)} \mod 187
  = \{(125^{64} \mod 187)(125^{32} \mod 187)...(125^2 \mod 187)(125)\} \mod 187 = 5
- 125^4 \mod 187 = (125^2 \mod 187)^2 \mod 187
Public Key (Cont)

- One key is private and the other is public
- $\text{Message} = \text{Decrypt}(\text{Public\_Key}, \text{Encrypt}(\text{Private\_Key}, \text{Message}))$
- $\text{Message} = \text{Decrypt}(\text{Private\_Key}, \text{Encrypt}(\text{Public\_Key}, \text{Message}))$
Confidentiality

- User 1 to User 2:
  - Encrypted_Message = Encrypt(Public_Key2, Encrypt(Private_Key1, Message))
  - Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message))
  \[\Rightarrow\] Authentic and Private
Bastions overlook critical areas of defense, usually having stronger walls.

Inside users log on the Bastion Host and use outside services.

Later they pull the results inside.

One point of entry. Easier to manage security.
Proxy Servers

- Specialized server programs on bastion host
- Take user's request and forward them to real servers
- Take server's responses and forward them to users
- Enforce site security policy
  ⇒ May refuse certain requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost transparent
VPN Security Issues

- Authentication methods supported
- Encryption methods supported
- Key Management
- Data stream filtering for viruses, JAVA, active X
- Supported certificate authorities (X.509, Entrust, VeriSign)
- Encryption Layer: Datalink, network, session, application. Higher Layer $\Rightarrow$ More granular
- Granularity of Security: Departmental level, Application level, Role-based
Private Addresses

- 32-bit Address $\Rightarrow$ 4 Billion addresses max
- Subnetting $\Rightarrow$ Limit is much lower
- Shortage of IP address $\Rightarrow$ Private addresses
- Frequent ISP changes $\Rightarrow$ Private address
- Private $\Rightarrow$ Not usable on public Internet
- RFC 1918 lists such addresses for private use
- Prefix = 10/8, 172.16/12, 192.168/16
- Example: 10.207.37.234
- NAT = Network Address Translation
  Like Dynamic Host Configuration Protocol (DHCP)
- IP Gateway: Like Firewall
- Tunneling: Encapsulation
Tunnel

- Tunnel = Encapsulation
- Used whenever some feature is not supported in some part of the network, e.g., multicasting, mobile IP

Raj Jain
VPN Tunneling Protocols

- GRE: Generic Routing Encapsulation (RFC 1701/2)
- PPTP: Point-to-point Tunneling Protocol
- L2F: Layer 2 forwarding
- L2TP: Layer 2 Tunneling protocol
- ATMP: Ascend Tunnel Management Protocol
- DLSW: Data Link Switching (SNA over IP)
- IPSec: Secure IP
- Mobile IP: For Mobile users

Raj Jain
<table>
<thead>
<tr>
<th>Delivery Header</th>
<th>GRE Header</th>
<th>Payload</th>
</tr>
</thead>
</table>

- Generic Routing Encapsulation (RFC 1701/1702)
- Generic ⇒ X over Y for any X or Y
- Optional Checksum, Loose/strict Source Routing, Key
- Key is used to authenticate the source
- Over IPv4, GRE packets use a protocol type of 47
- Allows router visibility into application-level header
- Restricted to a single provider network ⇒ end-to-end
PPTP

- PPTP = Point-to-point Tunneling Protocol
- Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics
- PPTP server for NT4 and clients for NT/95/98
- MAC, WFW, Win 3.1 clients from Network Telesystems (nts.com)
PPTP Packets

Private Network → PPTP Server → Internet → Network Access Server → Client

Public IP Addressing

IP/IPX/NetBEUI
Data

Internal IP Addressing

IP/IPX/NetBEUI
Data

Encrypted

PPP
GRE
IP

PPP
GRE
IP

Raj Jain
L2TP

- Layer 2 Tunneling Protocol
- L2F = Layer 2 Forwarding (From CISCO)
- L2TP = L2F + PPTP
  - Combines the best features of L2F and PPTP
- Will be implemented in NT5
- Easy upgrade from L2F or PPTP
- Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
- Allows multiple (different QoS) tunnels between the same end-points. Better header compression. Supports flow control

Raj Jain
IPSec

- Secure IP: A series of proposals from IETF
- Separate Authentication and privacy
- Authentication Header (AH) ensures data integrity and authenticity
- Encapsulating Security Protocol (ESP) ensures privacy and integrity

<table>
<thead>
<tr>
<th>IP Header</th>
<th>AH</th>
<th>ESP</th>
<th>Original IP Header*</th>
<th>Original Data</th>
</tr>
</thead>
</table>

Authenticated

Encrypted

* Optional

Raj Jain
IPSec (Cont)

- Two Modes: Tunnel mode, Transport mode
- Tunnel Mode $\Rightarrow$ Original IP header encrypted
- Transport mode $\Rightarrow$ Original IP header removed. Only transport data encrypted.
- Supports a variety of encryption algorithms
- Better suited for WAN VPNs (vs Access VPNs)
- Little interest from Microsoft (vs L2TP)
- Most IPSec implementations support machine (vs user) certificates $\Rightarrow$ Any user can use the tunnel
- Needs more time for standardization than L2TP
Application Level Security

- Secure HTTP
- Secure MIME
- Secure Electronic Transaction (SET)
- Private Communications Technology (PCT)
VPN allows secure communication on the Internet

Three types: WAN, Access, Extranet

Key issues: address translation, security, performance

Layer 2 (PPTP, L2TP), Layer 3 (IPSec), Layer 5 (SOCKS), Layer 7 (Application level) VPNs

QoS is still an issue ⇒ MPLS
References

- For a detailed list of references, see
  [http://www.cse.ohio-state.edu/~jain/refs/refs_vpn.htm](http://www.cse.ohio-state.edu/~jain/refs/refs_vpn.htm)