Internet infrastructure

Virtual Private Networking

Prof. dr. ir. André Mariën
Virtual Private Network

• Why VPN?
  – Use of network with insufficient protection
  – To provide communication on top of another, untrusted, communication network
  – Cost reduction

• Supports one or more of the following:
  – Integrity
  – Authentication
  – Confidentiality
SLA issue

• Each connection point has an SLA with its ISP
• If there are different ISPs involved, traffic in between these runs over non-contracting parties
• In case of issues, who to contact, who to blame?
VPN uses

• Between organization entities
  – Maintain illusion of one network
  – Cost reduction compared to real private networks (leased lines)

• Between organization and individuals
  – Part of remote access solutions
  – “work as if in the office”
  – Risks:
    • physical security different (lower?)
    • social control different (absent?)
VPN uses: partner connections

• Incoming:
  – Service companies
  – Maintenance
  – Access: high risk (management and monitoring activities, configurations)

• Commercial
  – Suppliers (delivery)
  – Customers (orders)

• Integrated processes
  – Industry standard solutions
IPsec

• Architecture: RFC 2401

• What is IPSec? Two protocols:
  – Authentication Header (AH): RFC 2402
    • Integrity and authentication
  – Encapsulating Security Payload (ESP): RFC 2406
    • Integrity and confidentiality

• How does IPSec work? Two modes of operation:
  – transport mode: point-to-point
  – tunnel mode
## Modes of operation

<table>
<thead>
<tr>
<th>Normal IP packet</th>
<th>IP header</th>
<th>TCP header</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport mode packet</td>
<td>IP header</td>
<td>IPsec header</td>
<td>TCP header</td>
</tr>
<tr>
<td>Tunnel mode packet</td>
<td>IP header</td>
<td>IPsec header</td>
<td>IP header</td>
</tr>
</tbody>
</table>
Modes of operation

A authenticates towards K (IPsec A & K)
X authenticates towards Y (IPsec X & Y)
X protects communication from 10.3.4.* to 10.7.6.* (IPsec X & Y)
Security policy

• Defines security services for connections
• Starting point to negotiate the Security Associations
• Policy is defined by:
  – source & destination IP
  – DNS name
  – protocol
  – source & destination port (if applicable)
Security Association (SA)

• SA = communication parameter agreement
  – SA_{out}(A) = SA_{in}(B)
  – SA_{in}(A) = SA_{out}(B)

• ID: Security Parameter Index (SPI)

• Parameters: generic or protocol specific (AH/ESP)

• SA DataBase (SADB)

• SA management
Internet Key Exchange: IKE

• RFC 2409
• Diffie-Hellman key exchange
  – Exchange messages that allow both parties to compute shared secret
• Authentication include:
  – shared secret, ex: HMAC-SHA
  – DSA / RSA signatures
Generic Routing Encapsulation
Generic Routing Encapsulation (GRE)

- Need to encapsulate protocols in other protocols
  - Example: IPX over TCP/IP
  - Example: broadcast across a VPN tunnel
- Request for Comments: 2784
GRE encapsulation

• Original packet: payload packet
• Payload packet is wrapped with a GRE header
• Other protocol, carrier protocol, is used to deliver the packet
• Focus on IPv4 as carrier protocol
GRE packet

IP packet

GRE packet

Payload packet
(original)
Linear form with IPv4 carrier

- IP header
- GRE header
- payload
GRE header

- Protocol version; 0x800: IP
  - Note: IP protocol ID for GRE is 47
- Optional checksum
GRE usage

Route IP4&5 via IPL
Route IP1&2&3 via IPR
GRE + IPSec usage
GRE example: problem

10.1.1.5

10.1.1.6

Internet

?  

10.2.2.15

10.2.2.16
GRE example: configuration

GRE:
From: 10.1.1.0/24
To: 10.2.2.0/24
Via 112.7.44.1

GRE:
From: 10.2.2.0/24
To: 10.1.1.0/24
Via 212.5.4.1
GRE example: routing

```
10.2.2.0/24 gw 10.1.1.1
10.1.1.5

10.1.1.1

10.1.1.6
10.2.2.0/24 gw 10.1.1.1

10.2.2.1

Internet

212.5.4.1

112.7.44.1

10.1.1.0/24 gw 10.2.2.1

10.2.2.0/24 gw 10.1.1.1

10.1.1.0/24 gw 10.2.2.1

10.2.2.15

10.2.2.16
```
Other VPN: PPTP

• PPTP: point to point tunneling protocol
• Extension of PPTP to allow VPN
PPTP protocol tasks

• Queries the status of communications servers
• Provides in-band management
• Allocates channels and places outgoing calls
• Notifies server of incoming calls
• Transmits and receives user data with bidirectional flow control
• Notifies server of disconnected calls
• Assures data integrity
• Coordinating packet flow
### PPTP packets

<table>
<thead>
<tr>
<th>Ethernet addresses: mac from, mac to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip addresses: IP from, IP to</td>
</tr>
<tr>
<td>GRE information</td>
</tr>
<tr>
<td>PPP information</td>
</tr>
<tr>
<td>Tunneled data</td>
</tr>
</tbody>
</table>