Other VPNs

TLS/SSL, PPTP, L2TP
Overview

- Introduction to VPNs
  - Why using VPNs
  - What are VPNs
  - VPN technologies
  - ...

- TLS/SSL

- Layer 2 VPNs (PPTP, L2TP, L2TP/IPSec)
Why using VPNs?

- fast, secure and reliable connection between separated networks

- full access on resources from everywhere -> building a virtual local connection

- reasonable access: building connection only to local ISP
What are VPNs?

„A virtual private network is the extension of a private network that encompasses links across shared or public networks like the internet“

VPN technologies

- Secure VPNs
  - Networks that are constructed using encryption
  - IPSec, L2TP/IPSec, TLS/SSL

- Trusted VPNs
  - VPN customer trusted the VPN provider to maintain integrity of the circuits
  - Layer 2 frames over MPLS

- Hybrid VPNs
  - Combined use of secure & trusted VPNs
  - Secure parts controlled by customer or provider providing the trusted part
Common uses (1/3)

- Remote access
  - User-to-LAN connection
  - Dial-up to local ISP
  - Employee needs external access on corporate network
Common uses (2/3)

- Connecting networks over internet
  - Dedicated lines to connect a branch office to corporate LAN
  - Dial-up line to connect a branch office to corporate LAN
Common uses (3/3)

- Connecting computers over intranet

  - e.g. departments LAN physically disconnected from intranet because of very sensitive data
  - Connection via separated VPN server
VPN requirements

- User Authentication
- Address Management
- Data Encryption
- Key Management
- Multiprotocol support
Method for transferring data of a private network over a public network

Tunnel:
- Logical path through which encapsulated packets travel
Tunneling (2/3)

- Voluntary tunnel:
  - User or client computer is tunnel endpoint
  - Acts as tunnel client
Tunneling (3/3)

- Compulsory tunnel:
  - User or client computer is not tunnel endpoint
  - VPN-capable access server creates tunnel and is tunnel endpoint
Layer 2 VPNs - PPP

- Point-to-Point Protocol (PPP) [RFC 1661, RFC 2153]
  - Standard method for transporting multiprotocol datagrams over point-to-point links
  - Originally developed as encapsulation protocol for IP traffic
  - Protocol Structure:

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>8 bits</td>
</tr>
<tr>
<td>Address</td>
<td>12 bits</td>
</tr>
<tr>
<td>Control</td>
<td>24 bits</td>
</tr>
<tr>
<td>Protocol</td>
<td>40 bits</td>
</tr>
<tr>
<td>Information</td>
<td>Variable</td>
</tr>
<tr>
<td>FCS</td>
<td>16-32 bits</td>
</tr>
</tbody>
</table>

- **Flag** ... indicates beginning or end of frame (b^01111110)
- **Address** ... contains standard broadcast address
- **Control** ... calls for transmission in user data
- **Protocol** ... identifier for encapsulated protocol in information field
- **Information** ... datagram for protocol
- **FCS** ... Frame Check Sequence
Layer 2 VPNs – PPTP (1/4)

- Point-to-Point Tunneling Protocol (PPTP) [RFC 2637]
- Mainly implemented and used by Microsoft
- Extension of PPP
- Allows tunneling of PPP datagrams over IP networks
- Easy to use and to implement
- Use of 2 connections
  - Control connection
  - Tunnel connection
Layer 2 VPNs – PPTP (2/4)

- Protocol only implemented by PPTP-Access-Concentrator (PAC) and PPTP-Network-Server (PNS)
- Uses Generic Routing Encapsulation (GRE) to carry PPP packets
- Many sessions multiplexed on a single tunnel
Creating a tunnel:

1. Establishing control connection between PAC and PNS on port 1723
2. Exchanging information between PAC and PNS (e.g. encryption)
3. Establishing tunnel connection
Structure of PPTP packet:

PPP payload can be encrypted and/or compressed

GRE header contains information about tunnel protocol and encryption algorithm
Layer 2 VPNs – L2F (1/2)

- **Layer 2 Forwarding (L2F)**
  - Developed by CISCO
  - Allows multiple tunnels and multiple connections on every tunnel
  - Tunneling PPP and SLIP frames
  - Supports UDP, Frame Relay, X.25
Layer 2 VPNs – L2F (2/2)

- Establishing connection:
  1. Remote user initiates PPP connection to ISP
  2. ISP undertakes authentication via CHAP or PAP
  3. No tunnel exists:
     - Tunnel will be created
     Tunnel exists:
     - New multiplex ID will be allocated -> notification to home gateway
     - Home gateway accepts or declines new connection
Layer 2 VPNs – L2TP (1/2)

- Layer 2 Tunneling Protocol (L2TP) [RFC 2661]
- Combines best features of L2F and PPTP
- Uses UDP
- Can be transported over Frame Relay, ATM, X.25, ...
- Allows multiple tunnels with multiple sessions inside every tunnel
- Commonly used with IPSec -> L2TP/IPSec
Layer 2 VPNs – L2TP (2/2)

Structure of L2TP packet:

<table>
<thead>
<tr>
<th>IP header</th>
<th>UDP header</th>
<th>L2TP header</th>
<th>PPP header</th>
<th>PPP payload (IP datagram, IPX datagram, NetBEUI frame)</th>
</tr>
</thead>
</table>

- PPP frame
- L2TP frame
- UDP message

payload can be encrypted (IPSec ESP) and/or compressed
Layer 2 VPNs – L2TP/IPSec

- Uses IPSec Encapsulating Security Payload (ESP)
- Structure of encrypted packet:
## Layer 2 VPNs – L2TP/IPSec vs. PPTP

<table>
<thead>
<tr>
<th>PPTP</th>
<th>L2TP/IPSec</th>
</tr>
</thead>
<tbody>
<tr>
<td>- data encryption begins after PPP connection is established</td>
<td>- data encryption begins before connection is established by negotiating an IPSec Security Association (SA)</td>
</tr>
<tr>
<td>- use Microsoft Point-to-Point Encryption (MPPE) -&gt; stream cipher using RSA RC-4 (40, 56, 128 Bits)</td>
<td>- use Data Encryption Standard (DES) or 3-DES -&gt; block cipher (56 Bits)</td>
</tr>
<tr>
<td>- requires only user-level authentication</td>
<td>- user-level and computer-level authentication</td>
</tr>
<tr>
<td>- still implemented in Windows</td>
<td>- VPN Client software needed</td>
</tr>
</tbody>
</table>
SSL/TLS (1/6)

- Developed by Netscape, actual version SSL 3.0 -> basis for TLS 1.0

- Goals:
  - **Cryptographic security**: secure connection between two parties
  - **Interoperability**: independent programmers should be able to develop applications
  - **Extensibility**: encryption methods can be incorporated as necessary
  - **Relative efficiency**: reduced CPU usage by using session caching scheme
SSL/TLS (2/6)

- Uses certificates for identification
- Private key used to prove identity
- SSL server provides all encryption keys
- Originally for HTTP/Web applications
- Encryption implemented in all today's browsers -> millions of clients
SSL/TLS (3/6)

SSL between Application Layer and TCP/IP
SSL/TLS (4/6)

- SSL protocol stack:
  - Handshake, cipher change and alert protocol for establishing connection
  - Record protocol for encryption and integrity

<table>
<thead>
<tr>
<th>SSL handshake protocol</th>
<th>SSL cipher change protocol</th>
<th>SSL alert protocol</th>
<th>Application Protocol (eg. HTTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Record Protocol</td>
<td>TCP</td>
<td>IP</td>
<td></td>
</tr>
</tbody>
</table>
SSL/TLS (5/6)

- Handshake Protocol:

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Client hello</td>
<td>2. Server hello</td>
</tr>
<tr>
<td>11. Finished</td>
<td>12. Change cipher spec</td>
</tr>
<tr>
<td>14. Encrypted data</td>
<td>13. Finished</td>
</tr>
<tr>
<td></td>
<td>14. Encrypted data</td>
</tr>
</tbody>
</table>
SSL/TLS (6/6)

- Record protocol:
  - Fragment data
  - Encapsulate data with appropriate header
    - Primary data + padding + MAC
  - Encrypting data
    - e.g. DES, 3-DES, AES
  - Sending completed record
Bibliography

- WindowSecurity, Secure Socket Layer
  [http://www.windowsecurity.com/articles/Secure_Socket_Layer.html]
- Microsoft, Virtual Private Networking in Windows 2000
- Netscape, SSL Version 3.0 Draft
- NetworkDictionary, Protocols
  [http://www.networkdictionary.com/protocols]
- Virtual Private Network Consortium
  [http://www.vpnc.org]