Overview

- Definition of terms
- Remote access methods
- VPNs
  » More definitions of more terms
  » Tunneling and tunneling protocols
    • PPTP, L2F, L2TP, GRE
    • IPsec
- VPN products and services
Why Use the Internet?

- The Internet is a “network of networks”
- Primary application is to enhance inter-organizational communication
  - Collaboration
  - Publishing and research
  - Sales and commerce
  - Customer service
  - Training and education
“Intranet”

- Applies TCP/IP technology for intra-organizational communication
  - Internal corporate memos
  - Customer records
  - Faster access to employee programs, benefits, etc.
- Results in cost savings, better service

“Extranet”

Extranet = Internet + Intranet
What is an Extranet?

- Extranet = Internet + intranet
  » Intranet servers accessible via the Internet, with password and/or other authentication protection
- Extranets allow *some* users of the public Internet with access to intranet servers, e.g.:
  » Customer access to sales/product information
  » Employee access to corporate information, e-mail
  » Students access to their records, assignments, etc.

Remote Access Security

- Major issue for remote access security is the ability to control and monitor access to network resources by users employing many different access technologies
- AAA
  » Authentication
  » Authorization
  » Accounting
RADIUS

- Remote Authentication Dial In User Service
  » Provides centralized storage of all AAA information (Accounting optional)
  » Developed by Livingston (now part of Lucent)
  » RFC 2138, 2139
  » Authentication uses PAP or CHAP
  » Runs over UDP (auth/auth on port 1812, acct on port 1813)
- Widely-used industry de facto standard
CHAP

- User identification and authentication *without* sending password over the network (RFC 1994)

![Diagram of CHAP process]

Alternatives to Passwords

- Passwords are "what you know"
- Alternatives include
  - "What you have"
    - Tokens
    - One-time Passwords
  - "What you are"
    - Click rate
    - Biometrics: Retina scan, fingerprints, voice prints
TACACS/TACACS+

- Terminal Access Controller Access Control System
  - Developed by Cisco to control access to terminal servers
  - RFC 1492
  - Runs over TCP (port 49 or other configurable port), sometimes UDP (port 49)

Virtual Private Networks

- **VPN**: Establishing private connectivity over a public network
- **Internet-based VPN**: Secure transmission over the Internet where the security is implemented at the Network Layer (rather than at the application)
  - *virtual* = something you pay for... and don't get!
VPN Applications

- Cost savings
  - VPNs (and local ISPs) can replace dial-up servers and toll calls... and even frame relay
- Enhanced connectivity
  - Can economically provide global access
- Build partner networks/extranets
  - Uses global, internetwork infrastructure to replace private facilities

VPN Applications (cont.)

- Enhanced security
  - Can use network to authenticate users prior to connecting to servers/applications
- Enhanced protocol support
  - Internet only carries IP...
  - ...but IP can tunnel IPX, NetBEUI, DDP, and more!
What Are We Really Worried About?

**Tunneling vs. Encapsulation**

• Both use "enveloping" à la OSI but only encapsulation respects OSI layering

HTTP encapsulated in TCP

SPX/IPX tunneled in IP

HTTP
TCP
IP
PPP

SPX
IPX
PPP
GRE
IP
PPP
Tunneling Scenarios

- Client-initiated
  - User dials ISP, sets up tunnel to remote tunnel server (e.g., firewall, router, VPN server)
  - Requires VPN client software
  - Transparent to network
- NAS-initiated
  - User dials ISP, ISP's dial-server sets up tunnel
  - Transparent to client
  - *No encryption on the dial-up line*
Some Advantages of Tunneling

- Uses IP for multiprotocol encapsulation
- Supports additional applications without having to change firewall (*double-edged!*)
- Allows network-based authentication (e.g., WINS, NDS)
- Supports compression for improved thruput

VPN Protocols

- Lots of protocols to choose from...
  » Ascend Tunneling Management Protocol (ATMP)
  » Generic Routing Encapsulation (GRE)
  » Layer 2 Forwarding (L2F)
  » Layer 2 Tunneling Protocol (L2TP)
  » Point-to-Point Tunneling Protocol (PPTP)
  » Secure Tunnel Establishment Protocol (STEP)
PPTP

- Developed by PPTP Forum
  » Ascend, ECI, Microsoft, & 3Com
  » RFC 2637
- Uses PPP and GRE to route over the Internet
- PPTP offers encapsulation (GRE), authentication (CHAP), encryption (PPP), compression (PPP), and management

RAS

- Standard feature with Windows NT Server
  » Supports direct dial-up users and tunneling
  » Employs MS-PPTP for tunneling
  » Employs PAP or MS-CHAP for authentication
- Depends upon WINS
  » Client configuration required
  » Open many more vulnerable ports in the firewall to deal with NetBIOS!
Sidebar: MS-PPTP Security

• Several security problems with MS-PPTP
  » Keys are *effectively* less than 128 bits in length
  » Uses RAS "shared secret" encryption
    • Shared secret is the password hash, which is weak
  » Poorly designed control channel leaves server open to attack
  » Encryption can be disabled via the "You Are Now in France" attack

Sidebar: MS-CHAP

• Server sends 8-byte challenge
• Client creates two 24 byte responses, using LAN Mgr. hash and then WinNT hash each to derive 3 DES keys
• Server uses stored hashes to decrypt response

MS-CHAP has a number of potential vulnerabilities:
- Use of LANMAN hash
- *change password* flaw allowed access to hash

DUN 1.3 introduced MS-CHAPv2
Sidebar: MS-CHAPv2

- Available in DUN 1.3
- Improved many weaknesses in PPTP
- MS-CHAPv2
  - Authenticates both client and server
  - Does not use LANMAN hash
  - Fixed change password flaw
- New MPPE uses different keys in both directions
- Because backward compatibility is retained, a version rollback attack may be possible even if MS-CHAPv2 is used

L2F

- Developed by Cisco
  - Defined in RFC 2341
- Tunnels data in HDLC, PPP, or SLIP over UDP across the Internet
- Uses PAP or CHAP for authentication
L2TP

• Developed by IETF
  » Combines PPTP and L2F
• Uses PPP for encapsulation, authentication, compression, & management
• Uses IPsec for encryption

GRE

• IETF specification (RFC 1701) for multiprotocol encapsulation
  » Not a tunneling protocol, per se; offers no authentication, encryption, etc.
  » Usually deployed in conjunction with additional security mechanisms, such as IPsec
• Firewall friendly!
  » Runs over IP or UDP
IPsec

- Mechanism to provide information for data integrity, authentication, privacy, and nonrepudiation to IP
- Defined by the IETF, primarily for IPv6
  » RFCs 2401-2406
- IP Authentication Header (AH)
  » Provides integrity and authentication for IP packets using MD5 or SHA-1

IPsec (cont.)

- IP Encapsulating Security Payload (ESP)
  » Provides message integrity and privacy using MD5/SHA-1 and DES
  » Preferred industry direction
- Key management uses ISAKMP/Oakley or IKE
- VPNet Technologies' scheme forms IP Payload Compression Protocol (IPcomp)
- *IP-level security will not make firewalls obsolete*
Security Association

• An SA is a simplex logical connection between two communicating IP endpoints
  » SA provides security services to the traffic
  » Endpoint can be host or security gateway
• An SA is uniquely identified by:
  » Security Parameter Index (connection i.d.)
  » IP Destination Address
  » Security protocol (AH or ESP) i.d.

IP Authentication Header

• RFC 2402
• Uses IPv4 PID/IPv6 Next Header = 51
• AH data follows mandatory IPv4/IPv6 header and precedes higher layer (e.g., TCP, UDP) information
• Includes:
  » Anti-replay mechanism (sequence numbers)
  » Authentication using HMAC with MD5 (RFC 2403) or HMAC with SHA-1 (RFC 2404)
IP ESP

- RFC 2406
- Uses IPv4 PID/IPv6 Next Header = 50
- ESP must use HMAC with MD5/SHA-1 authentication (RFCs 2403/2404) and DES-CBC encryption (RFC 2405)

IPsec ESP Transport Mode

- Encrypts only data portion of tunneled IP packet
- May only be used host-host

Adapted from RFC 2406
IPsec ESP Tunnel Mode

- Encrypts entire IP packet
- Used between hosts and/or security gateways

![Diagram of IPsec ESP Tunnel Mode]

VPN Protocols Compared

- **PPTP**
  - Available from a variety of vendors
  - Most common version is MS-PPTP, used with RAS and available with all "modern" Windows systems, but has many security problems

- **L2TP**
  - Early deployment; part of IETF's security framework
  - Not yet seen in many products but support expected in Windows 2000

Adapted from RFC 2406
VPN Protocols Compared (cont.)

• IPsec
  » Large base of products
    • Axent, BSDI, Check Point, Cisco, Data Fellows, DEC, FTP Software, IBM, Intel, Linux, Lucent, Mentat, Microsoft, Nortel, Novell, Process, Sun, 3Com, TimeStep
  » Integral portion of IETF’s security framework
  » Robust, flexible, scalable, extendable!!
  » Long-term direction for mainstream VPNs

Lucent VPN Gateway (Hardware)

• Lucent VPN Gateway "brick"
  » Acts as IPsec tunnel endpoint for LAN-to-LAN or client-to-LAN communication
  » Bridge-like device; no network configuration required
  » 333 MHz Pentium II, 10/100-BASET
Lucent VPN Gateway (Software)

- Management Server
  » Provides Java-based GUI VPN management
  » Employs SSL, IKE with ISAKMP/Oakley key management
  » Runs on Windows NT or Sun Solaris, with Netscape Enterprise Server

- Lucent IPsec Client
  » Enables remote host to set up encrypted link to "brick" over IP
  » Uses IPsec with DES, 3DES, MD5, and SHA-1, and IKE key management
  » Runs on Windows 95/98, NT

VPN Hardware Vendors

- Altiga
- Aventail
- Cisco Systems
- Compatible Systems
- Data Fellows
- Effnet
- Extended Networks
- Indus River

- Lucent (Livingston)
- Nortel Networks
- Radguard
- RedCreek Communications
- 3Com
- TimeStep
- VPNet Technologies
- Xedia
VPN/Firewall Product Vendors

- Axent Technologies
- Check Point Software
- Cisco Systems
- FreeGate
- Internet Devices
- Lucent
- NetSceen Technologies
- Technologic
- WatchGuard Technologies

A VPN Can Also Be...

- A public network provider's offering
- Service options vary widely
  » Remote access services to corporate LAN via dedicated, managed network
  » Corporate intranet on provider's dedicated facilities, possible employing Internet tunneling
  » Extranet access via managed service
UUNET VPN Service

• UUNET
  » Extralink Remote: Remote access network service available in 1000 cities worldwide; client is authenticated and data is encrypted; data transported over a private (non-Internet) frame relay network to customer's intranet.
  » Extralink: Managed VPN for multiple corporate sites over private facilities; offers SLAs for network availability and latency

Bell Atlantic Managed VPN Service

• Managed dial-up
  » Access control via X.500 directory
  » DES/3DES encryption
  » SLA: 97% availability, 99% at 26.4 kbps

• Managed dedicated
  » IPsec-based, X.509 certificates, DES/3DES encryption
  » SLA: 99.9% availability of VPN equipment, network connectivity, local loop, and CPE
Other VPN Services

- @Home's @Work Remote
- AT&T's WorldNet VPN Service
- Concentric's Enterprise VPN, RemoteLink VPN, CustomLink VPN
- Frontier VPDN
- GTE's VPN Advantage
- MCI WorldCom Advanced Network Service
- Qwest's Remote Access VPN
- Sprint's Data VPN Service

Some References

- *Building and Managing Virtual Private Networks*, Kosiur (Wiley)
- Thomas Porter’s VPN Web Page
- *Extranet Strategist* (Aventail)
  - http://www.extranet-strategist.com
- comp.dcom.vpn Usenet list
- GCK’s pointers to VPNs (www.sover.net/~kessfam/gck/library/commcomp.html#vpn) and security
  (www.sover.net/~kessfam/gck/library/securityurl.html)
Questions? Comments? Queries?

Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple DES</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, authorization, accounting</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header (IPsec)</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output Interface</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher block chaining mode</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer premises (or provided) equipment</td>
</tr>
<tr>
<td>DDP</td>
<td>Datagram Delivery Protocol (Apple)</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DUN</td>
<td>Dial-Up Networking (MS)</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload (IPsec)</td>
</tr>
<tr>
<td>FR</td>
<td>Frame relay</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol (IETF)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (IETF)</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical user interface</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-level Data Link Control</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed message authentication code</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol (IETF)</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (IETF)</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol (IETF)</td>
</tr>
<tr>
<td>IPcomp</td>
<td>IP Payload Compression Protocol</td>
</tr>
<tr>
<td>IPer6</td>
<td>Internet Protocol version 4/6</td>
</tr>
<tr>
<td>IPX</td>
<td>Internet Protocol (IETF)</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol (IETF)</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>LANMAN</td>
<td>LAN Manager (MS)</td>
</tr>
<tr>
<td>L2F</td>
<td>Layer 2 Forwarding (Cisco)</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol (IETF)</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MPPE</td>
<td>Microsoft Point-to-Point Encryption</td>
</tr>
<tr>
<td>MS</td>
<td>Microsoft</td>
</tr>
<tr>
<td>NAS</td>
<td>Network access server</td>
</tr>
<tr>
<td>NDIS</td>
<td>Network Driver Interface Specification (MS/3Com)</td>
</tr>
<tr>
<td>NDS</td>
<td>NetWare Directory Service (Novell)</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>NetBIOS Extended User Interface (MS)</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network Basic Input/Output System (MS)</td>
</tr>
<tr>
<td>ODI</td>
<td>Open Data Link Interface (Novell)</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>PID</td>
<td>Protocol Identifier (IP)</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol (IETF)</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol (MS)</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service (MS)</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments (IETF)</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm (NIST)</td>
</tr>
<tr>
<td>SLA</td>
<td>Service level agreement</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial Line IP (IETF)</td>
</tr>
<tr>
<td>SPX</td>
<td>Sequenced Packet Exchange (NetWare)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer (Netscape)</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System plus</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol (IETF)</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol (IETF)</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual private network</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Internet Name Service (MS)</td>
</tr>
</tbody>
</table>