Securing Your Telecommuters and Mobile Users

Session SEC-222

Outline

- Who Are They?
- Securing Remote Connections
- Challenges
Who Are They?

Traditional Remote Access

- Network access servers
- ISDN/modem dialup

Individual Dialup
- Hotel Dialup
- Airport Dialup
- ISDN Router Dialup
- ISDN PRI
- 1-800
- PSTN
- Enterprise Network
Telecommuters

- Accessing the enterprise network from an individual PC or small LAN at an employee's home

- Individual Dialup
- Cable
- Always-On
- ISP POP
- Internet
- Enterprise Network

Road Warriors

- Accessing the enterprise network from mobile and/or temporary locations

- On-Site Consultant
- Hotel
- Dialup Always On
- ISP POP
- Internet
- Enterprise Network

- Airport
- Dialup Always On
Road Warriors on Steroids

- Accessing the enterprise network from mobile and/or temporary locations using wired and wireless

So What’s the Problem?

- Communications can be intercepted, modified, and hijacked
- Computers can be attacked, compromised, or stolen
- Corporate data can be accessed
Scenario One

- When you trust the local network (home/SOHO), own or control your computer
  - Dedicated line to the office (e.g., FR, ISDN)
  - Public ISP access
    - Dialup
    - Always on broadband (e.g., DSL and cable modem)

Scenario Two

- When you’re using your computer on a foreign network
- Using wireless on the home or office network
Scenario Three

• When you’re using a foreign computer on a foreign network (e.g., cyber café)

Basic Requirements

• Provide world-wide mobility securely
  Enforce strong user authentication
  Secure the corporate traffic across the Internet
• Protect mobile devices from hostile networks
• Protect corporate assets
Tool Kit

- Use IPsec
  - IPsec user authentication
  - Wildcard pre-shared keys or certification authority
  - Client or LAN initiated IPsec VPN
- Use Firewalls
  - Personal firewalls on the PC
  - Hardware firewalls
- User security practices

Tools

- IPsec
  - End to end
  - LAN to LAN
- Set up ssh before leaving home
Securing Remote Connections

IPsec

- IETF proposed standard to provide the following for IP packets
  - Authenticity
  - Integrity
  - Confidentiality
  - Replay detection
- Two major components
  - Internet Key Exchange (IKE)
    - Authentication between devices
  - IPsec
    - Packet headers to handle encrypted data
IPsec Phase 1: IPsec Main Mode Authentication

- Authenticates a device
  - Not the PC users!
- Authentication is based on one of the following:
  - IP address or fully qualified domain name (FQDN) and preshared key
  - IP address or FQDN and public/private key
  - Digital certificate
- Preshared or private keys are never transmitted
IPsec Phase 1: Weakening IKE Main Mode

- RFC 2409 requires a unique IP address to be associated with each pre-shared key
  This is for good security
  But prevents the use of dynamic IP addresses
  Hence cannot use a dial client

Weakening IKE (Cont.)

- It is possible to use the same preshared key for a large range of IP addresses
- The most unsecured would be to use the same password for all IP addresses:

```plaintext
crypto isakmp key sameFORall address 0.0.0.0 255.255.255.255
```
IPsec Phase 1 (optional): IPsec Extended Authentication

- Applies only to user authentication

IPsec User Authentication (xauth)

- Allows authenticating a user after authenticating the gateway (e.g. the PC)
- Provides good authentication where certificates cannot be used
- Solves the issue of not knowing the IP address in advance
IPsec Extended Authentication with Radius

- Crypto Map Is for Client Authentication
- Beware That If a Remote Router Tries to Connect It Might Refuse xauth and Therefore IPsec Will Not Come up

```
aaa new-model
aaa authentication login xauth
radius local
crypto map fubar client authentication list xauth
```

IPsec Phase 2: IPsec Quick Mode

- IPsec SA Policy Negotiation
- Encryption, Integrity
- Life Time, Proxy
- IPsec SA Established
Securing Remote Connections

- Three options
  - Use VPN client with xauth
  - Use a local VPN hardware
  - Use a local router for LAN to LAN VPN

- Internet traffic
  - All through the tunnel
  - Split tunneling

Home VPN Termination

- Using a PC connected to a public ISP is identical to using a foreign network such as is found in an Internet Café.
- For multiple home PC use a “VPN hardware client”
- For more complex scenarios, specifically dial, use a VPN router
Client Software

- VPN client software is a crucial component
  - Provides IPsec (or PPTP) encryption
  - Provides “dialer” interface to user to start VPN connections

Client Software

- Significant benefits in centralizing configuration and administration
  - Mobile users unlikely to be skilled
  - Microsoft clients are not centrally managed, and do not support VPN concentrator pushing policies to clients
  - Allows users to be configured and managed within logical groups
  - Also needs to be:
    - Easy to use, preconfigurable, updateable, etc.
When Do We Need The IPsec Client?

- Scenario 1: When you don’t trust the telecom provider or you’re really paranoid
- Scenario 2: Definitely need it to protect data from Internet sniffers
- Scenario 3: Good to have but you’ll have to download and install the client code:
  - Administrative access to the PC
  - Knowledge about the client configuration including gateway addresses, group information, etc.

Firewalls

- Personal firewalls
  - Road warriors on the road and at home
  - Relatively inexpensive
  - Requires some system administration skills

- Hardware firewalls
  - SOHO
  - Low end ones may need little or no configuration but have limited capability
  - More traditional ones are expensive but very flexible when protecting more than one host
**Example Firewall Configuration**

- **Assign a Security Level to Each Interface**
  - PIX Version 5.2(3)
  - nameif ethernet0 outside security0
  - nameif ethernet1 inside security100

- **Configure Interface Addresses**
  - ip address outside 200.1.1.2 255.255.255.252
  - ip address inside 192.168.1.1 255.255.255.0

- **Translate inside address to outside interface address**
  - global (outside) 1 interface
  - nat (inside) 1 0.0.0.0 0.0.0.0 0 0 0 0

- **List Inside Addresses to Be Translated**
  - route outside 0.0.0.0 0.0.0.0 200.1.1.1

- **Configure Static Routing**

---

**Where Do We Need These Firewalls**

- **Scenario 1:** No real need
- **Scenario 2:**
  - Definitely need personal firewall if ever connecting to foreign networks
  - Add hardware firewall for SOHO
- **Scenario 3:** Not under your control
User Practices

- Laptops are easy targets for thieves:
  - Don’t leave unattended
  - Use locks
  - Protect data through use of encryption
  - Don’t keep sensitive information on the disk if it isn’t needed
- Guard against lurkers who may be trying to read data from your display
  - Use screen locks
IR Ports

- Infrared ports have a range of 50cm to 100cm, but amplifying systems can increase the range threefold.
- Notsync is new software that can capture passwords off targeted Palm Pilots by taking advantage of the PDA’s hotsync function.
- Make sure your IR ports are not available to your neighbor when working in public places.
Complex Home Office Connections: ISDN

- Keep link down when no traffic!
- Dynamic addresses
- SA life time must be equal to connection duration
  
  Need to use IKE keep alive to reset SPI after ISDN went down
  
  IKE keep alive must not keep ISDN up and cannot be filtered
- Time source with digital certificates

Keep Alive for Dialup

- IKE must be able to trigger the link
- Keep Alive cannot be separated from other IKE packets
- Plain IKE Keep Alive will keep ISDN/DDR line up
- Work-around for negotiated address DDR
  
  The first packet of IKE phase 1 has a source IP address of 0.0.0.0
  
  All other IKE packets have a real IP address
IP address for the ISDN interface is allocated by ISP

Interesting traffic that can trigger dial is:
- Either first packet of IKE
- Or ESP encrypted data traffic

interface bri 0
ip address negotiated
dialer-group 1
!
dialer-list 1 protocol ip list 100
!
access-list 100 permit udp host 0.0.0.0 eq isakmp host 200.1.1.208 255.255.255.240 eq isakmp
access-list 100 permit esp any 200.1.1.208 255.255.255.240

IKE Keep Alive Details

Let's check my peer
My peer is working
Let's check my peer
My peer is working
I'm down...
Always 5 attempts

Let's reply to my peer
NB: my peer is working
Let's reply to my peer
NB: my peer is working
No news from my peer
Let's check my peer
Try again
Try again
Try again
Try again

!!! My peer is down/unreachable !!!!!!
Tear down IKE and IPsec SA.
New traffic will trigger re-negotiation
Other Issues with DDR

- Digital authentication (CERT) requires the router to know the date
- Must use NTP to re-sync after power cycle (some device don’t have permanent time)
- NTP cannot maintain the dial link up ==> use time-based ACL

Small Routers and CERTs

- Small routers have no clock and lose time on power reset/reload
- IOS checks its own X.509 certificates validity at start-up while the clock is still at 1993 => own certificate is rejected
- ==> work around is needed
Configure NTP over Dialup Interfaces

- Configure NTP
- Use time based ACL to define NTP as interesting traffic when year is 1993
- Denied NTP traffic to be encrypted
  - No need for confidentiality: UTC is public!
  - Integrity and authentication built-in NTP
- Store the router certificate on the CA (Cert will not be valid at start time)
  
  ```
  crypto ca certificate query
  ```

Time-Based ACL

```bash
interface bri 0
dialer-group 1
!
dialer-list 1 protocol ip list 101
!
no shutdown
!
time-range NTP_start-up end 12:00 1 January 2000
!
access-list 101 permit ip any time-range NTP_start-up
```

- At start-up, date is Jan 1st 1993
- NTP can trigger the ISDN link
- After 3 NTP packets the clock will be in sync and NTP won’t trigger ISDN again
Internet Traffic: Options and Trade-offs

- All traffic goes into the IPsec tunnel
  - Doubles traffic at Headquarters (gets in encrypted and out to the Internet)
  - Increase CPU impact
  - Single point of control
- Split tunneling
  - Corporate traffic goes into VPN, Internet traffic goes to local ISP
  - Home office may be used to redirect traffic into VPN

Split Tunneling

- VPN endpoints usually end up with Internet connectivity and VPN connection
- Potential backdoor around corporate firewall and introduces multiple enforcement points
- Particularly an issue with always-on broadband access (cable, DSL, etc.)
Split Tunneling Solutions

- Apply policy
  - Disable Internet access while VPN connection is active
  - Direct Internet traffic via HQ
  - Download ACL’s to client
- Integrated and low end firewalls
  - IOS Firewall, PIX 506, Hardware VPN client
- More powerful policy-based management
  - Cisco Security Policy Manager
- Personal firewall software
  - eg. Zone Alarm, Black Ice

NAT and IPsec VPNs

- IPsec is designed to detect attempts to modify packets
- Network Address Translation modifies IP packets
- Native IPsec cannot pass through a NAT operation that modifies TCP/UDP ports
NAT and IPsec VPNs Solution

- Many VPN solutions provide a “wrapper” option to make IPsec pass through a NAT process
- IPsec packets are wrapped in UDP (VPN 3000) or TCP (VPN 5000) headers to allow them to pass the NAT process

Human Factors

- There are limits on how much technology can do
- User must be aware that the environment may not be secure
  - Airport lounge, customer or client building
- The screen and disk contents of the PC may need to be secured in other ways
Summary

- Remote access VPN benefits
  - Reduced cost
  - Improved service
  - Expanded connectivity
- Standard IPsec needs user authentication
  - Range of client/tunneling solutions
- Users and managers need to be aware of implementation issues
  - Human factors, split tunneling, NAT
- Connecting to public broadband increases the need for personal firewalls

Securing Your Telecommuters and Mobile Users

Session SEC-222
Please Complete Your Evaluation Form

Session SEC-222