What are you trying to secure?

- Confidentiality
  - Avoid snooping
  - Encryption?
- Integrity
  - Deletes, changes
  - Backups
- Availability
  - (D)DoS attacks
- Authentication
  - Is that you?
- Nonrepudiation
  - No denying it
- Access control
  - Hands off!
- Reputation
  - Name = MUD
Internet security really bites

- LOTS of hosts are hard to secure
- Bad default configurations
- Poor software implementations
- Fixes/patches rarely applied
- Average user/admin is security clueless
- It is difficult to coordinate among sites
- Any weak link can break the security chain
Why doesn’t telco security bite?

Telco

- Central authority
- Network intelligence
- Billing records per call
- Legalese understood
- Wiretapping laws
- Circuit connections

Internet

- No central authority
- End host intelligence
- No packet accounting
- Legalese fuzzy
- Privacy issues
- Ease of anonymity
So where do you put security?
Physical security

• Trash bins
• Social engineering
  • It’s easier to trust a face/voice than a packet
• Protect from the whoops!
  • Don’t trip over the power cord
  • Don’t spill your coffee
  • Hit the right switch
  • Software really can kill hardware
End host security

- The end–to–end argument
- This is usually where the problem is
- But, ultimately you want to protect data
- End hosts are in control of data
- Users are in control of hosts
- Users often don’t secure hosts sufficiently
- There are LOT of hosts and LOTS of users
Network security

• Inspect and act on packets as they go
• Boy, this is really hard!
  • Evasive tactics like tunneling get through
  • Uh–oh... encryption
  • What am I breaking?
  • Can I relay, inspect and act fast enough?
• This might help, but it's not a panacea
Probably need layered defenses

• The *belt* and *suspenders* approach
• Attackers might hit a layer they can’t break
• Multiple layers tend to slow attacks down
• Use the laws of statistics
  • If defense A stops 90% of all attacks,
  • And if defense B stops 90% of all attacks,
  • Then combined they may stop 99% of all attacks
    • $(1-.9)*(1-.9) = .01, 1 - .01 = .99$ or 99%
The network is just a highway

- How do you secure the highway
- Police patrol
- Toll booths
- Licensed drivers
- Vehicle inspections and standards
- Rules of the road
- Are the highways completely safe now?
Perimeter security

- Separate trusted net from untrusted net
- Define the *boundary*
What network firewalls do

- Define untrusted and trusted boundaries
- Inspect traffic traversing firewall boundary
- Limit communication traversing boundary
- Help shield insecure hosts
Network firewalls illustrated
Key ideas

• Firewalls should be unnecessary
• They’re a network solution to a host problem
• They don’t solve the real problem and...
• ..make it hard/impossible to do certain things
• Ultimate control of hosts is out of our hands
• Securing a LOT of hosts is hard!
• But.. network solutions are *sigh* necessary
Packet filtering firewalls

- Filter everything – not very useful
- Filter by IP address
- Filter by application type (TCP, UDP)
- Filter on field/flag settings (source route)
- Filter invalid packets (SYN/FIN packets)
- Other pattern match
Screened subnet implementation
Application Layer Gateway (ALG)

- Also commonly called a proxy firewall
- These permit no direct communication
- Firewall intercepts all traffic in each direction
- Very intelligent device...
- ...must understand what a user is doing
- Difficult to install if it doesn’t currently exist
Proxy/ALG illustrated
Other common firewall features

- Stateful inspection
- Network address translation (NAT)
- Authentication (VPNs)
- Dynamic triggers
- Reporting, logging and IDS support
Example: Linux ipchains

Don’t want to see packets with private IP addresses

-A input -s 192.168.0.0/255.255.0.0 -d 0.0.0.0/0.0.0.0 -j DENY
-A input -s 172.0.0.0/255.240.0.0 -d 0.0.0.0/0.0.0.0 -j DENY
-A input -s 10.0.0.0/255.0.0.0 -d 0.0.0.0/0.0.0.0 -j DENY

Let SSH, established TCP connections, FTP data, UDP and BOOTP/DHCP in

-A input -s 0.0.0.0/0.0.0.0 -d a.b.c.d/255.255.255.255 22:22 -p 6 -j ACCEPT
-A input -s 0.0.0.0/0.0.0.0 -d a.b.c.d/255.255.255.255 1024:65535 -p 6 ! -y -j ACCEPT
-A input -s 0.0.0.0/0.0.0.0 20:20 -d 0.0.0.0/0.0.0.0 1024:65535 -p 6 -y -j ACCEPT
-A input -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 1024:65535 -p 17 -j ACCEPT
-A input -s 0.0.0.0/0.0.0.0 -d 0.0.0.0/0.0.0.0 67:67 -p 17 -j ACCEPT

Drop any packets that don’t have our source IP and log those attempts

-A output -s 140.192.0.1/255.255.255.255 -d 0.0.0.0/0.0.0.0 -j DENY -l
Example: Cisco ACL

Block private IP addresses

access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 172.0.0.0 0.15.255.255 any
access-list 100 deny ip 10.0.0.0 0.255.255.255 any

Block reserved, loopback and Class E IP addresses

access-list 100 deny ip 0.0.0.0 0.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any

Block source port of 111 from going anywhere

access-list 100 deny tcp any eq sunrpc any
access-list 100 deny udp any eq sunrpc any

Allow DNS and TELNET (log it) to 1.2.3.4, deny everything else

access-list 100 permit tcp any host 1.2.3.4 eq domain
access-list 100 permit tcp any host 1.2.3.5 eq telnet log
access-list 100 deny ip any any
What can’t a network firewall stop?

- Bad packets that look good
- Denial of service (DoS) attacks
  - Well, they can stop them at the firewall
  - But then the firewall has just been DoS’d
- Stupid user tricks
- Things that go around the firewall
- Things that don’t cross the firewall boundary
So you’re saying...?

- It would be nice if all hosts could be secured
- Network solutions can help
- Malicious insiders can get by anything you got
- A holistic approach is needed. Including:
  - Audits, detection and response
  - Education
  - Standards and best practices
Encryption or Fodszquijpo

• Try to make something readable, unreadable
• Usually math intensive
• Plain text to cipher text to plain text
• Need strong algorithms and secure keys
  • Public versus private keys
  • How do you exchange keys securely?
  • Key escrow, recovery and trusted 3rd parties
Shared secret key

- Each party knows the secret key
- The secret key decrypts the cipher text
  - Book = Ulysses
  - Key = 7, 23, 4
  - ...or page 7, line 23, word 4
- Ulysses is the secret key, don’t tell anyone!
- How do the trusted parties learn the key?
Shared secret key illustrated

My Plain Text Message → Algorithm → Message Sent Encrypted → Algorithm → My Plain Text Message

Our Private Key

Our Private Key
Public key cryptography

• Advertise your well known public key
  • Everyone uses it to encrypt messages to you
  • Once encrypted, no one can decrypt it
• Private key
  • Only you have the private key
  • Private key decrypts the public key encryption
• Keyrings and secure public key distribution
Public key illustrated
Pretty Good Privacy (PGP)

- Crypto software for mail, files and disks
- Uses public (and private) key technology
- Supports *digital signatures*
- Public key servers maintain public keys
- Free for non–commercial use
Many challenges and trade-offs
Sound like a host security problem? Yep.
Endpoints must be secure
Secure/encrypted tunnels between endpoints
Use Internet instead of building your own
Make an insecure public network secure

Virtual Private Networks (VPNs)
VPNs illustrated

Internet
What and Who is In Here?

You

DePaul Network

Internet
SECRET!

You
Potential VPN problem

Diagram showing the flow of data between DePaul Network, Internet, and a user's computer. The diagram illustrates a trust relationship and the potential for a bad guy to hack and gain unauthorized access.
IP Security (IPSec)

- Standardized by IETF
- Authentication Header (AH)
  - Authenticates sender and packet contents
- Encapsulating Security Payload (ESP)
  - Encrypts data before transmission
- Internet Key Exchange (IKE)
  - Governs exchange of keys between end hosts
- IPSec is often used in VPNs
Kerberos

- Popular for network based authentication
- Also for authorization
- Also used to encrypt network traffic
- Uses the concept of issuing *tickets* to users
- Uses centralized server for management
  - Must be secure of course!
- Been around for awhile, becoming popular
Network Address Translation

• Meant to be a IPv4 address depletion solution
• NAT is wrongly applied as a security solution
• Deployment of NAT has hurt the Internet
• Using NAT is expensive
• NAT breaks many things
• If you have addresses, don’t use NAT
• I don’t like NAT – can you tell?
NAT illustrated

10.20.15.63
Private intranet address

Source IP 10.20.15.63

Network Address Translation Table

New Source IP 1.2.3.4

Internet

10.20.15.63
Private intranet address

Source IP 10.20.15.63

Port Address Translation Table

New Shared Source IP Unique Source Port 1.2.3.4:39291

Internet
Enough already, how do we hack?

• We’ll focus on over the network attacks
• Password cracking
  • Brute force, keystroke capture, sniff
• OS/Application attacks
  • Buffer overflows, cgi–bin attacks, email exploits
• Protocol abuses
  • Spoofing, session hijacking, redirects
• Denial of service attacks
Anatomy of a typical compromise

- Do some reconnaissance work
- Remotely scan networks and hosts
- Launch the exploit
- Maintain compromised access with backdoors
- Fix system so no one else gets in
- Use/abuse system
- Make it look like you were never there
Network scanning/mapping

- PING
- DNS information
- `rpcinfo -p <hostname>`
- `nmap`
- `nbtstat`, `net use` commands
- Search the Internet for information on target
- If you’re on the Internet, you’ve been scanned
Session hijacking

• Pretend to be someone you’re not
• Take over or insert commands into a session
• You may to need to
  • Know IP addresses
  • Predict TCP sequence numbers
  • Keep one end of the real session busy
  • Run blind for awhile
Session hijacking illustrated
Password cracking

- Encrypted passwords can be broken
  - If nothing else, by brute force
  - Don’t let passwords be the only line of defense
- Sending logins in plain text over net is bad!
  - Many apps do this (e.g. FTP, TELNET)
  - Even HTTP!
- Things like kerberos, SSL and SSH help a lot
Viruses and worms

- Programs whose goal is to spread
- ...and possibly cause you a great deal of grief
- Worms are common (e.g. ILOVEYOU)
- Viruses infect other programs
- Somehow code has to be executed
  - Proves users are too trusting
  - Easy to use software becoming a problem
Weak input validation

• Buffer overflows and format string attacks
  • `strcpy(destvar, srcvar)` type of stuff
• Try to get your overflowed data to execute
• If program was running as root/Admin...
  • ...and you can successfully overflow a buffer...
• It’s probably *game over* for said system.
• Remote overflows are very possible/popular
Denial of service (DoS) attacks

- Prevents or impairs standard service
- SYN flooding
- SMURF attacks
- Distributed DoS attacks
- Source address spoofing helps attacker
- How to discern valid from DoS packets?
- No perfect solution exists today
DoS attack illustrated

ICMP Echo Request: 1.2.3.255
Spoofed Src IP: 2.3.4.5

Bad Guy: a.b.c.d

ICMP Echo Reply to 2.3.4.5
All hosts on 1.2.3.0/24 Respond!

Network: 1.2.3.0/24
DDoS attack illustrated
Partial (D)DoS solutions

- Gotta find the sources – not trivial if spoofed!
- Ingress/egress filtering
- ICMP traceback (itrace)
- Packet marking (pushback)
- Rate limiting
- Shunning and black hole routing
- Work with upstream provider
How do I secure Windows?

• `echo Y | del c:/*.*` Just kidding...
• Keep up to date on patches
  • Run Windows Update
• Remove unnecessary protocols like NETBIOS
• Be very wary of running unknown programs
• Do not use file/print sharing
• Install and use virus protection, security tools
How do I secure UNIX/Linux?

- Remove unnecessary services
  - Empty out inetd.conf if possible
  - Start removing rc.d scripts and programs
- Keep up to date on patches
- Avoid RPC, wu–ftpd, BIND, sendmail
  - And others that continue to have probs
- Use security tools
How do I secure network devices?

- Remove unnecessary services
- Disable IP source routing
- Disable directed broadcasts
- Install spoofing filters
- Put device IP on secured management net
- Secure routing protocols
- Keep up to date on system software
How do I secure ...?

- Web servers
- FTP servers
- Mail (SMTP/POP/IMAP) servers
- Printers, webcams, toasters
- Others...?
Any last bit of advice?

• Use Network Time Protocol (NTP)
• syslog like you’ve never syslog’d before
• SSH is your friend
• Learn and make use of perl
• Find a couple of good mailing lists/digests
• Monitor a few good security web sites
• Please do not attack DePaul’s network
References

http://networks.depaul.edu/security/
http://condor.depaul.edu/~jkristof/
news://news.depaul.edu/dpu.security
http://www.cert.org
http://www.sans.org
http://www.cerias.purdue.edu
http://www.neohapsis.com
http://www.securityfocus.com