
Introduction to Computer Security

Ellen Mitchell © 2003

<http://net.tamu.edu/~ellenm/papers/ics.ppt>
ellenm@net.tamu.edu

Ethics

- Use Your Power For Good
- Protect Free Speech
- Protect Privacy
- Make Sure You're Authorized
- Some Ethical Dilemmas

Topics

- Why care about security?
- What is computer security?
- Trends in attacks
- Securing your machine
- Securing your network
- Intrusion detection
- Responding to an incident

Why Care About Security?

The Internet—A Collection of Networks

- There are no standard policies
- There is no central control
- There is no central authority
- There are no common computer crime laws

Access Points

- In many schools/universities
- In most companies
- In almost all US cities
- In almost every country

If Compromised...

- Used as a launch pad for other attacks
- Liability
- Research stolen

Typical Computer Security Problems

- Exploiting known system vulnerabilities
- Exploiting known protocol vulnerabilities
- Sniffing of computer traffic/data
- Denial of Service attacks
- Spoofing IP source addresses
- Cracking weak passwords

Computer Users Unaware

- In 1998, an Incident Response Team reported that only 3% of the sites they attacked detected the attack. 97% of the sites never knew about the attacks.

Some Statistics...

- From the “2002 Computer Crime and Security Survey” by CSI (503 respondents)
(<http://www.gocsi.com/press/20020407.html>)
- 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- 80% acknowledged financial losses due to computer breaches.

...Statistics

- 44% (223 respondents) were willing and/or able to quantify their financial losses. (\$455,848,000.00)
- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- 34% reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Types of attacks

- 40% detected system penetration from the outside.
- 40% detected denial of service attacks.
- 78% detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- 85% detected computer viruses.

E-Commerce...

- 98% of respondents have WWW sites.
- 52% conduct electronic commerce on their sites.
- 38% suffered unauthorized access or misuse on their Web sites within the last twelve months.

...E-Commerce...

- 21% said that they didn't know if there had been unauthorized access or misuse.
- 25% of those acknowledging attacks reported from two to five incidents.
- 39% reported ten or more incidents.

...E-Commerce

- 70% of those attacked reported vandalism (only 64% in 2000).
- 55% reported denial of service (only 60% in 2000).
- 12% reported theft of transaction information.
- 6% reported financial fraud (only 3% in 2000).

Internal Attacks

- Disgruntled Employees
- Financial Problems
- Blackmail
- Robert Hanssen (spy)
- Corporate Raiders

Who Are These People?

- Hacker

- Tinkerer
- In-Depth Knowledge

- Cracker

- Unauthorized Access

- Script Kiddies

- No real understanding of what they're doing

Motivation

- Learn
- Prestige
- Fame
- Money
- Fun

What is Computer Security?

- Security is a Process
 - Can't set it up once and go away
- The Inverse of Convenience
- Best Implemented in Layers

Goals of Security

- Confidentiality
- Integrity
- Availability

Security Policies

Why Does A Site Need Policies?

- Promote user awareness
- Reduce security incidents
- Handle incidents more effectively

Policy Areas

- Authentication
- Authorization
- Privacy
- Acceptable use
- Computer security incidents

Security Policies...

- What is Allowed?
- What is Prohibited?
- Is the Policy Published?
- Is the Policy Legal?
 - First Amendment right in companies

...Security Policies

- Is the Policy Enforced?
- Who Interprets Policy when Questions Arise?
- RFC #2196 -- Site Security Policy
- (Request For Comments,
www.ietf.org/rfc.html)

Acceptable Use Policies

- RFC2196 addresses:
 - ❑ Account sharing
 - ❑ Password selection
 - ❑ Accessing files not owned by the user
 - ❑ Breaking into other accounts/systems
 - ❑ Disruption of service

Policies for System Administrators

- A system administrator has access to e-mail, files, and network traffic in the normal course of business.
- Under what circumstances may a system administrator
 - ❑ Access users' data
 - ❑ Create new accounts
 - ❑ Shutdown a service

Policy Violations

- Violations must be documented
- Policies must be enforced
- Enforcement must be enforced

Guidelines for the Secure Operation of the Internet

- RFC1281
 - Vendor and User responsibilities

Trends: Biggest Threats

- Viruses, Worms, Trojans, BackDoors
- Web Server Vulnerabilities!
- Plaintext traffic/sniffing
- Denial of Service Attacks
- Others

Viruses, Worms, Trojans, and Backdoors

Why Care About These?

- Viruses can not only mail out documents, they scan address books and *documents* for e-mail addresses
- This can cause embarrassing situations
- They can create a Denial-of-Service Attack against your own network

Virus

- Self-replicating code
 - Infects a host program
 - Runs when that program executes
 - “Sircam” is an example
 - Spreads through network shares and e-mail
 - ✓ I send you this file in order to have your advice
 - ✓ I hope you can help me with this file that I send
 - ✓ I hope you like the file that I sendo you
 - ✓ This is the file with the information that you ask for
-

Virus Countermeasures

- Run anti-virus software
- Virus Checkers are USELESS if Signatures Aren't Kept Up To Date
- C, Scripts, VisualBasic
- There are Virus Creation Kits
- Exploit User's Trust—Educate users
 - Don't open attachments unless they are expected
 - Do not "hide extensions"
- Upgrade Outlook Explorer

Anti-Virus Software

- “If you can afford \$3,000.00 for a computer, you can afford \$30 for anti-virus software.”
- AVG AntiVirus:
http://www.grisoft.com/html/us_index.htm
- Trend Antivirus:
http://housecall.antivirus.com/pc_housecall/
- AntiVir Personal Edition: <http://www.free-av.com/>
- Panda's ActiveScan:
<http://www.pandasoftware.com/activescan/>

Worms

- Independent Program
- Copies Itself To Other Computers
- “Morris Worm” of 1988
- Moves on its Own

Code Red Worm

- “Code Red” is an example
 - IIS Indexing Server Vulnerability
- Welcome to [http:// www.worm.com](http://www.worm.com) !
- Hacked By Chinese!
- Tried to DOS whitehouse.gov
- Caused DOS for many sites

Trojans

- Useful program with a hidden agenda
- Usually “attractive”

What is a Backdoor?

- Another (unauthorized) way in, usually giving root/Administrator access
- Allows you to come back in if original entry-way is removed
- Backdoor “goals”
 - ❑ Insert backdoor
 - ❑ Backdoor remains undetected

Backdoors

- Back Orifice (UDP 31337)
- NetBus (TCP 12345)
- rootkits
- MANY others

Remaining undetected...

- Make the backdoor look like it belongs
 - Create and install documentation for it
 - BoSniffer
 - Rename to something familiar
- Hide the backdoor
 - /dev, /var/tmp/X,

...Remaining undetected...

- ..., .profile
- Make sure nothing is logged, delete log entries
- Decoy “footprints”
- Timestamps
 - touch

...Remaining undetected

- Cryptographic hashes
 - md5
- Login records (utmp/wtmp)

Web Server Vulnerabilities!

Web Security

- old, bad cgi-bin scripts distributed with servers
- Do not allow users to submit any input
 - `user input ; some bad command`
- Secure Socket Layer (SSL) for encryption
- Protect files with user name/passwords
- Look for “padlock” on your browser during sensitive transactions

Web Page Defacement

- RameN
- <http://www.attrition.org/>
- UDP flood attacks
- CERT Incident Note IN-99-07

IIS hints

- “IIS lockdown tool”
- Remove “unused mappings”
- Remove sample programs
- Consider replacing with Apache

Securing FrontPage

- http://office.microsoft.com/assistance/2002/articles/fp_collearningactivities.aspx

Plaintext Traffic/Sniffing

- Sniffing tools freely available
- Need to protect wireless users

Denial of Service Attacks

- Define Denial of Service (DOS)
- Describe Objectives of a DOS attack
- Host based, Network based attacks
- Why Worry About DOS?
- Liability
- Some DOS Attacks

Service

- Exhaustible resource
 - disk
 - cpu
 - memory
 - bandwidth
 - application resource
 - tcp stack
 - web connections

Objectives of DOS Attack

- Hide something else that is going on
- “Punish” company
- ...Could be unintentional

Host Based Attacks

- Unix fork()
- Fill up disk (mail bomb, etc.)
- Echo/chargen
- ...Can be accidental

Network Based Attacks

- Bandwidth
- Too-large ICMP packet panics kernel
- echo/chargen

Why Worry About DOS?

- “Agents” on your host could be used in a D-DOS against a company with lawyers better than yours

Liability

- Unknown at this time
- ...but probably something to worry about

Ping of Death

- Large ICMP packets crash Operating Systems
- <http://www.insecure.org/spl0its/ping-o-death.html>

Teardrop

- TCP sequence numbers overlap, can crash server

Land Attack

- Source and Destination addresses are the same -- can crash server

DNS Vulnerabilities

- Poisoned entries
- Names removed -- emory.edu, mindspring, colorado.edu, exodus.net, sprynet
- Misconfigurations/Poor Architecture

Syn Attack

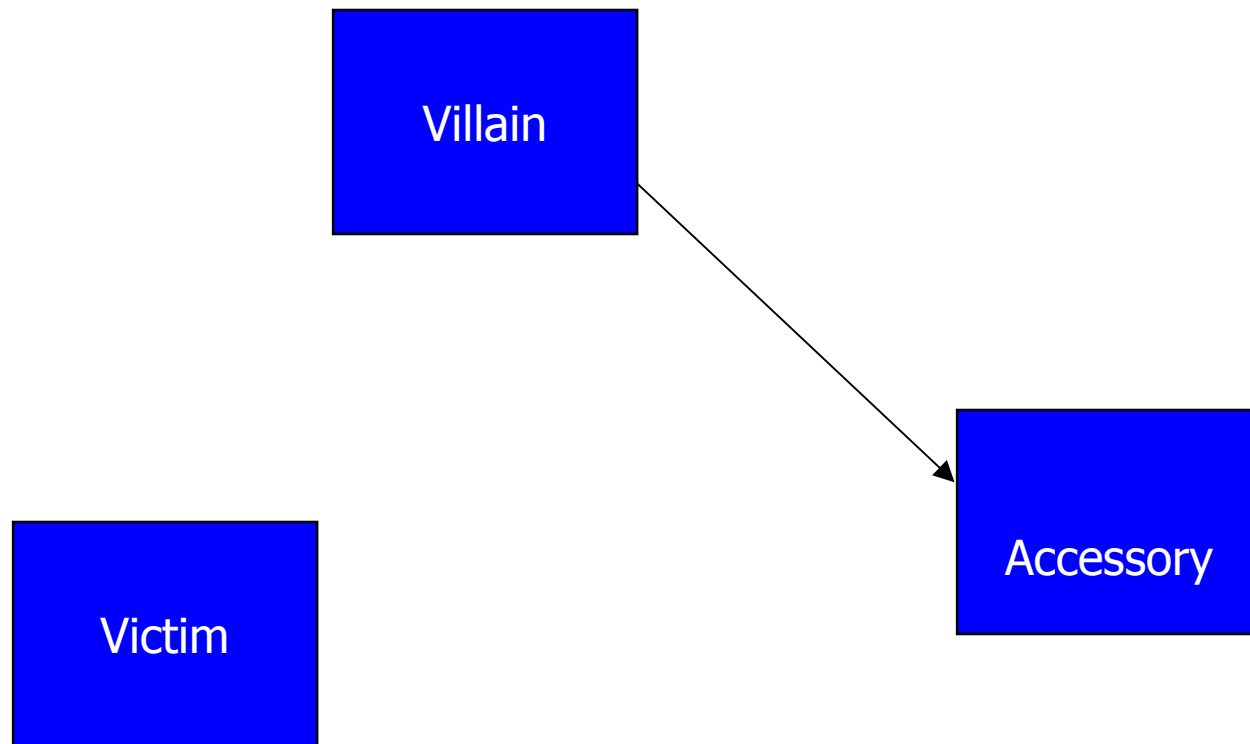
- Three-way handshake...
- Can use up resources

Smurf Attack

- Spoofed ICMP packets sent to broadcast address of network
- Replies pound the spoofed victim

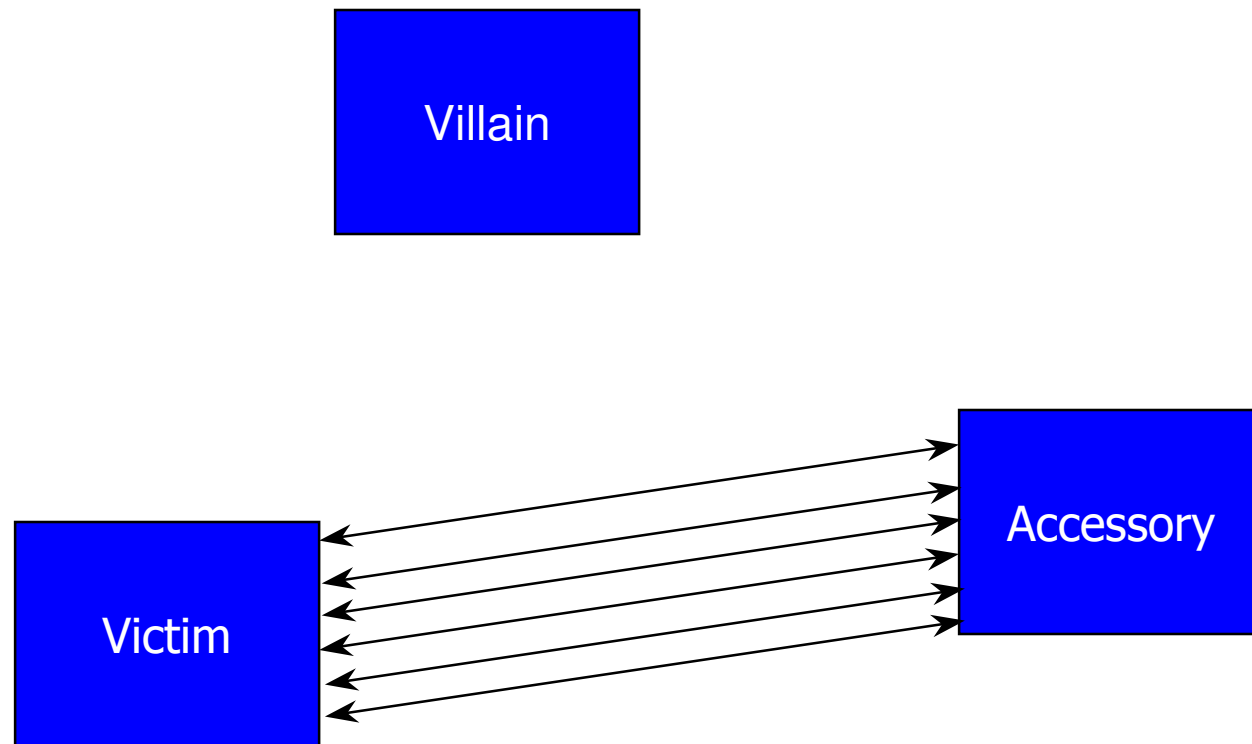
Smurf Attack

- Sends forged ping request to accessory



Smurf Attack

- Replies are sent to victim



Trin00/Tribal Flood

- “slave” compromised hosts respond to directions of master

Trin00

- Distributed SYN DOS attack
- 27665 TCP Intruder to Master
- 27444 UDP Master to Daemon
- 31335 UDP Daemon to Master

Apache DOS

- *//////////*
- $v < 1.2.5$

Preventing a DOS Attack...

- Configure routers to reject directed broadcasts
 - RFC2644
- Ingress/egress packet filtering
 - RFC2267
- Distribute services over multiple machines

...Preventing a DOS Attack

- Keep up to date with patches
- Become familiar with your service provider and know how to contact them in an emergency

Responding to a DOS Attack

- May require coordinated effort because of spoofed addresses
- May need to inspect each router interface
- Operating Systems tend to deal with issues, Network just passes traffic

Other Attacks

Buffer Overflows

- Dependent Upon Host Architecture
- Assembly Language Instructions
- Software bug, usually quickly fixable

Social Engineering...

- “Shoulder surfing”
- Manipulation
 - rebooting a machine
- Faked e-mail

...Social Engineering

- Dumpster diving
- Gullibility
- ...User Education
- It's amazing what you can get away with if you are brazen enough

Spoofing Packets

- Masquerading as another host
- Requires root-level access or promiscuous mode
- Tools available to make this easier
- http://www.nessus.org/doc/nasl2_reference.pdf

Securing Your Machine

“That which can’t be detected
should be prevented; That
which can’t be prevented
should be detected...”

Prevention

User Education

- Train your users not to open attachments they are not expecting
- Even if they are from your
 - Mom
 - Sister
 - Friend from high school
 - CEO

Remove Unnecessary Services

- Many computers come with software pre-installed, running at system boot-up time
 - Sendmail
 - IIS
- Remove demo software
 - IIS/Apache sample scripts
- Change software passwords from default
 - Microsoft's MSSQL sa account
 - http://www.iss.net/security_center/static/1459.php

Tighten Things Up Some More

- Turn off shares if unneeded
- Disable bindings for unused protocols
- Remove setuid permissions from Unix files if possible

Choose Better Services

- Ssh instead of telnet
 - www.ssh.org
 - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
 - Tip: “run from current location” or “open file”
- Scp or sftp instead of ftp
 - <http://winscp.vse.cz/eng/>
- Apache instead of IIS

Secure the Remaining Services

- [Windowsupdate.microsoft.com](https://windowsupdate.microsoft.com)
- https instead of http
- Subscribe to software mailing list for updates
- Virtual Private Networks (VPN)

User Accounts...

- ❑ Know what they do
- ❑ Watch your log files
- ❑ Use groups and access control
- ❑ Users should have only the permissions necessary to perform their job

...User Accounts

- ❑ Educate users so that privileged access is used only as necessary (don't read news as Administrator/root, for example)
- ❑ Remove accounts when employees leave
- ❑ Remove “guest” and service accounts that may come with the operating system

Use Good Passwords...

- ❑ Don't use words from the dictionary
- ❑ Don't use names of pets, children, family members
- ❑ Do not write down, e-mail, or tell anyone your password
- ❑ Improve your password by including non-alphanumeric characters (#\$,) and mixed case

...Use Good Passwords

- ❑ Do use a password cracker periodically
- ❑ Windows:
 - L0phtcrack (commercial, <http://www.atstake.com/>)
- ❑ Unix:
 - Crack (free, <http://www.crypticide.org/users/alecm/>)
- ❑ Windows or Unix:
 - John the Ripper (free, <http://www.openwall.com/john/>)

Configure Good Logging

- Event logs
- Log Access and Applications
- Automatically Digitally Sign Your Log Files
- Read-Only Logs
 - Log Host
 - CDROM or printer

Obtaining More Logs

- www.snort.com
- Firewalls
- Intrusion Detection Systems

Software to Manage Log Files

■ Read & Rotate

- ❑ Logcheck/logsentry (www.psionic.com)
- ❑ SI2 (<http://www.ip-solutions.net/syslog-ng/>)
- ❑ swatch (swatch.sourceforge.net)
- ❑ Logrotate
- ❑ Kiwi syslog for Windows
(http://www.kiwisyslog.com/info_syslog.htm)

Network Time Protocol (NTP)

- Synchronizes the time on your computer to a known good source
- <http://bigben.stanford.edu/LabSuite/>
- www.ntp.org

Host Audits

- Integrity Checkers
 - www.tripwiresecurity.com

Port Scans...

- Why scan?
- Who scans?
- Scanners
 - www.nessus.org
 - www.nmap.org

...Port Scans

- Scan all hosts looking for one service
- Scan one host looking for any vulnerabilities
- “Stealth Scans”

Encryption

- IPsec
- Virtual Private Networks (VPN)
- Secure Shell (ssh)
- Secure Socket Layer (ssl)

IPsec

- Originally for IPv6, but available in IPv4
- VPN
 - Encrypt (ESP)
 - Authenticate (AH)
 - Or Both
- IPsec implementation required for IPv6

VPN

- Provides Encryption and Authentication
- Point to Point Network Connections
- Host to Network Connections

SSL

- Can be used to protect information sent to/from web pages
- Can “wrap” other insecure applications

Kerberos

- Provides Authentication and Authorization
- Ticket-Based
- Windows 2000 and Active Directory

Backups

- Can't *prevent* intrusion
- Can be used for comparison and restore

Communication

- You need to know who makes changes to your system and why
- You need to understand what is running on your system

Securing Your Network

Services

- Distribute services over multiple machines to reduce single point of failure possibility

Network Equipment

- Repeaters, Switches, Hubs, Routers
 - Eavesdrop prevention
 - Filtering Rules
 - Lock MAC address to a port
 - MAC layer authentication (authenticated VLANs)
- Multi-User Hosts
- Firewalls

Reviewing The Basics...

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
 - Stream oriented, reliable way to transmit data
 - Used for applications such as mail, web, pop, FTP

...Basics...

- User Datagram Protocol (UDP)
 - Packet oriented
 - Used for applications such as Domain Name Service (DNS)
 - Is easier to “spoof” than TCP because of the weak authentication

...Basics

- Internet Control Message Protocol (ICMP)
 - Used for diagnostics and network operation
 - “Ping”

IP versions...

■ IPv4

- IP version 4 is most commonly used in the United States
- `nnn.nnn.nnn.nnn`

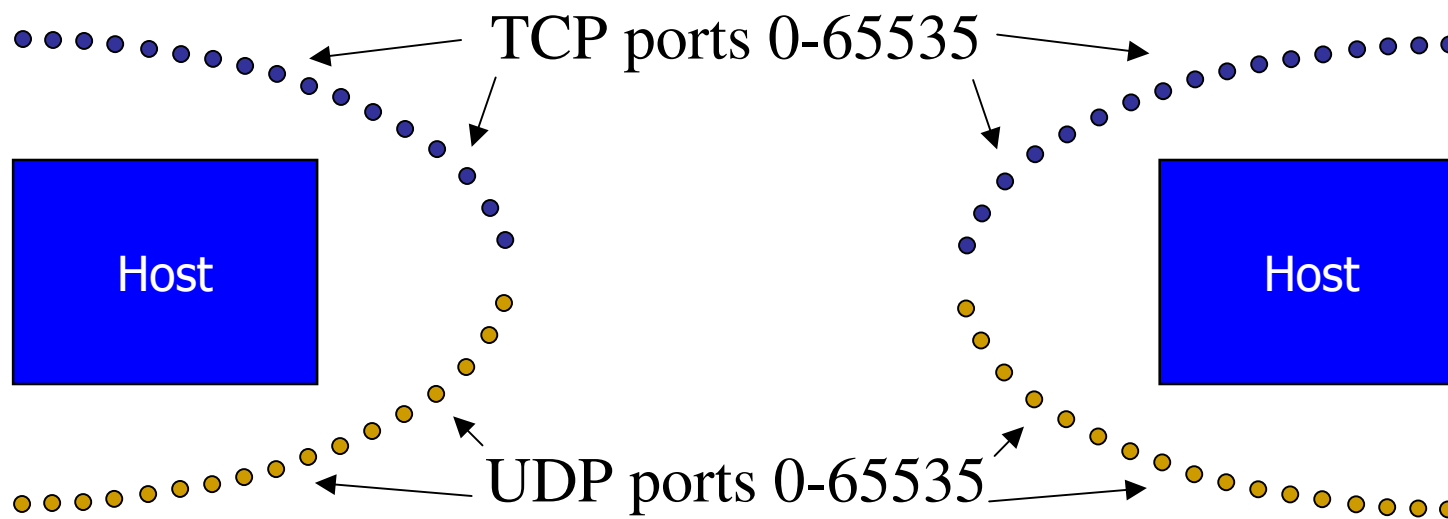
■ IPv6

- `www.ipv6.org`
- IPv6 invented to address shortage of IP addresses
- `nnnn:nnnn:nnnn:nnnn:nnnn`

Important Data

- Source IP address (or host name)
- Destination IP address (or host name)
- Source Port
- Destination Port
- TCP or UDP (or ICMP)
- Date and Time (and Time Zone)
- TCP Sequence Numbers

TCP/UDP ports



A Few Words About Port Numbers...

- Agreed-Upon Ports for Internet Communications
 - “Well-Known” are 0-1023
 - “Registered” are 1024-49151
 - “Dynamic and/or Private” are 49152-65535

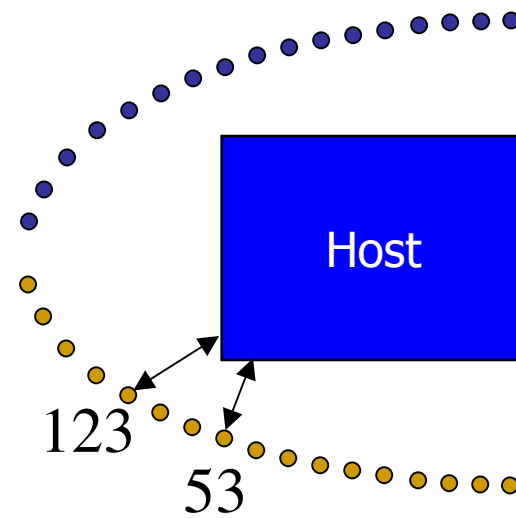
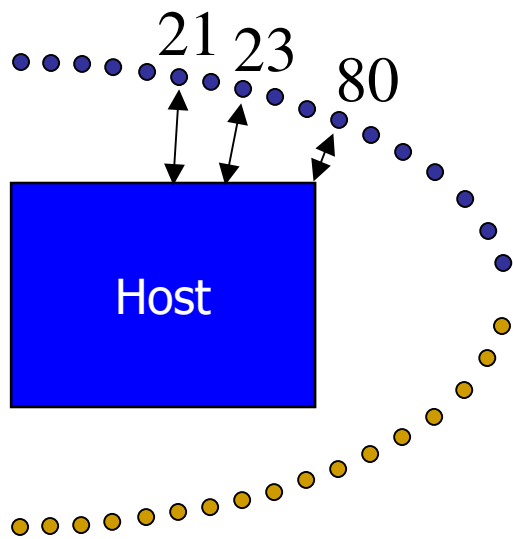
...Port Numbers

- Process For Registering Ports
- Database on Internet
- <http://www.iana.org/assignments/port-numbers>
- Internet Assigned Numbers Authority

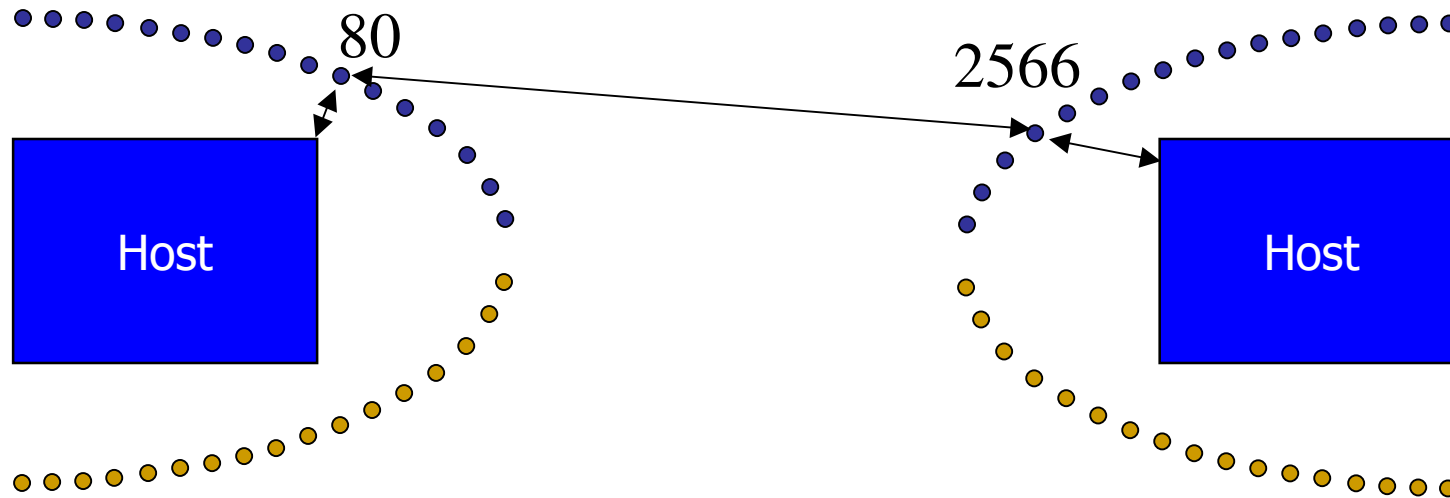
Example Applications

- NTP -- UDP port 123
- SMTP -- TCP port 25
- HTTP -- TCP port 80
- DNS -- UDP 53/TCP 53

Running Services



Sample Session



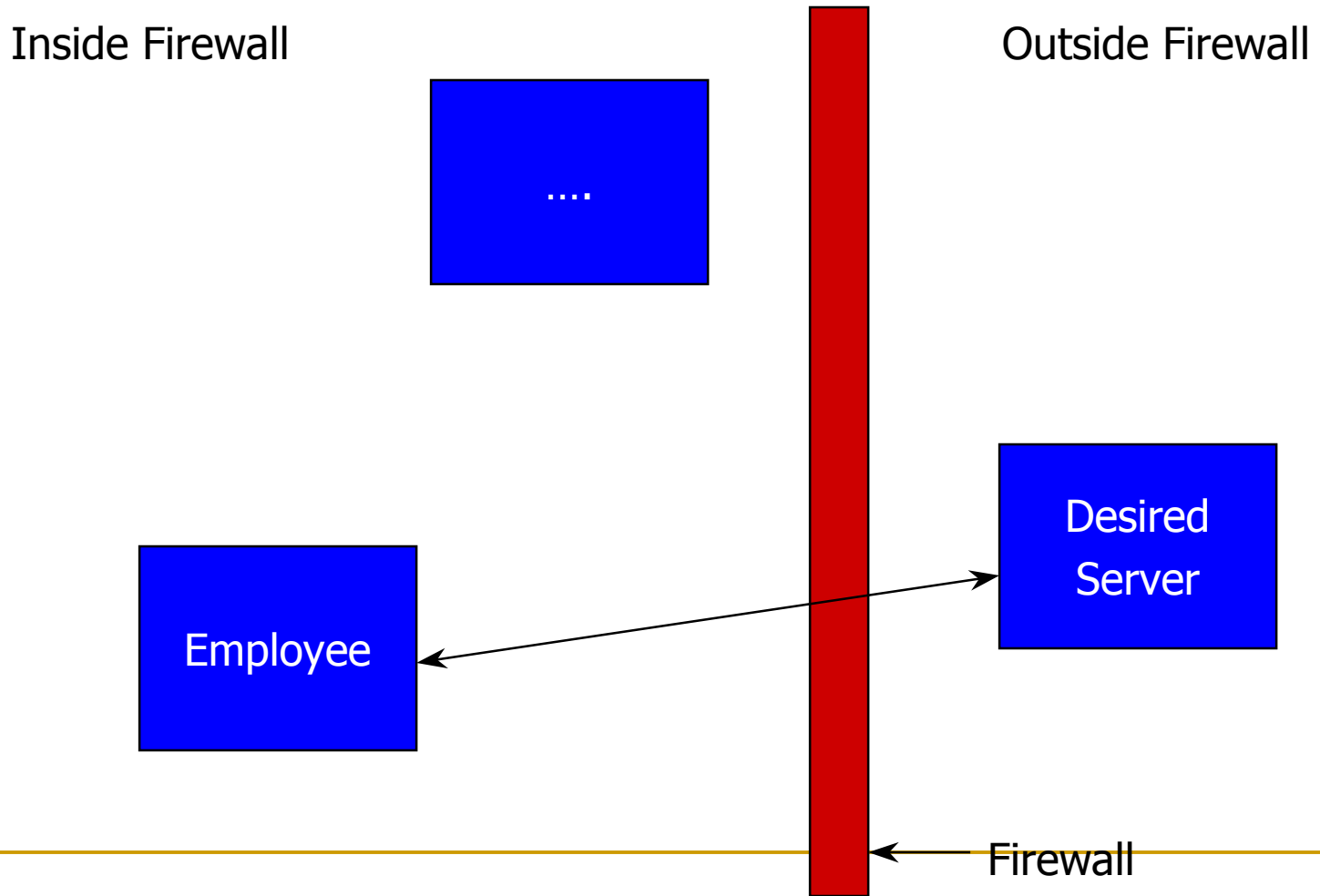
Wrappers and Firewalls

- Permit or Deny Access to Services
- Security “Stances”
 - Deny-Based (closed by default)
 - Allow-Based (open by default)

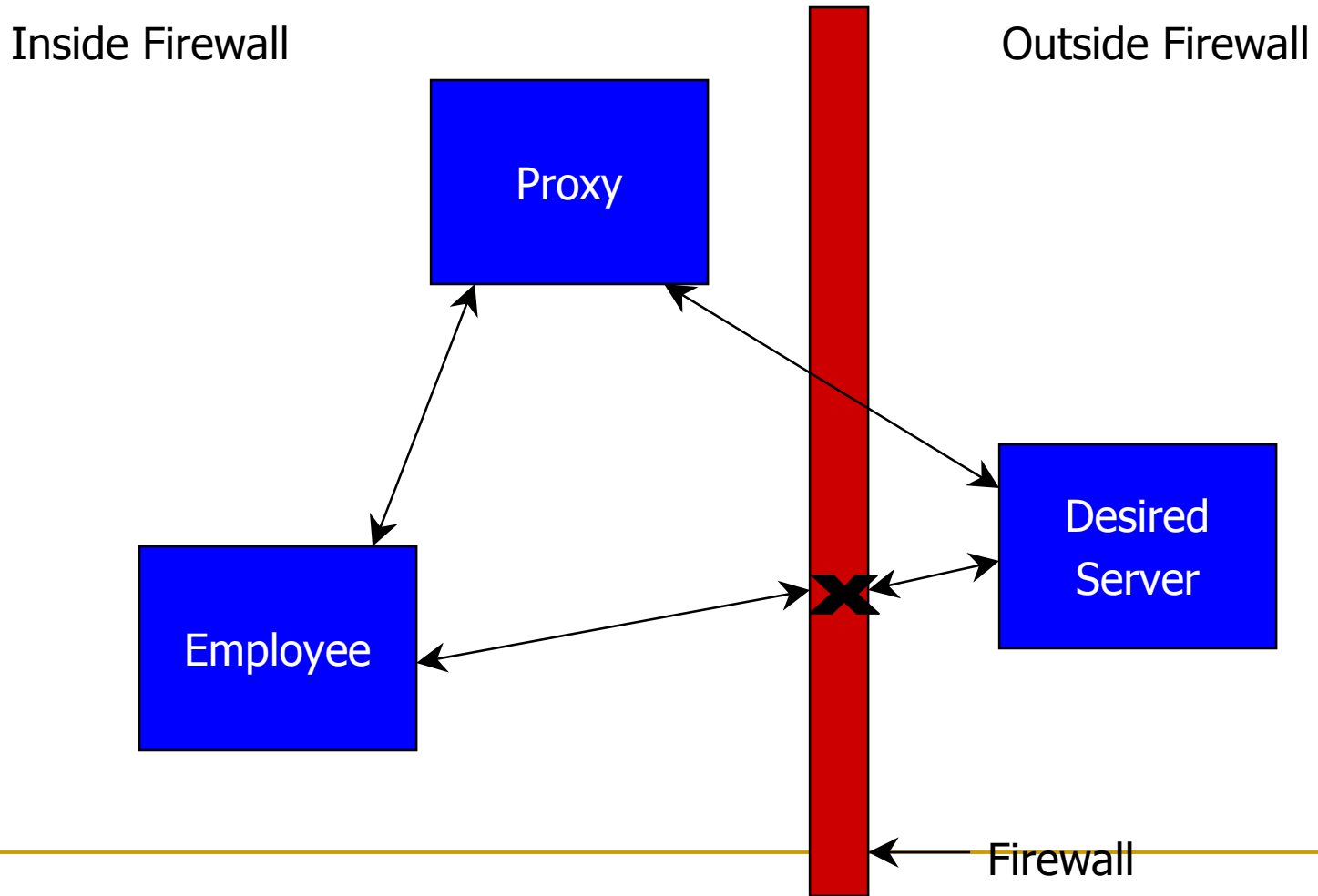
Firewalls

- Proxy
 - Application Level Decisions
- Packet Filter
 - Packet Level Decisions
- Stateful Packet Filter
 - Keeps Track of Sessions

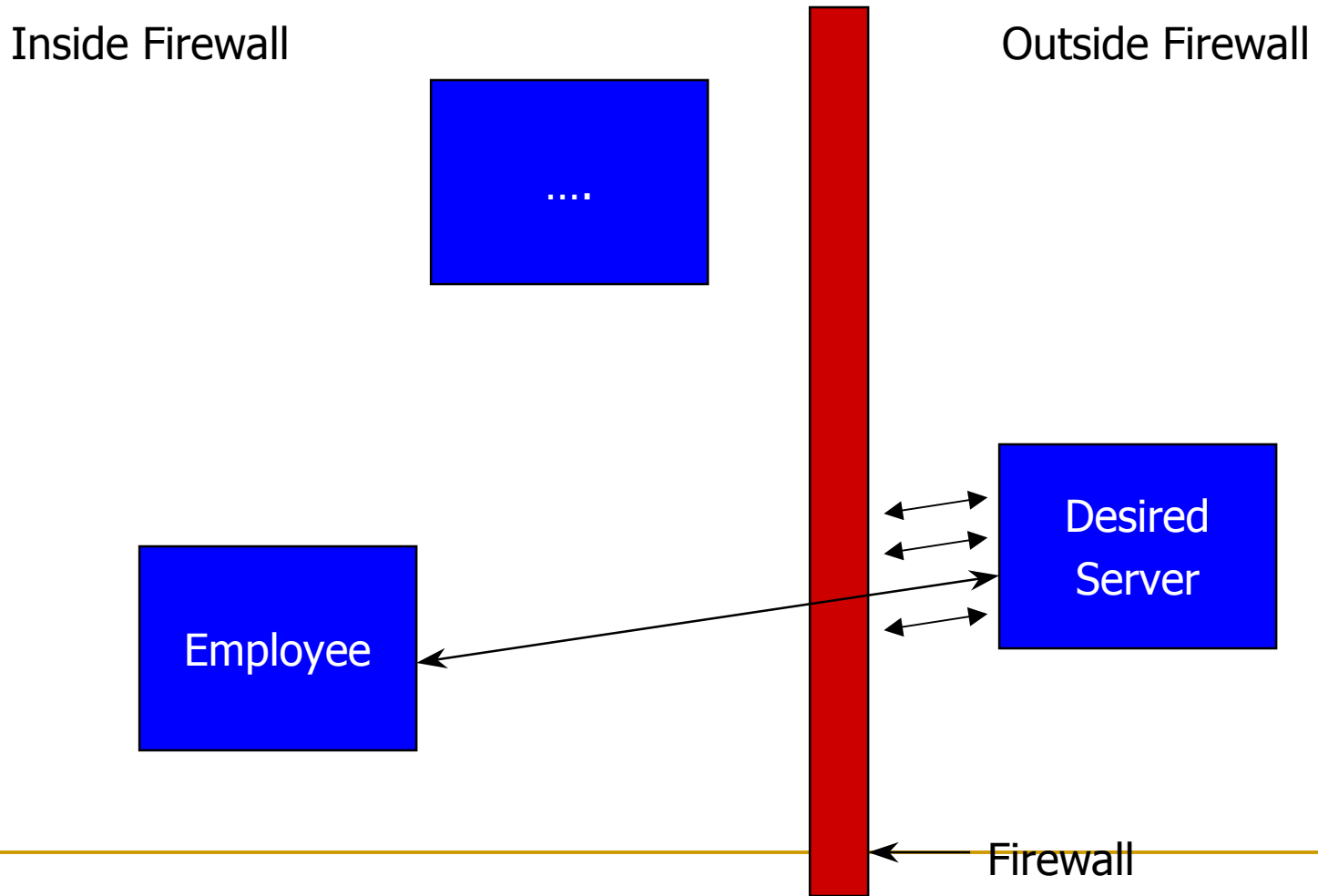
Before Proxy Firewall



Using Proxy Firewall



Packet Filtering Firewall



Personal Firewalls

- BlackIce -- <http://www.netice.com/> (\$39.95)
- ZoneAlarm -- <http://zonelabs.com/> (Free)
- ConSeal -- <http://www.signal9.com/> (\$49.95)
- IPChains -- linux kernel (Free)

Notes About Firewalls

- Secure the services open through the firewall!
- Services not secure are still vulnerable from inside the firewall!

Being a Good Neighbor

- Configure routers to reject directed broadcasts
 - RFC2644
- Ingress/egress packet filtering
 - RFC2267

Intrusion Detection

Intrusions

- Attempted and/or Successful Unauthorized Access
- Depends on Site Policy
- Doorknob Rattling
 - Law is vague, social norm
 - Usually precursor to attack
- “Script kiddies” vs. Real Genius
- Never Underestimate Determination!

Intrusion Detection Systems

- Many different types of attacks, each with a unique “signature”
- Intrusion Detection is a VERY difficult problem
- Host-based
- Network-based
- Signature database needs regular updates

Host-Based IDS...

- Log File Checkers
- Personal Firewalls
- Wrapper Programs
- www.snort.org

Network IDS

- Similar to Host-based, but:
- Watch traffic to and from an entire network
- A few NIDS:
 - Netwatch
 - NFR
 - RealSecure
 - Shadow
 - SecureNet Pro
 - Dragon

Host and Network Intrusion Detection

- Use a Combination of IDSs (Host and Network)

Honey Pots

- “Sacrificial”, attractive host used to bait intruders
- Can serve as a “tripwire” to alert you to their presence
- Distracts them from more valuable resources
- Keeps them busy

Intrusion Detection

Looking For Trouble

- How does an intrusion come to your attention?
- Log Files
- System Integrity
- Intrusion Detection Systems

How Does an Intrusion Come To Your Attention?

- Machine starts “acting funny”
- Files are missing
- ...Or file system fills up
- Secretaries login from Hong Kong

Log Files

- Signs of an attack can be found in your log files
- ...if the logs are not deleted
- ...and if you read the logs!

Digital Signatures

- Compare current files to known good files
 - Tripwire
 - Tiger
 - Sun's Fingerprint Database

Selecting an Intrusion Detection System

Desired IDS Features...

- Able to process at your network's speed
- TAMU has OC-3 (155.52 Mbps)
 - (Optical Carrier; OC-1 is 51.84Mbps)
- Customizable
 - Write your own signature detection scripts
 - Receive updates from vendor promptly
 - Change priority levels and system responses

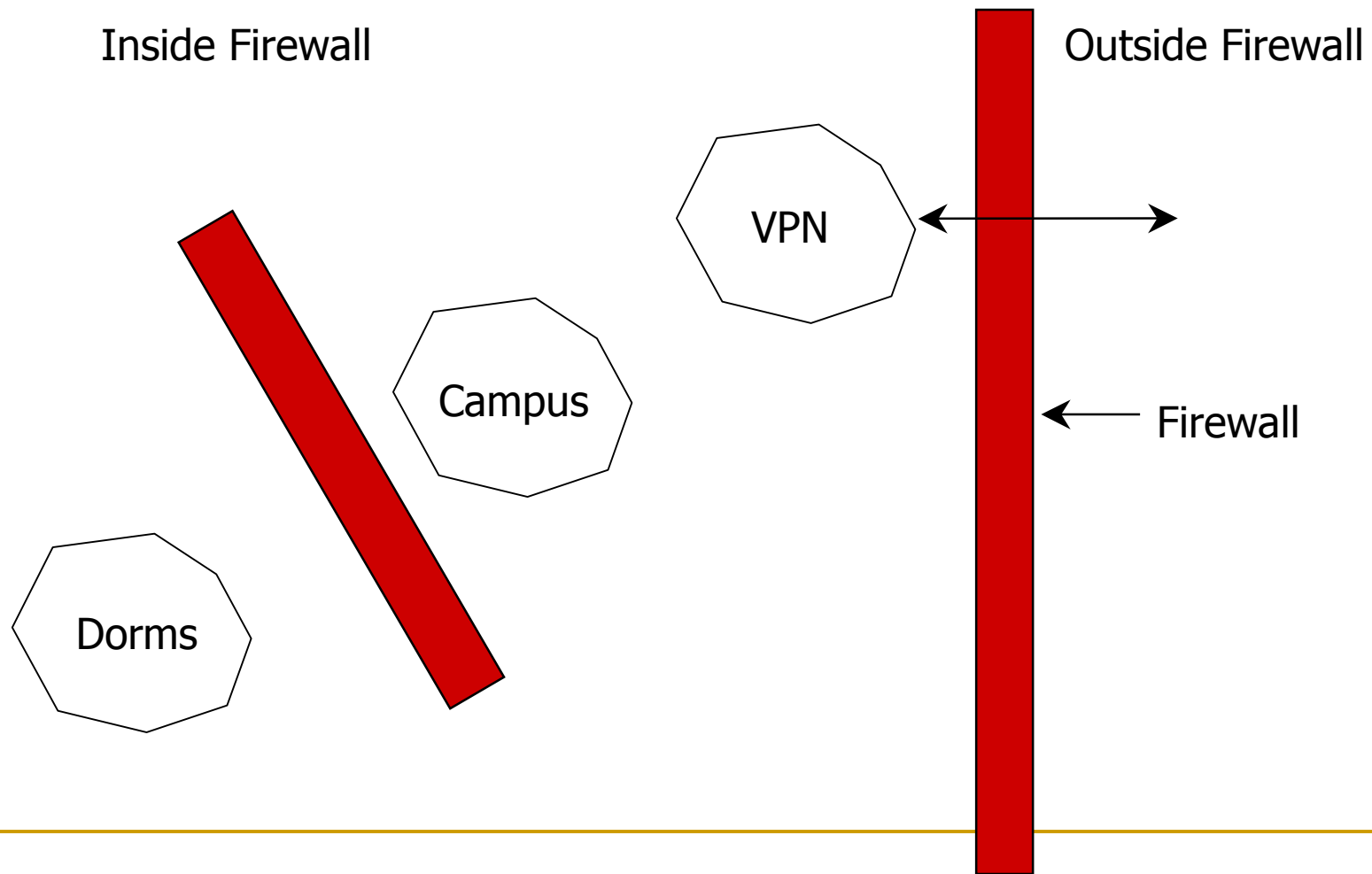
...Desired IDS Features

- List all current sessions
- Disconnect sessions
- Reports (known) virus
- Reports port scans
- Lots of logging

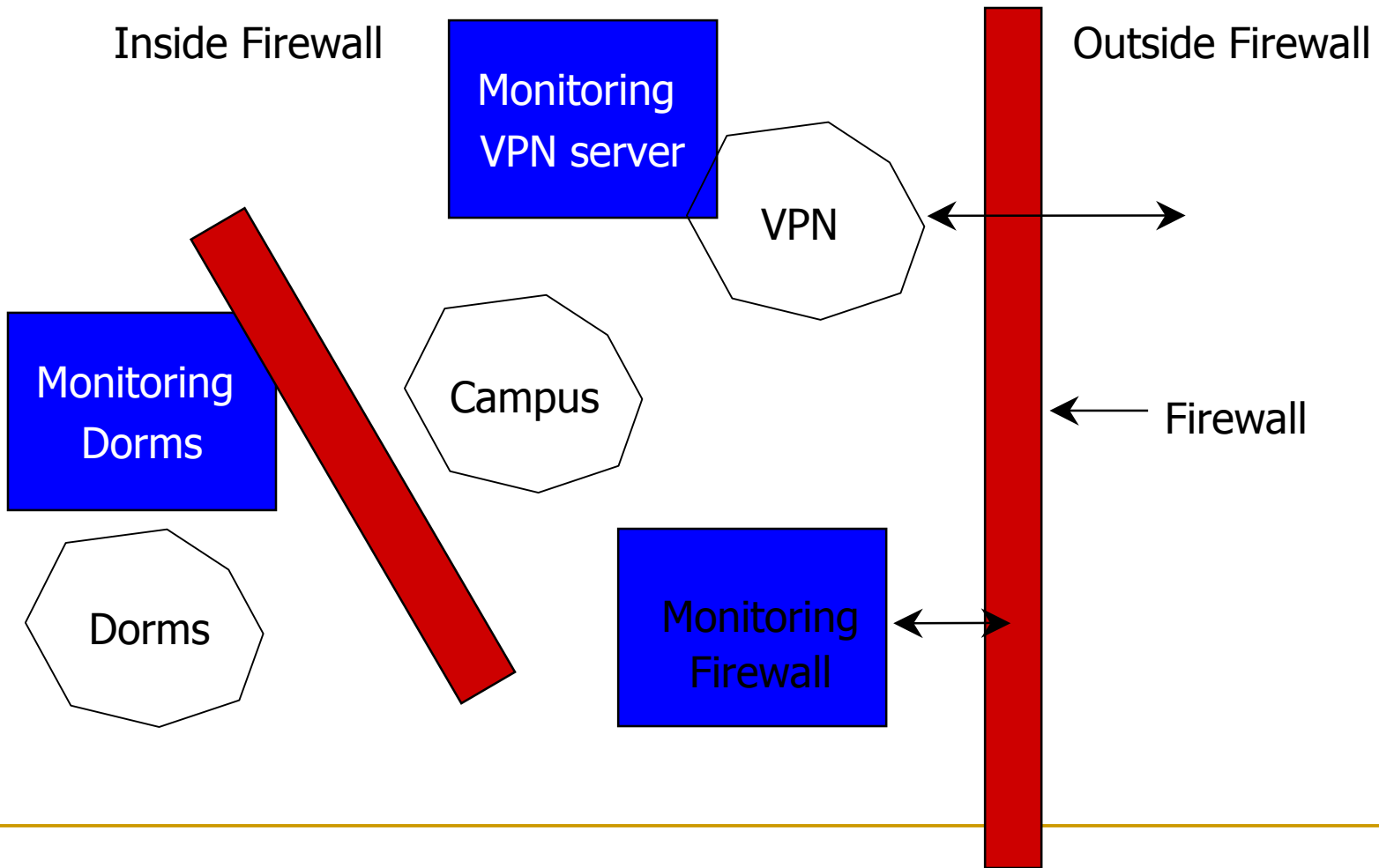
IDS Location

- At Firewall
- Inside VPN end-point

Sample Network



Implementation



Network Flight Recorder

- www.nfr.com
- Provides scripting language (N-code)

ISS Real Secure

- www.iss.net
- Detects many signatures
 - Games, napster show up as an attack
 - Network Time Protocol (NTP)
- 100Mbps

SHADOW

- www.nswc.navy.mil/ISSEC/CID/
- Very low-level, requires background with tcp_dump and knowledge of packet structure

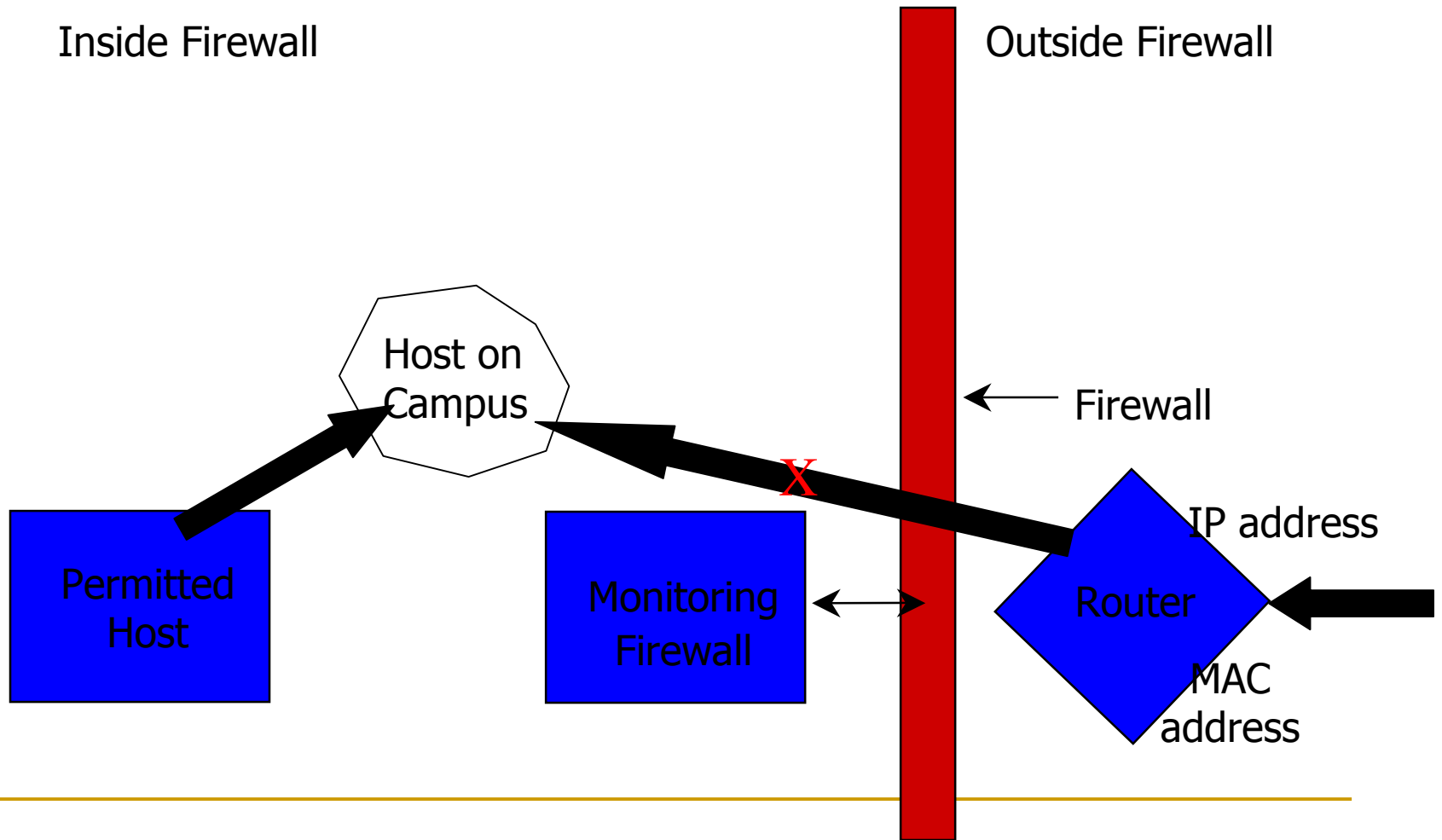
SecureNet Pro (SNP)

- www.intrusion.com
- Runs on linux or you can buy an “appliance”

Snort

- www.snort.org
- www.sourcefire.com

IDS Illustration



Encryption

- Will make ID harder
- ...if not impossible

Responding To An Intrusion

Computer Laws

- Digital Millennium Copyright Act
- napster, gnutella
- Freedom of speech
- U.S. and State Code on computer crimes
- Offensive vs. Illegal

What Are Your Goals?...

- Determine identity of attacker and press charges
 - May require ongoing investigation while intrusion continues
 - How do you know when to pull the plug?
 - Often extremely difficult because intruders hop from host to host; coordination of many sites is required

...What Are Your Goals?

- Identify method of compromise, clean up, and move on

Procedures...

- Should you report the incident?
 - No, we're a business
 - Yes, to whom?
- Pulling the plug
- Tipping off the intruder
- Depending on scope of investigation, may require additional hardware

...Procedures...

- Working with law enforcement...
- Keep a written log of your actions
- Be prepared to handle subpoenas and/or testify
- Know ahead of time who, if anyone, should talk to media

...Procedures

- Is a search warrant required before you will release data? Who is responsible?
- Back up your system
- FBI is usually the contact, but follow your chain of command
 - University contacts UPD

Sniffers

- Capture traffic and inspect it
 - tcpdump
 - tcpflow, tcpslice
 - Solaris' snoop
 - ethereal

Other Utilities

- lsof (“list open files”)
- netstat -na
- ps
- Beware, these are often replaced by copies that do not report the intrusion!
- make sure your tools are not tainted, database signatures are read-only

Contacting Other Sites

- “whois” server
- Whois -h geektools.com example.com

Forensics

- Some rather amazing forensics are possible
- The Coroner's Toolkit
- mount compromised disk read-only on another system

Suggested References...

- Center for Education and Resources in Information Assurance and Security (CERIAS): <http://www.cerias.purdue.edu/>
- North American Network Operators' Group (NANOG): <http://www.nanog.org/>
- bugtraq mailing list: <http://www.netSPACE.org/>

...Suggested References

- ntbugtraq: <http://www.ntbugtraq.com/>
- incidents mailing list:
<http://www.securityfocus.com/>
- Practical Unix and Internet Security,
Garfinkle & Spafford
- Firewalls and Internet Security, Cheswick
& Bellovin

Web Resources

- <ftp://ftp.ox.ac.uk/pub/wordlists/> (wordlists for Crack)
- <http://ftp.ee.lbl.gov/> (tcpdump, tcpslice, libpcap)
- www.cert.org (incident response and prevention information)
- www.circlemud.org/~jelson/software/tcpflow/ (tcpflow)

-
- <http://www.crypticide.org/users/alecm/> (crack)

...Resources...

- <http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp>
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iischk.asp>

...Resources...

- www.nessus.org (port scanner)
- www.netice.com (Blace Ice firewall)
- www.nmap.org (port scanner)
- www.openwall.com/john (John the Ripper password Cracker)
- www.porcupine.org (tcp_wrappers, for access control and logging; The Coroner's Toolkit)

...Resources

- www.psionic.com (logcheck, port sentry, host sentry)
- www.securityfocus.com (lots of security info and good mailing lists)
- www.signal9.com/ (ConSeal firewall)
- www.zonelabs.com/ (Zone Alarm firewall)