Securing The Linux Environment

- Craig Ozancin
- Senior Security Analyst
- Symantec Corporation
- cozancin@symantec.com

September 7, 2004

Agenda

- **Who is who**
- **The threat**
- **The solution**
- **Where can I find more information**
- **Conclusion**
- **Questions?**

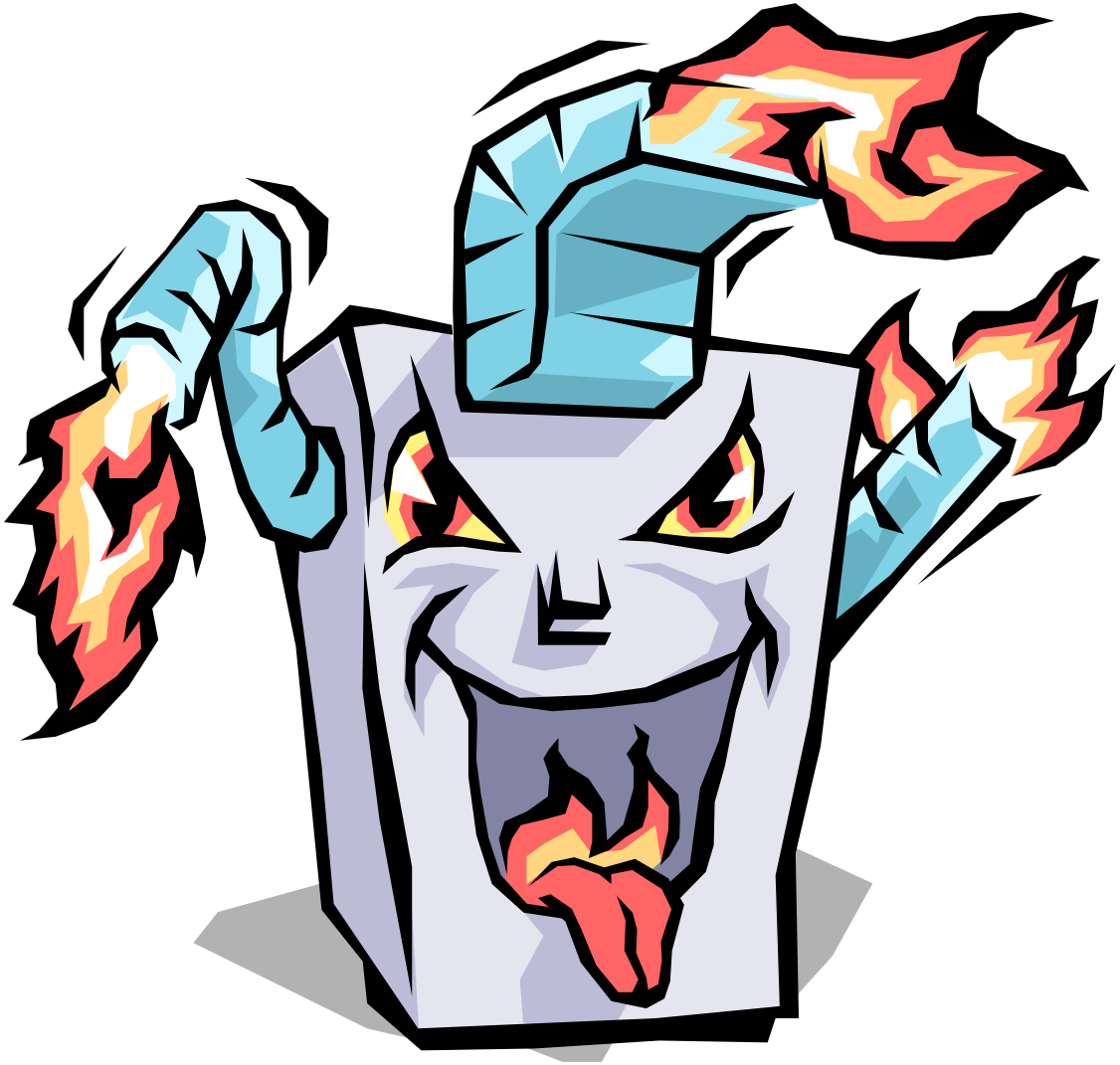
Who Is Who?

- **Hackers**
- **Crackers**
- **Script kiddies**
- **Social engineer**
- **Phone Phreaks**
- **Packet monkeys**

- **White hat hacker**
- **Black hat hacker**
- **Criminal**
- **The kid next door?**

Attackers

II: The Threat



The Threat

- **Steps to breaking in**
- **Scanning**
- **Getting and keeping control**
- **Covering your tracks**
- **Extend the attack**
- **Denial-of-service**
- **Worms**

Steps to breaking in

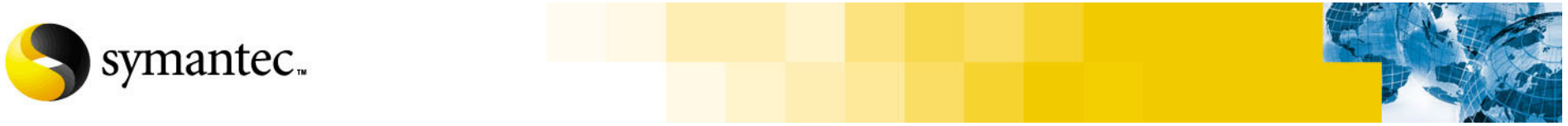
Common Steps of an Attack

- Identify target
  - Pick one
  - Scan
  - Random
  - Link from another location
- Find more information
  - Research / footprint
  - Scan
- Identify way in and use it
  - Identify vulnerability
    - Password cracker
    - Buffer overflow
    - Configuration flaw
    - Many others
  - Exploit it
- Elevate privilege (if necessary)
- Remove evidence of exploit
  - Logs
  - Intrusion detection systems
- Explore, look for new targets or abuse
  - Network sniffing
  - Steal content
  - Deface website
  - Backdoor
  - Destroy system
  - Others

Scanning

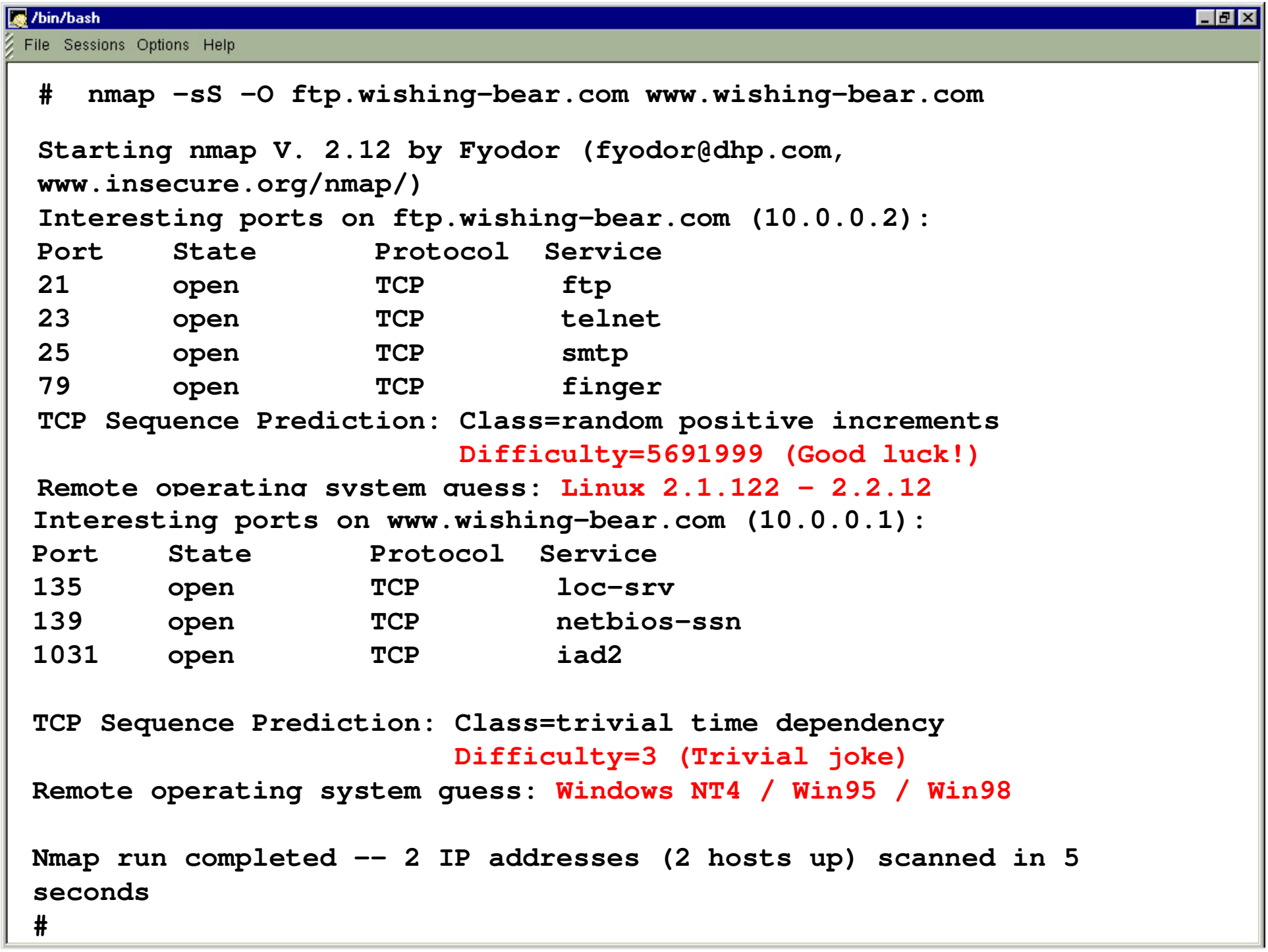
Scanning

- **Port scanning**
  - **Acquires accessible port information from remote systems**
  - **Operating system discovery**
- **Look for specific vulnerable services**
- **Dialup modems (war dialing)**
- **Wireless networks (war driving)**
- **Firewall rule discovery**



Port Scanning

- **Acquires accessible port information from remote systems**
- **Can be used to identify potentially vulnerable services**
- **Some popular port scanners are:**
  - **Strobe**
    - **Attempts to open ports and report success**
  - **Nmap**
    - **Can be used to gather extensive network mapping of a network**
    - **Adds the concept of stealth scanning**
    - **Operating system type and version discovery**
    - **Identifies both open TCP and UDP ports**


/bin/bash
File Sessions Options Help
nmap -sS -O ftp.wishing-bear.com www.wishing-bear.com
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on ftp.wishing-bear.com (10.0.0.2):
Port State Protocol Service
21 open TCP ftp
23 open TCP telnet
25 open TCP smtp
79 open TCP finger
TCP Sequence Prediction: Class=random positive increments
Difficulty=5691999 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.12
Interesting ports on www.wishing-bear.com (10.0.0.1):
Port State Protocol Service
135 open TCP loc-srv
139 open TCP netbios-ssn
1031 open TCP iad2
TCP Sequence Prediction: Class=trivial time dependency
Difficulty=3 (Trivial joke)
Remote operating system guess: Windows NT4 / Win95 / Win98
Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 5 seconds
#

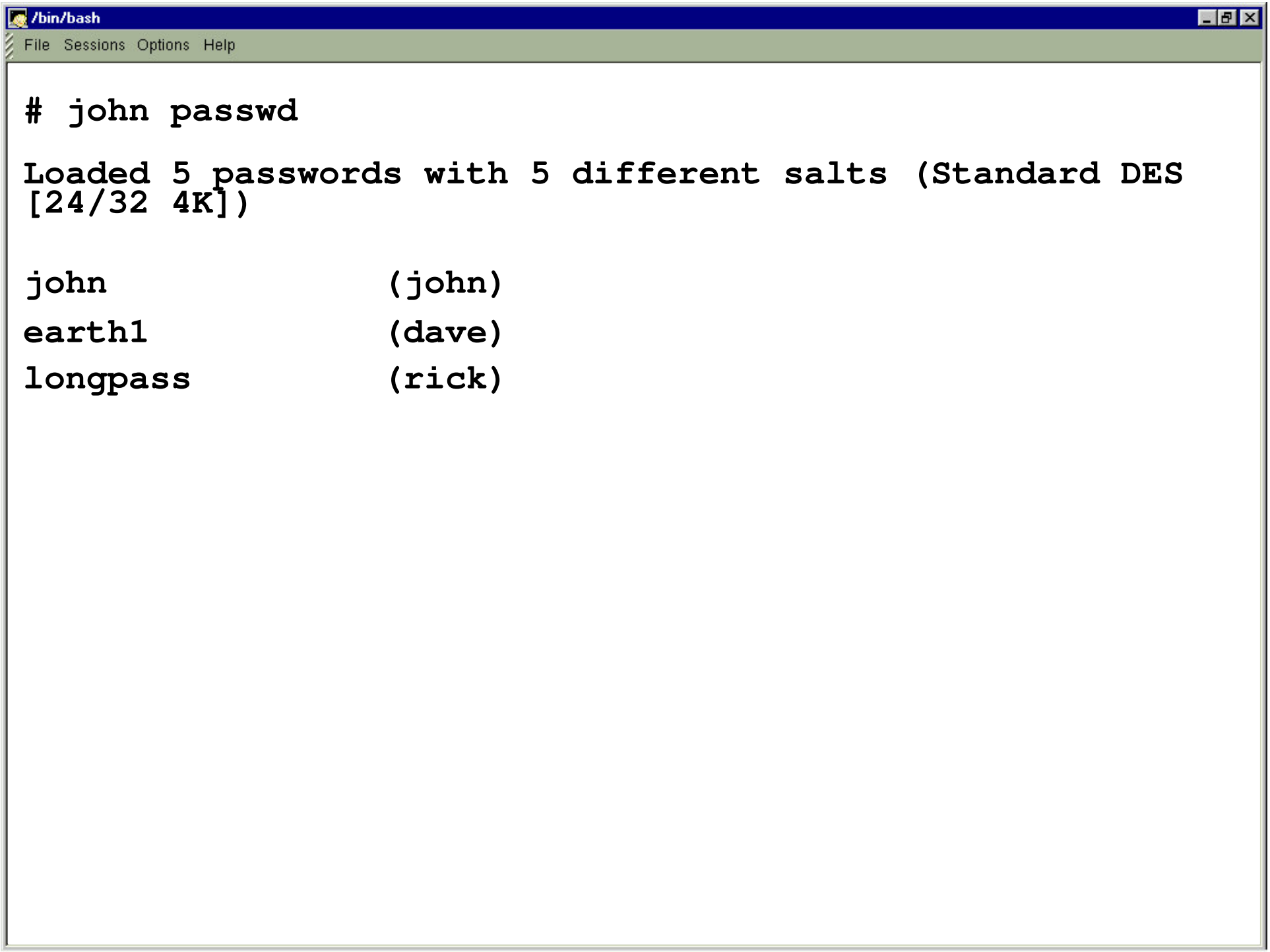
Password stealing / Cracking

Passwords Abuse

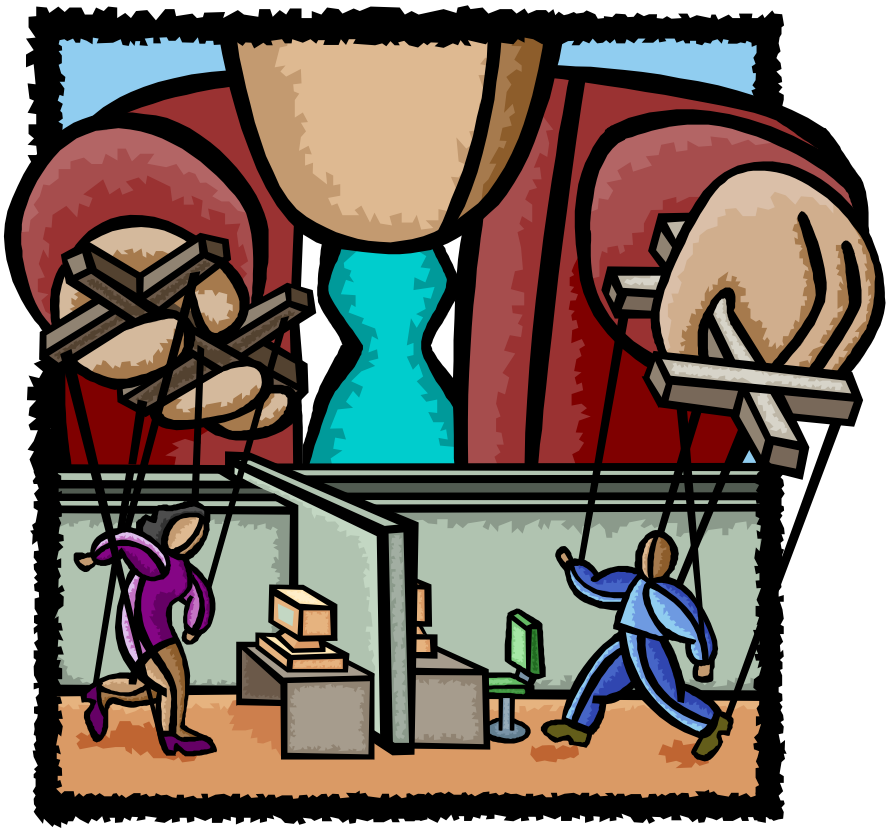
- **Password stealing**
  - **CGI script exploits**
  - **shoulder surfing**
  - **Many others**
- **Network sniffing**
  - **reading the password directly from network traffic**
- **Password guessing**
  - **Predictable passwords**
    - **Blank**
    - **“guest”**
    - **user name**
  - **Dictionary attack**
  - **Brute force**

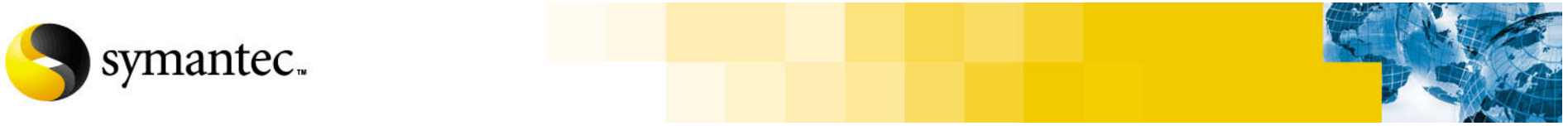
Passwords Crackers

- **Automated tools that attempt to discover passwords**
- **Requires user name and raw password hashes as input**
- **Unix / Linux tools**
  - **Crack**
  - **John the ripper**
  - **Distributed password crackers (shares the load among many systems)**
    - **Mio-star**
    - **Saltine-cracker**
    - **Slurpie**
  - **Many others**


/bin/bash
File Sessions Options Help
john passwd
Loaded 5 passwords with 5 different salts (Standard DES [24/32 4K])
john (john)
earth1 (dave)
longpass (rick)

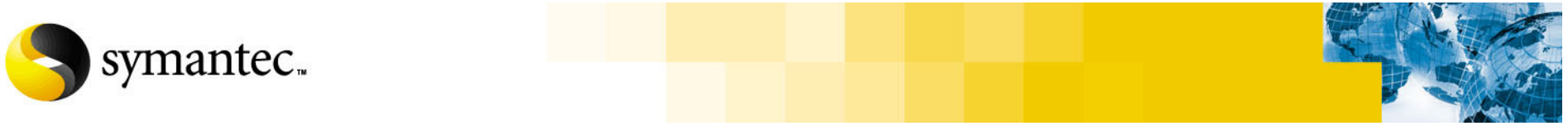
Getting And Keeping Control





Privileged Access

- **Exploit buffer overflow**
- **Exploit configuration errors**
- **Exploit other OS or application bugs**
- **Use a system or application backdoors**
  - **this continues to plague the community**
- **Keep control by inserting backdoor**

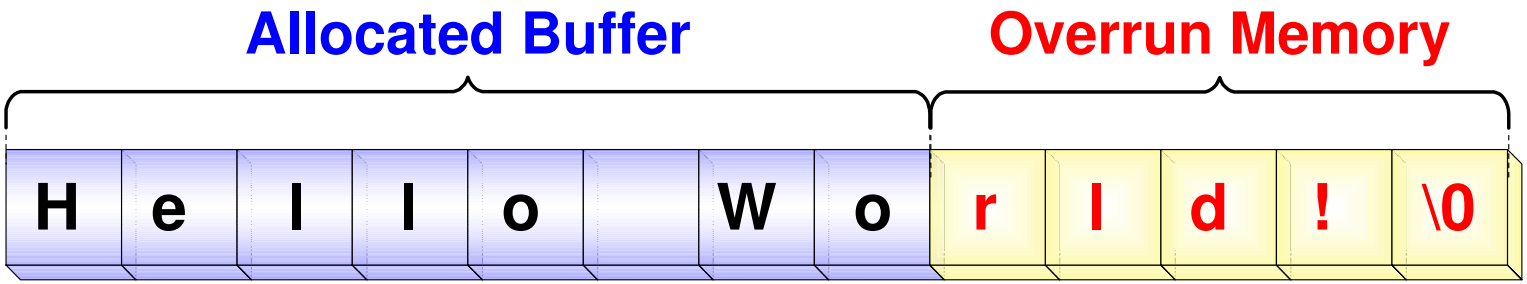


Taking Control – Buffer Overflows

- **Common attack to gain complete access**
- **Buffer overflows exploit software bugs that cause it to overwrite segments of memory**
- **Types of buffer overflows**
  - **Stack smashing**
  - **Heap overflow**
  - **Return into libc overflow**
- **New buffer overflows continue to be discovered**

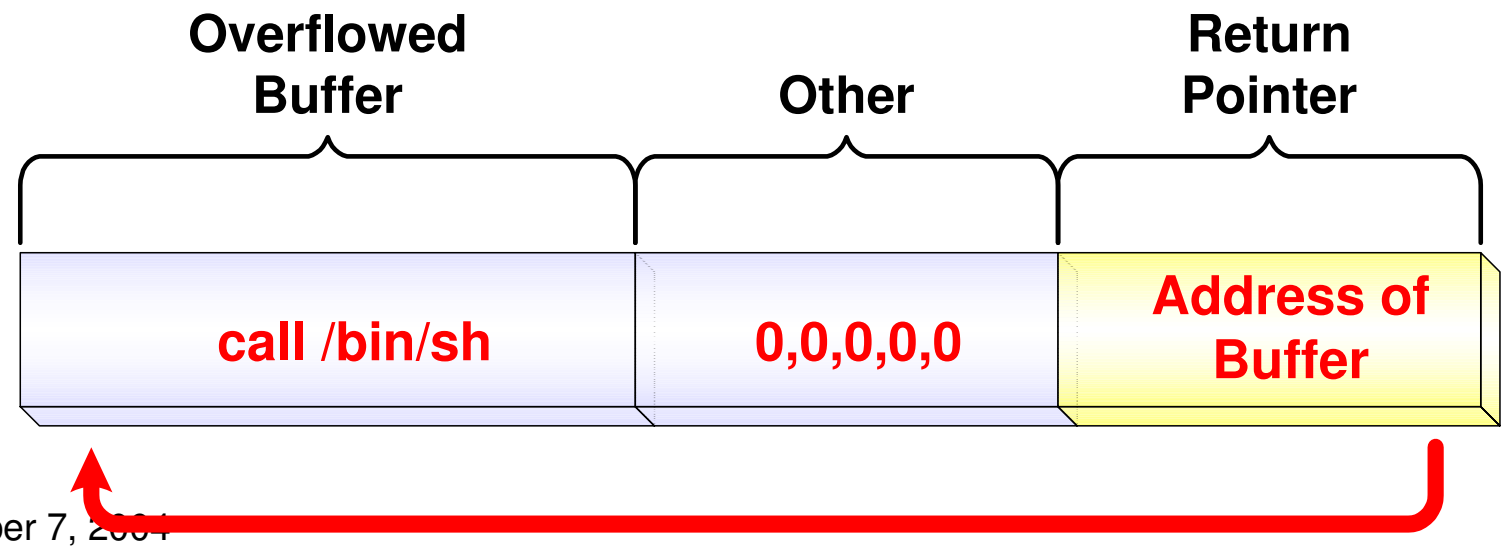
Buffer Overflows

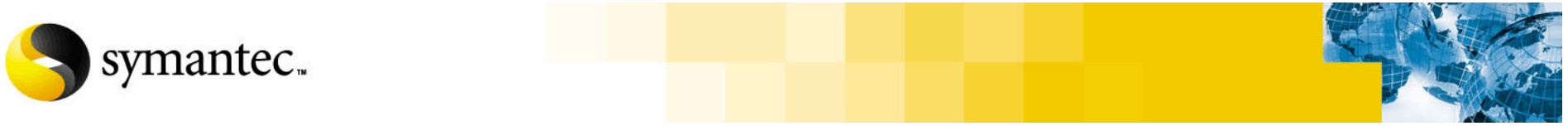
- **Cause vulnerable program to write more data to buffer than is allocated**
  - **May cause the program to crash**
  - **Modify other elements on the stack**
- **May result in privilege access**



Buffer Overflows

- **Overflow buffer with executable code**
- **Fill space between buffer and return pointer with random or null data**
- **Over write return pointer with address of buffer**
- **When function returns, the exploit coded is executed**



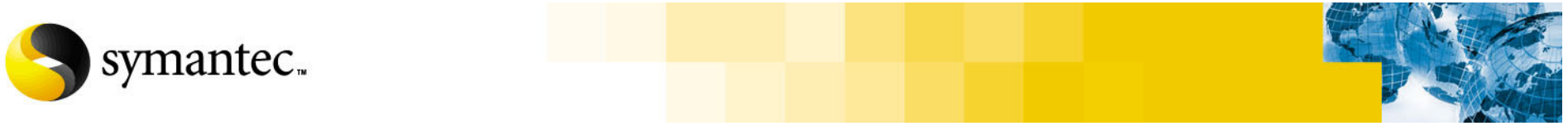


Keeping Control

- **Backdoors**
  - **Allows attackers to bypass normal authentication**
- **Trojan horses**
  - **May replace system program**
  - **Can appear to have the same behavior as the program they are replacing**
  - **May appear to be a normal or reasonable executable**
  - **Are traps that can be used to compromise system**
  - **Appear to have the same behavior as the program they are replacing**

Rootkit

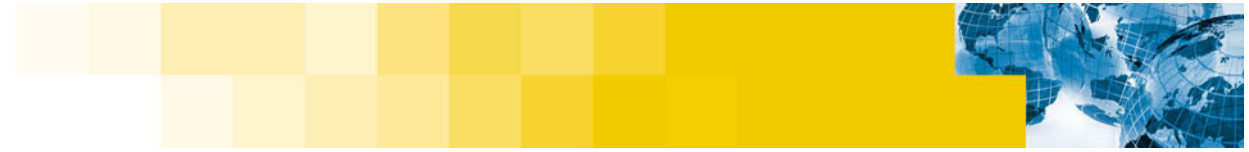
- **New tools**
  - **Bindshell - connects a shell to a network port**
  - **Packet sniffer specialized to look for user names and passwords**
- **Trojan tools**
  - **Ls, ps, crontab, du, find, ifconfig, netstat, pidof and top (hide presence of bindshell, sniffer)**
- **Tools that have backdoors added**
  - **Inetd, login, rshd - allow remote access without authentication**
- **Tools to remove entries from wtmp, utmp and last log**
- **Tools to modify checksum and timestamp to that of the original non-Trojan executable**
- **Other miscellaneous backdoors and tools**



Knark (Kernel Level) Rootkit

- **Knark implemented as a loadable kernel module**
- **Knark means “drugs” in Swedish**
- **Knark contains the following features:**
  - **Hide/unhide files or directories**
  - **Hide TCP or UDP connections**
  - **Execute redirection**
  - **Unauthorized privilege escalation (“rootme”)**
  - **Utility to change UID/GID of running processes**
  - **Unauthenticated, privileged remote execution daemon**
  - **Kill –31 to hide a running process**

Covering Your Tracks



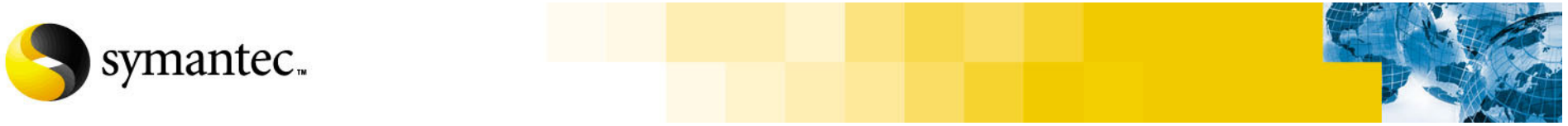
Covering Your Tracks

- **What logging is active?**
  - **syslogd**
  - **Tripwire**
  - **Aide**
  - **Samhain**
  - **Event log**
  - **Commercial monitoring and intrusion detection packages**
- **Find logs**
- **Turn them off**
- **Flood them with noise**
- **Remove incriminating audit trail entries**

Extend The Attack

Extend the Attack

- **Once inside, the attacker can get almost any information they want**
- **Packet sniffers**
- **On-line network maps and management tools**
- **More probing to find new systems**
- **Attack other locations**
  - **Use the current site to hide their tracks**
  - **Denial-of-service**

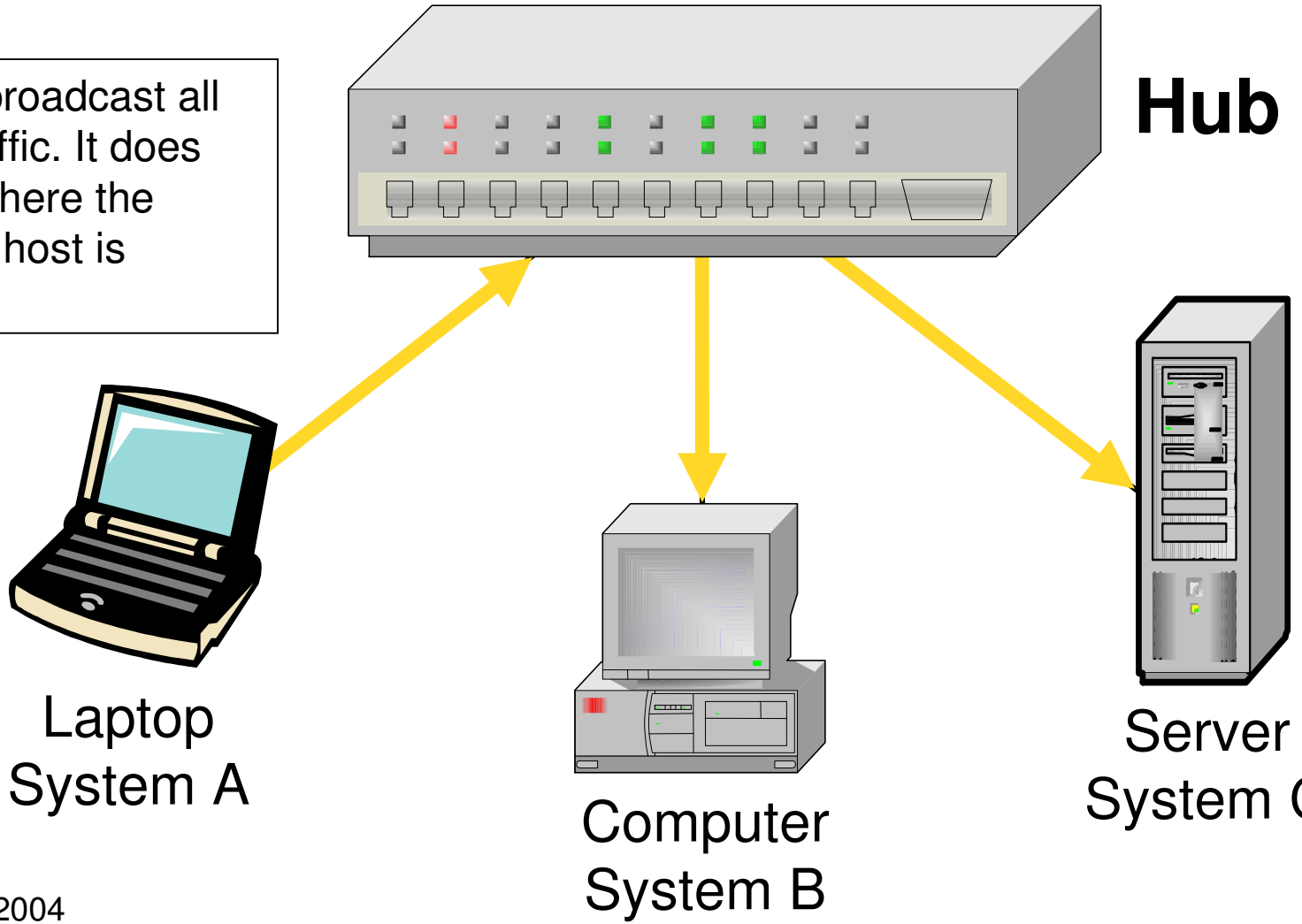


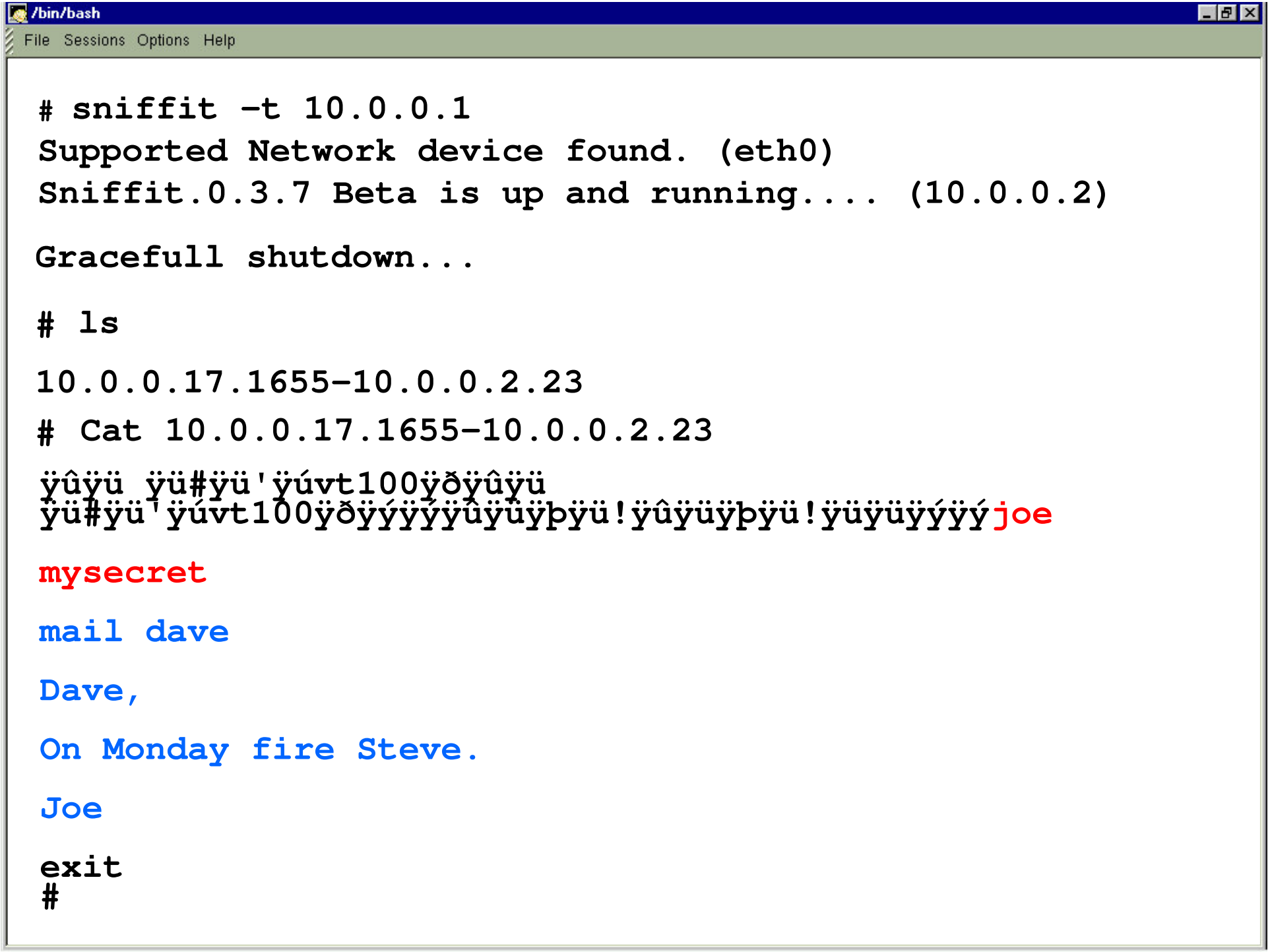
Packet Sniffers

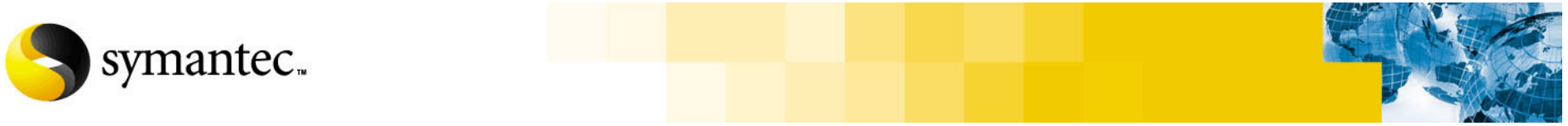
- **Designed as a network diagnostics tool**
  - **User can dissect network packets looking for problems**
- **Places network-interface-card in promiscuous mode**
  - **All network traffic can now be read (not just that sent to the host)**
- **Can also be used to read packet payload**
  - **User name**
  - **Password**
  - **Other private content**
- **Many open source and commercial packet sniffers available**
- **Specialized versions that target user names and password information**

Packet Sniffers

A hub will broadcast all network traffic. It does not know where the destination host is located.




/bin/bash
File Sessions Options Help
sniffit -t 10.0.0.1
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (10.0.0.2)
Gracefull shutdown...
ls
10.0.0.17.1655-10.0.0.2.23
Cat 10.0.0.17.1655-10.0.0.2.23
ÿûÿü ÿü#ÿü'ÿúvt100ÿðÿûÿü
ÿü#ÿü'ÿúvt100ÿðÿýýýýûýüýþÿü!ÿûÿüýþÿü!ÿüýüýýýýjoe
mysecret
mail dave
Dave,
On Monday fire Steve.
Joe
exit
#

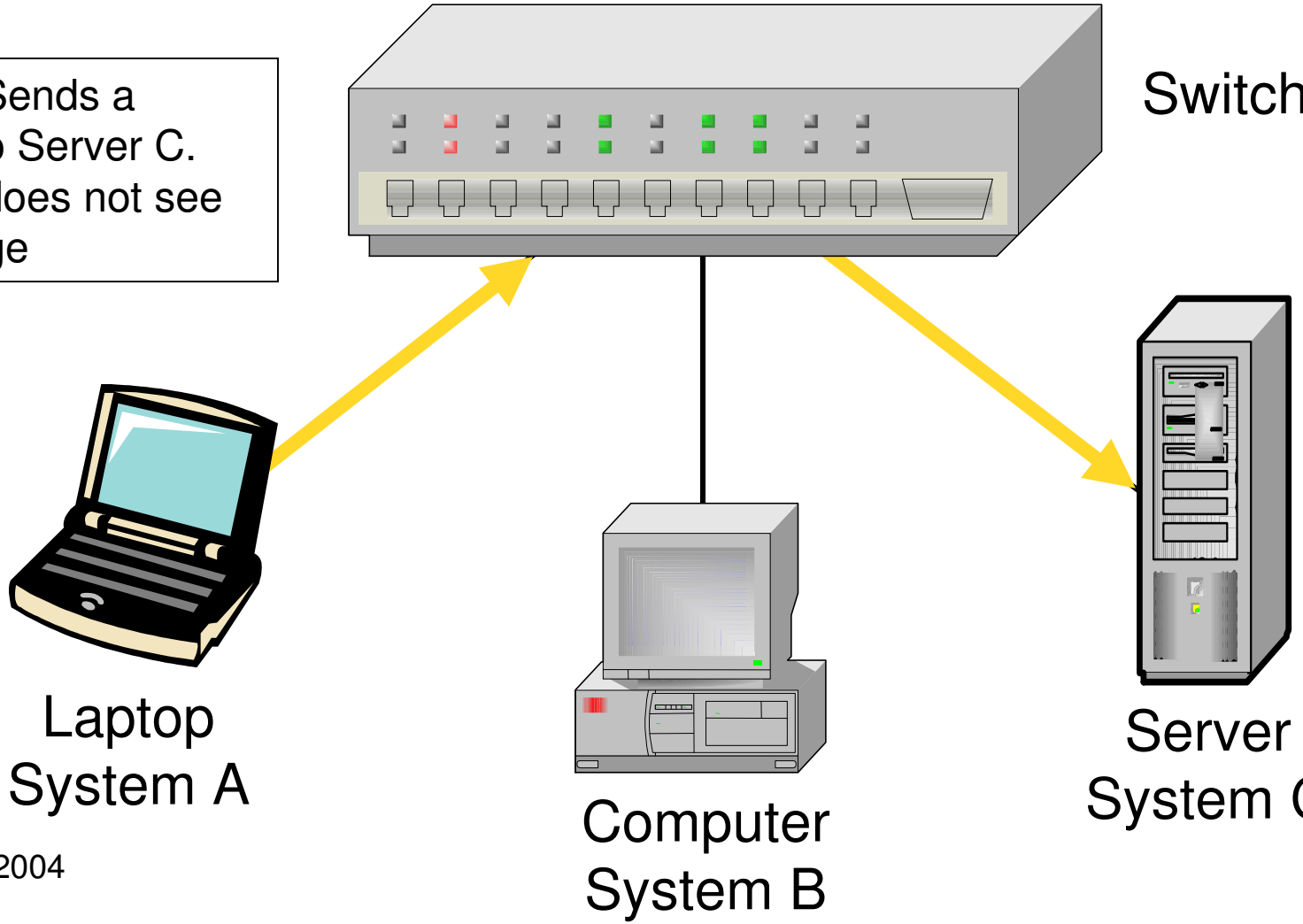


Network Switches

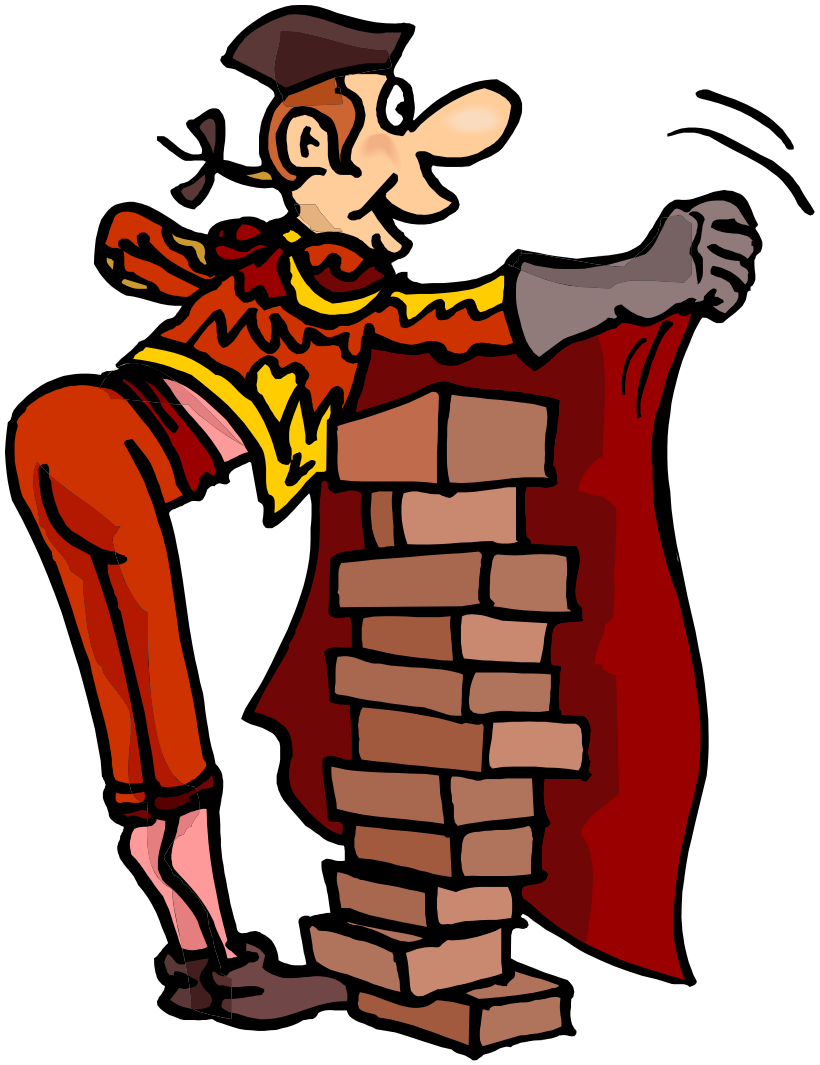
- **Switches were designed to reduce network traffic**
- **They do not send every network packet to every system under its control**
- **This inadvertently protects against packet sniffing (this was not the original goal of the switch design)**

The Switch

System A Sends a message to Server C. System B does not see the message



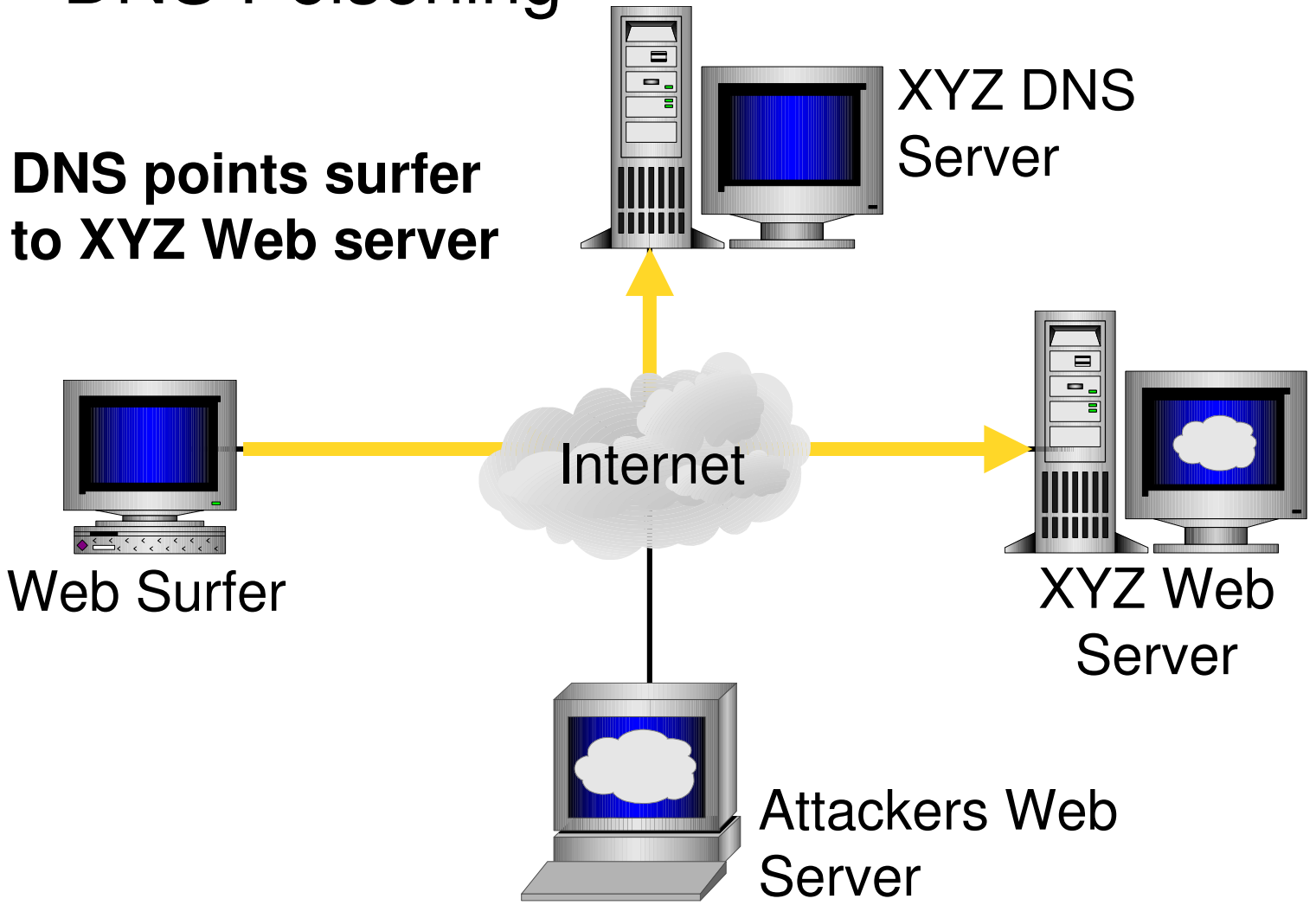
Denial-of-Service Attacks



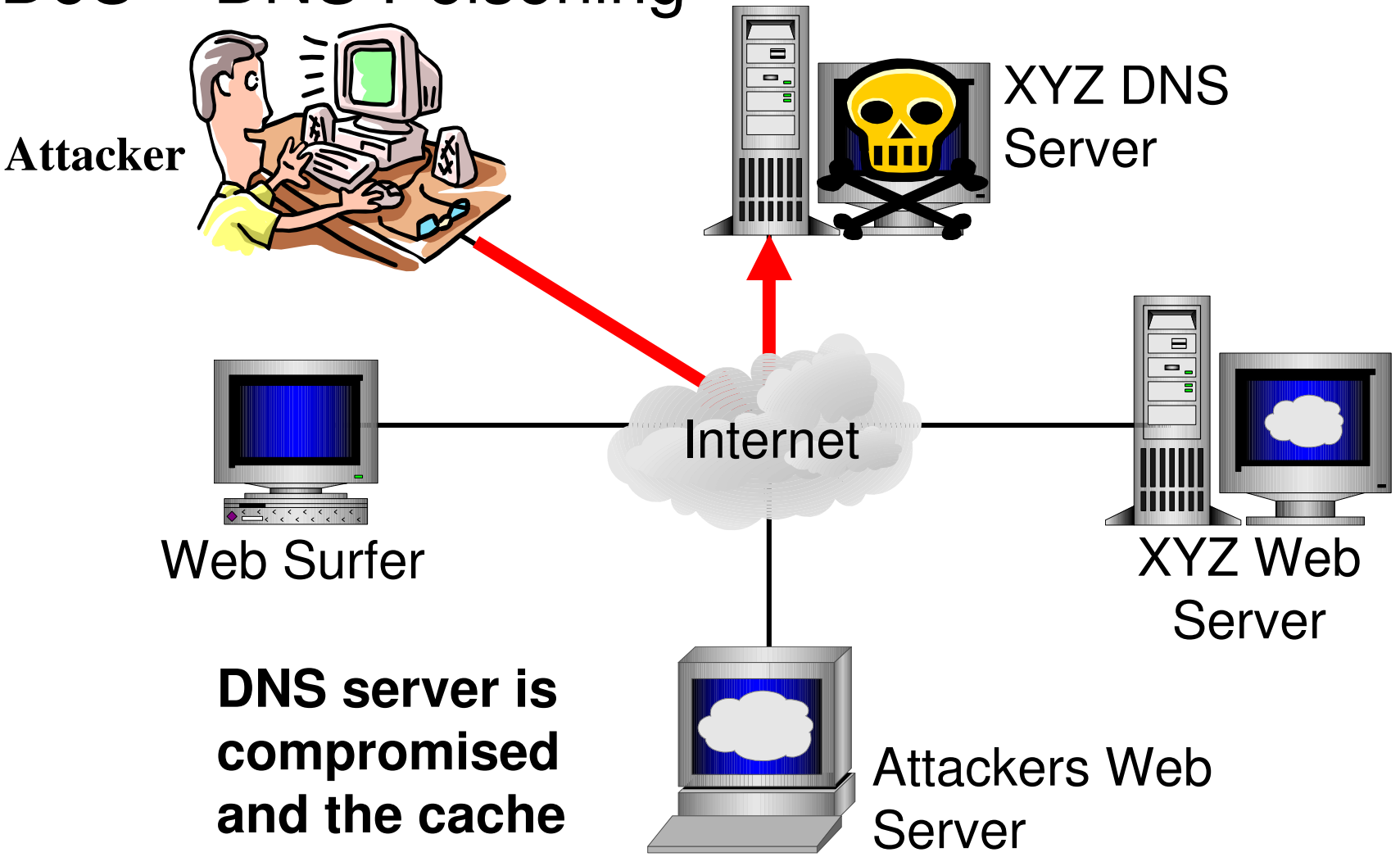
What Is a Denial-of-Service

A Denial-of-Services is when someone or something is prevented from performing a desired task or operation.

DoS – DNS Poisoning



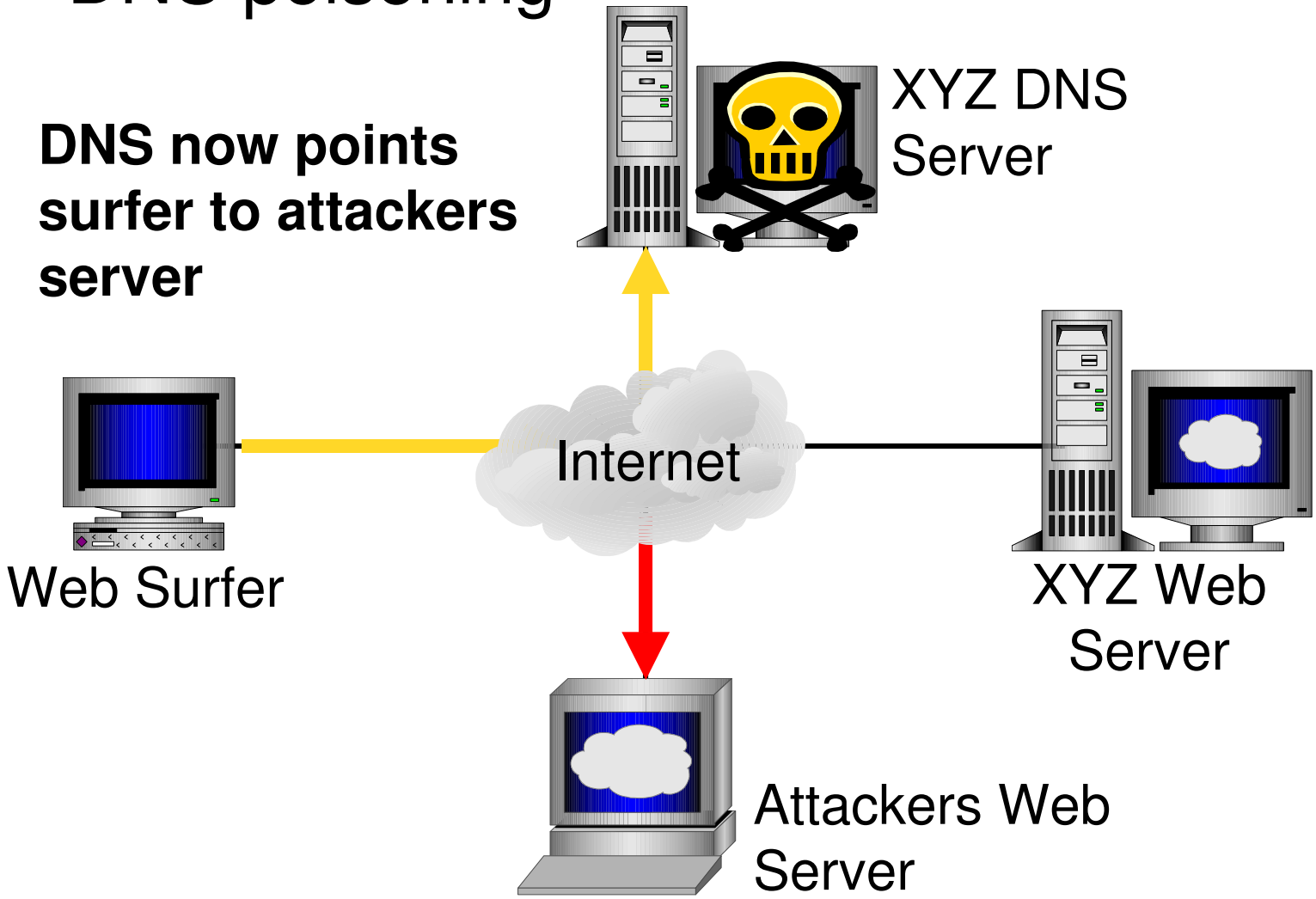
DoS – DNS Poisoning



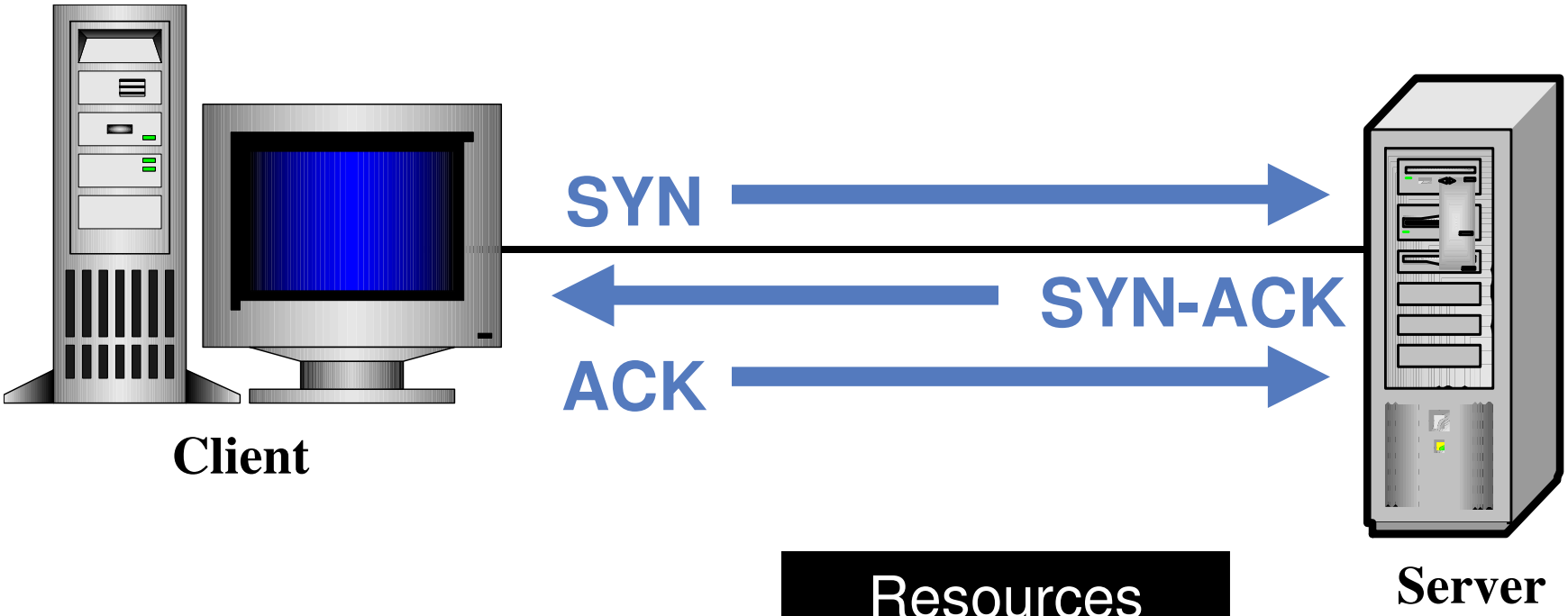
DNS server is compromised and the cache poisoned

DoS – DNS poisoning

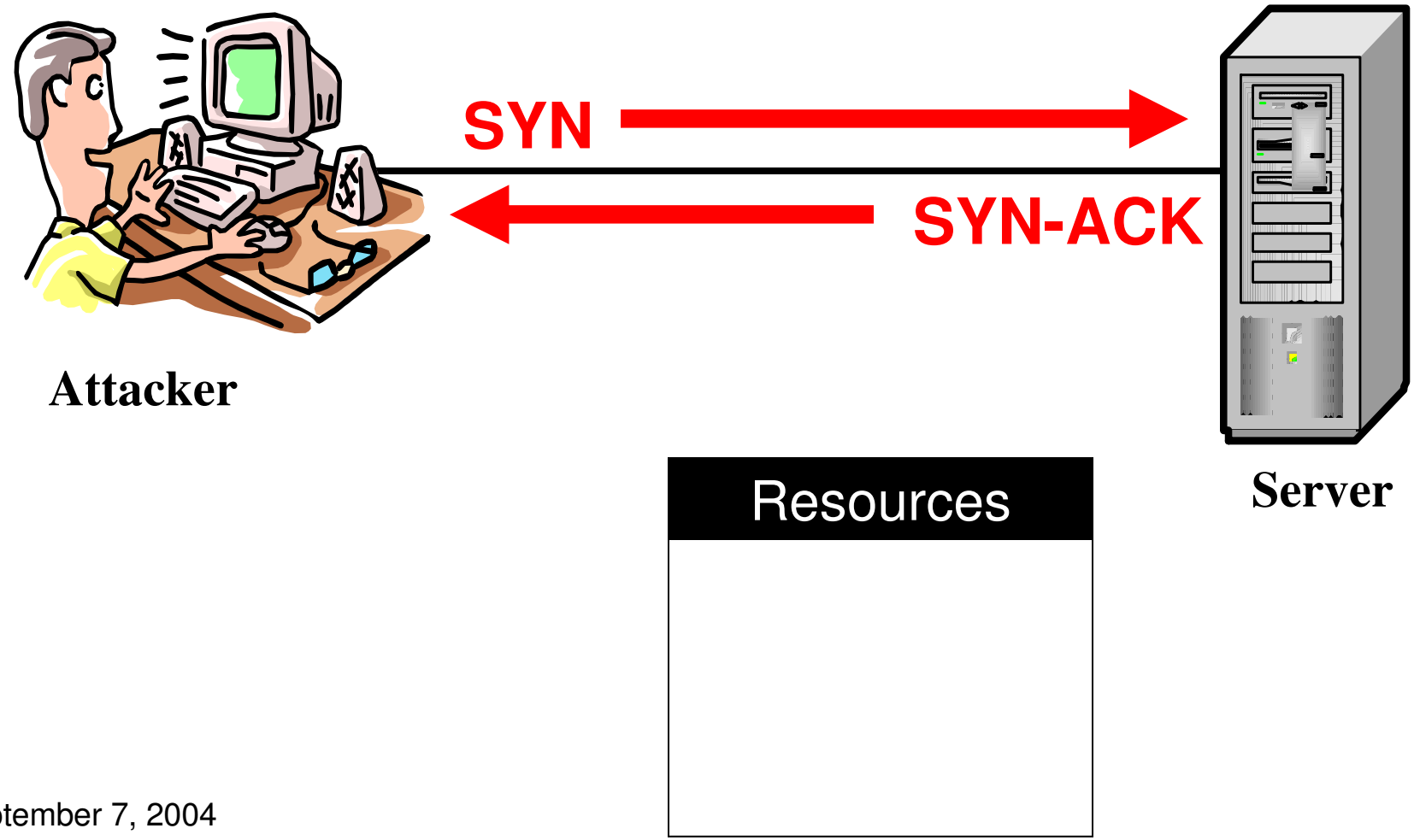
DNS now points surfer to attackers server



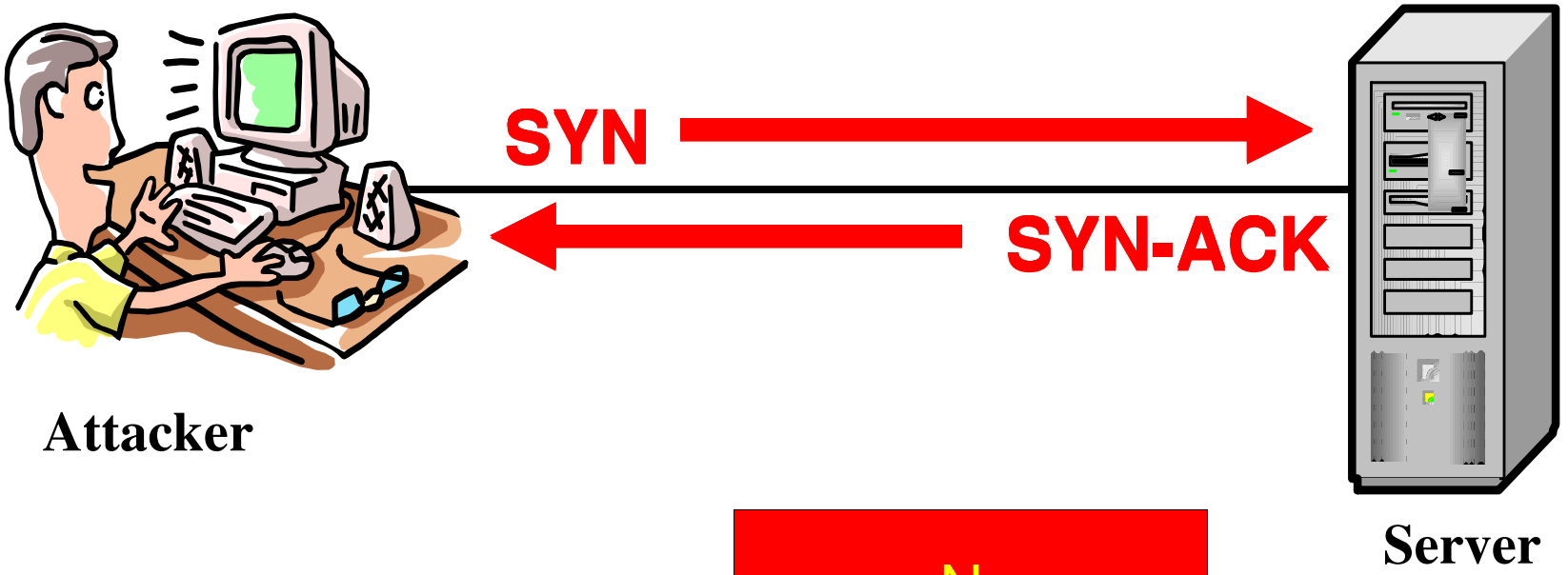
Connection Oriented 3-Way Handshake



Beginning of a Syn-flood Attack



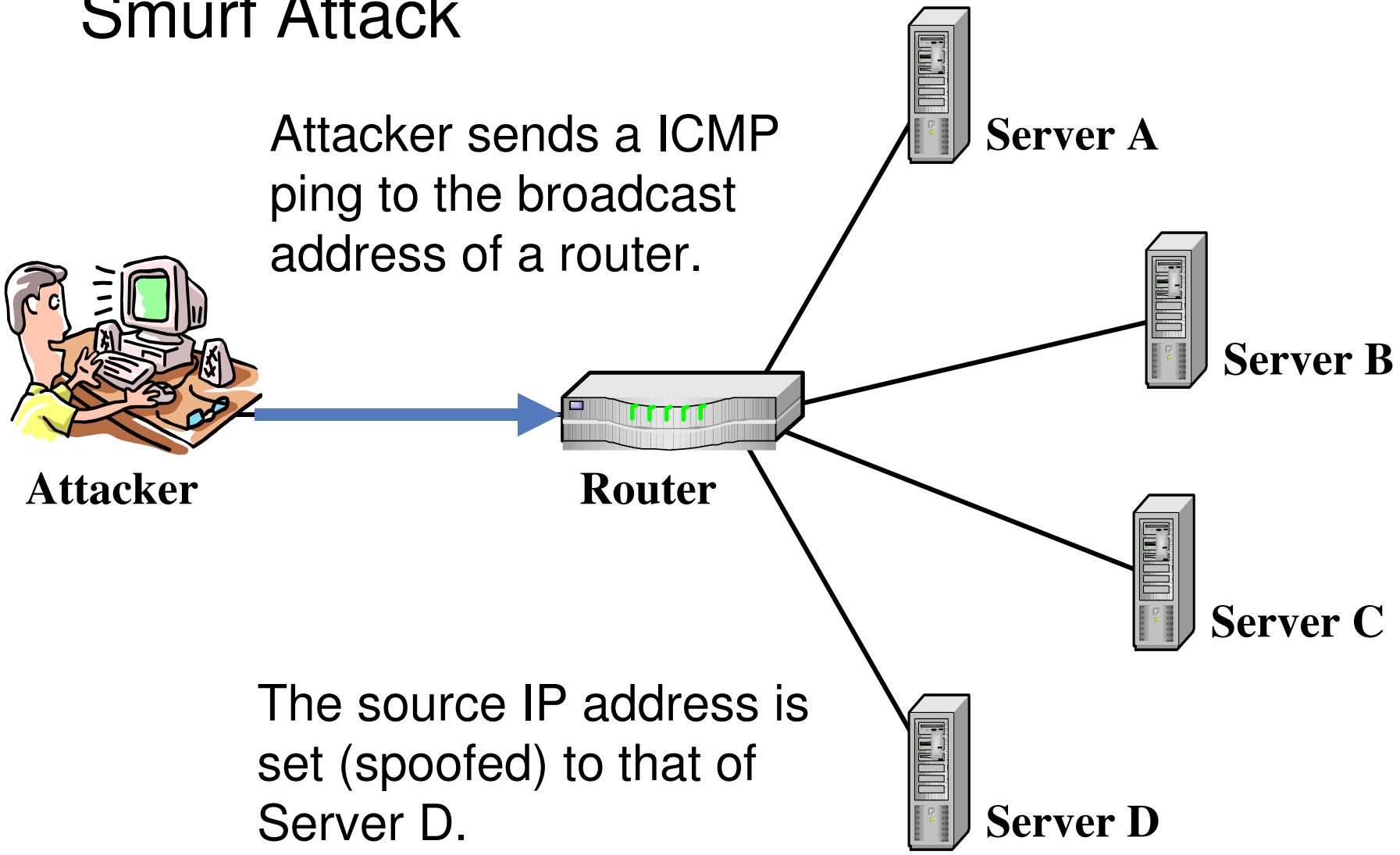
The Complete Syn-flood



No More Resources

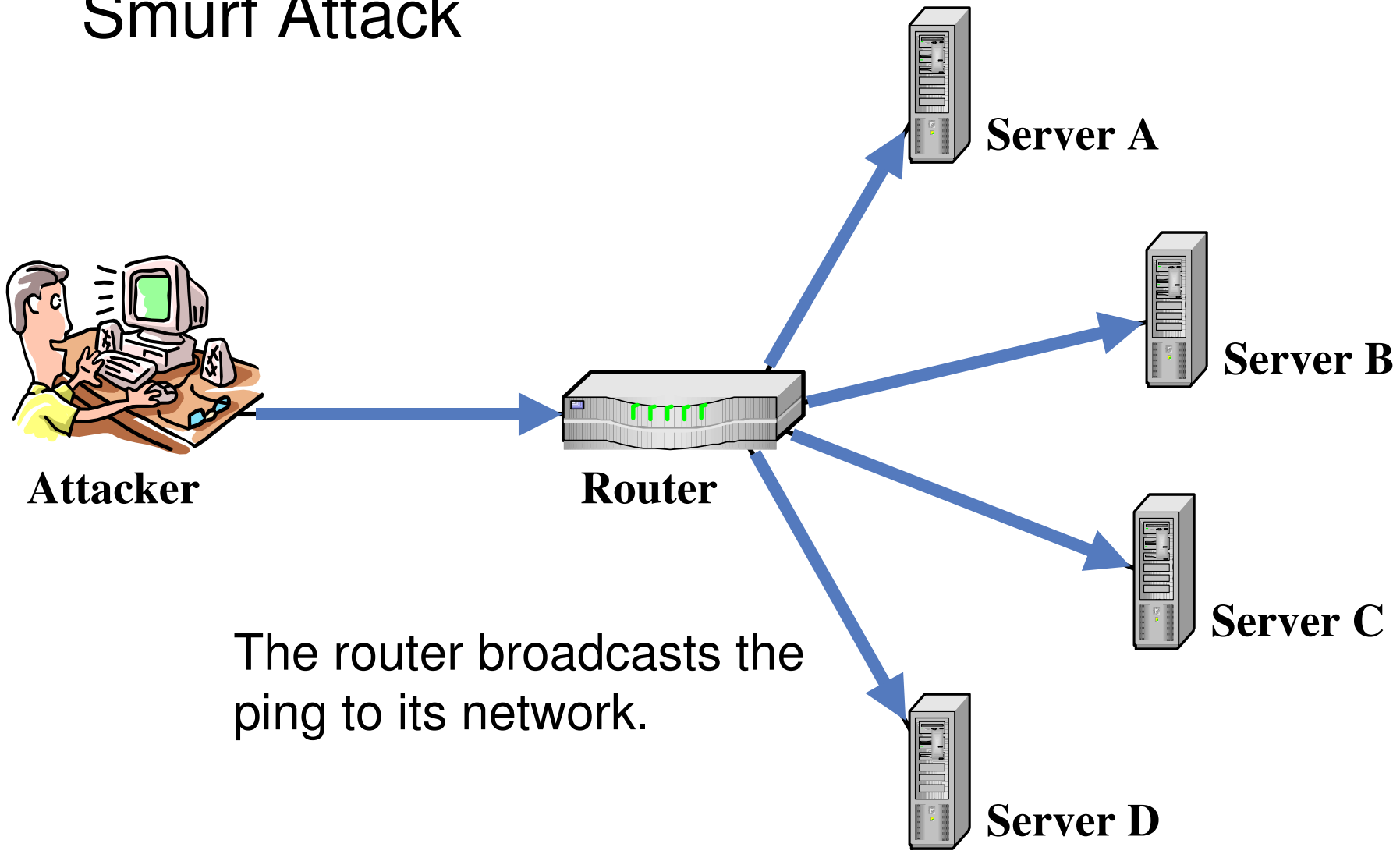
Smurf Attack

Attacker sends a ICMP ping to the broadcast address of a router.



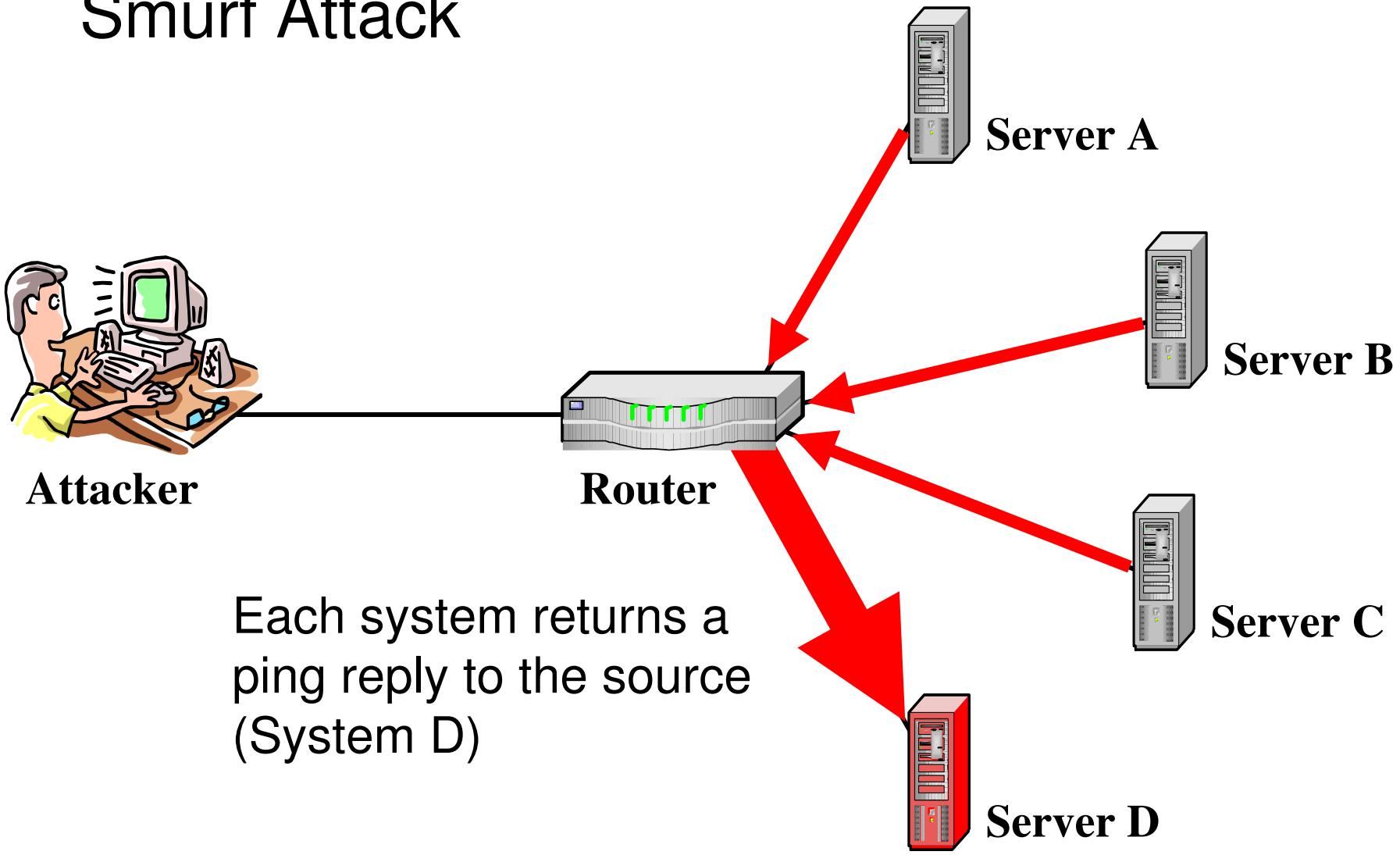
The source IP address is set (spoofed) to that of Server D.

Smurf Attack



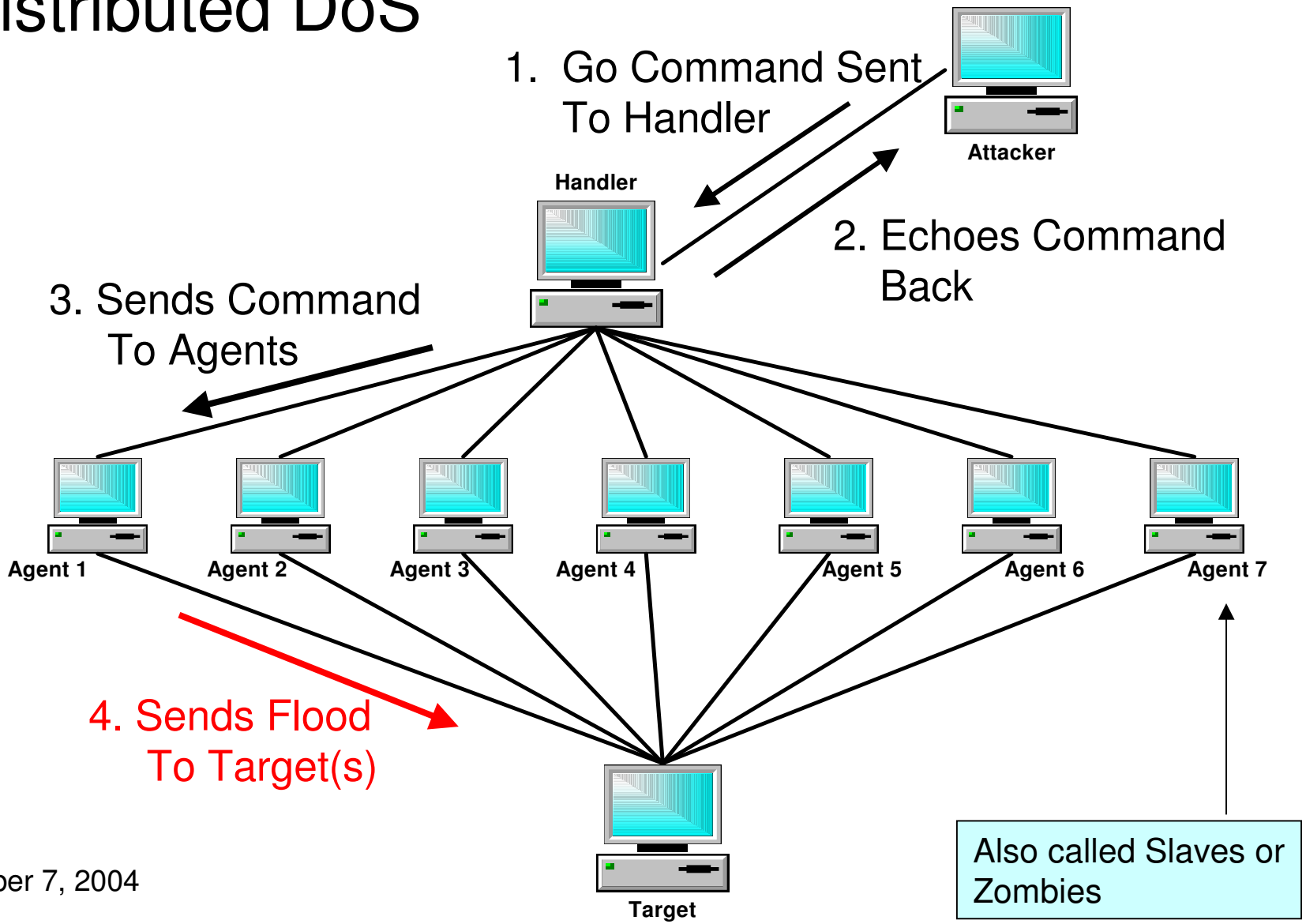
The router broadcasts the ping to its network.

Smurf Attack

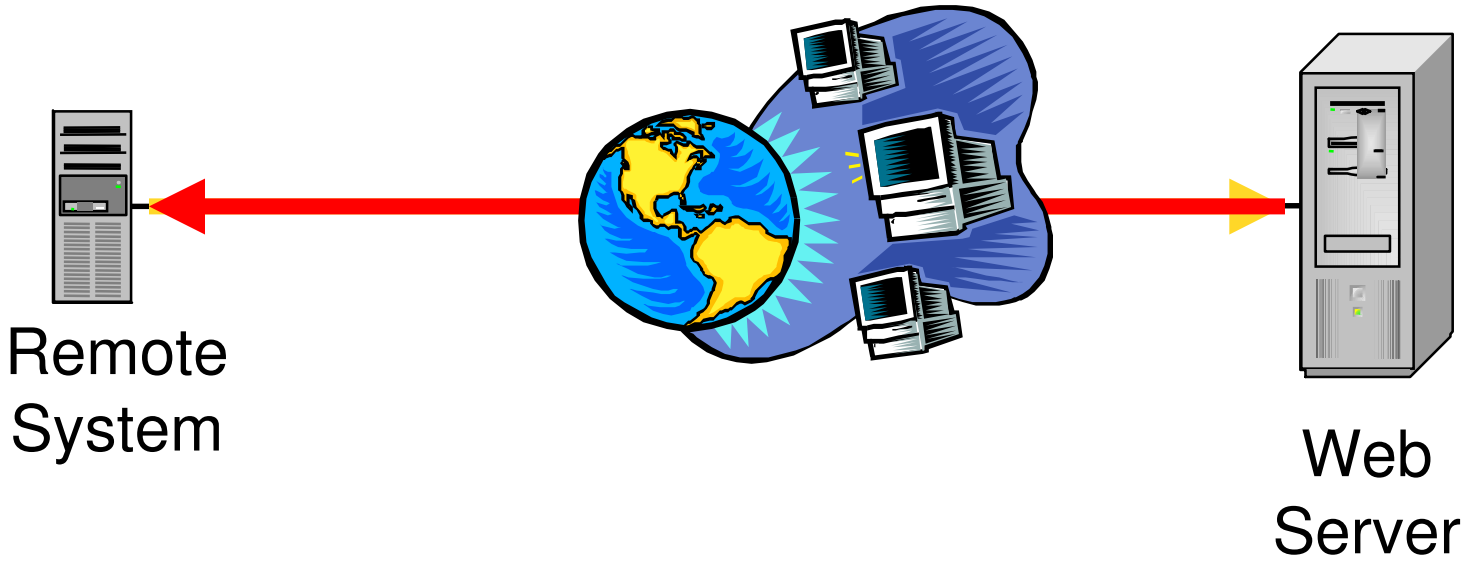


Each system returns a ping reply to the source (System D)

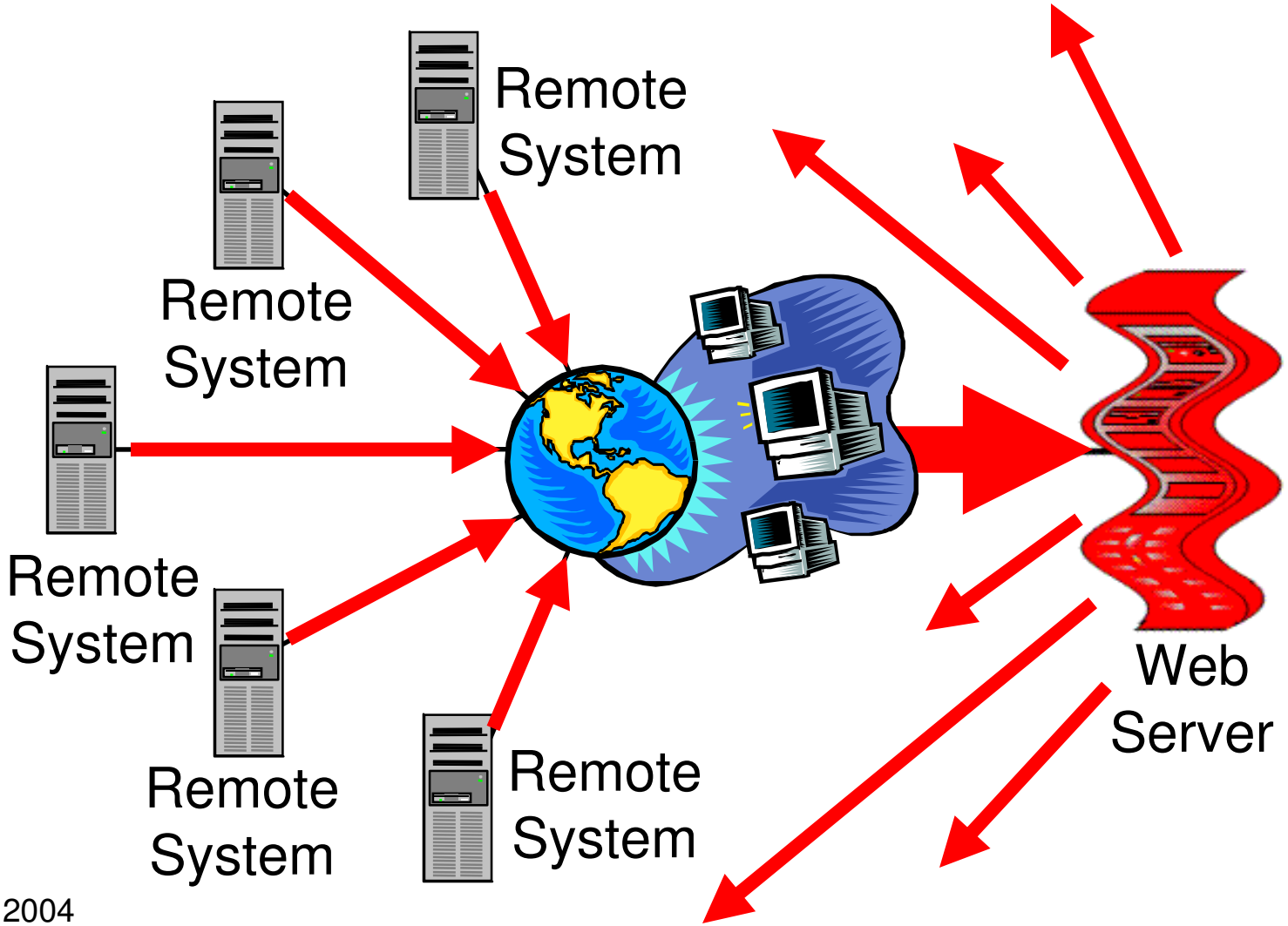
Distributed DoS



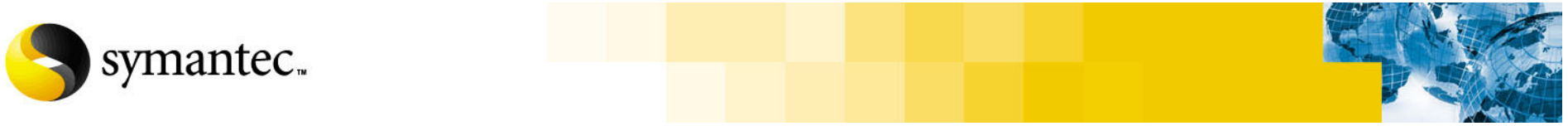
DDoS – ICMP (Ping)



DDoS – ICMP (Ping) Flood



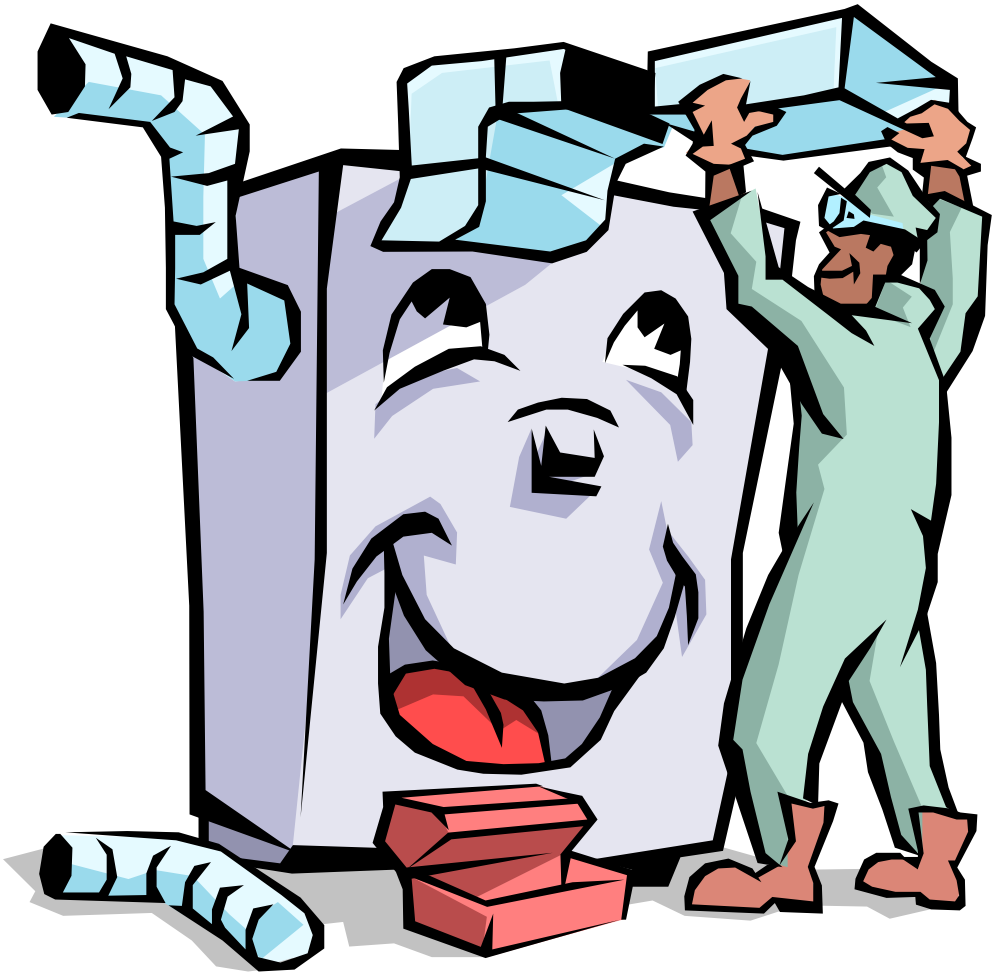
Viruses and worms



Viruses and Worms

- **Viruses**
  - **Historically more effective on desktop environments**
  - **Linux viruses have been very rare**
  - **Ineffective so far**
- **Worms**
  - **Historically more effective on server environments**
  - **A number of Linux worms have been written**
    - **Lion**
    - **Adore**
    - **Cheese**
    - **Recent Apache worm**
    - **Some others**
  - **Have had moderate effect**

III: The Solution

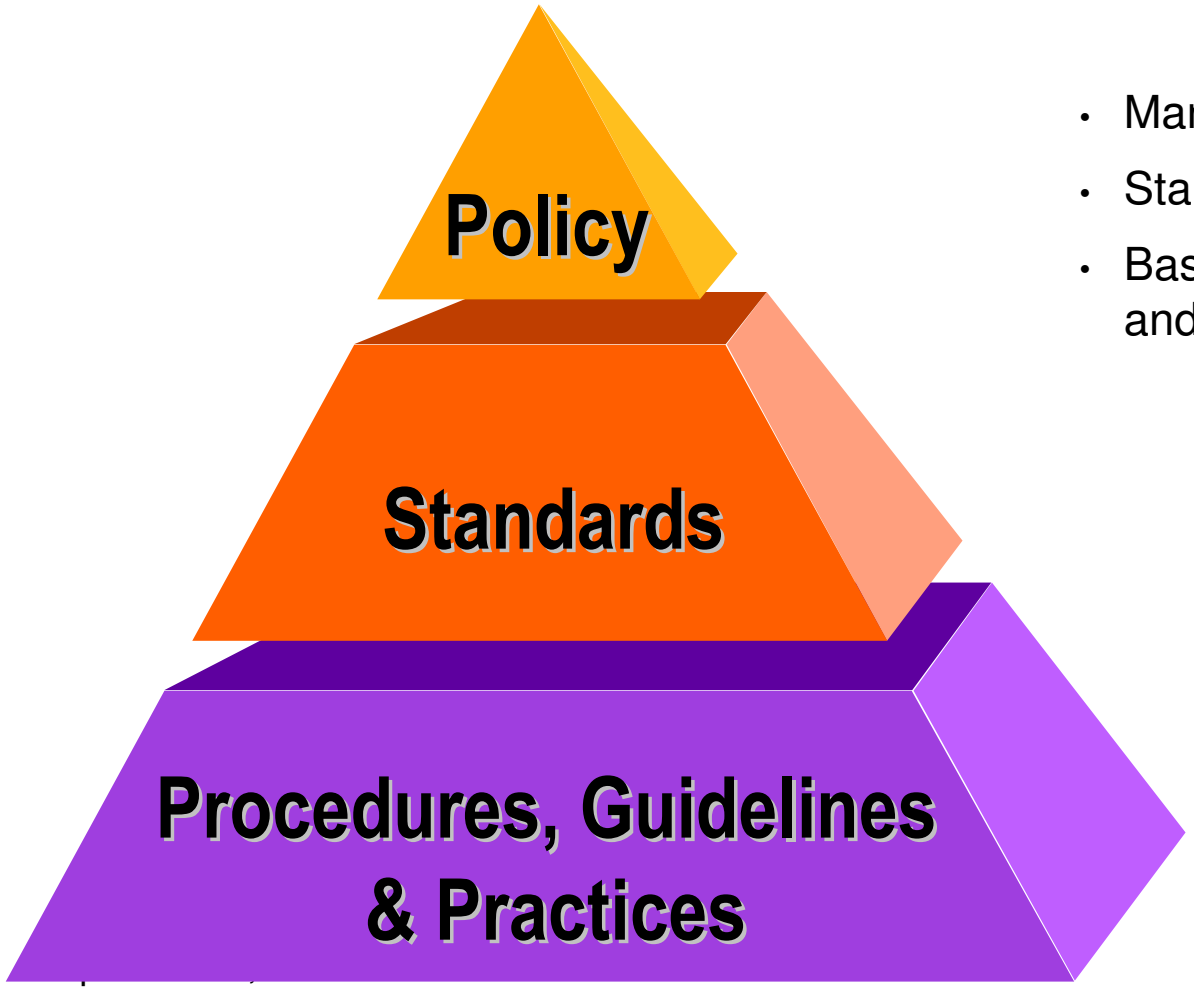


The Solution

- **Start with a security policy**
- **Physical security**
- **Installation**
- **Network / system services**
- **System logging**
- **Firewalls**
- **Delegating Root**
- **Intrusion Detection**
- **Securing Email**
- **Buffer Overflows**
- **Virtual Private Networks**
- **Keep it Updated**
- **Website Security**
- **Backups**
- **Layers of Defense**
- **Managing with Clustered Servers**
- **Assessment**

Start with a Security Policy

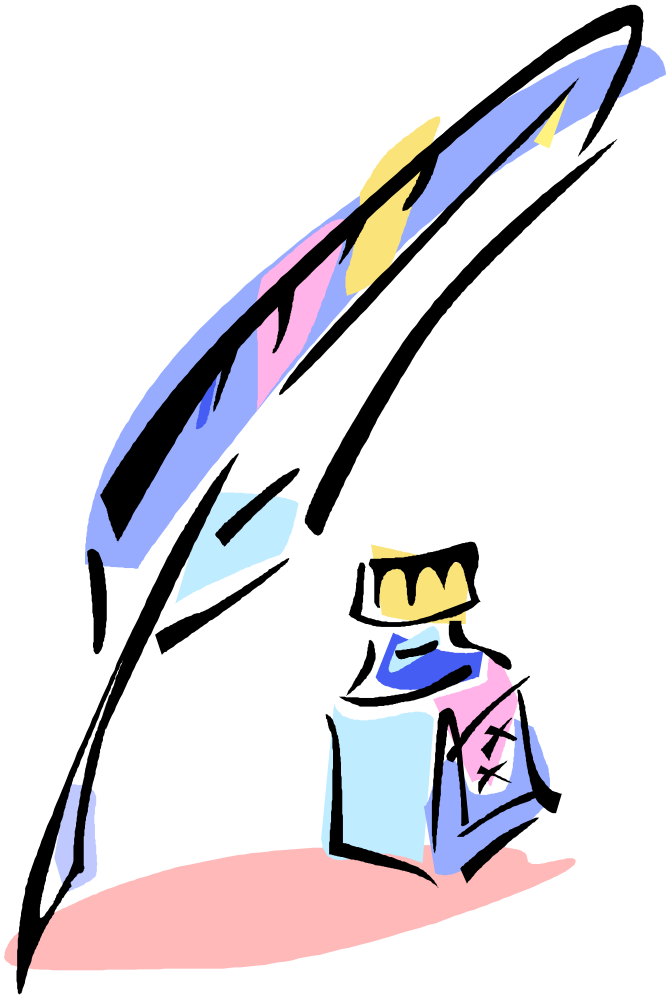
Policy Is Key to Security



- Mandate to implement security
- Standard to measure security
- Basis for all security technology and procedures

What Is A Security Policy

- **Plan or Course of action**
  - **Deploy an Information security solution**
  - **Meets your needs**
- **Provide a metric that you can measure compliance**
  - **Identifies roadmap to compliance**
- **Insure consistency**
- **Define acceptable use**
- **Develops a security culture**



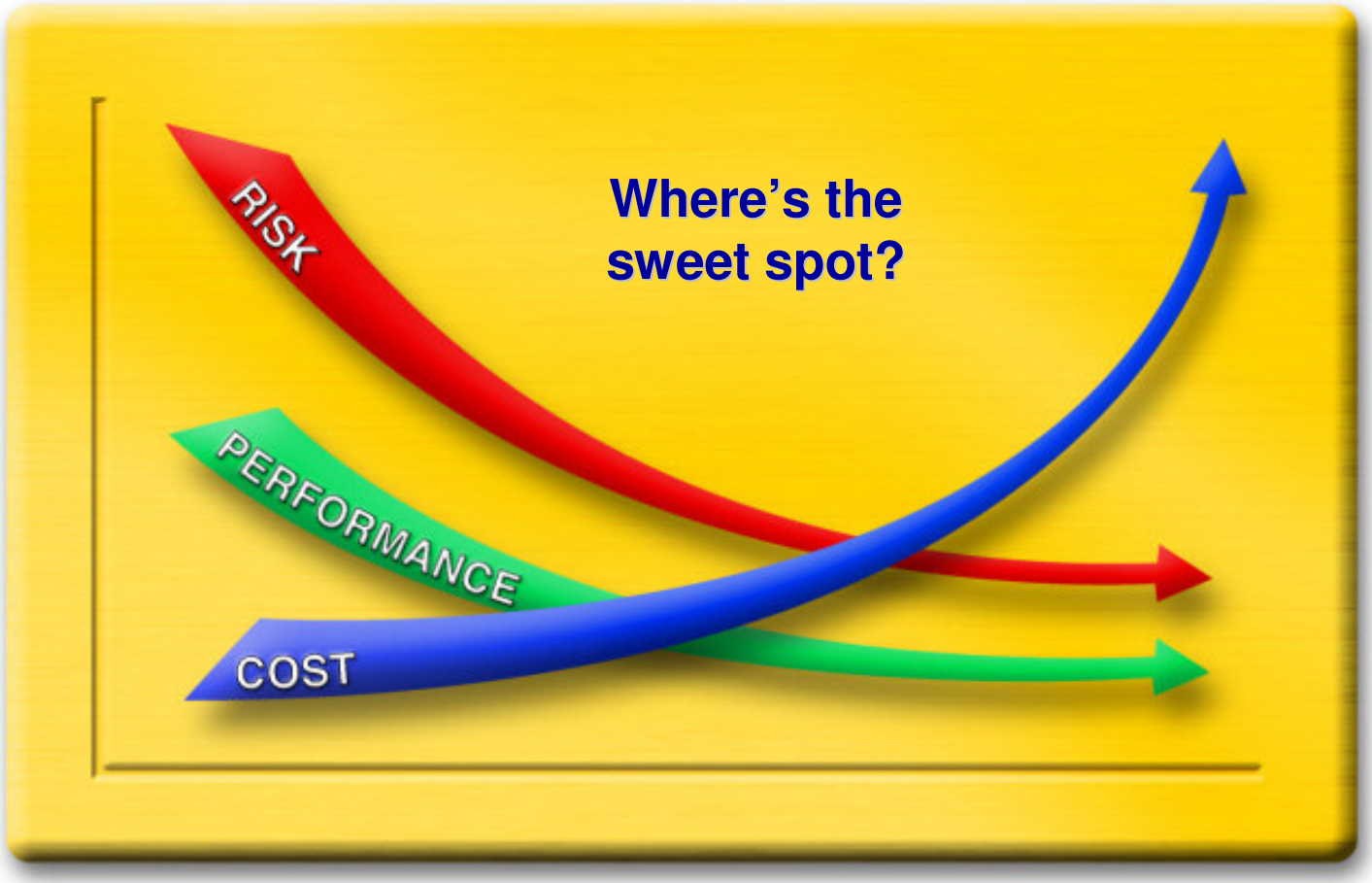
Planning a security policy

- **Identify all resources**
  - **Know what needs protecting**
  - **Be complete**
- **Find a working balance**
  - **Don't stop development in favor of security**
  - **Don't protect $100 item with a $10000 solution**
- **Keep it simple and straight forward**
  - **Easier acceptance and deployment**

No Need to Start From Scratch

- **Use existing standards and "Best Practices"**
- **Look at what others are doing**
- **Meet standard of due care**
- **Pay attention to regulations and requirements**
  - **Government (HIPAA, FDIC, …)**
  - **Industry (ISP 17799, …)**
  - **Partner (VISA, …)**
- **Make sure core business and key assets are covered**
- **Consult with security experts to help develop policy**

Managing Security Risk



Security Policy Objectives

- **Confidentiality**
- **Integrity**
- **Availability**

The Sans Security Policy Project

- **Link to a short primer on security policies**
- **Contains example policies components**
- **Lists other resources on the web**

- **http://www.sans.org/resources/policies/**

Physical Security

Physical Security

- **Physical security is often ignored or misunderstood**
- **At risk is the access to:**
  - **system and resources**
  - **user space**
  - **trash/dumpsters**
  - **network and equipment**

Access to System and Resources

- **They can be stolen**
  - **From a desk or computer room**
  - **Laptops at the airport**
  - **…**
- **They can be damaged**
  - **Power cord cut**
  - **System destroyed**
  - **…**
- **Reconfigured or modified**
  - **Systems boot differently (BIOS)**
  - **Operating system runtime parameters are different**
  - **…**
- **Information accessed**
  - **Confidential files copied**
  - **Data base read**
  - **…**

Access to User Space

- **Password information**
  - **Written on sticky notes (possibly stuck to monitor)**
  - **Written in notebooks**
  - **…**
- **Contact information**
  - **Possible targets for social engineering**
  - **People in charge of key resources**
  - **…**
- **Confidential documents**
- **Access through unattended terminals**
  - **Owner has temporary left their desk**
  - **The attacker can gain short term access**
  - **…**

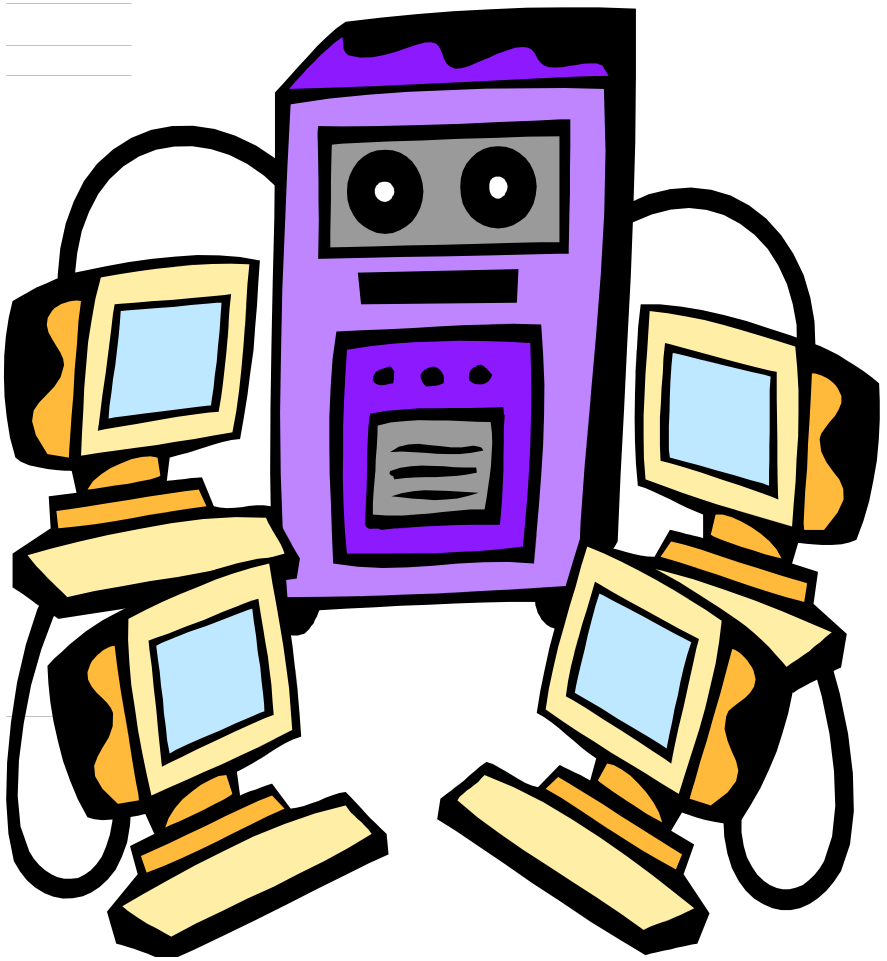
The Trash

- **Confidential information is often just thrown in trash**
- **Trash bins are often placed in easy to access location**
- **Attackers can simply search trash**

This is called "Dumpster Diving"

Access to Network and Equipment

- **Direct connection (DHCP)**
  - **From a laptop for example**
- **Wiretap (Cut the lines)**
- **Denial-of-Service Attack**
- **DNS cache poisoning**
- **Reconfigure**



Locking down the office

- **Place critical systems in computer room and restrict access**
- **Password protect BIOS**
- **Restrict booting from removable media**
- **Avoid duel booting Linux with other operating systems**
- **Network cables should be removed from outside building walls**
- **Users should lock their terminals when away**
- **Passwords should not be written down (use a password safe if many passwords must be remembered)**
- **Network maps should not be posted in open areas**

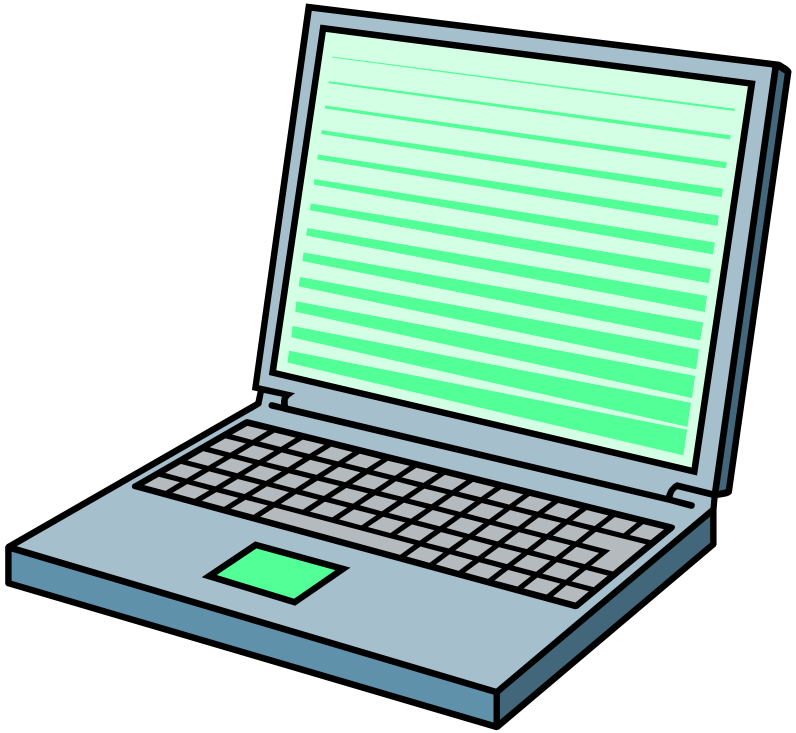
“Boot access is Root access”

Locking down the office

- **Phone lists should be kept online only**
- **All confidential documents must be shredded before being discarded**
- **Garbage cans and dumpsters should be located in locked and monitored area**
- **Company organization charts should never be posted in open area**
- **While a security policy is important, it should never be posted**
- **Company letter head should be controlled**

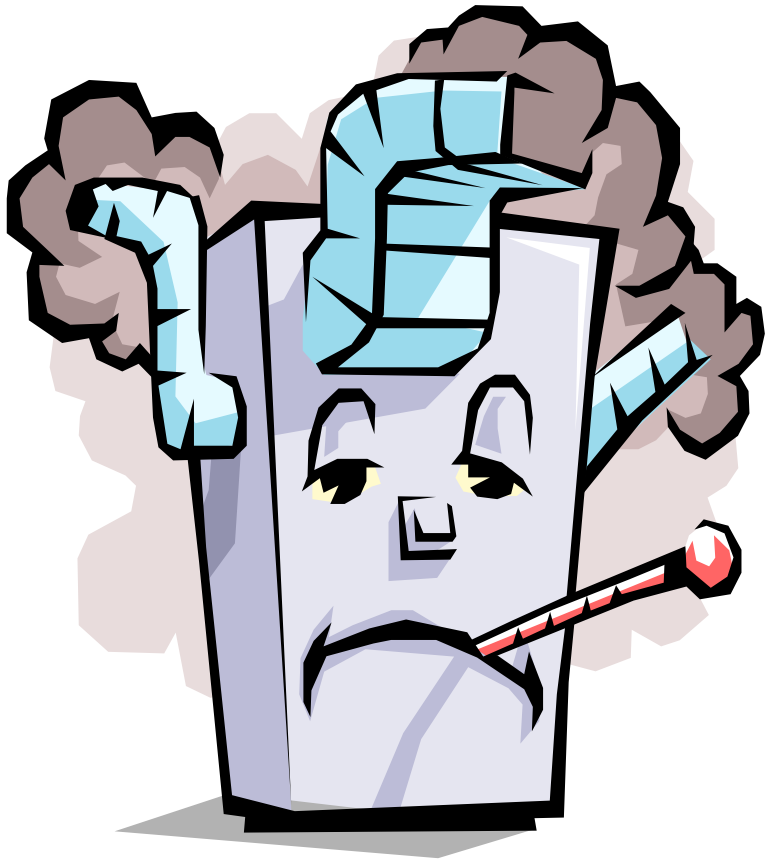
Locking down the remote user

- **If a laptop is stolen, the thief will gain access to it**
- **Confidential Information should be encrypted (individually or grouped in an encrypted file system)**
- **Laptop should be regularly backed up**
- **Laptop should be to a physically secure object (desk, wall, …) with a locking security cable**

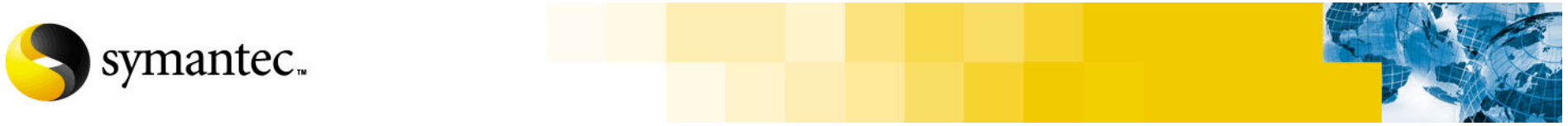


Securing The BIOS

- **BIOS passwords are limited**
  - **7 character max with known master passwords**
  - **Should still be used**
- **Disable booting from removable media**
  - **Can be used to circumvents any security measures that you have made**



Installation



Install Only What You Need and Use

- **Do not use default install**
  - **Can include may utilities and services that you will never use**
  - **Only install the minimal packages required for the system to function as desired**
- **Each additional application increases the chance of abuse**
- **Add at least one non-privileged user**
  - **This should be your default login**
  - **Use su or other delegation tools to elevate privilege (discussed later)**
- **Avoid installing servers with multiple functions (web, FTP, e-mail, …)**
  - **Move these onto separate and dedicated server systems**

Separate User Areas From System Areas

- **Divide installation into separate partitions**
  - **Increase system robustness**
  - **Prevent user level denial-of-service**
    - **Filling up file systems)**
- **Consider the following:**

  / (This partition must exist)

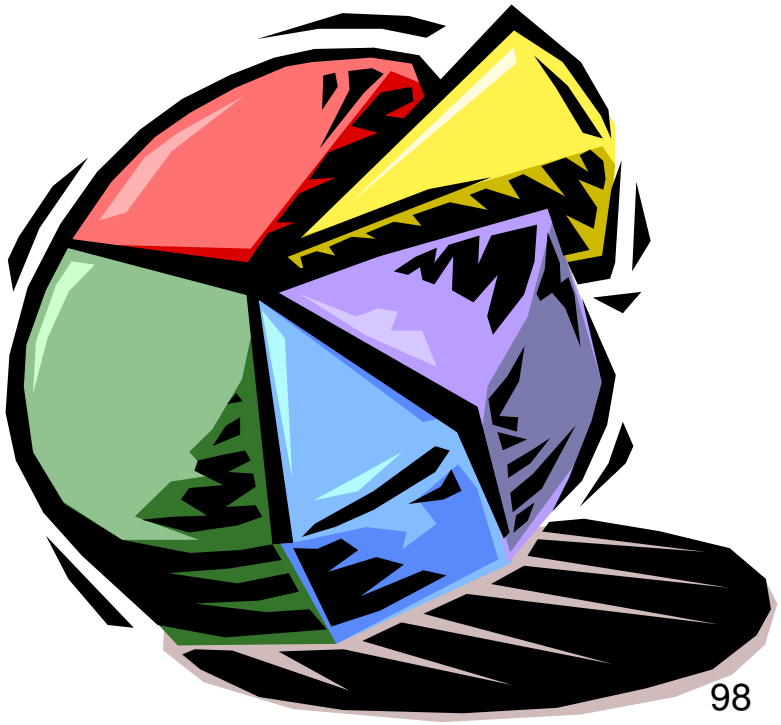
  /Home

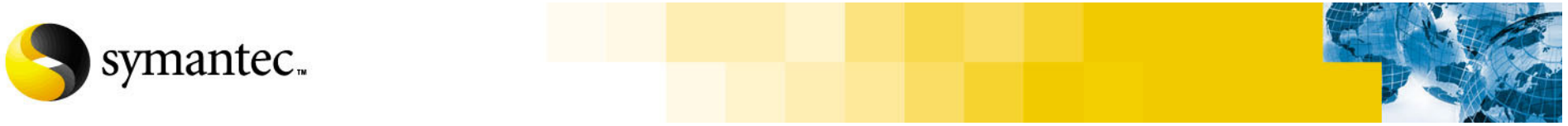
  /tmp

  /var

  /Usr (possibly as read only)

  Just a start





Mounting Partitions

- **All but / and /usr file systems should be mounted with the "nosuid" option**
  - **So that set-UID or set-GID programs cannot be created in user space**
  - **This is especially true for /tmp**
- **When possible**
  - **Mount file systems read-only**
  - **Use noexec to control where executables can be located**

Is Your Password “Hard to Guess?”

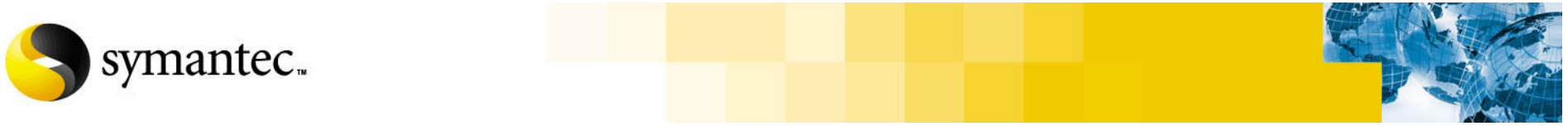
- **Don’t use easy to guess passwords**
  - **No password**
  - **Login name (login name = password)**
  - **Predictable names**
    - **Toor for root (root spelled backwards)**
- **Don’t use familiar names, dates and numbers**
  - **Family members (spouse, children, parents, your name)**
  - **Last name**
  - **Pet’s name**
  - **Birth date**
  - **Age**
- **Don’t use words that can be found in a dictionary**
  - **susceptible to dictionary attack**

Pick a Strong Password

- **At least 8 characters long**
- **Use a combination of alpha/numeric characters**
- **Intermix upper case with lower case characters**
- **Combine with special characters in passwords such as punctuation marks**
- **Using the first character of each word in a phrase is a good way to create a strong password**

"A strong password, can make the difference" becomes "Asp,cmtd"

- **Avoid using common phrases**



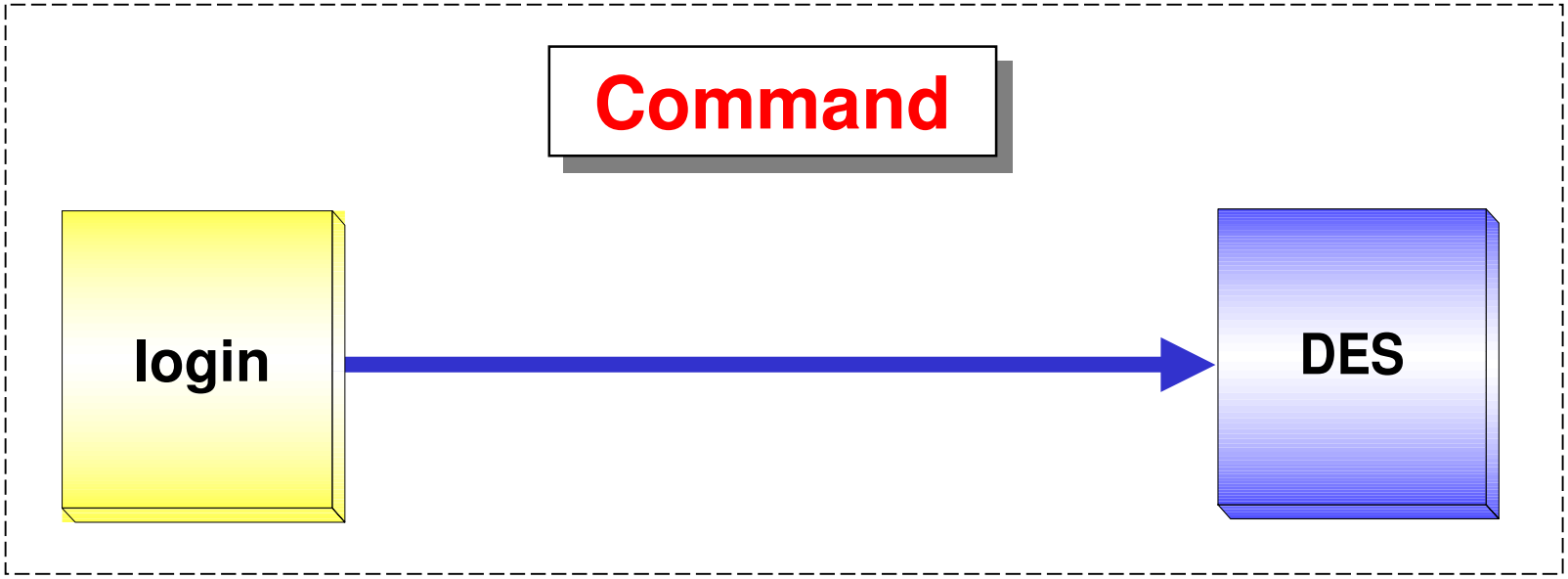
Use a Shadow Password

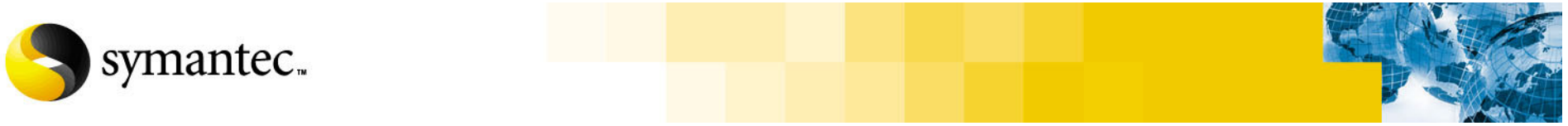
- **Password information originally combined with login information**
  - **/etc/passwd**
- **Required to be readable by everyone**
- **Passwords were easy to discover using a password cracker**
- **Shadow passwd file was implemented**
  - **Readable only by root only**
  - **User name information is to readable by everyone**
- **The Linux shadow password file is located at /etc/shadow**

Traditional User Authentication

- **Password are represented by a unique one-way hash (DES)**
- **The actual password is never stored on the system**
- **No way to derive password from hash**
- **When a user attempts to login:**
  - **Has is calculated for given password**
  - **Compared with known password hash**
  - **If they match – access is granted**
- **The password is limited to a maximum of 8 characters by DES**
- **All authentication commands linked with DES library**
- **New access methods require recompile**

The Traditional Authentication Method

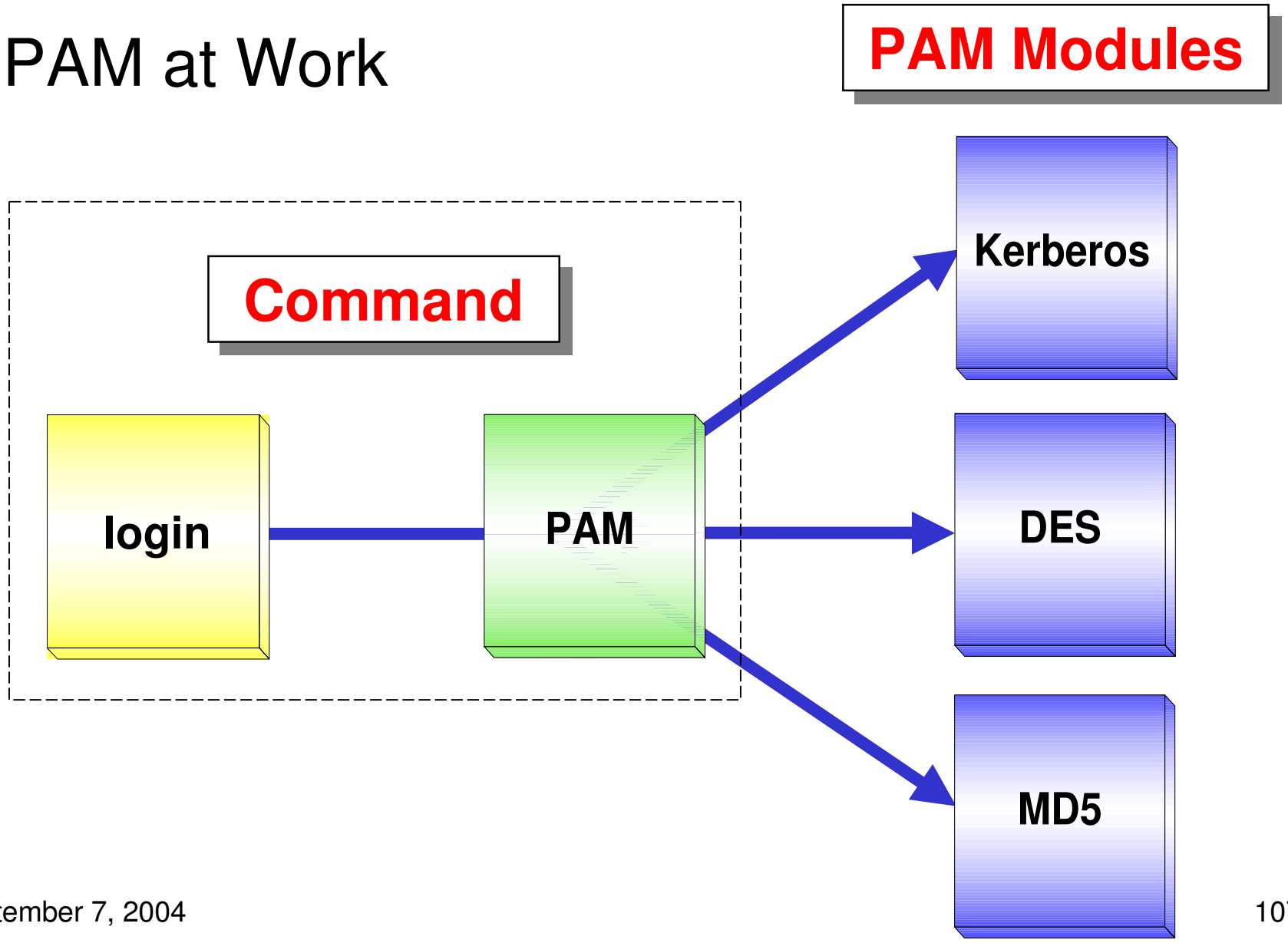


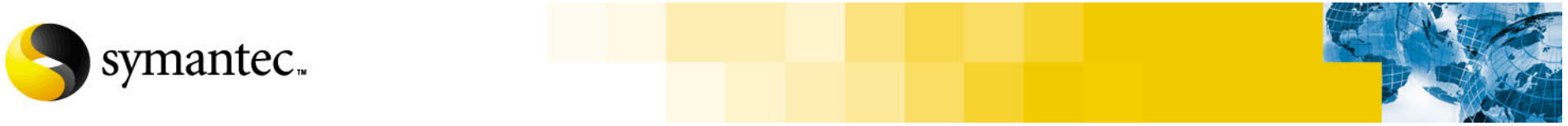


PAM – A New Face to Authentication

- **PAM functions as an abstraction layer**
- **Linked with each authentication command**
- **Access control method is determined through config files**
- **Recompile is no longer required**
- **A large number of authentication modules are available**

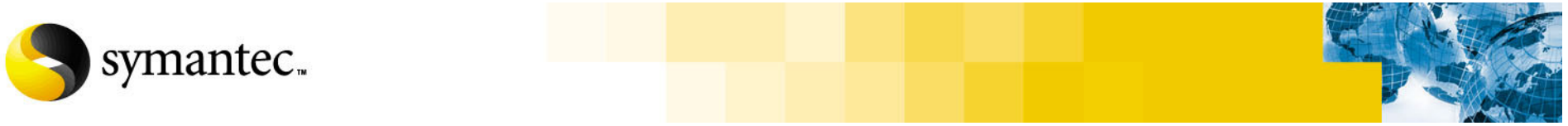
PAM at Work





Using PAM

- **Most distributions now include PAM integration**
- **A set of configuration files are used to control PAM**
- **The DES one-way hash is used by default**
- **Additional authentication methods can be added**
  - **Install new authentication library and PAM configuration files**
  - **Change PAM configuration to use new authentication method**
- **PAM MD5 hash modules is commonly included**
  - **Has no limit on password length**
  - **Takes more time to calculate a password hash**
    - **Increases time to crack MD5 passwords**
  - **Excellent alternative to DES**

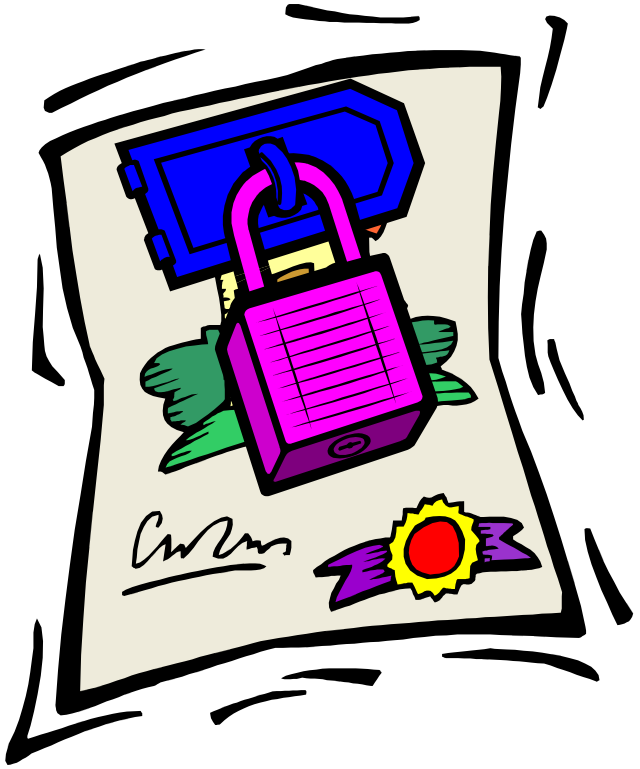


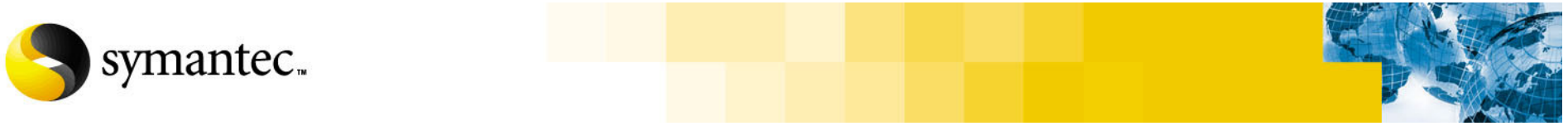
Boot Loaders

- **Used to select what to boot**
  - **Multiple Linux kernels**
  - **Other operating systems**
- **Can pass startup parameters to the Linux kernel**
  - **Specify a initial run level**
    - **Overrides the default in /etc/inittab**
    - **Possibly single-user mode forgoing user authentication**
  - **Override the default init command**
    - **Used to spawn a shell as root forgoing any user authentication**
- **LILO (LInux LOader) is used to select what to boot**
- **GRUB (GRand Unified Bootloader) is used to select what to boot**

Password Protect The Boot Loader

- **Limit access to single user mode**
- **Limit access to boot load consoles**
- **Limit access to insecure operating system (win9x, DOS, …)**





Dual Booting

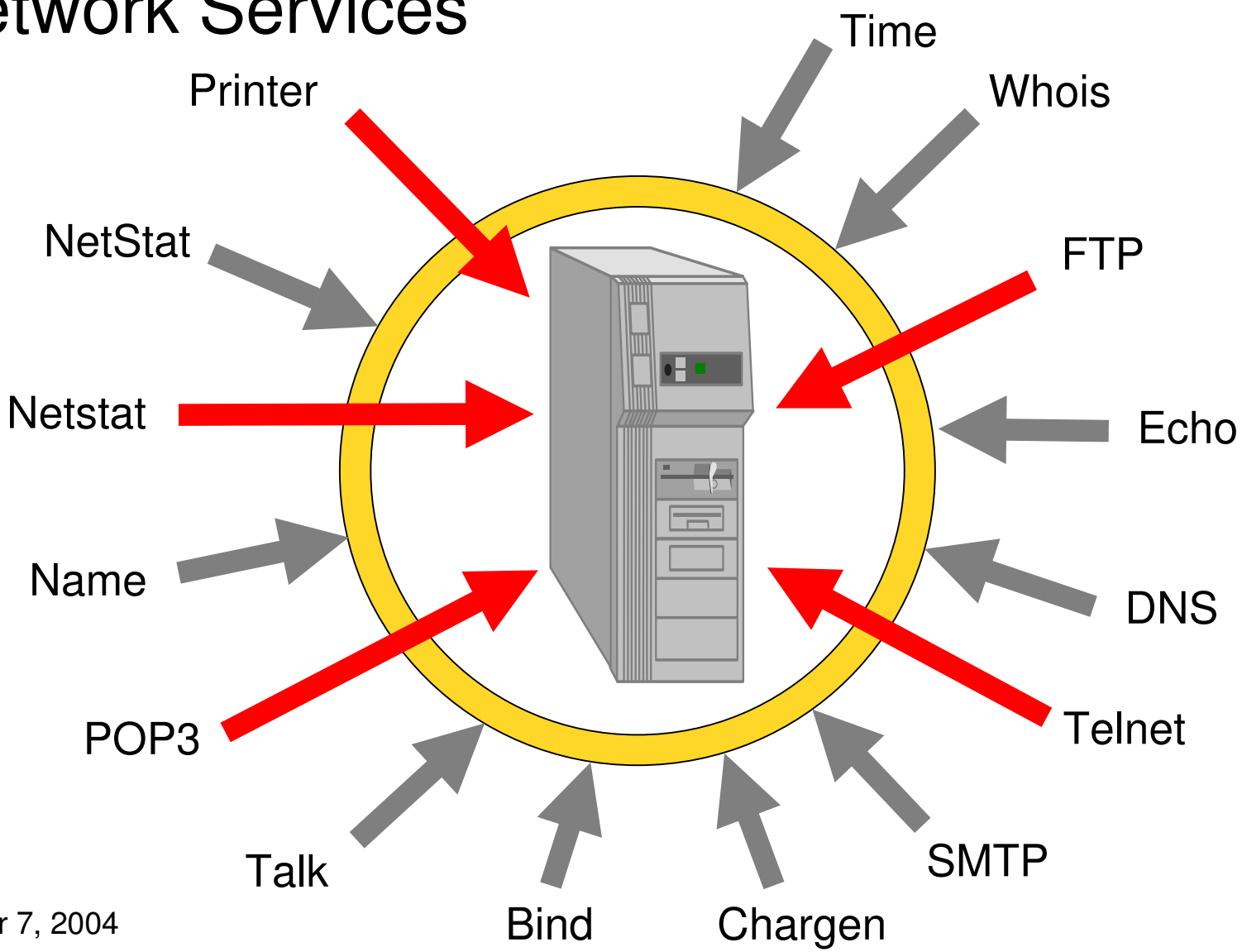
- **A computer system with multiple operating systems**
  - **Is no more secure that the weakest one**
- **Only install operating systems that meet your security needs**
- **Add password protection for each insecure operating system**

Network and System Services

Network Services

- **Network services allow one system to communicate with another**
  - **Apache web server is a network service that provides web site based capabilities**
  - **Typically run on port 80 (can run on additional or different ports)**
- **Vulnerabilities in network services are common attack points**

Network Services



Securing Network Services – Best Practices

- **Separate services onto separate systems**
  - **www**
  - **ftp**
  - **SMTP**
  - **Others**
- **Identify all network services**
  - **Remove all but required services**
- **Use "netstat –at" to identify all listening services**
- **Use "lsof –i +m" to find associated process for each listening port**

Using Netstat to find Network Services

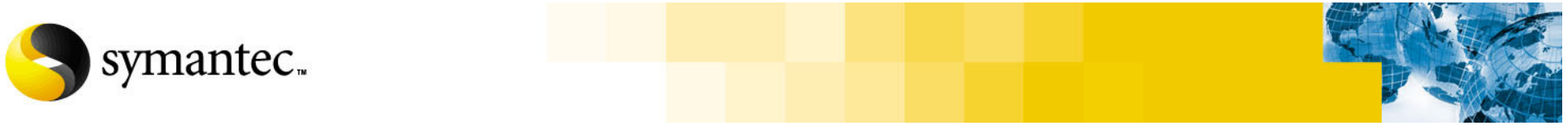
```
# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               State
tcp        0      0 *:printer                   LISTEN
tcp        0      0 *:http                      LISTEN
tcp        0      0 *:https                     LISTEN
tcp        0      0 *:32768                     LISTEN
tcp        0      0 *:sunrpc                    LISTEN
tcp        0      0 *:ssh                       LISTEN
#
```

Note: **Output has been modified for readability**

Using lsof to Find Associated Processes

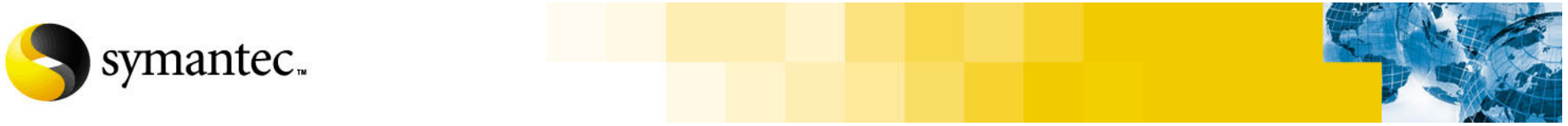
```
# lsof -i +M
COMMAND     PID USER   TYPE DEVICE SIZE NODE NAME
portmap     726 root   IPv4  UDP *:sunrpc[portmapper]
portmap     726 root   IPv4  TCP *:sunrpc[portmapper]
rpc.statd   755 root   IPv4  UDP *:32768[status]
rpc.statd   755 root   IPv4  TCP *:32768[status]
sshd        904 root   IPv4  TCP *:ssh
lpd         998 root   IPv4  TCP *:printer
httpd      1028 root   IPv4  TCP *:https
httpd      1028 root   IPv4  TCP *:http
#
```

Note: **Output has been modified for readability**



Eliminating Unwanted Network Services

- **Most distributions start and stop network services from two locations**
  - **Init.d directory (/etc/init.d on most systems)**
  - **Inetd or xinetd**
- **Stop all unwanted network services and disable or remove them**
  - **If a network service is not needed, it is better to remove it to prevent accidental restart (also saves space)**



The init.d directory

- **Contains scripts to start and stop processes (including services)**
- **Links are made from each of these scripts to the run-level specific directories: rc0.d, rc1.d, rc2.d, rc3.d, rc4.d, rc5.d and rc6.d**
- **Part of the “Process Control Initialization” (see man-pages on init, Inittab, initscript and runlevel)**

Stopping a network service

- **To stop the portmap service:**
  - **cd /etc/init.d**
  - **./portmap stop** **# shutdown the service**
  - **chkconfig portmap off** **# disable service from starting**

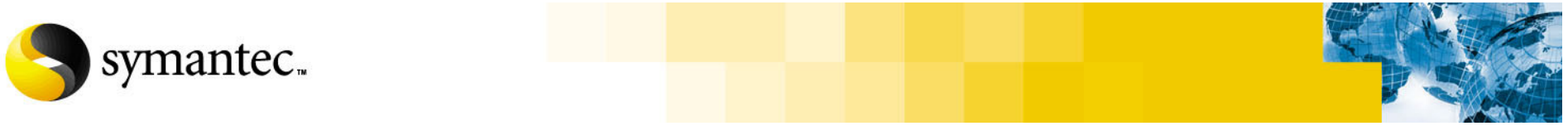
    or
  - **rpm –qf /etc/init.d/portmap** **# which packages contains startup script**
  - **rpm –e portmap** **# remove the service completely**
  - **Apt-get remove portmap**

The Inetd Service

- **A supper service for starting other services**
  - **Saves memory and process table usage**
- **Configuration file (/etc/inetd.Conf) defines what network services inetd will monitor and the executable to call to handle each request**
- **Inetd monitors each network port specified in the "/etc/inetd.Conf" files**
- **When a connection is made to the system, inetd will identify the service type and call the appropriate executable to handle the request**
- **No ability to control access or throttle network connections**

A typical exert from the /etc/inet.d file

```
#echo          stream  tcp     nowait  root    internal
#echo          dgram   udp     wait    root    internal
#daytime       stream  tcp     nowait  root    internal
#daytime       dgram   udp     wait    root    internal
#chargen       stream  tcp     nowait  root    internal
#chargen       dgram   udp     wait    root    internal
#time          stream  tcp     nowait  root    internal
#time          dgram   udp     wait    root    internal
ftp     stream  tcp     nowait  root    in.ftpd -l -a
telnet  stream  tcp     nowait  root    in.telnetd
```



Some Problems With Inetd

- **All or nothing access control**
  - **All enabled services are available to every one**
  - **The TCP Wrappers package was written to compensate for this deficiency**
- **No connection limit**
  - **Attackers could continue to open connections until the process table is full and the system becomes unusable (DoS)**
- **Poor or nonexistent logging**
  - **By default connections are not logged**
  - **This is true for both successful for failed connection attempts**

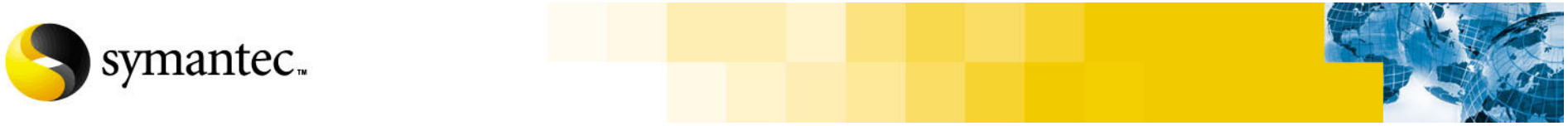
Securing Inetd

- **Remove or comment out all unwanted services in the /etc/inetd.conf file**
  - **Each available service increases the change that the attacker will be able to gain access or use the system to attack another**
  - **Two common debug services, echo and chargen, are typically left on. These should be commented out**
- **Use TCP Wrappers tool to add access control**
  - **Provides fine grain access control for each service**
  - **Adds enhanced logging**
  - **Called in place of the service daemon executable**
  - **Arguments to TCP Wrappers is the service daemon executable**
  - **Verifies that access is allowed for the specific service and call the executable with arguments**
  - **Simple addition to Inetd.conf**

TCP Wrappers

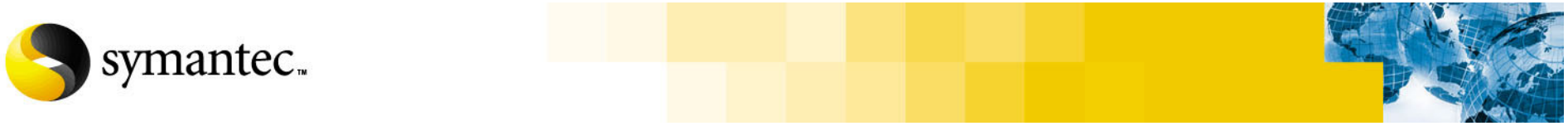
```
ftp      stream  tcp nowait  root    in.ftpd -l -a
telnet   stream  tcp nowait  root    in.telnetd
```

```
ftp      stream  tcp nowait  root tcpd in.ftpd -l -a
telnet   stream  tcp nowait  root tcpd in.telnetd
```



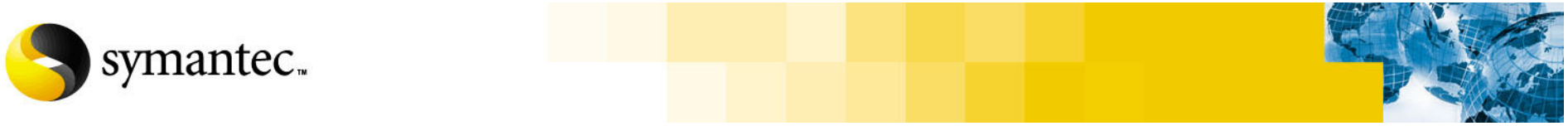
The Xinetd Service (An Inetd Replacement)

- **Includes fine grained access control**
- **Adds enhanced logging features**
- **Provides process throttle to prevent Process-table flooding Denial-of-Service**
- **Forwarding of services requests to another system.**
- **The ability to specify unique banners for each network service.**
- **Xinetd monitors each network port specified in the “/etc/xinetd.Conf” file**
- **Generally configured to also monitor files in directory “/etc/xinitd.d”**
- **See man-page on xinetd, xinetd.conf and xinetd.log**
- **Allows for default settings (can be overridden on a per service basis)**



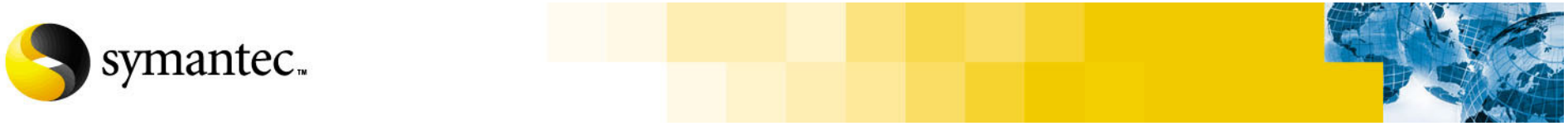
Default settings (/etc/xinetd.conf)

```
# defaults
defaults
{
  instances         = 25 # Max connections per service
  log_type          = SYSLOG authpriv # Log to syslog
  log_on_success    = HOST PID # What to log on success
  log_on_failure    = HOST RECORD # What to log on fail
  only_from         # Deny all access
}
```



Controlling Access (/etc/xinetd.d/finger)

```
# finger service
service finger
{
  socket_type      = stream
  wait             = no
  user             = nobody
  server           = /usr/sbin/in.fingerd
  only_from        = 192.168.1.0/24 # localdomain only
}
```



A disabled service (/etc/xinetd.d/echo)

```
# echo server
service echo
{
  type            = INTERNAL
  id              = echo-stream
  socket_type     = stream
  protocol        = tcp
  user            = root
  wait            = no
  disable         = yes # This service is disabled
}
```

Eliminating services – Our example

- **Shutdown and removed the following services with scripts in /etc/init.d**
  - **Portmap** (portmap service)
  - **nfs-utils** (statd service)
  - **LPRng** (printer service)
  - **yp-tools** (nfs-utils dependency)
  - **Ypbind** (nfs-utils dependency)
  - **Ypserv** (nfs-utils dependency)
- **Xinetd was not being used for any network services and was also removed**

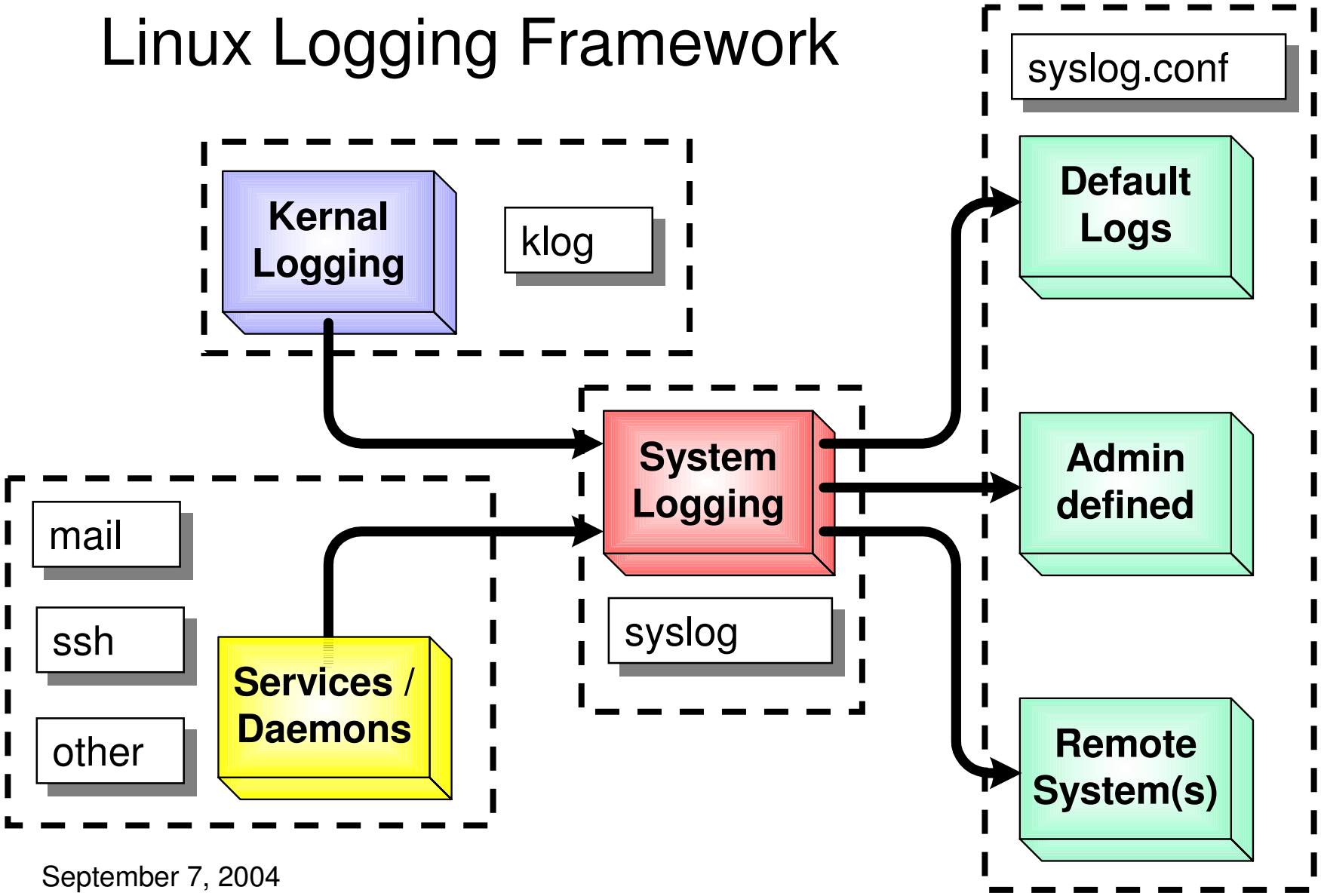
The results

```
# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               State
tcp        0      0 *:http                      LISTEN
tcp        0      0 *:https                     LISTEN
tcp        0      0 *:ssh                       LISTEN
#
```

Note: **Output has been modified for readability**

System Logs

Linux Logging Framework



Securing Syslog

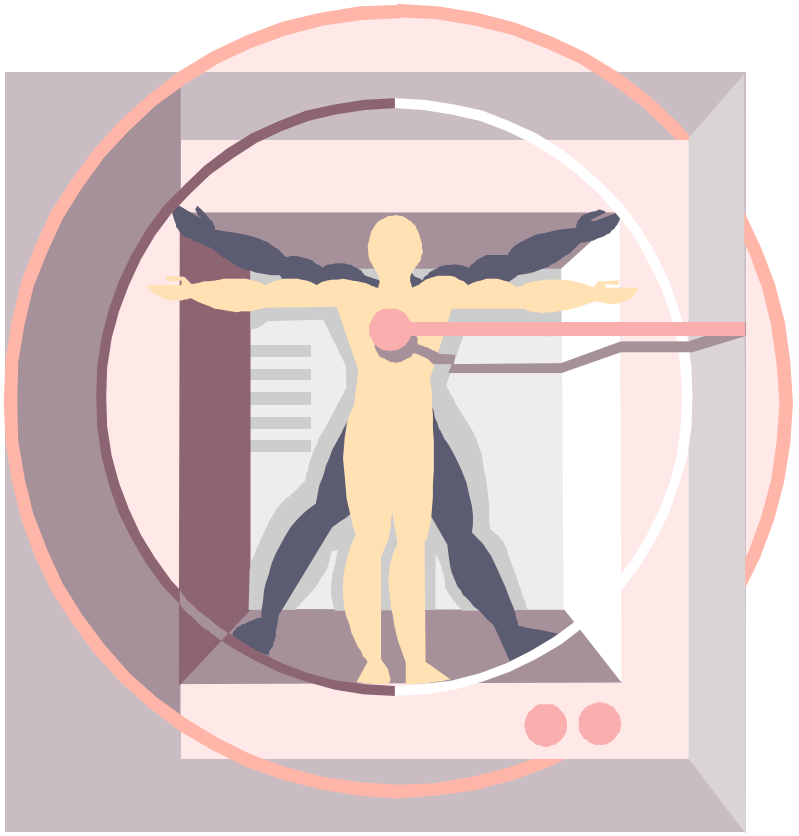
- **Protect the logs by making them unreadable by anybody other than root**
  - **chmod 700 /var/log**
- **Export log information to another system**
  - **if the system compromised, the attacker will also need to compromise this external system to remove the evidence**
  - **Adding the following to syslog.conf:**

```
*.* @external-system
```

sends everything to external-system

Time Synchronization

- **Attacks often affect multiple systems**
- **System logs may record attack**
- **Inaccurate time synchronization can lead to confusion**
- **Use ntpd (Network Time Protocol Daemon)**
  - **All systems**
  - **Log information is accurate**
  - **Correct order of events**

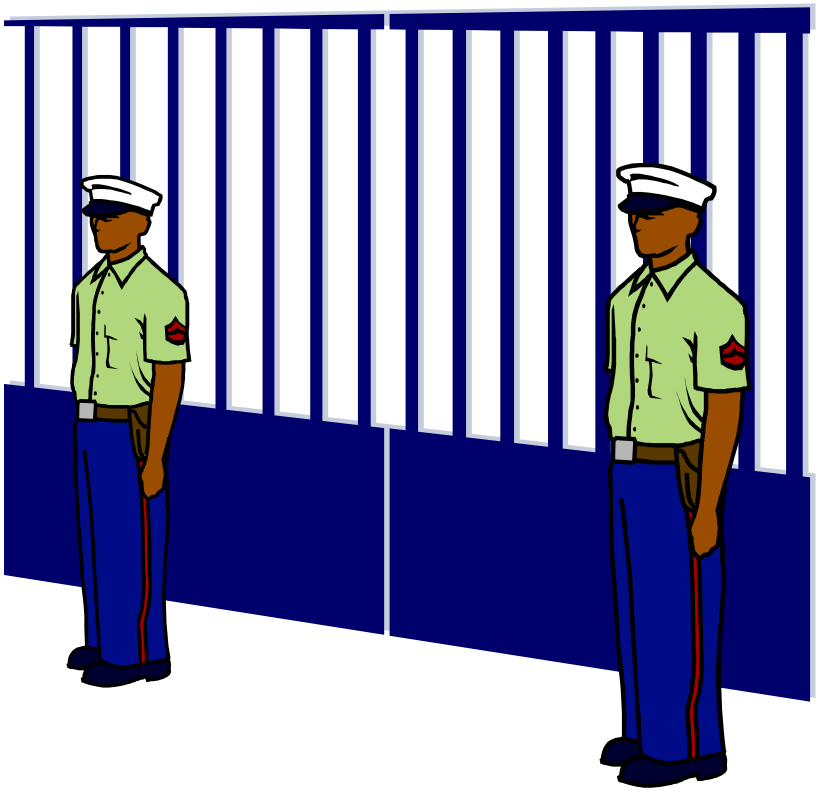


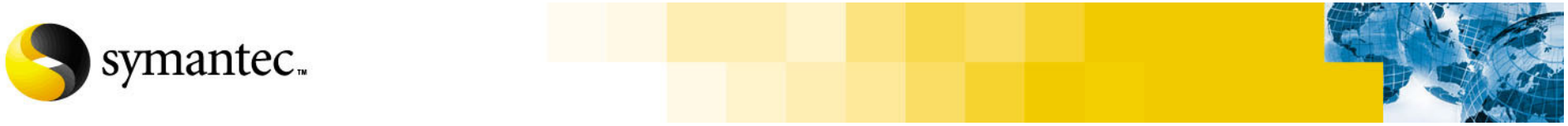
Firewalls

Firewalls

- **Controls network connectivity**
  - **Single system**
  - **Entire Network**
- **Controls what gets in and out**
  - **Traffic types**
  - **Traffic volume**
- **Firewalls enforce security policy**
  - **Intranet / Internet**
  - **Intranet / Extranet**
  - **Extranet / Internet**

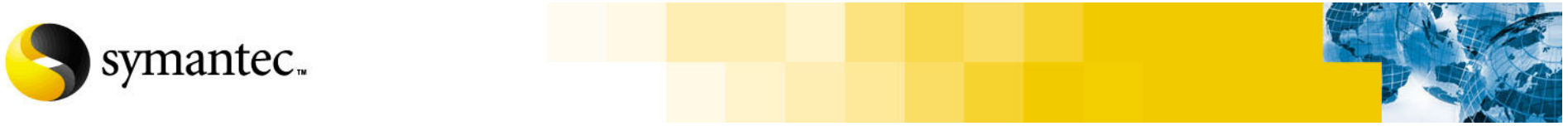
- **Goal: Keep the bad guys out!**





Packet Filtering Firewall

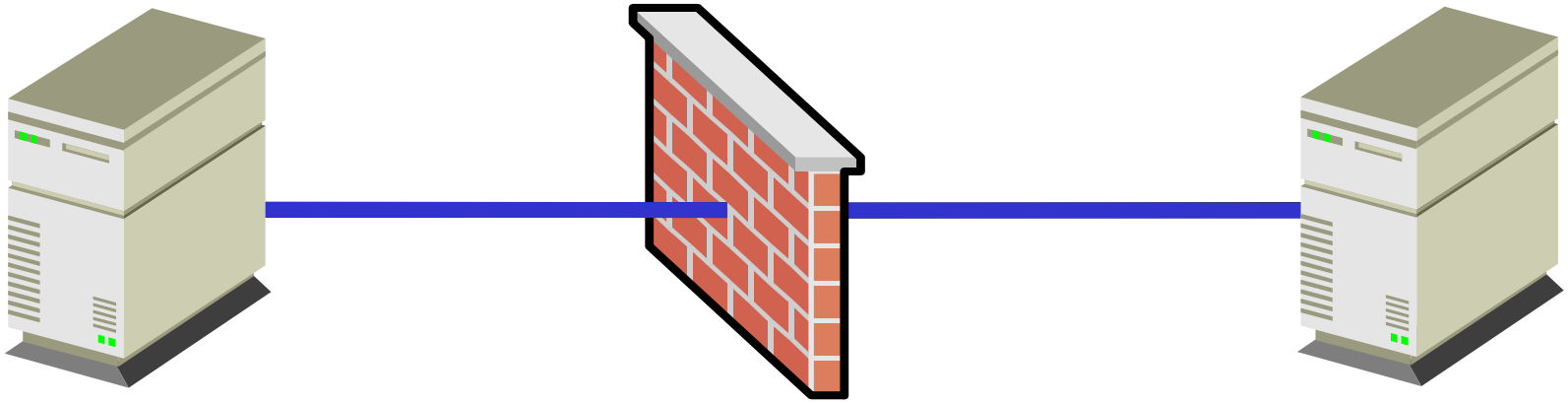
- **Control at network level**
- **Ruled base traffic filtering**
  - **Type**
  - **Source / destination address**
- **User authentication not possible**
  - **Source / destination IP addresses only valid identification**
  - **Problematic when used with DHCP networks (Dynamic Addresses)**
- **Filtering firewalls are more transparent to the user**
  - **No user setup**
- **Packet Filtering Firewall build into the Linux kernel (iptables)**



Proxy

- **Commonly used to control, or monitor, outbound traffic**
- **Some proxies cache requested data**
  - **Lowers bandwidth requirements**
  - **decreased access time next time data is requested**
- **Detailed logging of requests**
- **Two types of proxies servers**
  - **Application proxies - that do the work for you**
  - **SOCKS proxies - that cross wire ports**

Application Proxy



An Application proxy acts as a go-between (proxy) – Content can be verified and logged – authentication can also be established

Types of Firewalls – Application Proxy

- **Because proxy servers are handling all the communications, they can log everything**
  - **Every web URL**
  - **Every ftp download**
  - **Verify that content if valid (http requests are valid http)**
- **Authentication can also be performed at the application proxy**
  - **Before a connection to the outside is made, the server can ask the user to login first**
  - **To a web user this would make every site look like it required a login**

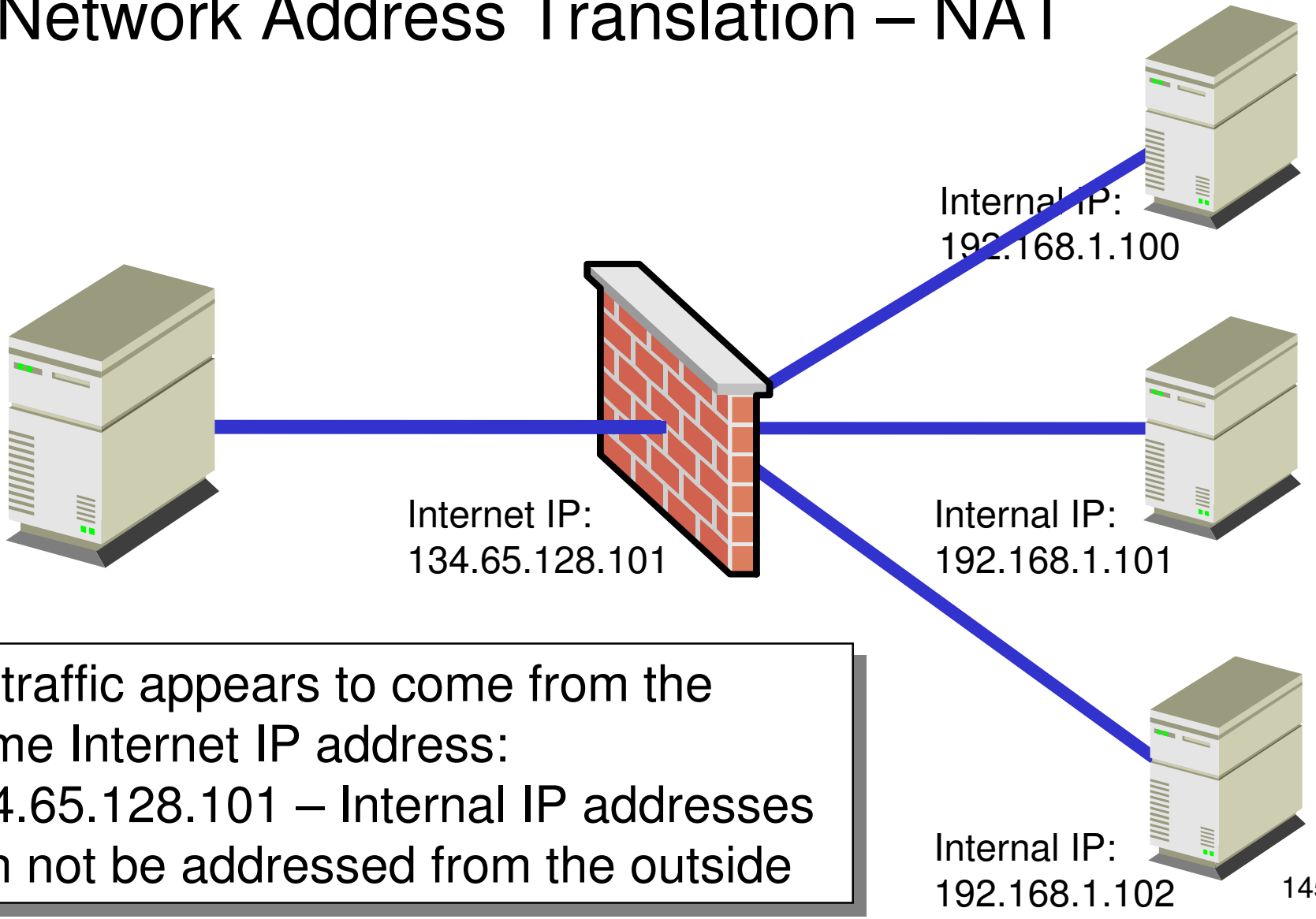
Types of Firewalls – SOCKS Proxy

- **A SOCKS server is a lot like an old switch board**
  - **It simply cross wires your connection through the system to another outside connection**
- **Most SOCKS server only work with TCP type connections**
  - **And like filtering firewalls they don't provide for user authentication. They can however record where each user connected to**

Network Address Translation – NAT

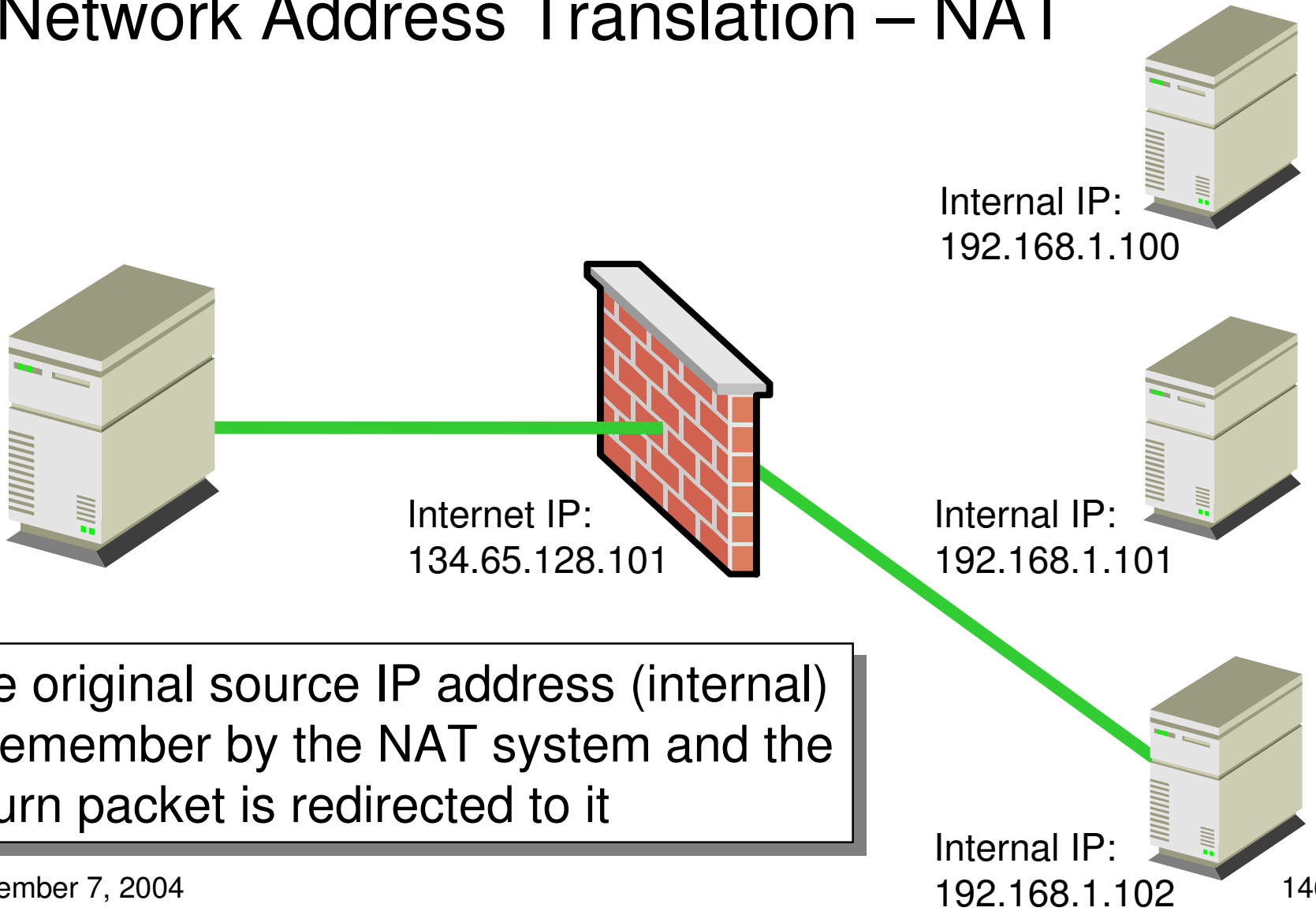
- **Normally, network traffic will travel from a source (such as your home computer) to the destination (such as a web site)**
  - **Through multiple links**
  - **The package is typically forwarded to the next link unaltered**
- **On a system doing Network Address Translation (NAT) the source IP address will be changed to its own**
- **The original source IP address (usually an non-routable internal address) is remembered by the NAT system**
- **Return packets (sent to the NAT system) will be redirected to the correct originating system**
- **This level of indirections make the internal systems non-addressable and protected from direct outside attacks**

Network Address Translation – NAT



All traffic appears to come from the same Internet IP address:
124.65.128.101 – Internal IP addresses can not be addressed from the outside

Network Address Translation – NAT

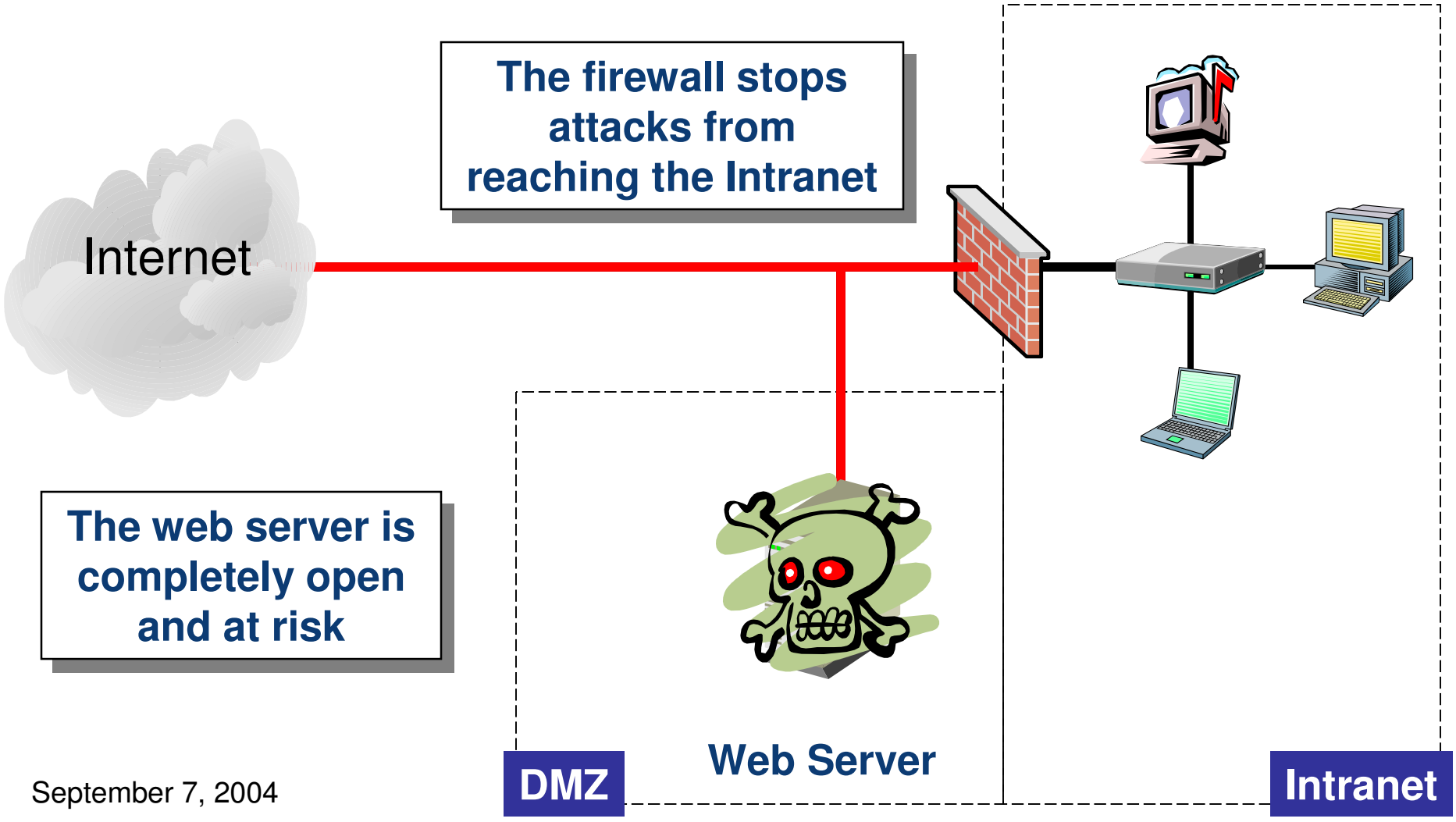


The original source IP address (internal) is remember by the NAT system and the return packet is redirected to it

Best Practices For Firewall Deployment

- **Disable everything**
  - **All incoming and outgoing traffic should be stopped**
- **Slowly allow required network traffic to pass through**
  - **Take this step with great care**
- **The inverse of this is problematic and very dangerous**
  - **Opening up all traffic**
  - **Close that which you don't want**
  - **You will inevitably make a mistake**

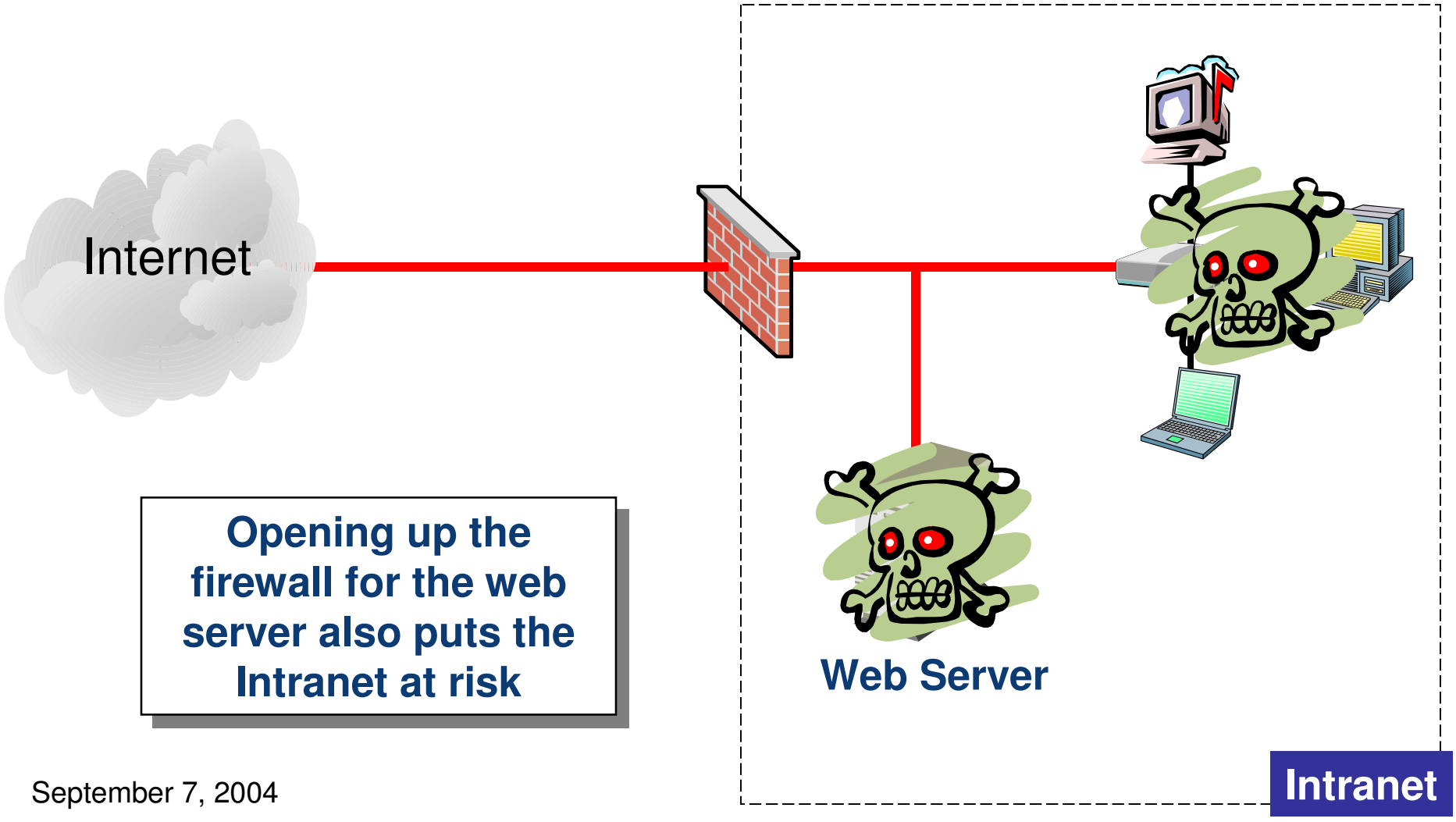
Common Enterprise Firewall Configuration



Placing Web Server Behind Intranet Firewall

- **Web server no protected**
- **Tools to tunnel through http**
- **Pass directly though the firewall**
- **The entire Intranet is then at risk**

Placing the Web Server in the Intranet

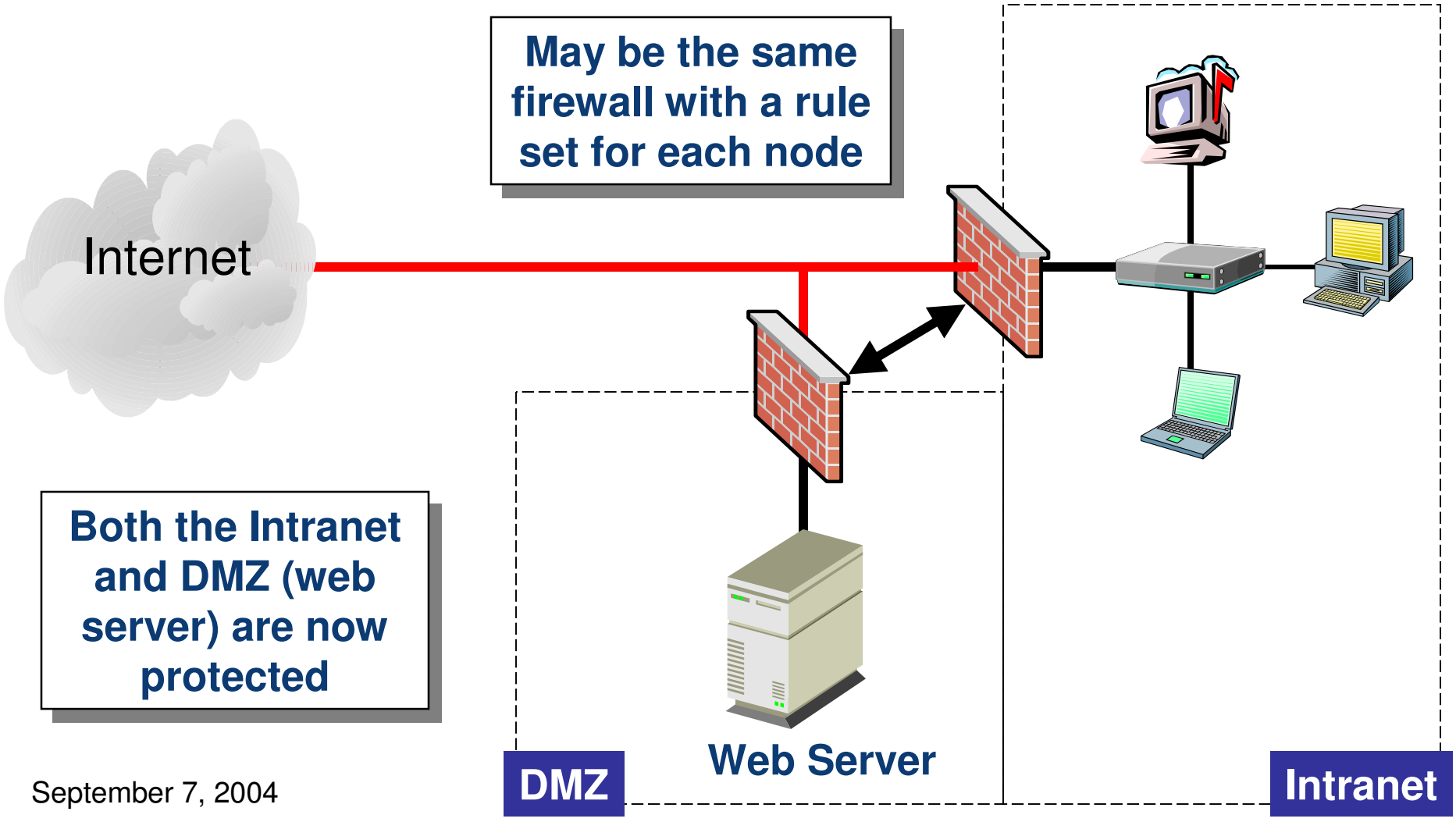


Opening up the firewall for the web server also puts the Intranet at risk

Protect DMZ With It's Own Firewall

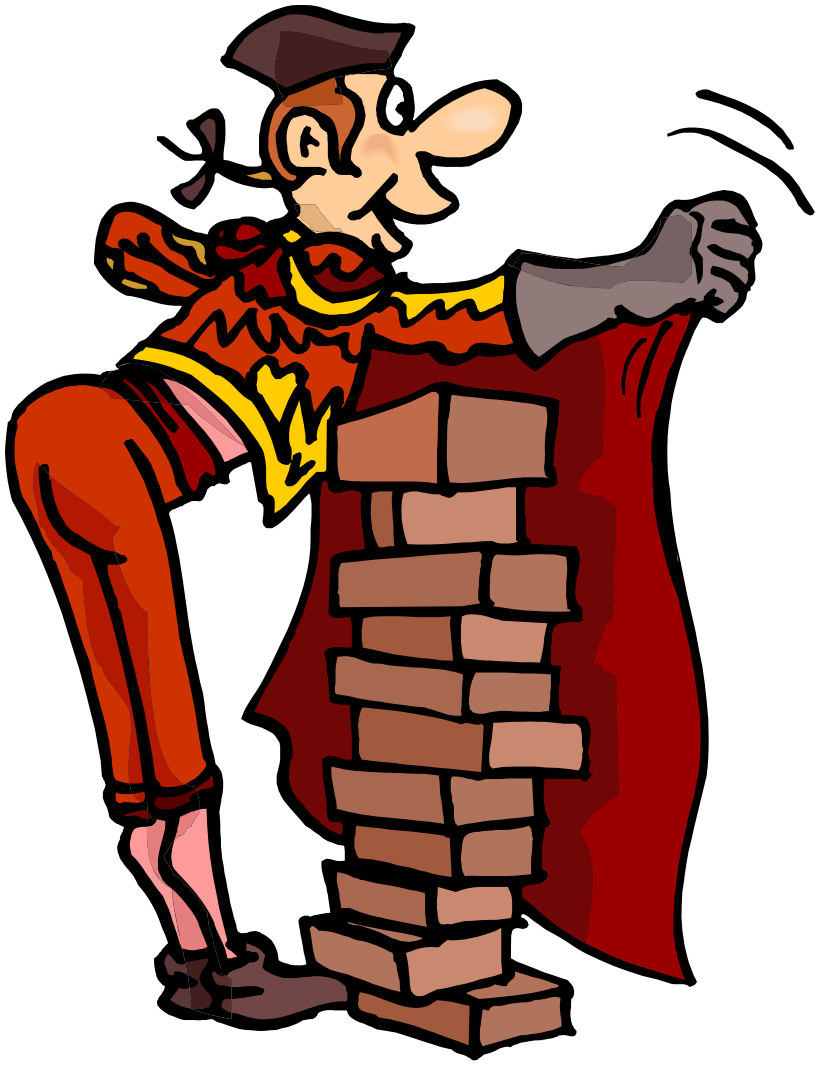
- **Separate firewalls**
  - **One for the Intranet**
  - **Another for the DMZ**
- **Each has a unique rule set**

Adding a DMZ firewall



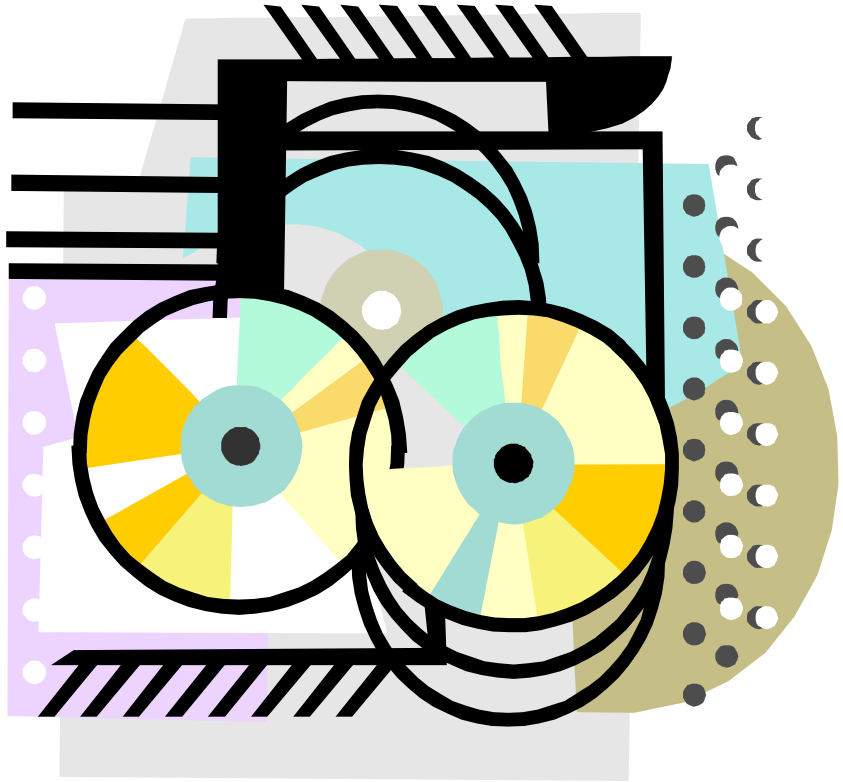
Firewalls and Configuration Tools

- **Built-in**
  - **Ipchains (Linux 2.2)**
  - **Iptables (Linux 2.4, 2.6)**
- **Proxies**
  - **Squid**
  - **SOCKS**
  - **Hogwash**
- **Configuration Tools**
  - **Firestarter**
  - **Kfirewall**
  - **Guarddog**
  - **shorewall**



The Sentry Firewall CD Project

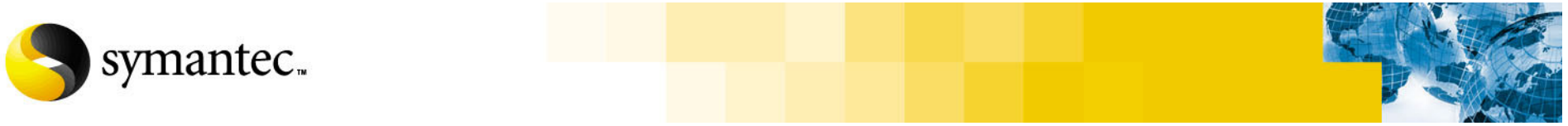
- **Minimal Linux distribution**
  - **Firewall**
  - **Intrusion Detection System (IDS)**
- **Bootable from CD-ROM**
- **Configuration on removable media**
  - **Write protected**
- **Updates distributed as new CD-ROM ISO image**



Locking Down Root Access

Delegating Root Access

- **Need to give root access to others**
  - **Example: User who needs to perform system backup**
- **SU (supper user) allows users to change or elevate their access Privileges**
  - **Requires knowing the root password**
- **SU is all or nothing**
  - **User with elevated privileges have complete access to the system**
  - **Users could damage your system accidentally or intentionally**
- **You loose control of the password by giving it to others**
  - **They may give it to others**

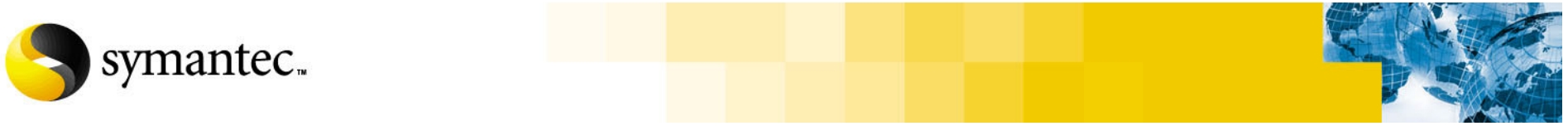


Delegating Root With Sudo

- **Delegate limited root access with sudo (Supper User Do)**
- **Root access is restricted to specific task (commands)**
- **Control is maintain in a configuration file: “/etc/sudoers”**
- **Example – User who must do a system backup**
  - **Granted root level access to backup utility only**
  - **All other actions are with the users normal privilages**

- **Sudo is called as:**

  sudo [sudo args] command [command args]

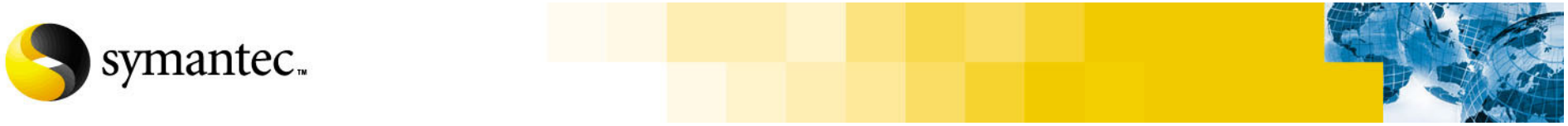


Sudo configuration file – sudoers

```
# User alias specification
User_Alias    ADMIN = jim
User_Alias    BACKUP_ADMINS = steve, sue
User_Alias    DEVELOPERS = mark, louis, james

# Host alias specifications
Host_Alias    BACKUP_SYSTEMS = news, mail
Host_Alias    DEV_SYSTEMS = dev1, dev2, redsys

# Command alias specifications
Cmnd_alias    BACKUP = /usr/local/bin/backup

# Users
root          ALL (ALL) = ALL
ADMIN         ALL (ALL) = ALL
BACKUP_ADMINS ALL = BACKUP
DEVELOPERS    DEV_SYSTEMS = /usr/local/test/
```

What Does It Say

- **ADMIN users are allowed to execute any command**
  - **They have full root access**
- **BACKUP_ADMINS are allowed to execute the /usr/local/bin/backup command only**
- **DEVELOPERS may access the /usr/local/test/ areas on those systems designated DEV_SYSTEMS**
- **Delegate root access with caution**
  - **User given privilege to run vi with as root**
  - **Can spawn shell from vi**
  - **Has root level access to entire system**



Linux Intrusion Detection System (LIDS)

- **On traditional Unix / Linux systems**
  - **root is exempt from file-system restrictions**
  - **root may read any file regardless of access permissions**
  - **If root access is gained – the game is over**
- **The Linux Intrusion Detection System (LIDS) is a Linux kernel patch**
  - **Removes special all-powerful nature of root**
  - **Give programs exactly the access they need, and no more**
  - **The root user is no more powerful than any other user**

Intrusion Detection

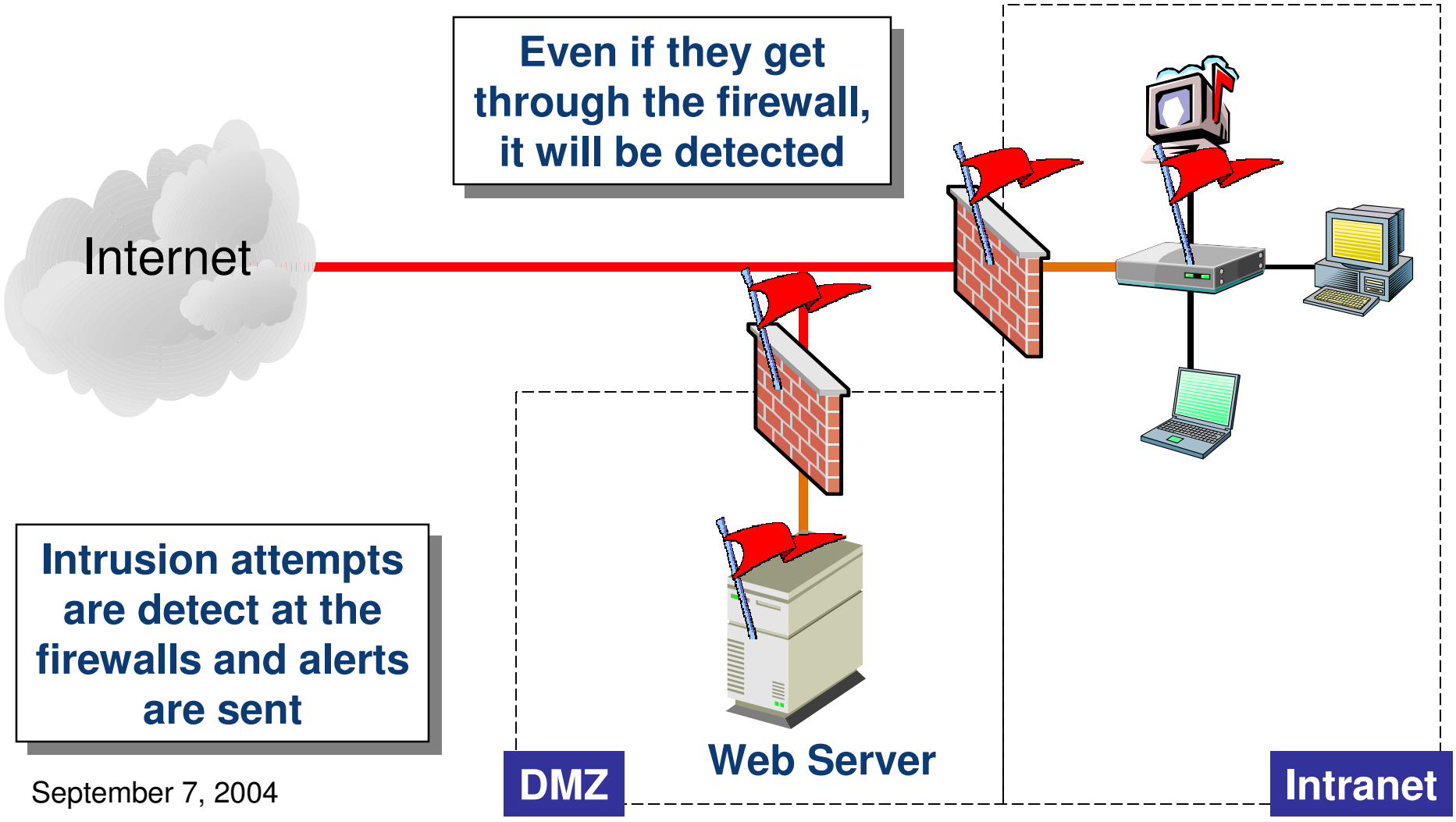
Intrusion Detection Systems (IDS)

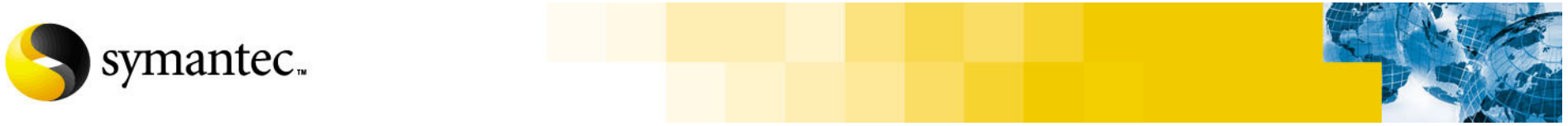
- **Looks for evidence of**
  - **Suspicious activity**
  - **Identified attacks**
- **Gathers all available details**
- **Logs event information**
- **Notify interested parties**

The Intrusion Detection Model (2 types)

1. **Network based intrusion detection**
   - **Installed on dedicated server (one per network node)**
   - **Configures system as a network traffic sniffer**
   - **Monitors network data**
   - **Identifies data signatures that may identify a known attack**
   - **Early warning system (hints at the possibility of attack)**
2. **Host based intrusion detection**
   - **Installed on each system to be monitored**
   - **Monitors systems (logs, files, MS registry, ,,.)**
   - **Advanced systems included client/server management system**
     - **event data from multiple hosts is collated**
   - **Provides solid evidence of attacks and abuse**

Intrusion Detection Monitoring



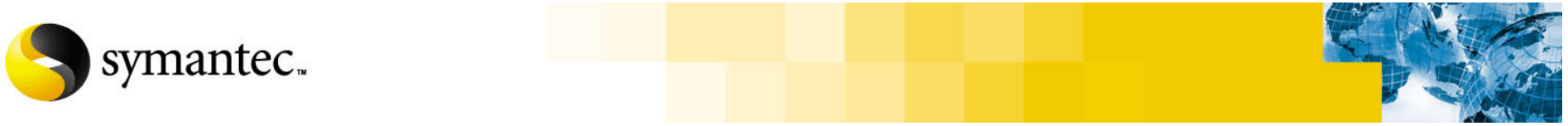


Snort

- **A lightweight network intrusion detection system**
  - **capable of performing real-time traffic analysis and packet logging on IP networks**
  - **It can perform protocol analysis, content searching/matching**
  - **can be used to detect a variety of attacks and probes**
- **Uses a flexible rules language to describe signatures**
- **Has a real-time alerting capability**
  - **Alerting mechanisms for syslog**
  - **A user specified file**
  - **A UNIX socket**
  - **WinPopup messages to Windows clients using Samba's smbclient**

Snort – Three Primary Uses

- **Basic packet sniffer**
  - **Monitoring network traffic**
- **Packet logger**
  - **Debugging network connections**
- **full blown network intrusion detection system**

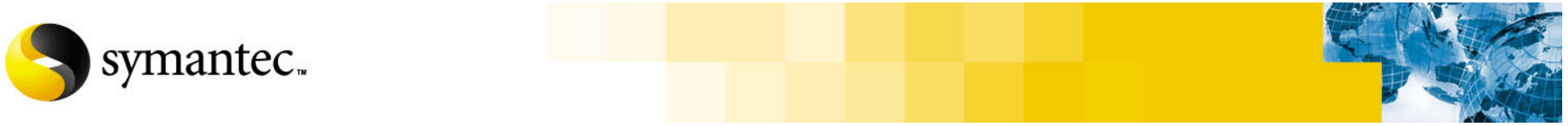


Tripwire and other derivatives

- **Tripwire**
  - **Checks to see what has changed on your system**
  - **Monitors attributes of files that should not change**
    - **including binary signature, size, expected change of size, etc**
- **AIDE (Advanced Intrusion Detection Environment)**
  - **A free alternative to Tripwire**
- **Both create a signed database of file specific information such as owners, groups, file size, file md5 sum, …**
- **If changes are made to a file being monitored, tripwire or AIDE will log or notify the system administrator**

Port Scan Detection – Portscan

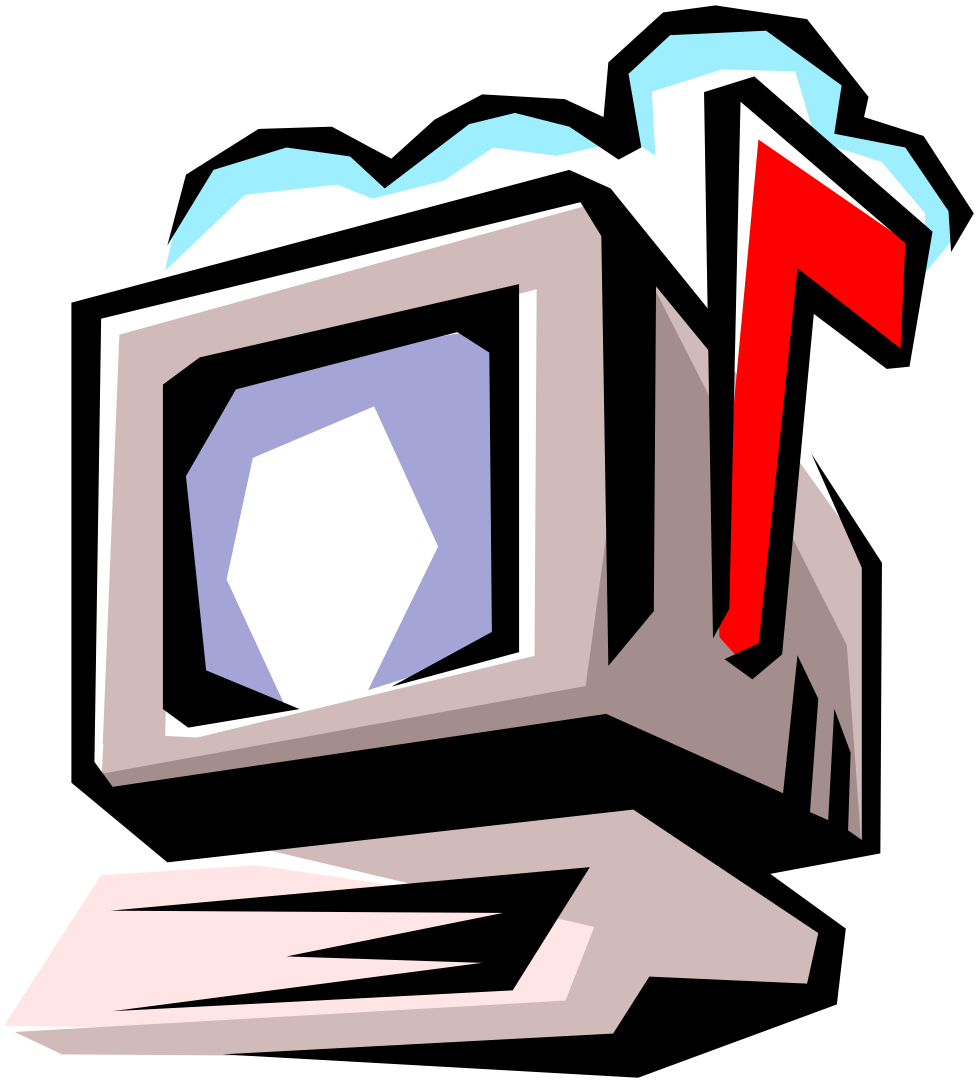
- **Monitors network connection attempts**
- **Identifies connection patterns that are indicative of some form of portscan activity**
- **Logs these events**

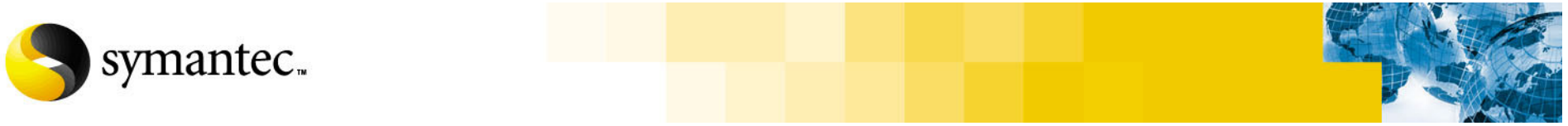


Log Monitoring

- **There are a number of programs that can be used to monitor system logs**
- **Do event correlation**
- **Identified attack or probing patterns**
- **Some of these are”**
  - **Psionic Logcheck**
  - **Color Log**
  - **WOTS**
  - **Swatch**

Email Security





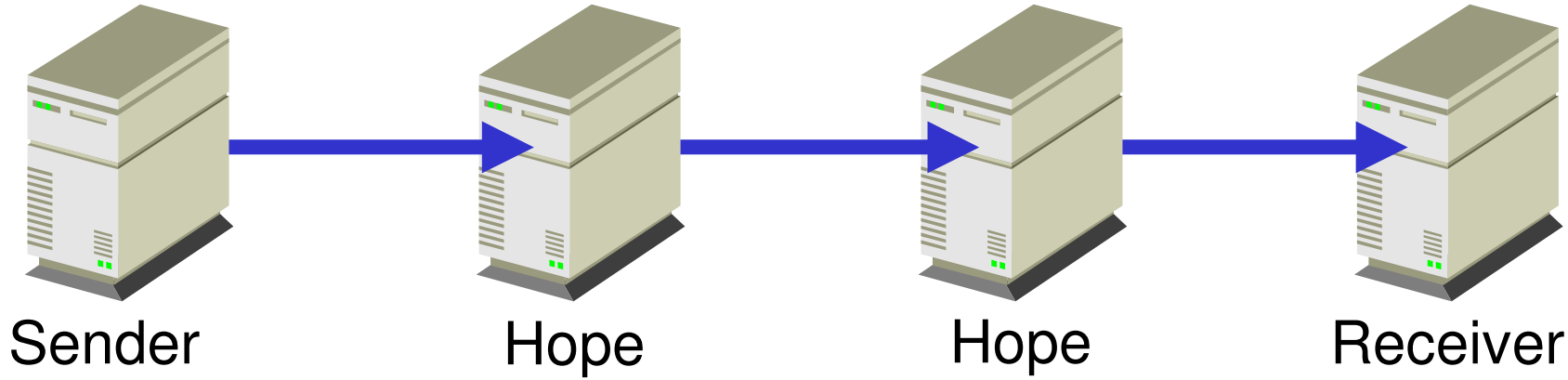
SMTP Servers

- **Managing Denial-of-Service attacks**
  - **Number of connections per-second**
  - **Number of children allowed**
  - **Minimum number of free buffers available before accepting email**
  - **Maximum size of email (header and body)**
- **Hop abuse (avoid SPAM)**
  - **Accept email from known trust sources only**
  - **Configure to listen on localhost only for workstations**
  - **Configure to internal network for gateways**
- **Use SPAM and AntiVirus**
  - **Spamassasin**
  - **ClamAV**

The Insecurities of Email

- **Sending email to another party across the Internet must pass across one or more mail hopes**
- **Theses hopes are not under your control and therefore are not to be trusted**
- **Anyone on any of these hopes could intercept and read you email**
- **Do you send confidential email this way?**

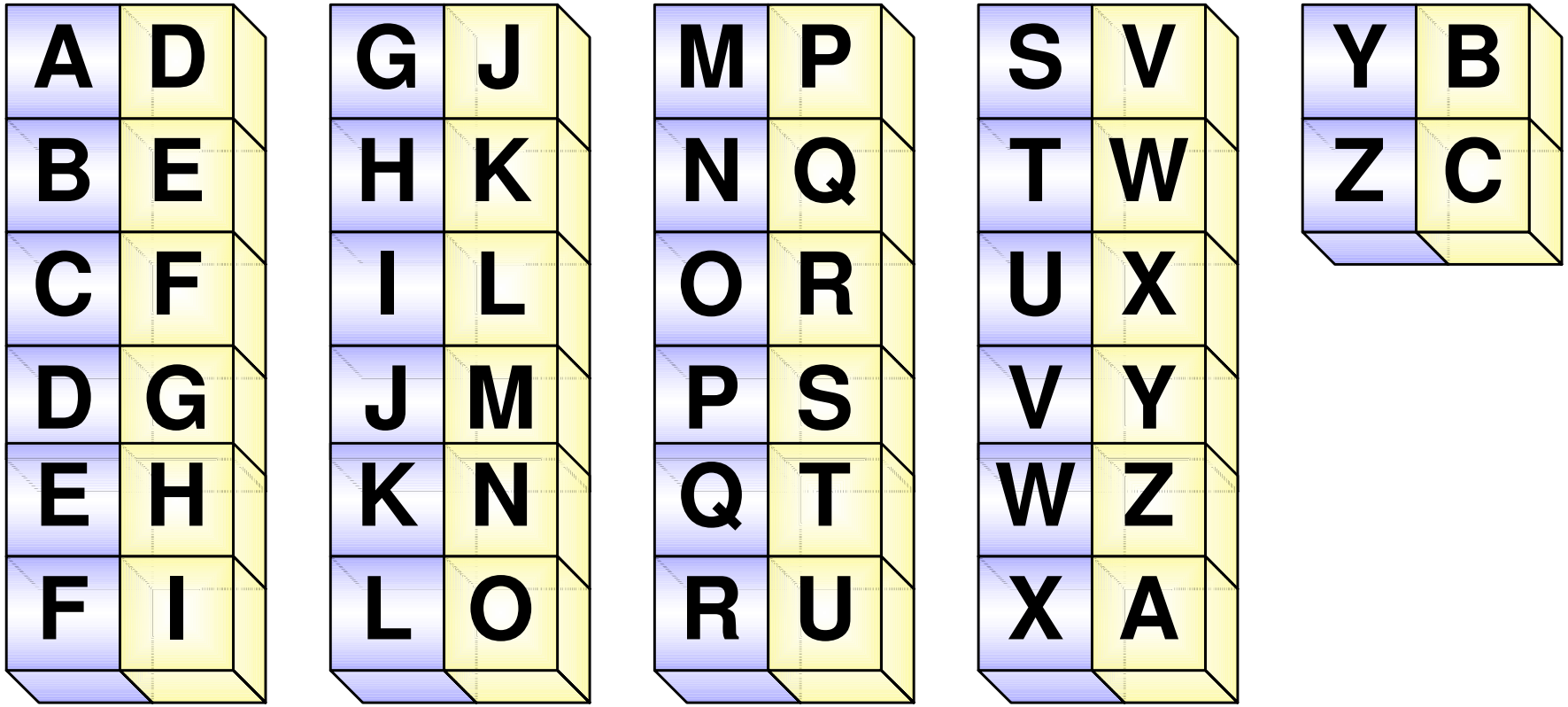
Email Passes Through Multiple Hopes



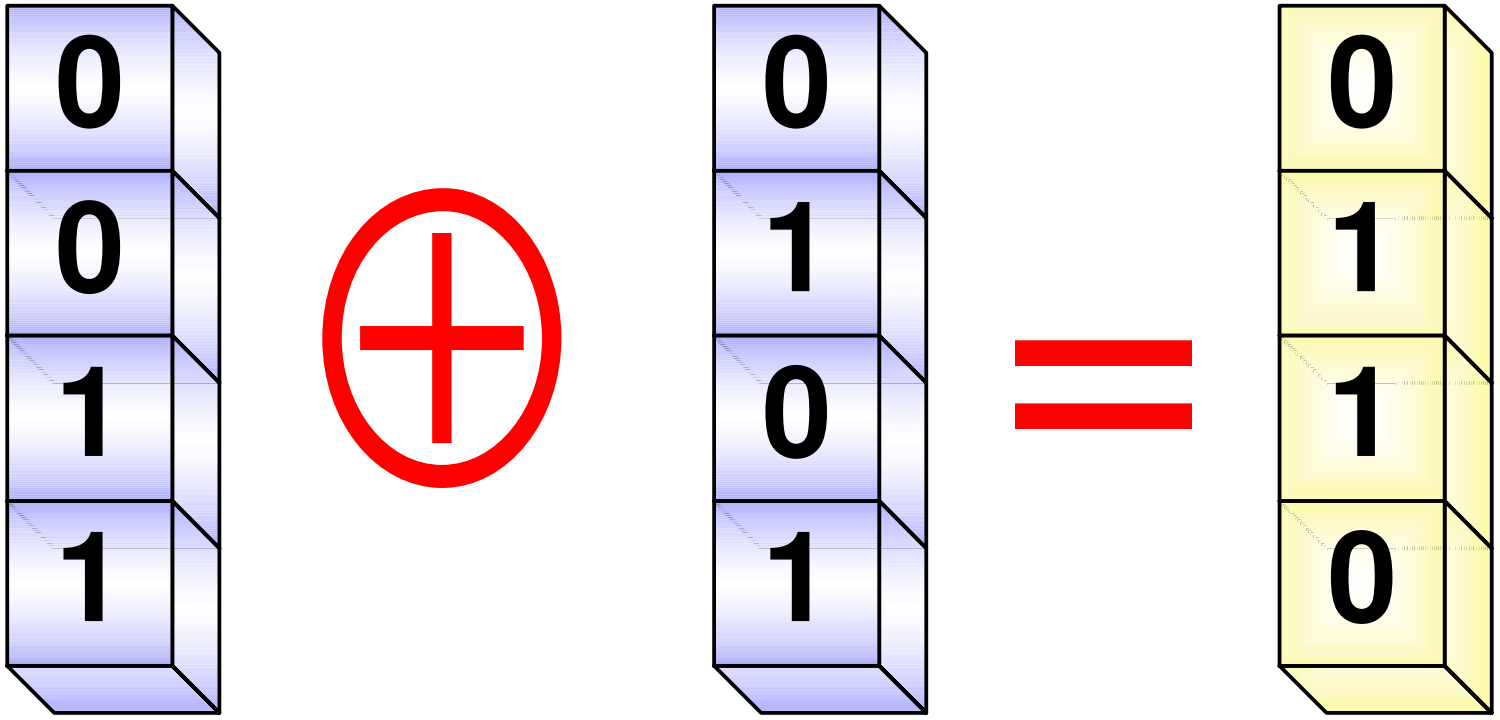
Encrypting Basics

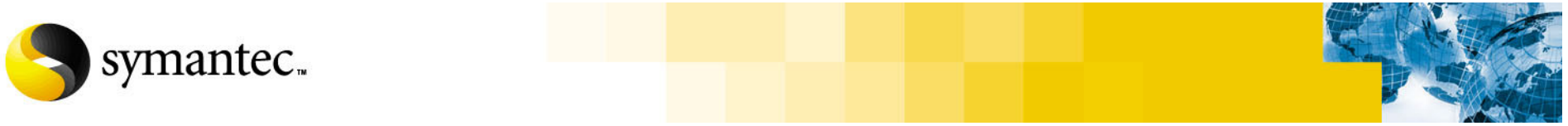
- **Prevent intercepted email from being read**
- **Encryption has has a long history**
  - **The earliest encryption was the substitution Cipher**
  - **Julius Ceasar used a substitution cipher to send encoded messages to his generals (called the Ceasar Cipher)**
  - **Using the Caesar Cipher, the text "LINUX SECURITY" becomes "OLQXA VHFXULWB"**
- **Another form of encryption is known as XOR Encryption (Exclusive Or)**
  - **The message is XORed with an known seed to produce an obfuscated result**
  - **It is considered a very weak form of encryption**

The Caesar Cipher



Exclusive OR (XOR)

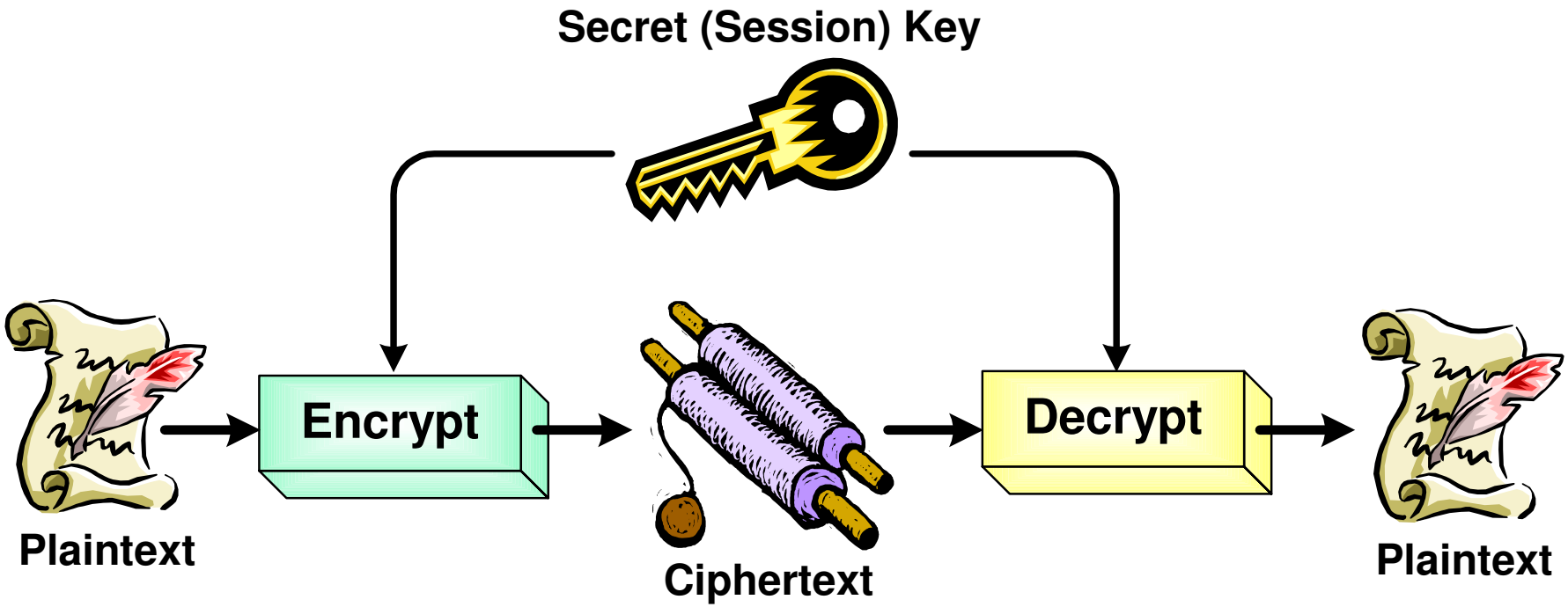




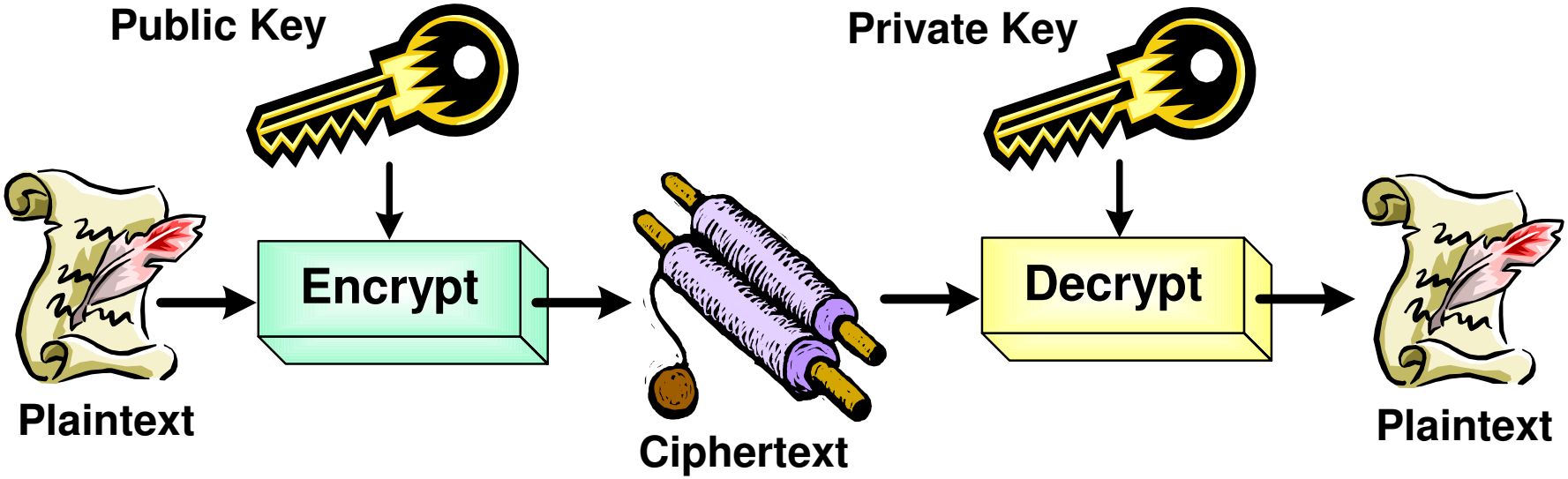
Modern Encryption

- **Use keys to identify the mapping being used**
- **Keys are typically measured in the number of bits in the key (key size)**
- **Larger key sizes increase the number of possible mappings**
  - **Decreasing the chance that the cipher will be broken**
- **Key-based cryptogrophy can be categorized into two types (each has its strengths and weaknesses)**
  - **Secret key (symmetric) cryptography uses a single key to encrypt and decrypt messages**
  - **Public key cryptography (asymmetric encryption) uses a key pair – the private key is used to encrypt and the public to decrypt**

Secret (Symmetric) Key Cryptography



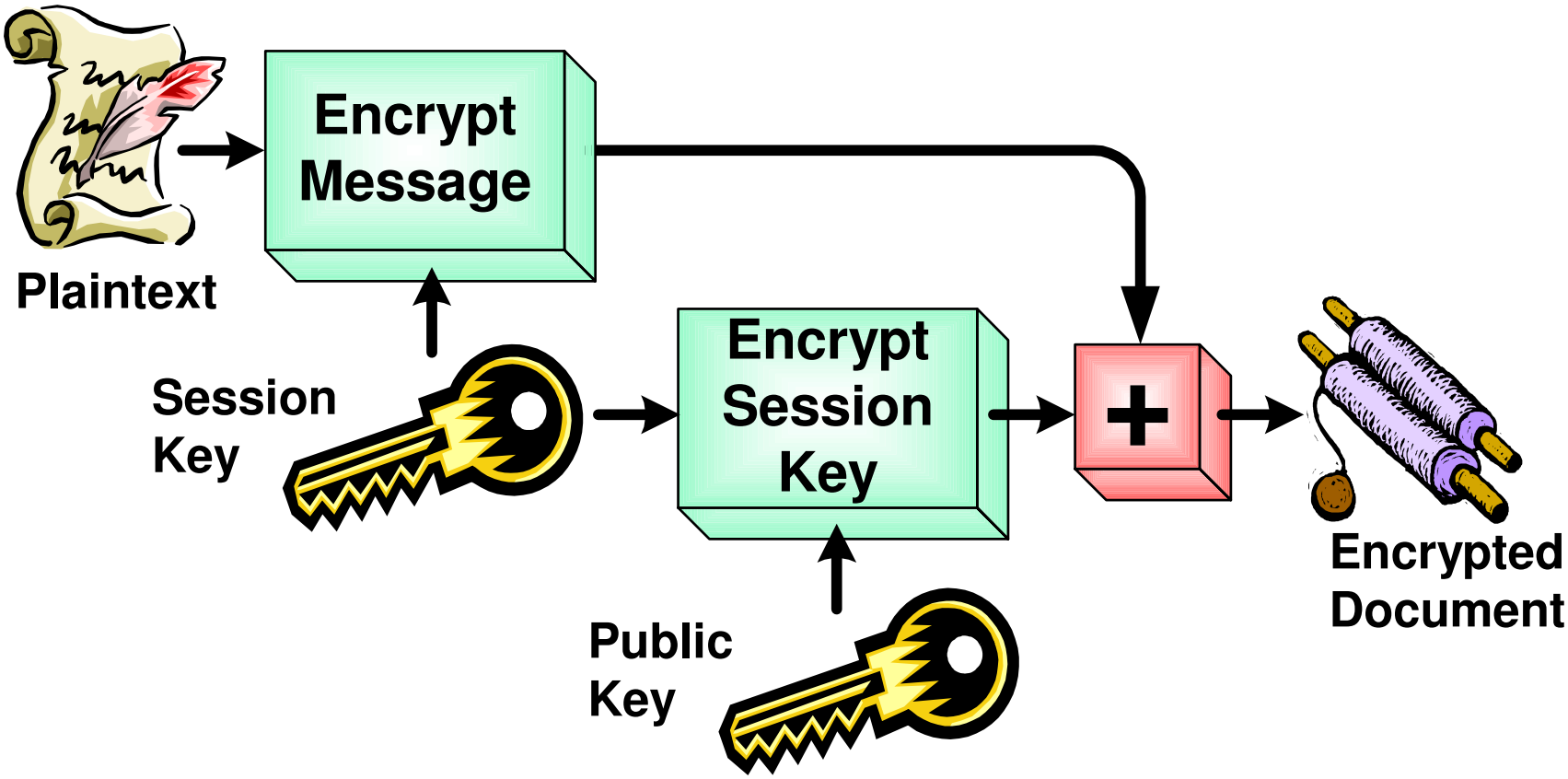
Public Key Cryptography



Encrypting Email

- **PGP (Pretty Good Privacy) was designed to ease the sending of encrypted email**
- **GnuPG (GNU Privacy Guard) was designed as a free replacement for PGP of follows the OpenPGP standard**
- **Both follow the same steps to encrypt email**
  1. **Generate a Symmetric Key (Symmetric encryption is substantially faster that public key encryption)**
  2. **Encrypt the email message**
  3. **Encrypt the symmetric key with the recipients public key and append to the encrypted email message**
  4. **Send the encrypted email message**

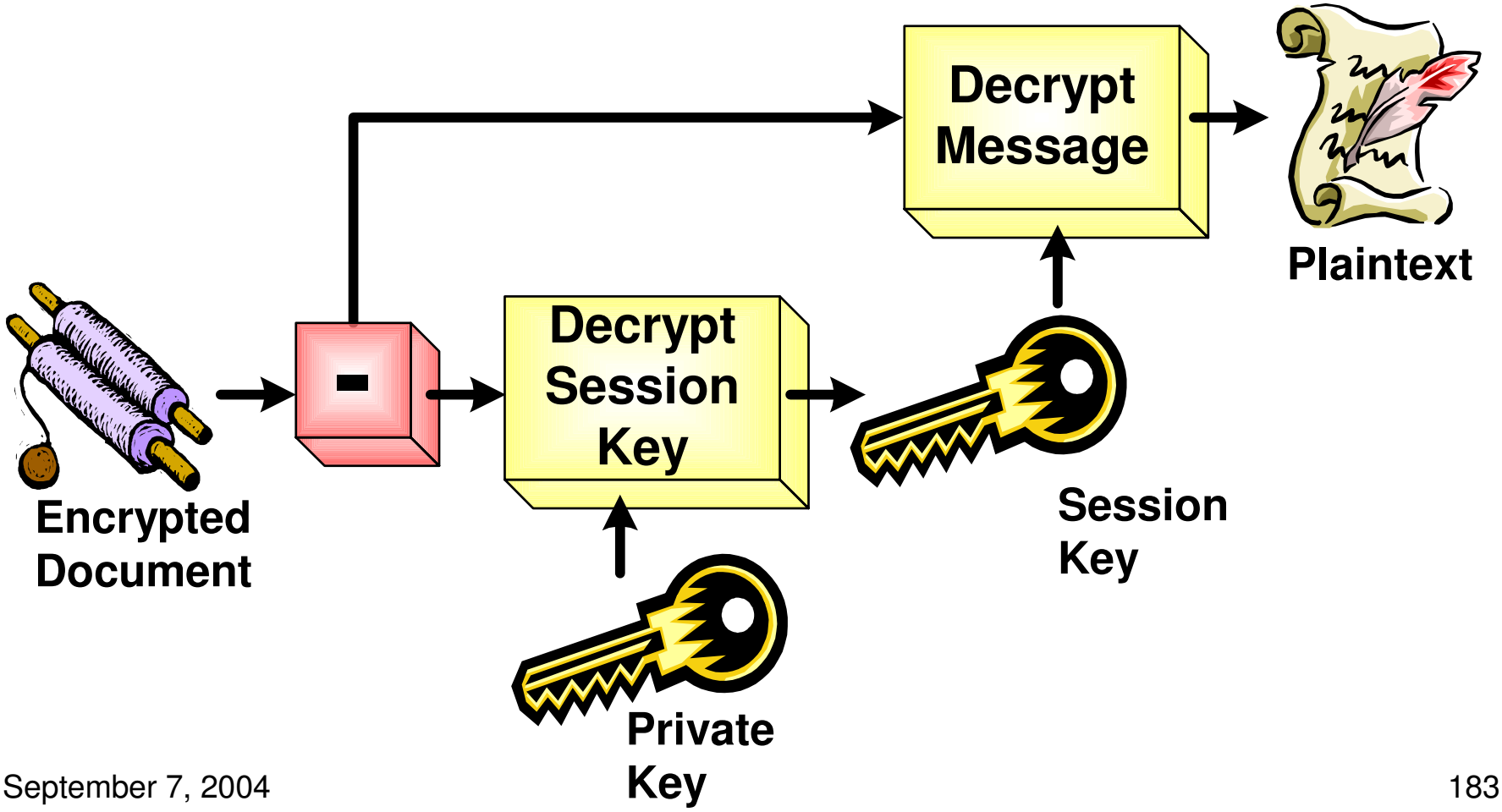
Encrypting Email - OpenPGP



Decrypting Email - OpenPGP

- **To decrypt an received encrypted email, PGP or GnuPG will perform the following steps**
  1. **Detach the encrypted symmetric key from the message body**
  2. **Decrypt the symmetric key with the recipients private key**
  3. **Use the now decrypted symmetric key to decrypt the email message**
  4. **Display the decrypted email message**

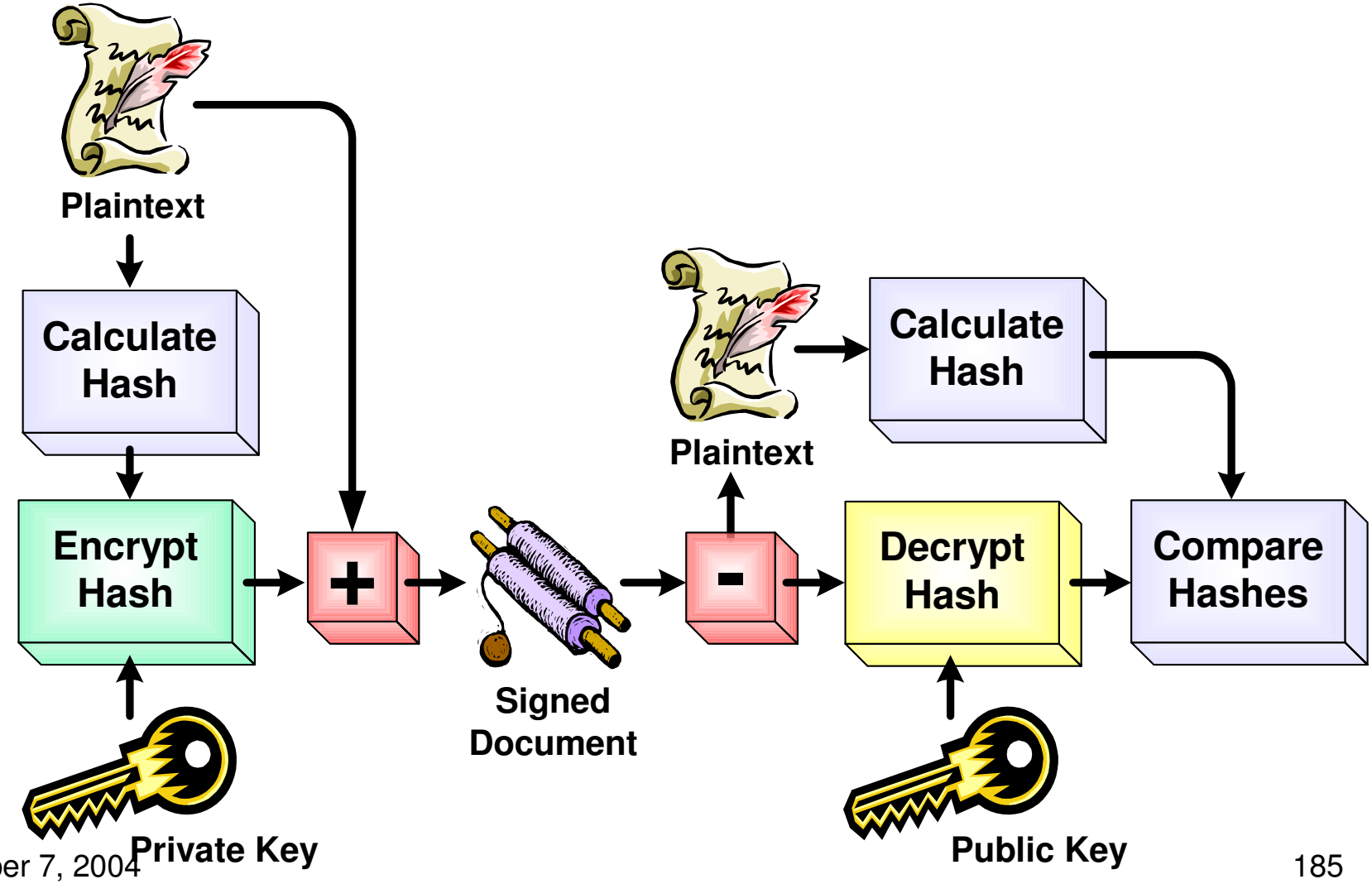
Decrypting Email - OpenPGP



Digitally Signing Email

- **It is possible to digitally sign email contents**
- **This give a level of confidence that:**
  - **The contents have not been modified during transit an**
  - **The message is indeed from the sender and not an imposter**
- **To sign a message the following steps are made to the email message**
  1. **Calculate an MD5 checksum of the email message**
  2. **Encrypt the MD5 checksum with the senders public key**
  3. **Attach the encrypt checksum to the mail message**
- **The following steps are made To verify the signature of for a signed email**
  - **Decrypt the encrypted MD5 checksum using the sender public key**
  - **Verify the decrypted MD5 checksum with the real MD5 checksum of the received message – the signature is valid if they match**

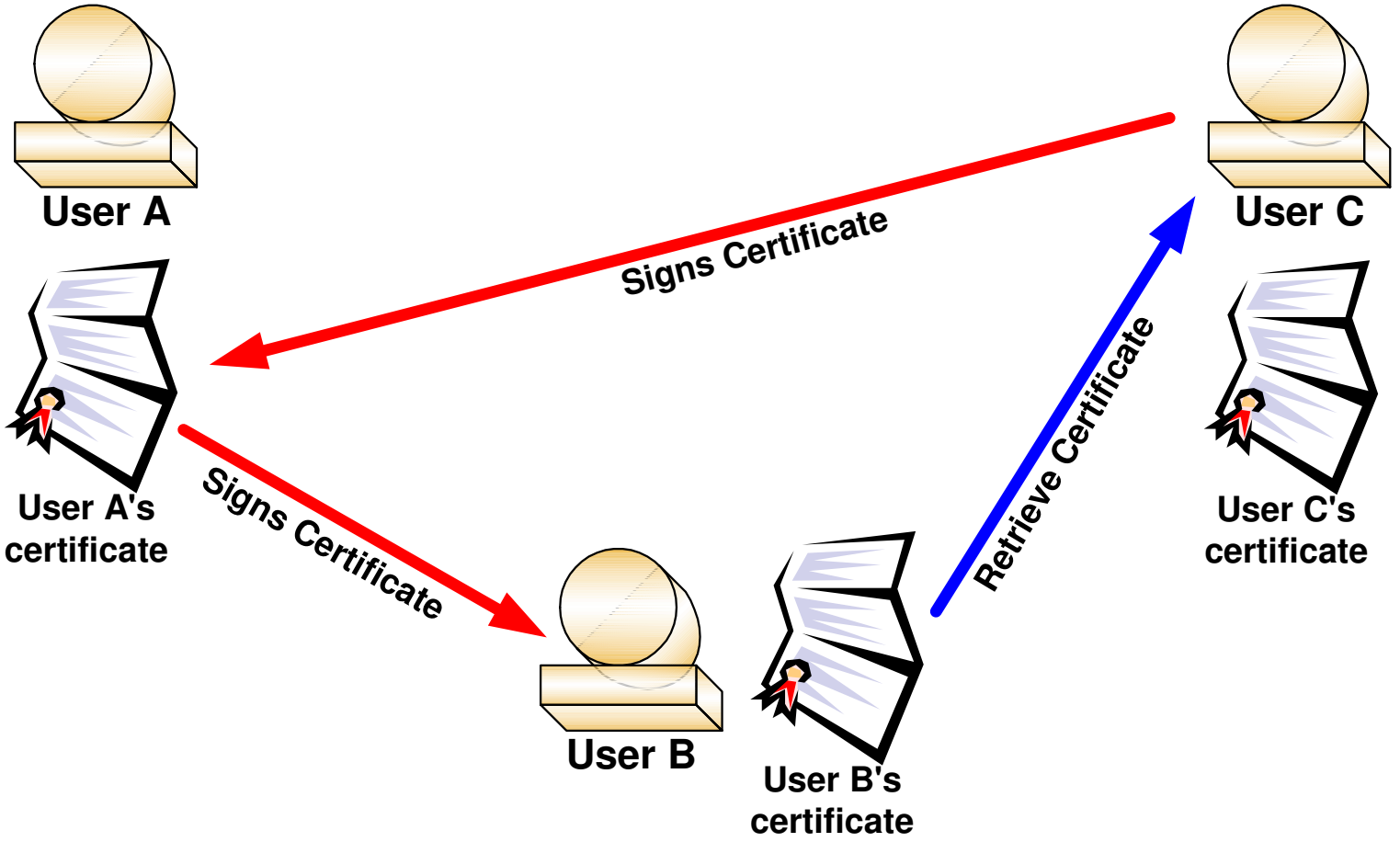
Signing an email message



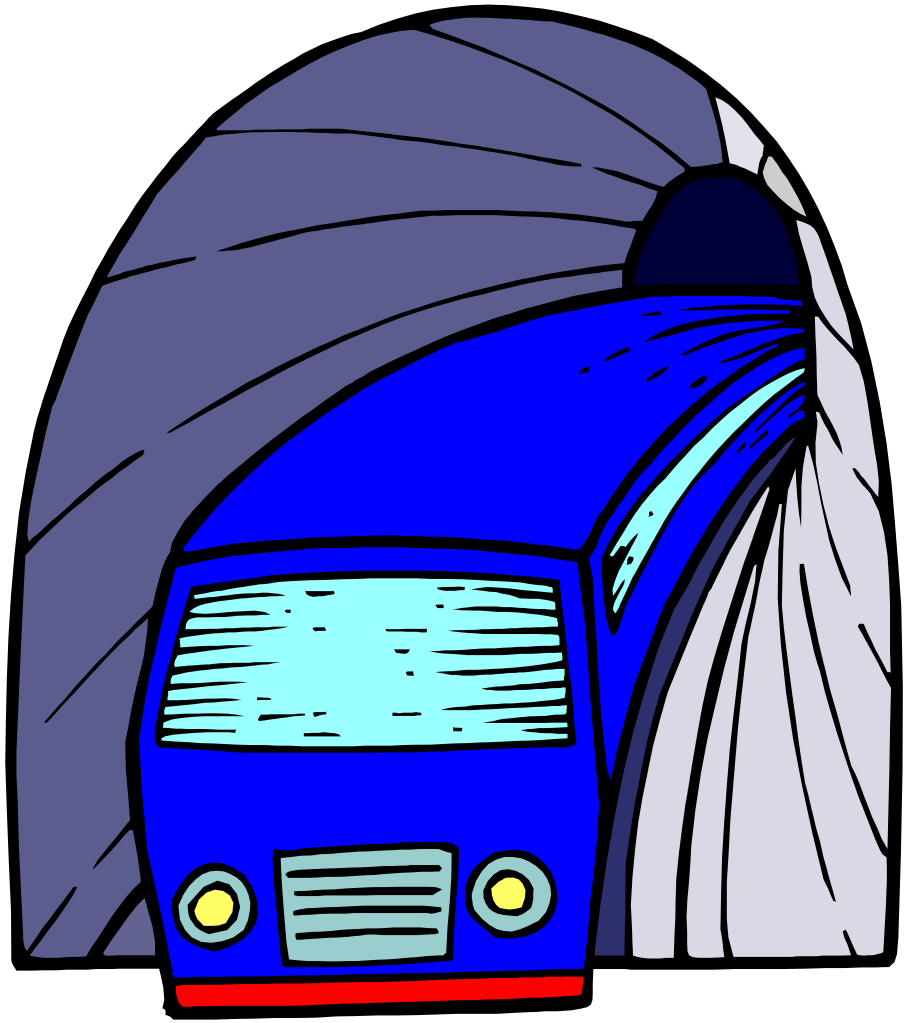
Developing a web of trust

- **For email encryption to be successful, you must distribute your public key to others**
- **There are public keyrings available that allow you to place you public key for others to find**
- **But how do you trust that the public keys that you receive or retrieve from public key servers are valid?**
- **The OpenPGP standard allows you to sign other persons public key**
  - **If you have verified and trust the other persons key**
  - **Others will then see you signature**
  - **If they trust your signature the then can trust this key**

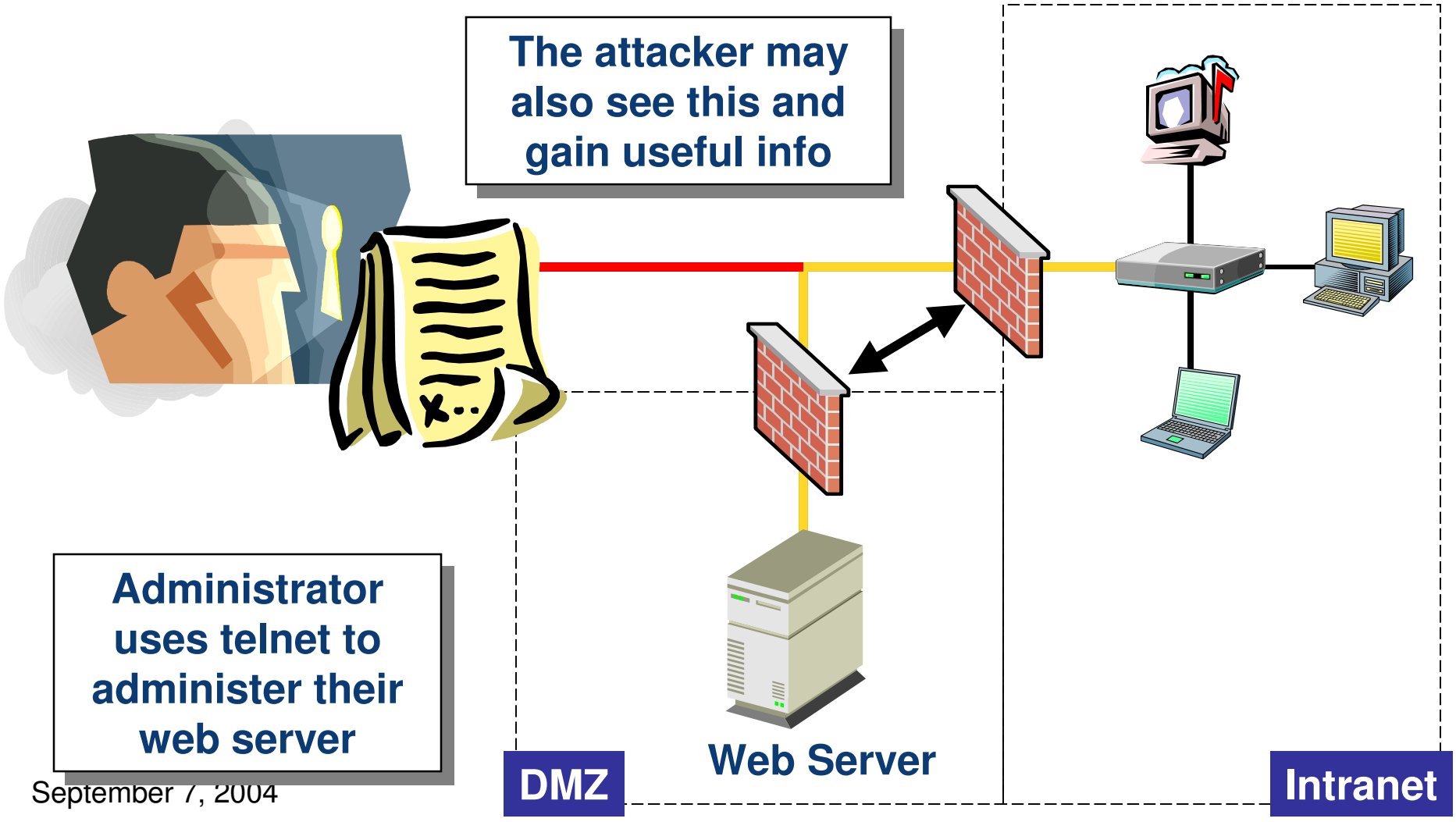
Developing a Web of Trust



Virtual Private Networks



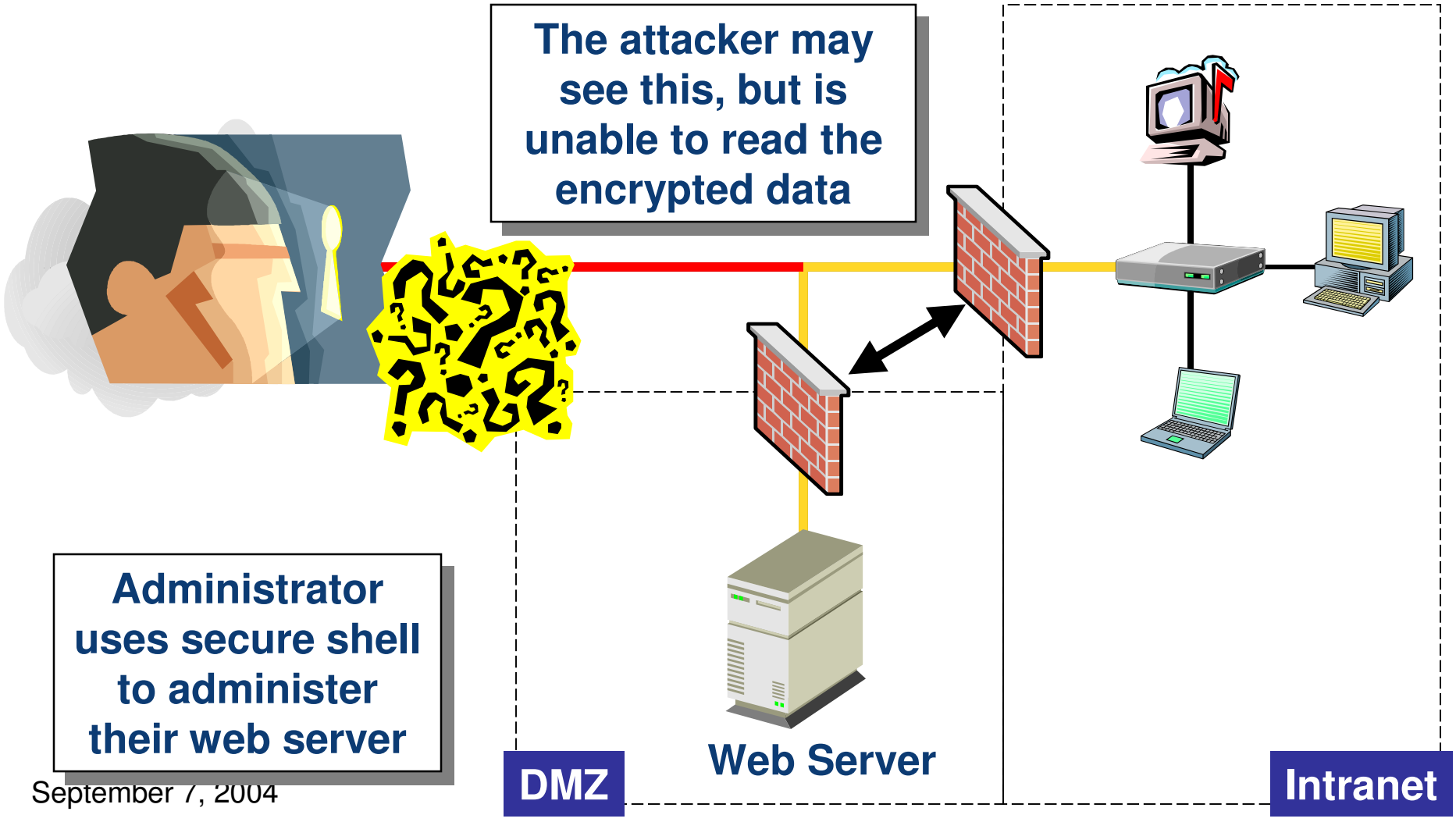
Network Traffic Is Sent in Clear Text

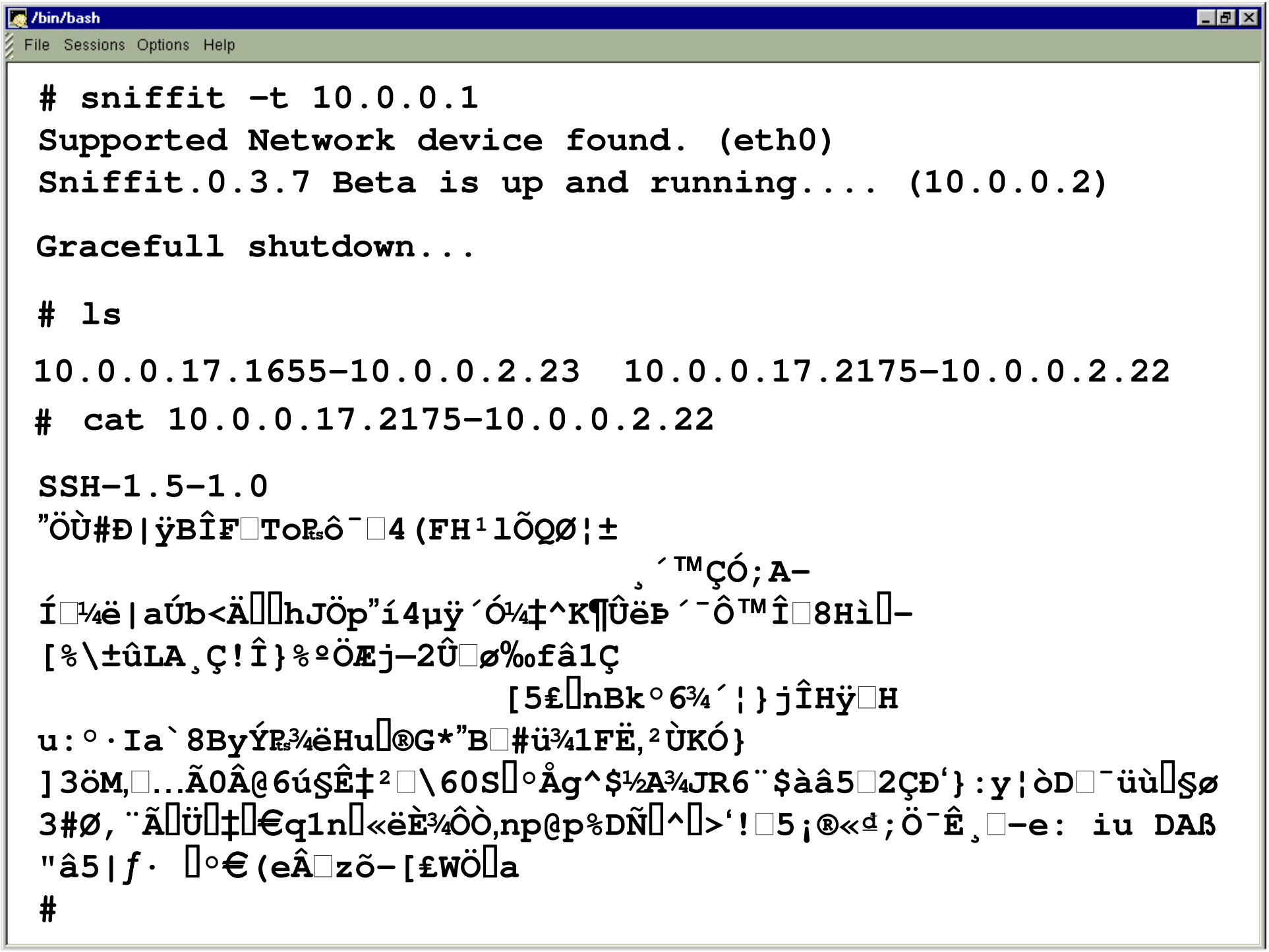


Encryption Is the Key

- **Encrypting the data being transmitted will prevent others from understanding the administrative information**
  - **They will still be able to sniff the encrypted data**
  - **It simply will not be readable**
- **For example, one very common tools is the SSH (or OpenSSH) program**

Protecting data with SSH

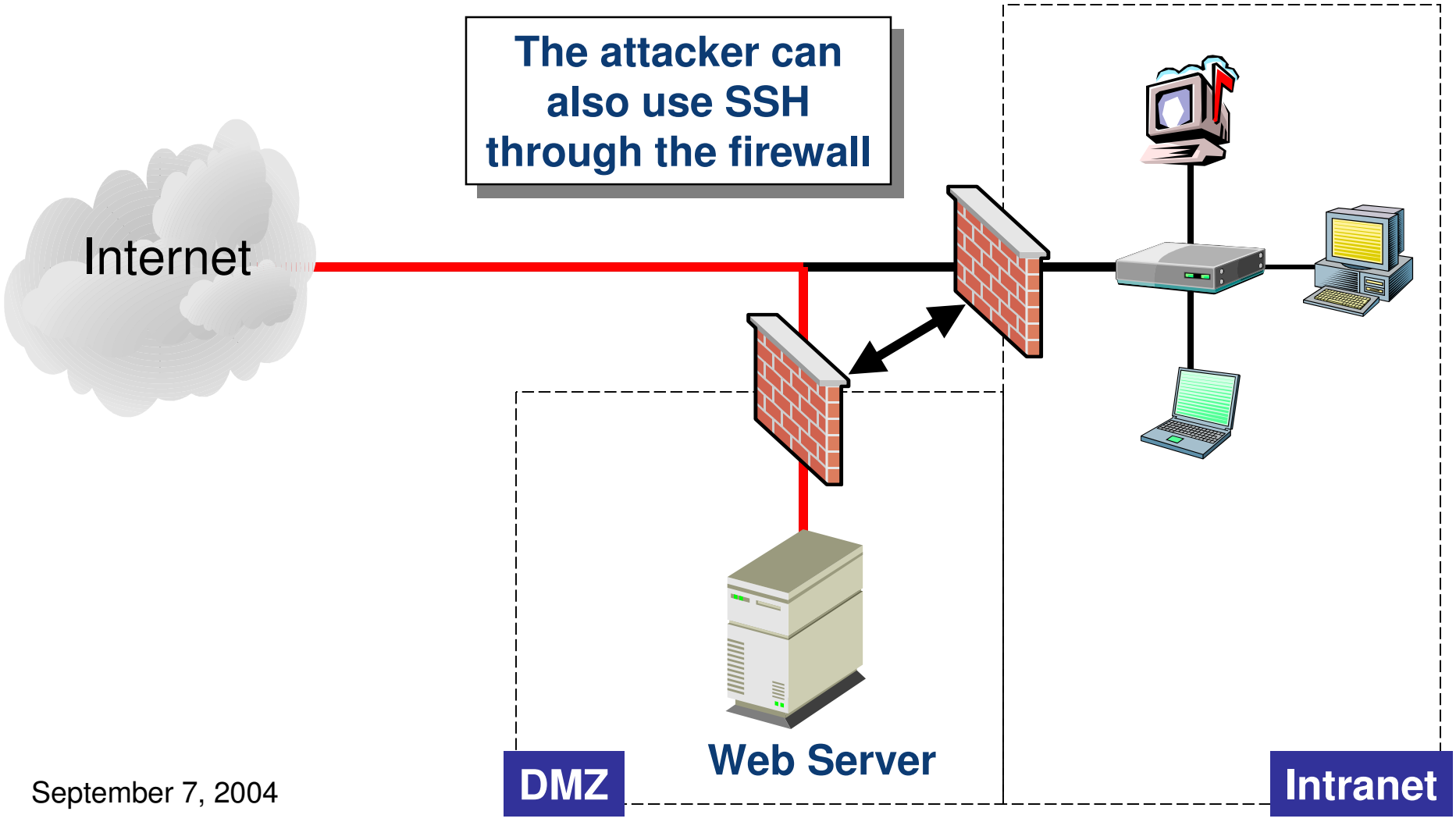



/bin/bash
File Sessions Options Help
sniffit -t 10.0.0.1
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (10.0.0.2)
Gracefull shutdown...
ls
10.0.0.17.1655-10.0.0.2.23 10.0.0.17.2175-10.0.0.2.22
cat 10.0.0.17.2175-10.0.0.2.22
SSH-1.5-1.0
”ÖÙ#Ð|ÿBÎF□ToRsô¯□4(FH¹lÕQØ¦±
´™ÇÓ;A-
Í□¼ë|aÚb<Ä□□hJÖp”í4µÿ´Ó¼‡^K¶ÛëÞ´¯Ô™Î□8Hì□-
[%\±ûLA¸Ç!Î}%ºÖÆj-2Û□ø‰fâ1Ç
[5£□nBk°6¾´¦}jÎHÿ□H
u:°·Ia`8ByÝRs¾ëHu□®G*”B□#ü¾1FË,²ÙKÓ}
]3öM,□...Ã0Â@6ú§Ê‡²□\60S□°Åg^$½A¾JR6¨$àâ5□2ÇÐ‘}:y¦òD□¯üù□§ø
3#Ø,¨Ã□Ü□‡□€q1n□«ëÈ¾ÔÒ,np@p%DÑ□^□>‘!□5¡®«ª;Ö¯Ê¸□-e: iu DAß
"â5|ƒ· □°€(eÂ□zõ-[£WÖ□a
#

Issues With SSH

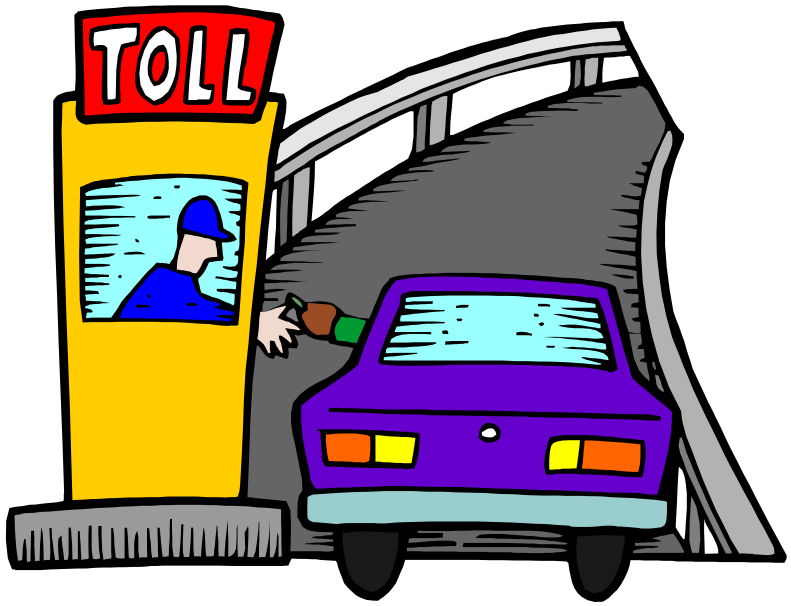
- **SSH (and OpenSSH) is an excellent program**
- **It provides good encryption and authentication**
- **Unfortunately its use in this situation does require that you open your firewall to allow SSH traffic through**
  - **There have been a number of SSH vulnerabilities discovered that that can lead to compromise**

Using SSH


The attacker can also use SSH through the firewall
Internet
DMZ
Web Server
Intranet

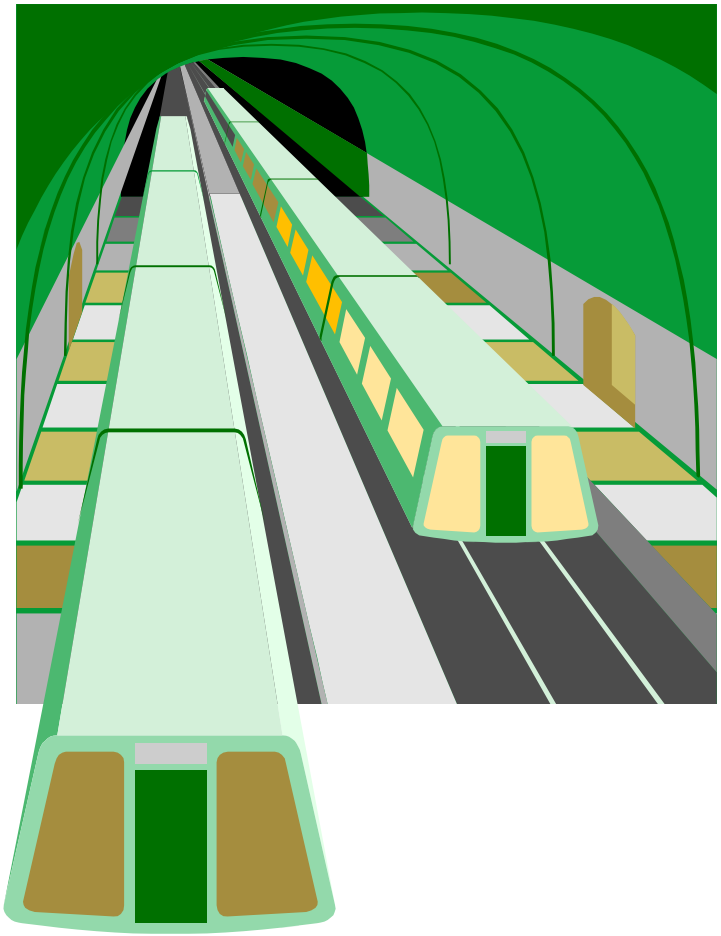
Virtual Private Network (VPN) to the Rescue

- **The use of a Virtual Private Network (VPN) provides a more secure alternative**
- **It can provide strong authentication at the firewall**
  - **You will still need to open up the fire wall to allow VPN traffic**
- **Only authorized traffic will be allowed through the firewall to the web server**

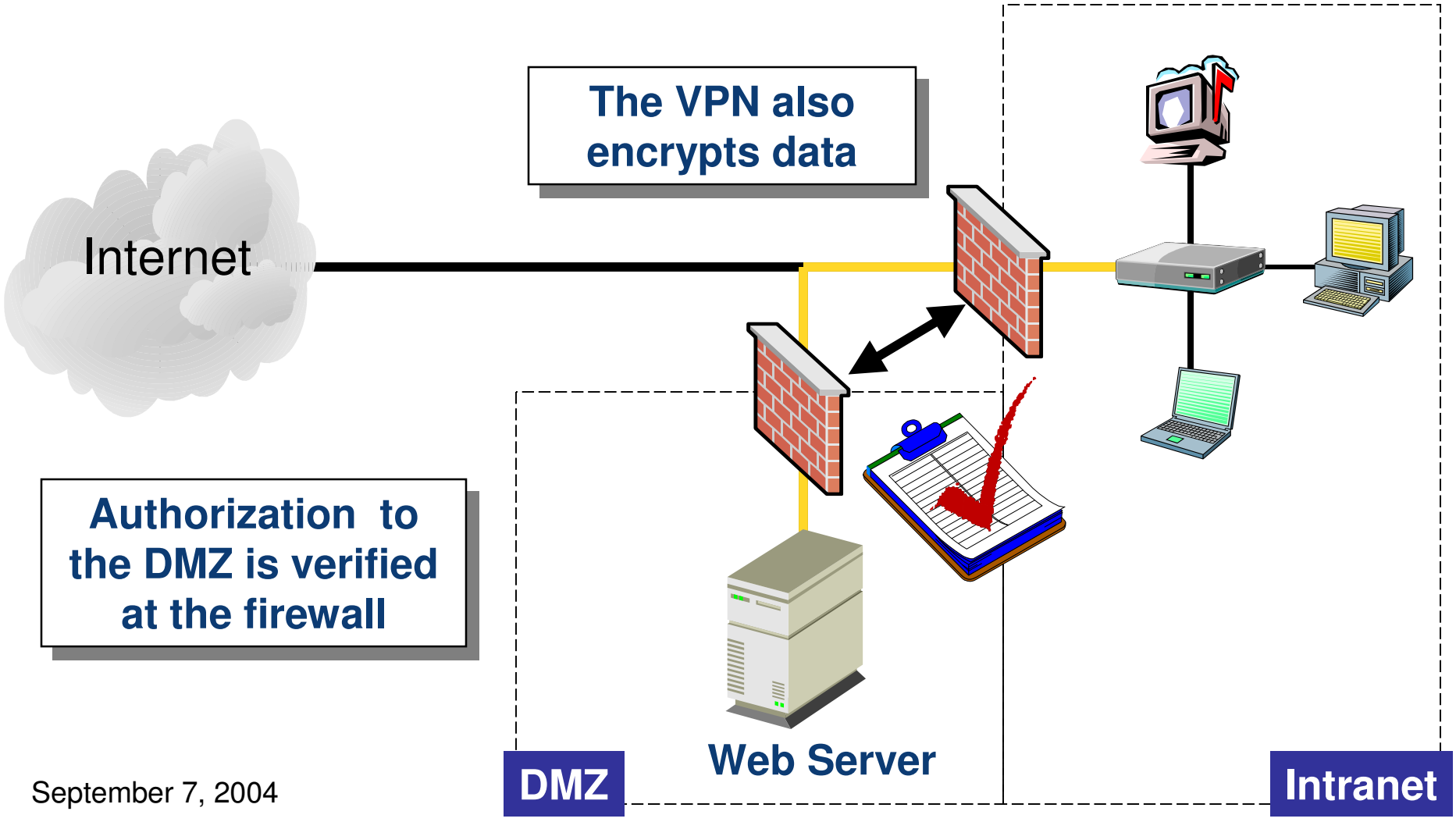


What VPN's are available

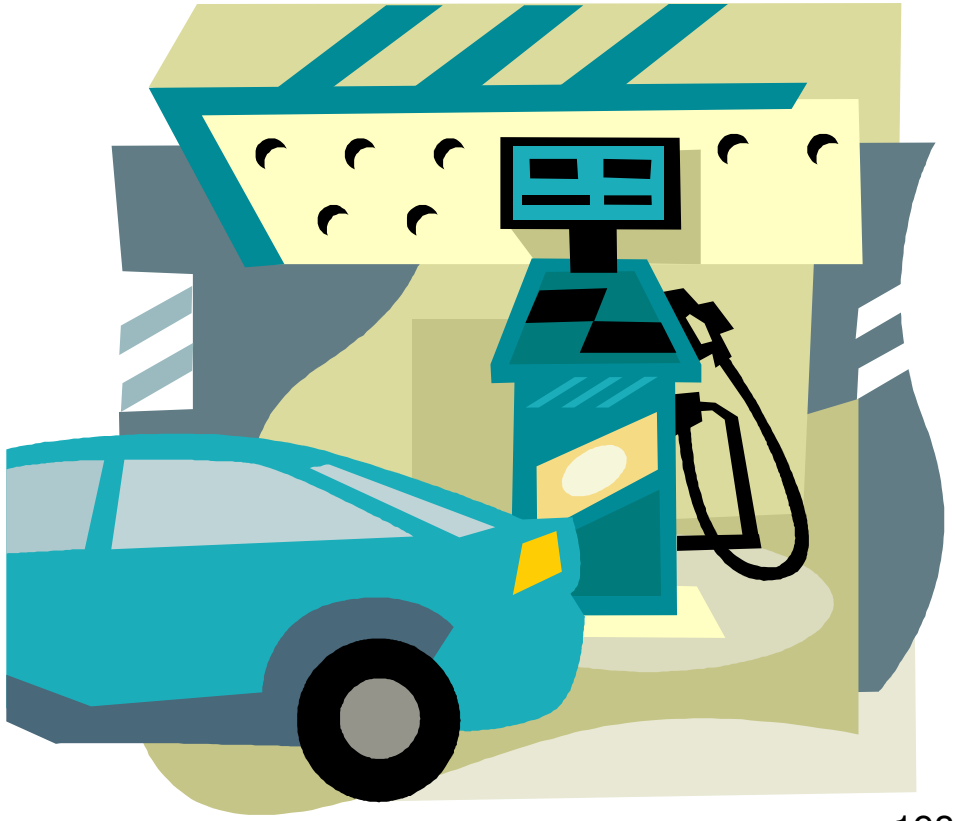
- **ssh**
- **Vpnd**
- **Free / SWAN**
- **CIPE**
- **OpenVPN**

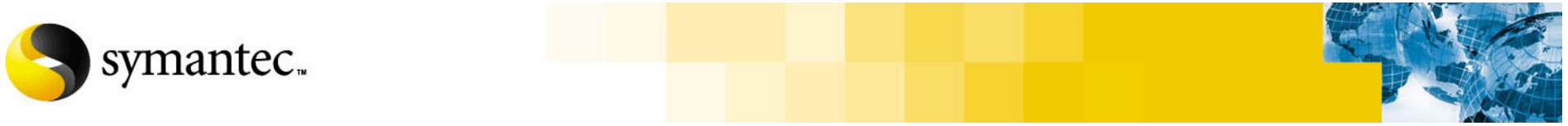


Using a Virtual Private Network (VPN)



Keep it Updated

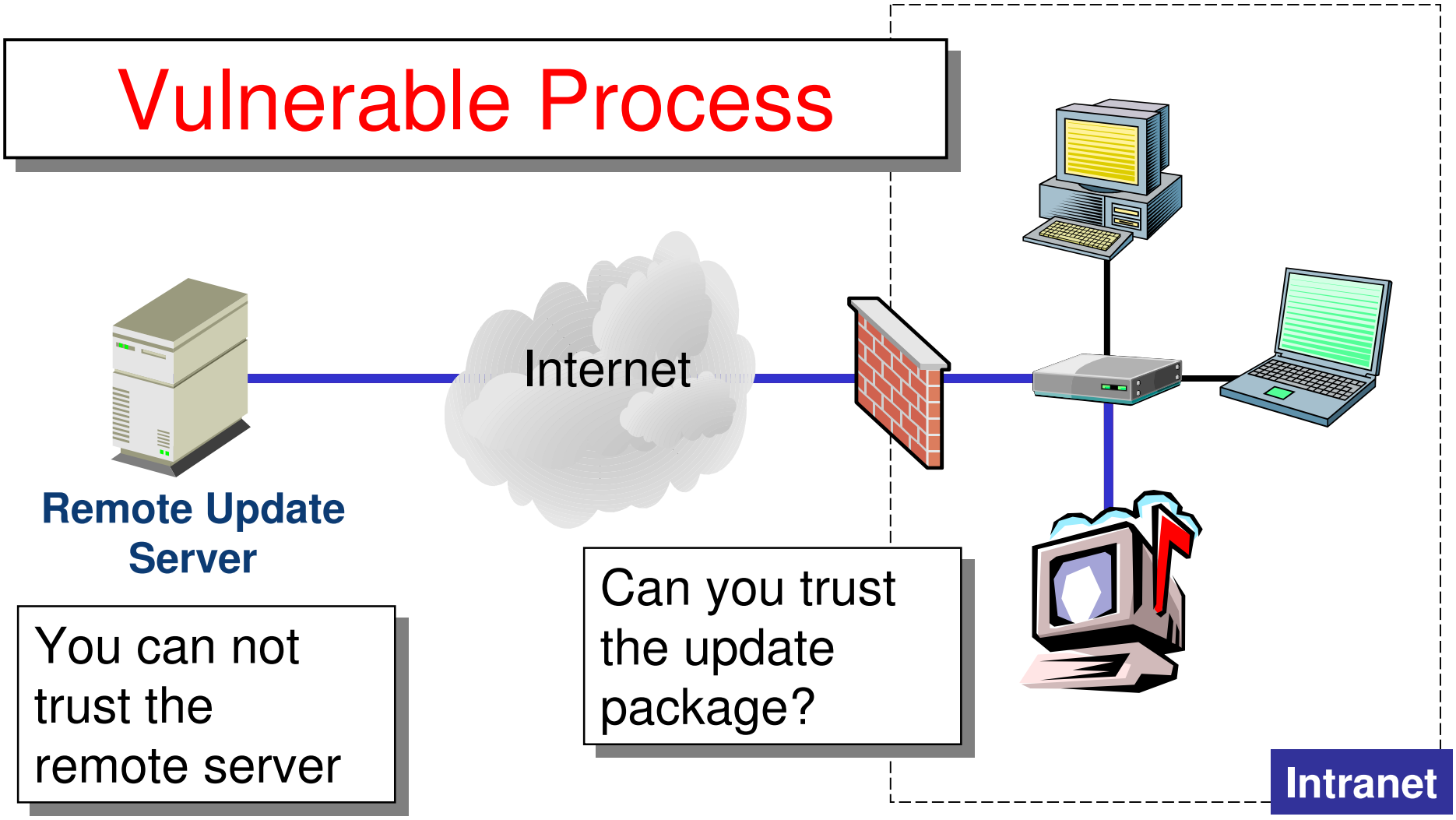


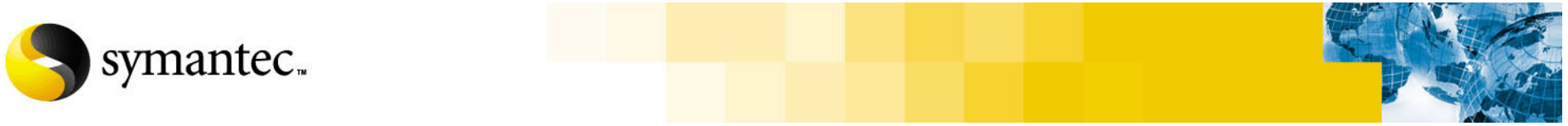


The need to keep your system updated

- **When a new version of Linux is released by a vendor, it will usually contain the latest versions of each software package**
- **Over time vulnerabilities will generally be found for multiple software packages**
- **The vendor will respond to this vulnerability by providing an updated version of the software package for download**
- **It is then up to you to download these updates and apply them to your system**
- **Failure to do this will leave your system vulnerable to attack**
- **Currently there are three types of packages in use — Red Hat Packages (RPM), Debian Packages (DEB) and tar archives generally compressed with gzip or bzip2**

Downloading and Installing updates



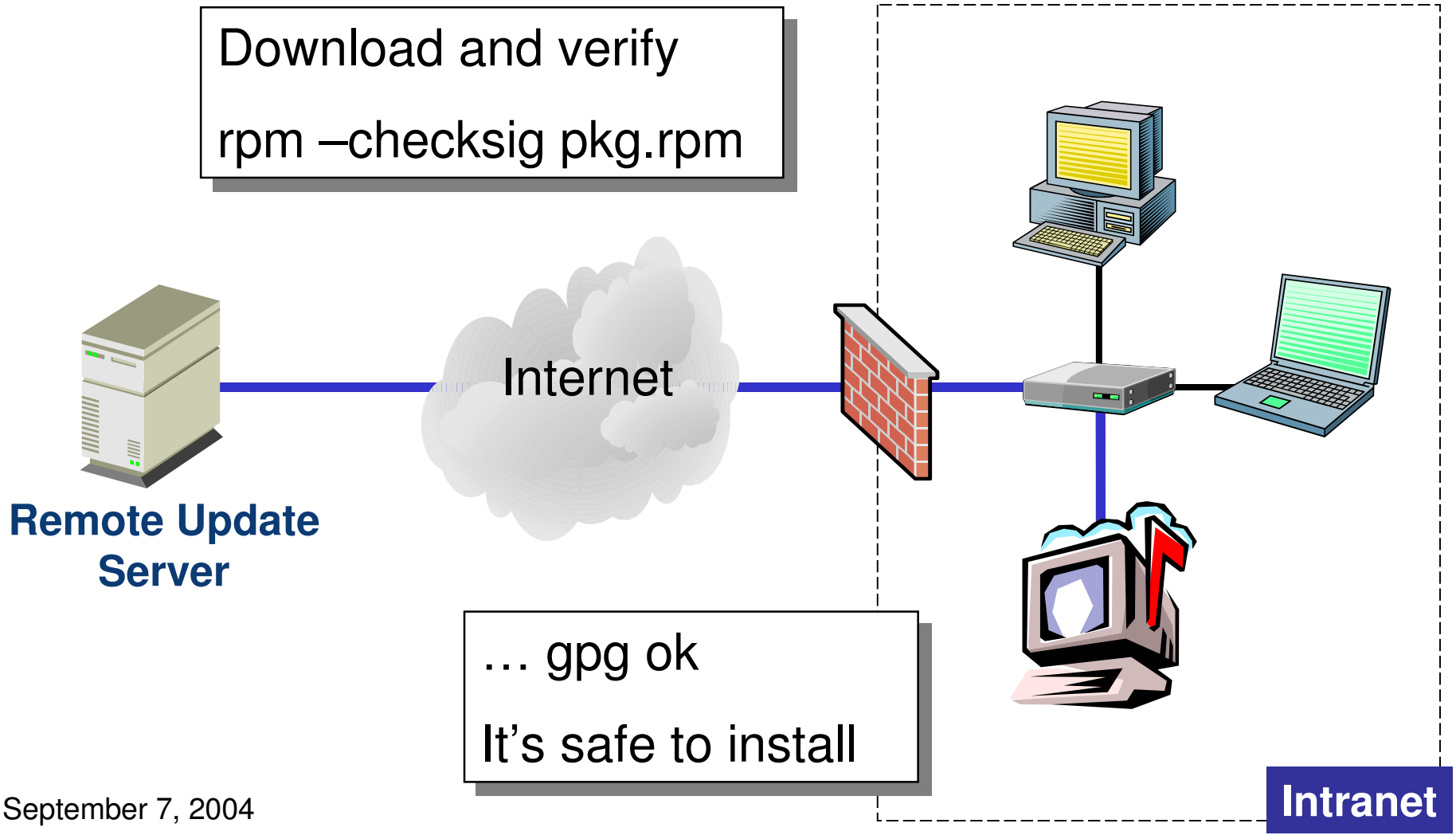


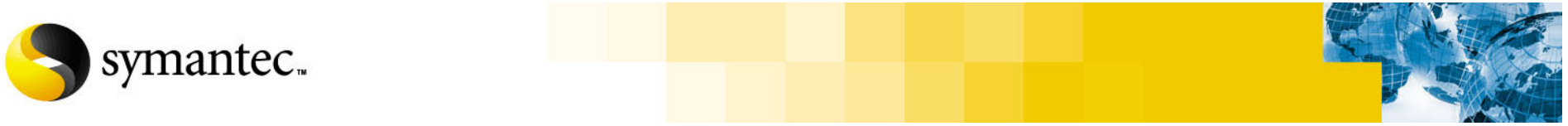
Verifying Update Packages

- **The problem**
  - **The remote server is also at risk from attack and therefore it's content is also at risk**
  - **Update packages can be modified by attackers**
  - **Users may download modified packages that include a backdoor or other hostile code**
- **RPM packages can be signed by the vendor or other third party**
  - **Based on a md5 hash of the package contents**
  - **Allows the user to verify the package source and content integrity**
  - **If the package is modified the signature will not verify**

    rpm –checksig package.rpm
- **Debian and tar packages currently lack this capability and therefore will never be able to obtain the same level of trust**

Downloading and Installing updates



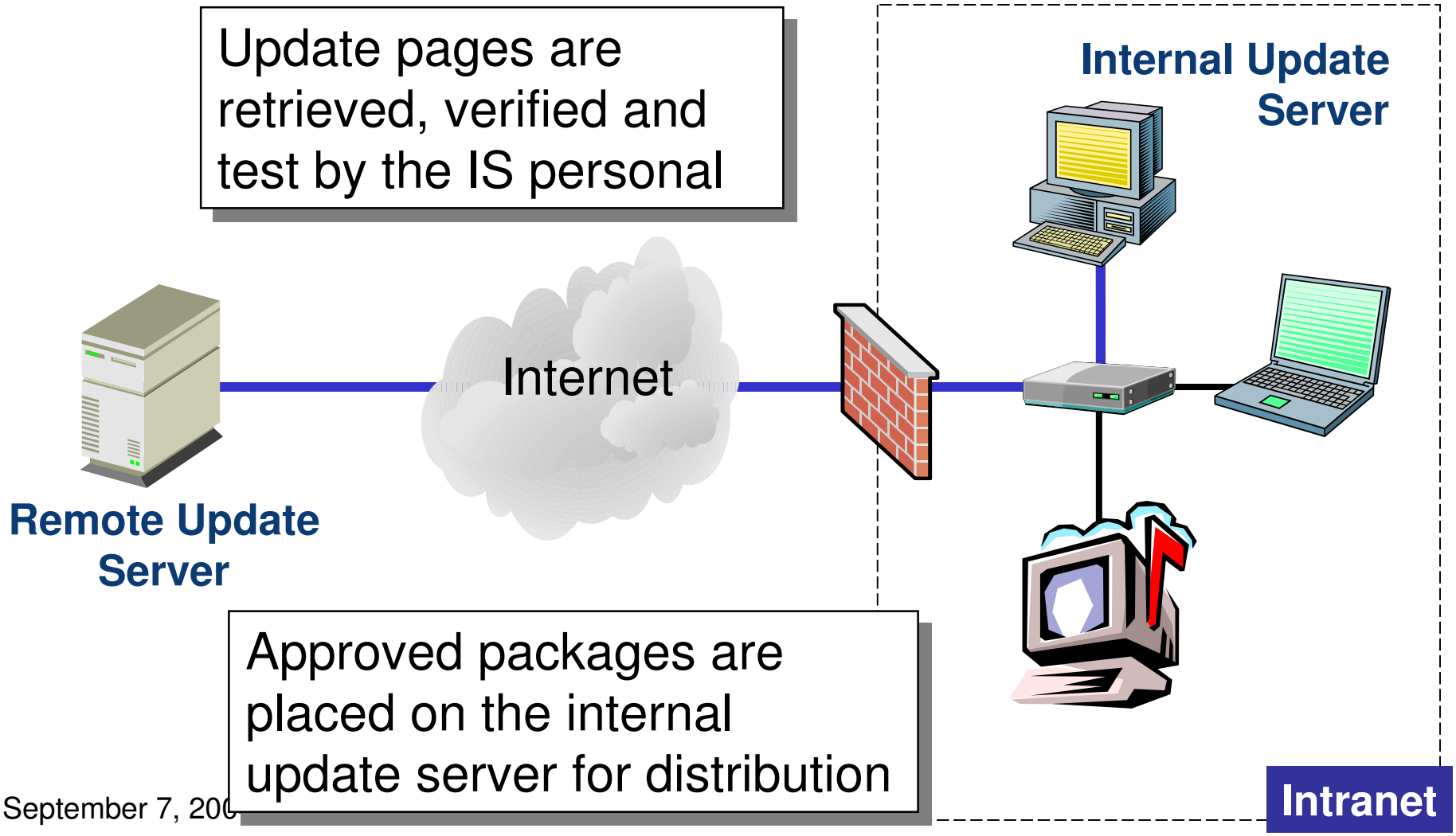


Large scale update management

- **Vender QA time on update packages is usually much less than that performed prior to a distribution release**
- **There is a significant larger chance that an update could potentially break other functionality in an unpredictable way**
- **For this reason most IS departments will wish to test update packages before distributing them to others**
- **An internal ftp server can be used to distribute approved packages**
- **The package can be signed by the IS department**

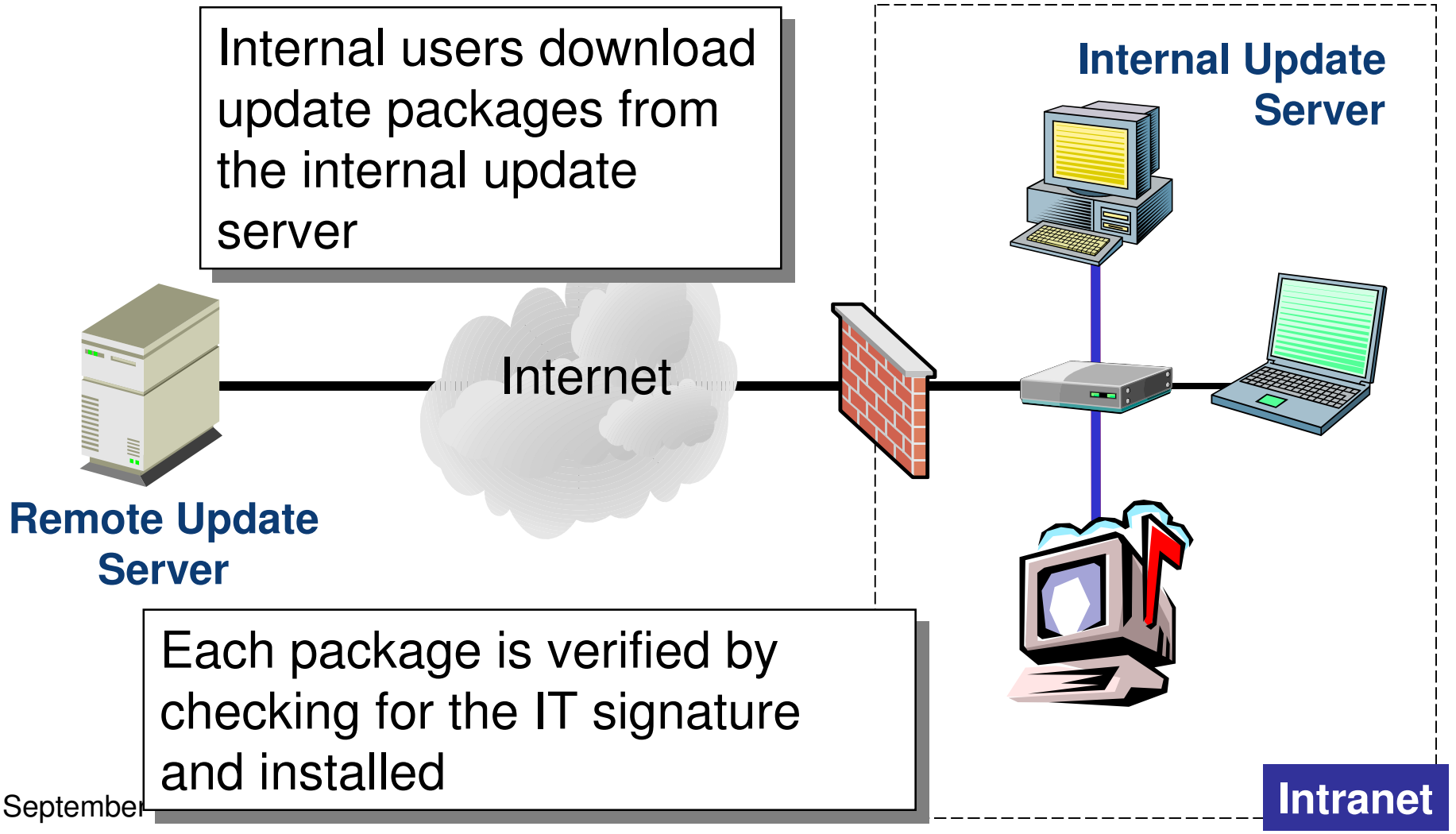
Downloading and Installing Updates

Update pages are retrieved, verified and test by the IS personal



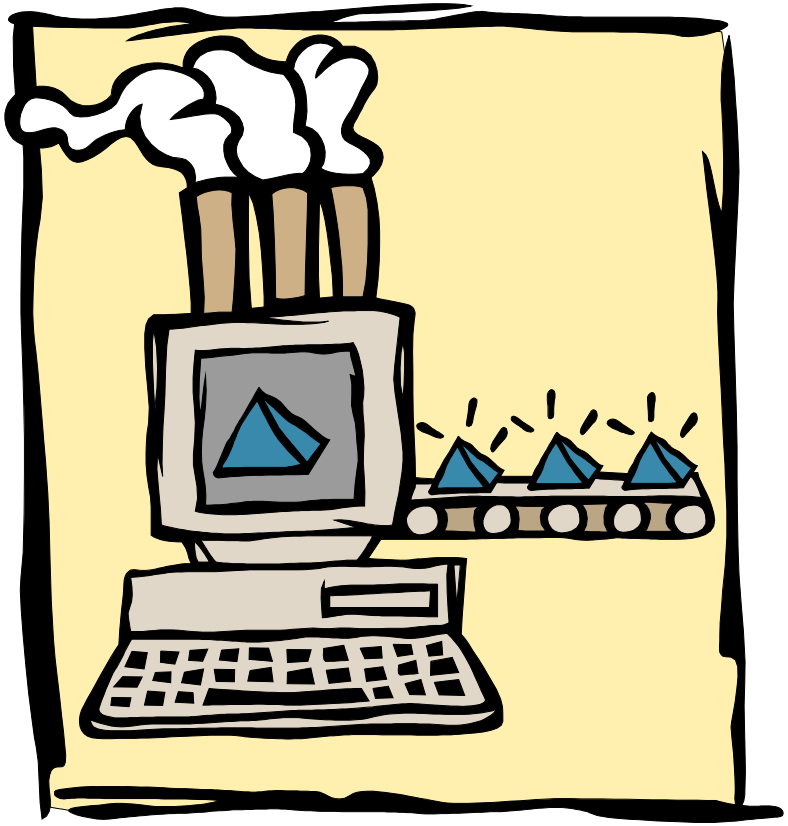
Approved packages are placed on the internal update server for distribution

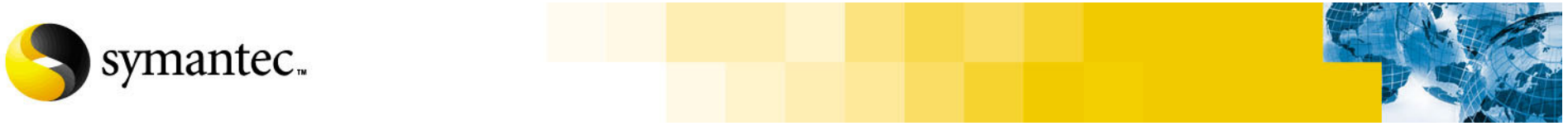
Downloading and Installing Updates



Automating the Process With autorpm

- **Autorpm is designed to help automate much of this process**
  - **Mirror RPMs from an FTP site**
  - **Keep installed RPMs consistent with an FTP site or local directory**
  - **Keep installed RPMs in a cluster or network of systems consistent**
- **Autorpm can be configured to check and all cryptographic signatures and only install those packages that can be verified**

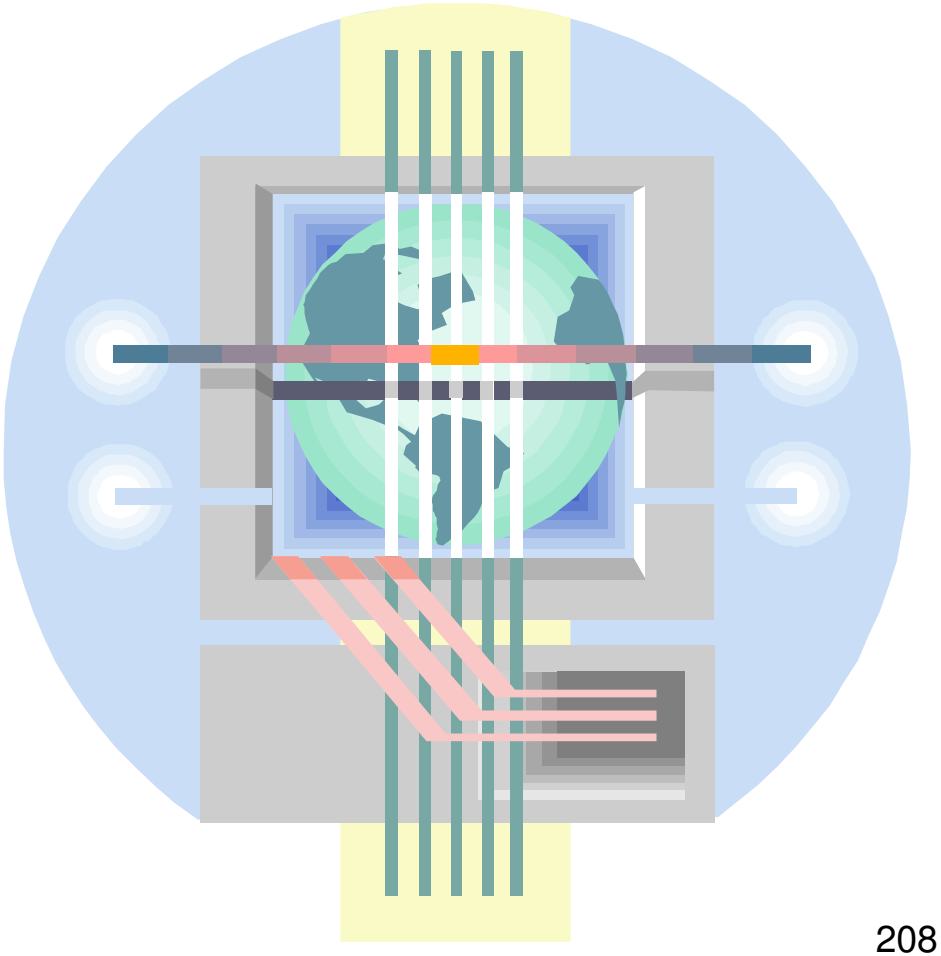




An Example Autorpm Scenario

- **The IS department installs autorpm reconfigured to update from the internal update server on all Linux desktop systems**
- **The IS public key plus the Linux distribution key (RedHat, Mandrake, …) are also installed onto the root account**
- **A cron entry is added to run autorpm once a day**
- **Update package that the IS department verifies and places on the internal update server will now be automatically distributed**

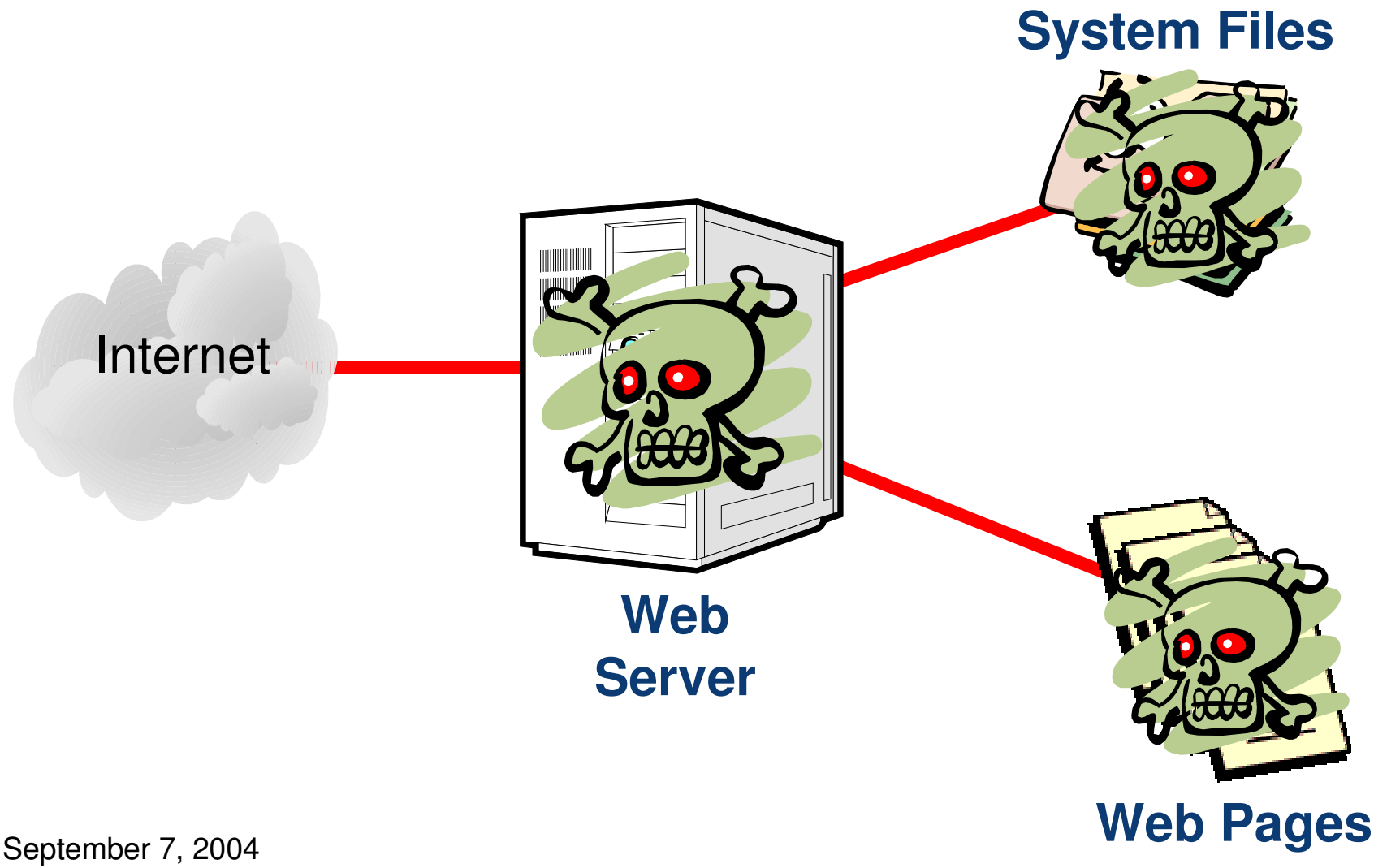
Website Security



Don’t run Web Server as Root

- **Some web servers run with administrative access**
  - **Microsoft IIS**
- **The server has complete access to all files on the system**
  - **Read**
  - **Create**
  - **Modify**
- **If the server is compromised, the attacker has complete control of the system**

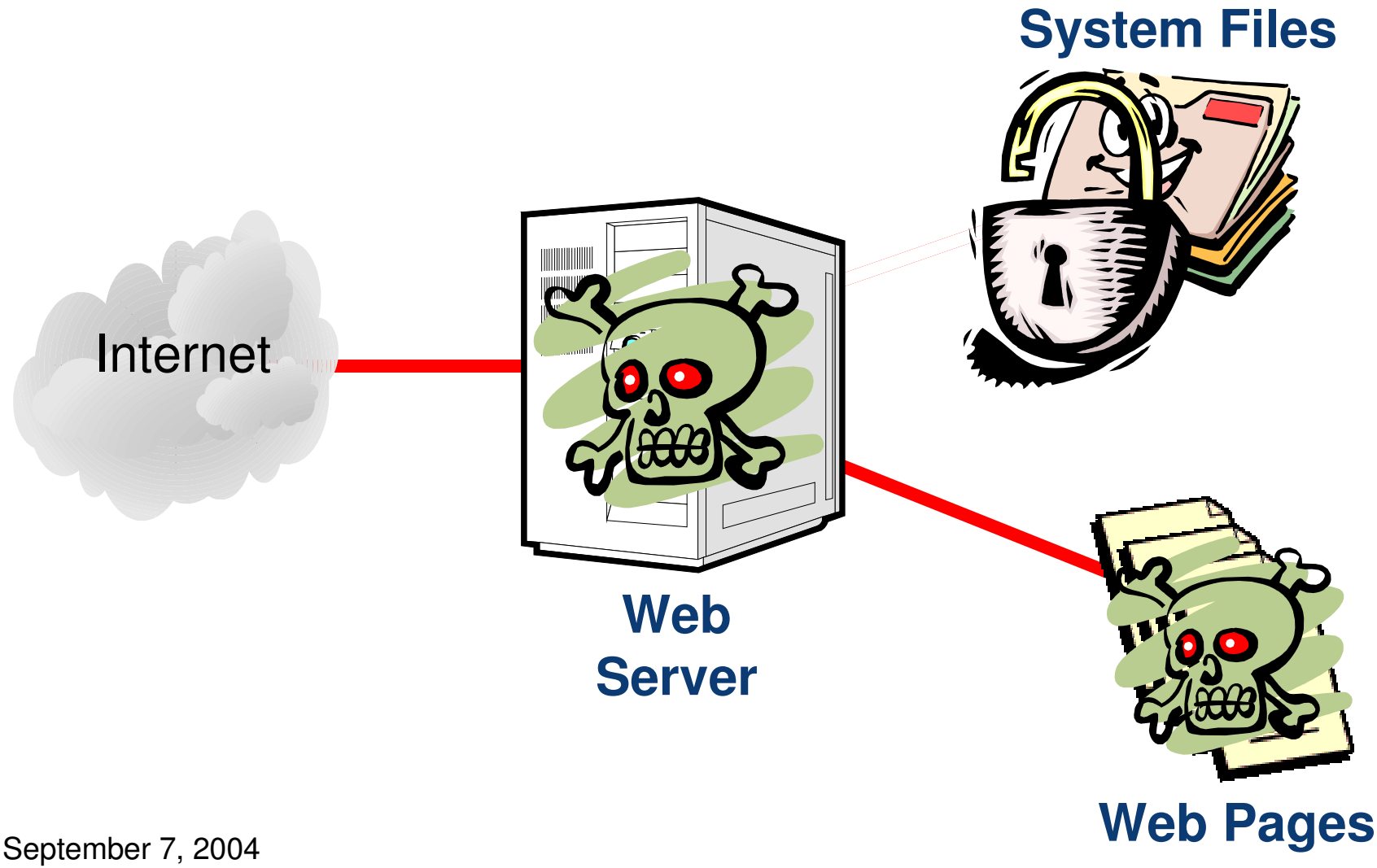
Running Servers As Administrator



Who Should The Web Server Be Run As?

- **Change the user that the web server runs as**
- **For example, lets change the configuration so that the web server is run as another user**
  1. **Add a non-root account called web-server**
     - **The Apache web server is often configured to use the 'apache' user**
  2. **Change the system / server configuration to start the web server as this user**
- **This same process should work for other web servers**

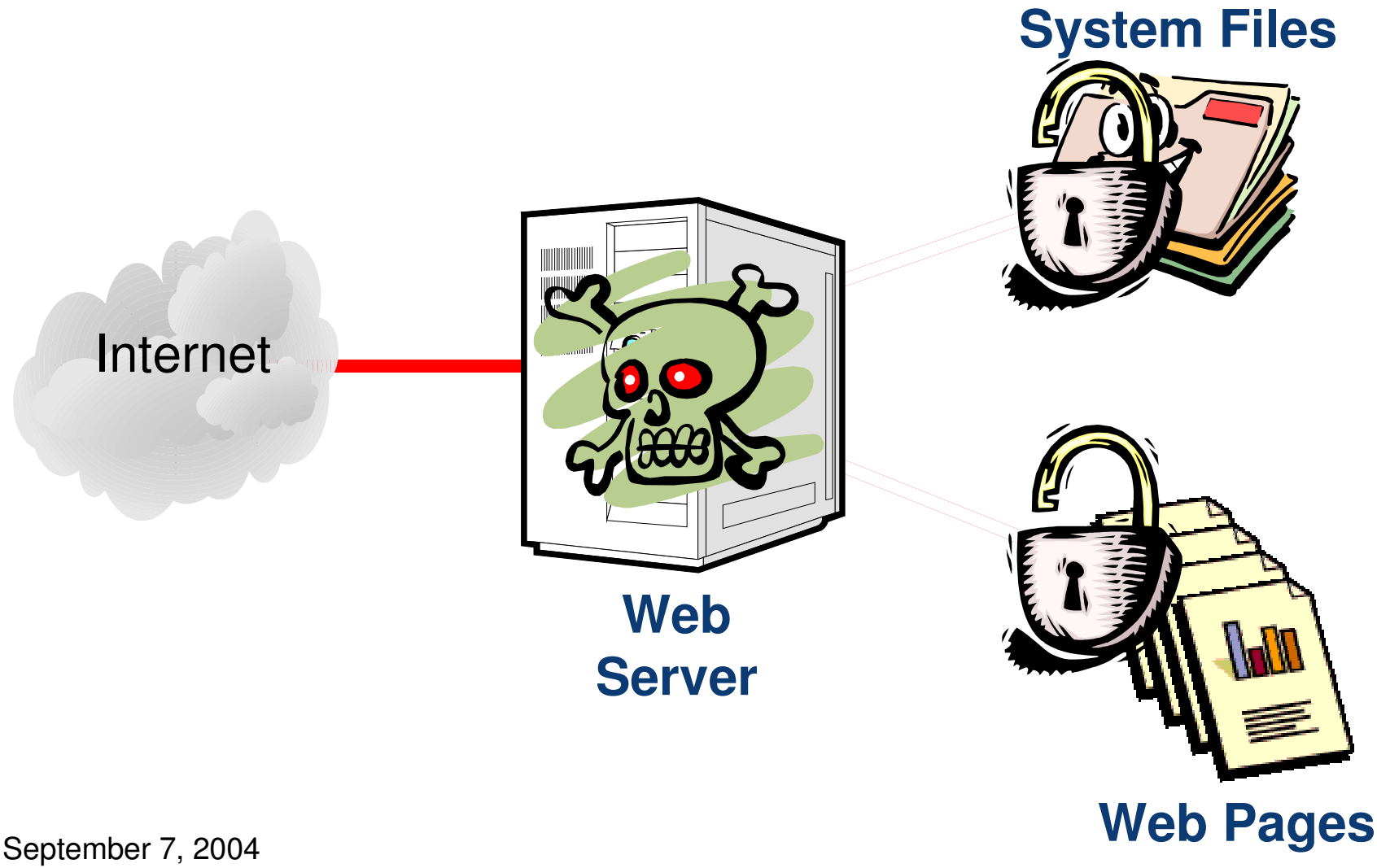
Running Web Server As Web-Server User



Who Should Own The Web Pages?

- **It is common that the web pages are own by the same user that the web server runs as**
- **Either add another user, web-pages, and make it the owner**
- **Give the web-server user read only access to the pages**
- **On Unix / Linux:**
  - **Add each web page to the web-server group**
  - **Change the access permissions for each to give the group read only rights**

Web Pages Owned by Web-Page User



Master Server

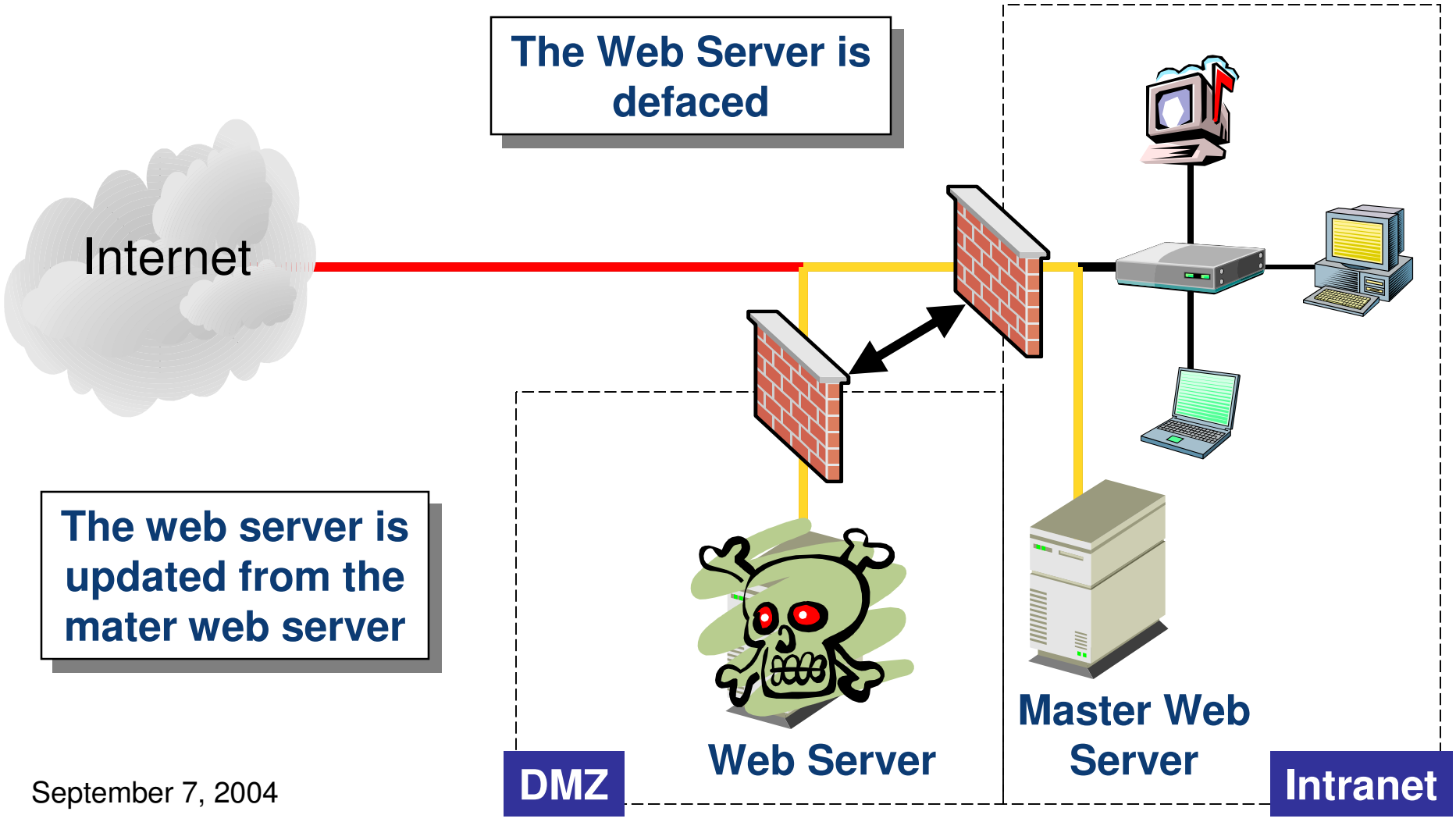
- **It is important to remember that even after making efforts to secure you site, your web site may still be defaced**
  - **Security is only a preventive effort to protect your site**
  - **It can never be 100% effective**
- **A solution to this potential, is to use a master web site**

Make the Public Web Server a Slave

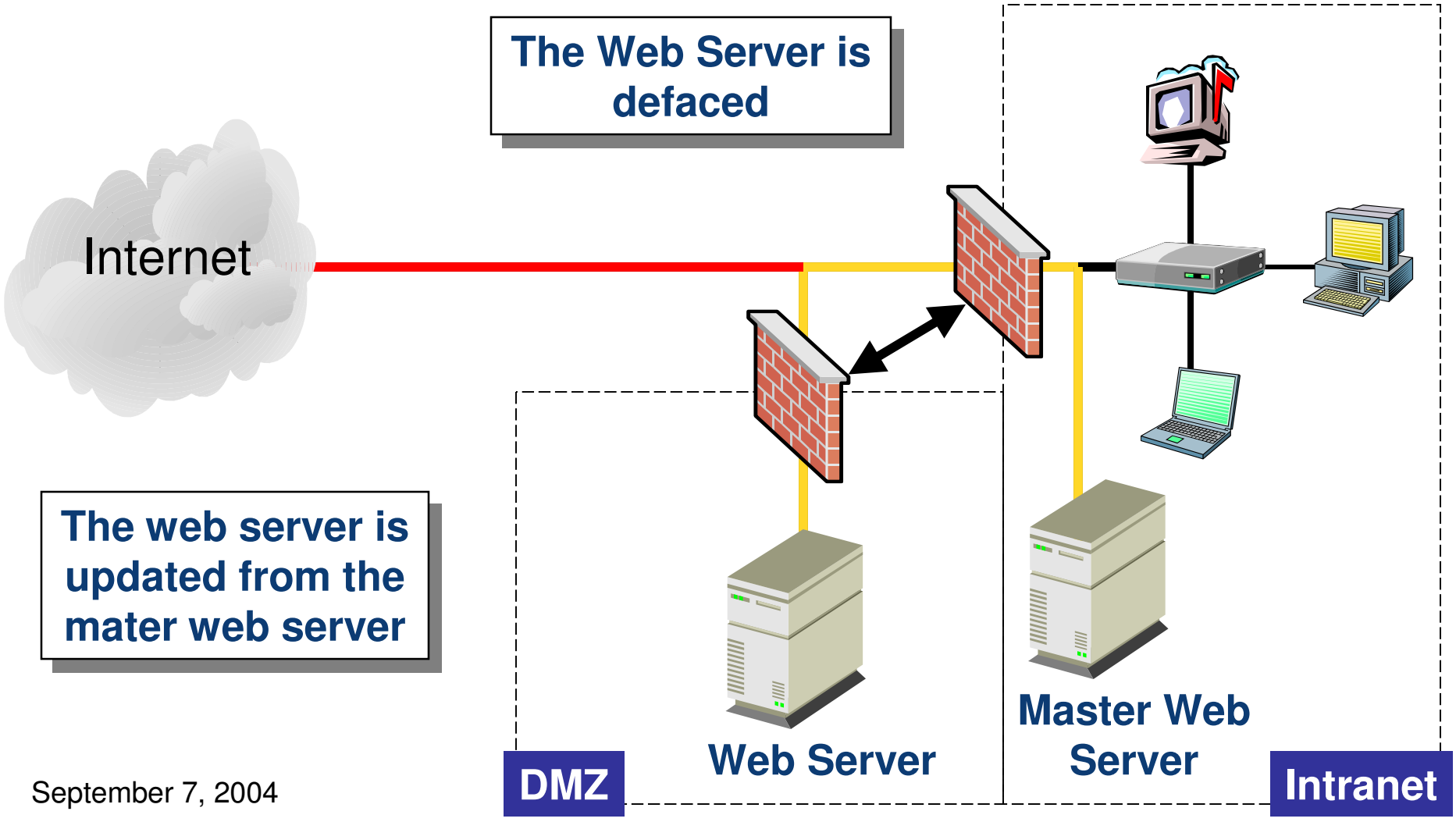
- **The master web site is located inside your intranet and is not accessible from the internet**
- **All changes for you public web site are made here**
- **The contents of the master web site are copied to the public web site at scheduled times (for example, every hour)**
- **If your public web site is defaced, it will automatically be restored at the next scheduled interval**

Important Note: **This process can be used to restore certain components of the server only – if the web server is compromised the entire system should also be considered compromised**

Using a Master Web Server



Using a Master Web Server



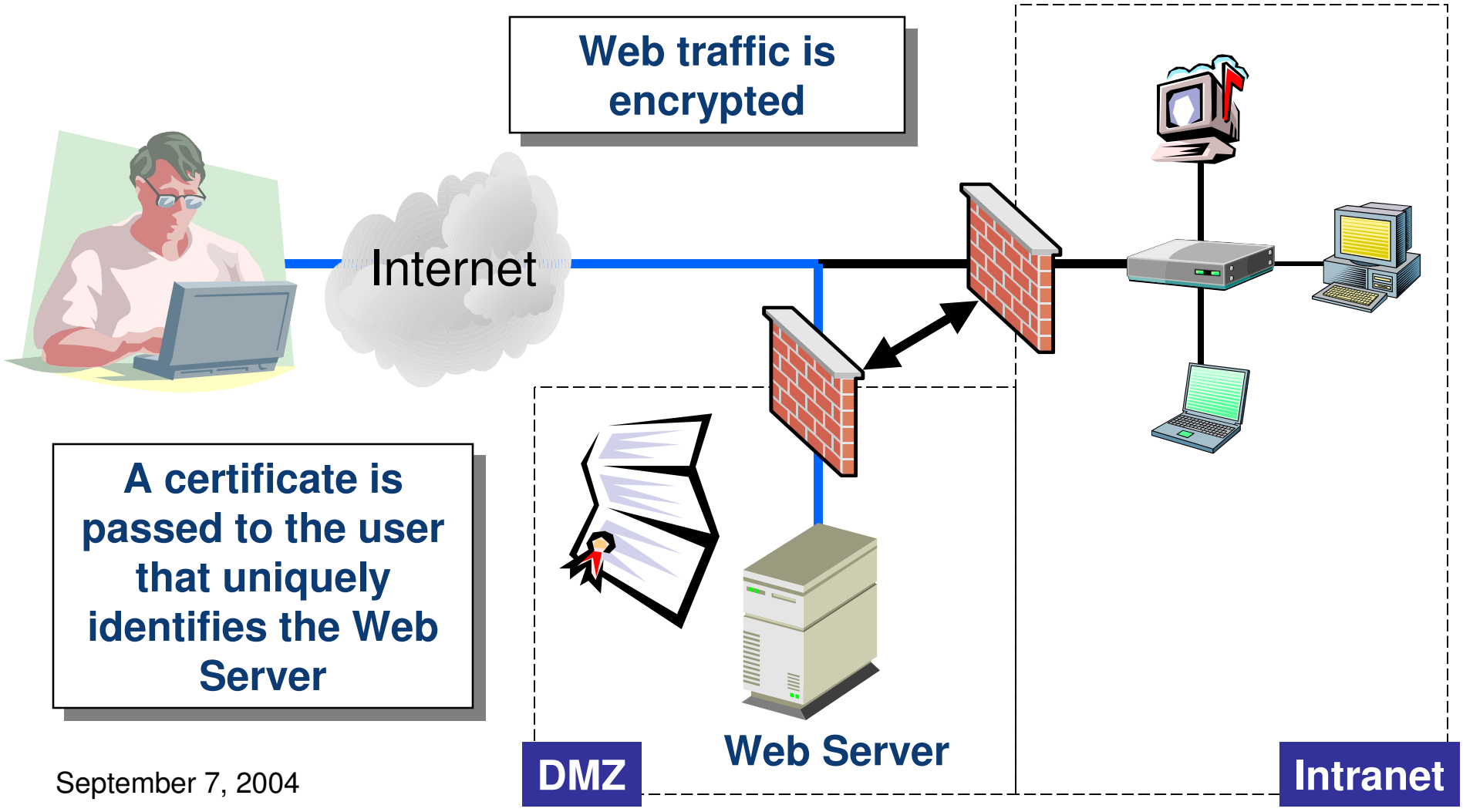
Secure Web Transactions

- **With the ever increasing use of the Web for eBusiness, a new focus on protecting confidential data arises**
  - **Normal web traffic is in clear text (it is viewable to anyone who is able to install a network sniffer into your network)**
  - **The threat of a DNS attacks removes any certainty that you really are communicating with the indented web server**
    - **An attacker can create a fake web site and attack the DNS server and redirect web traffic to this site**

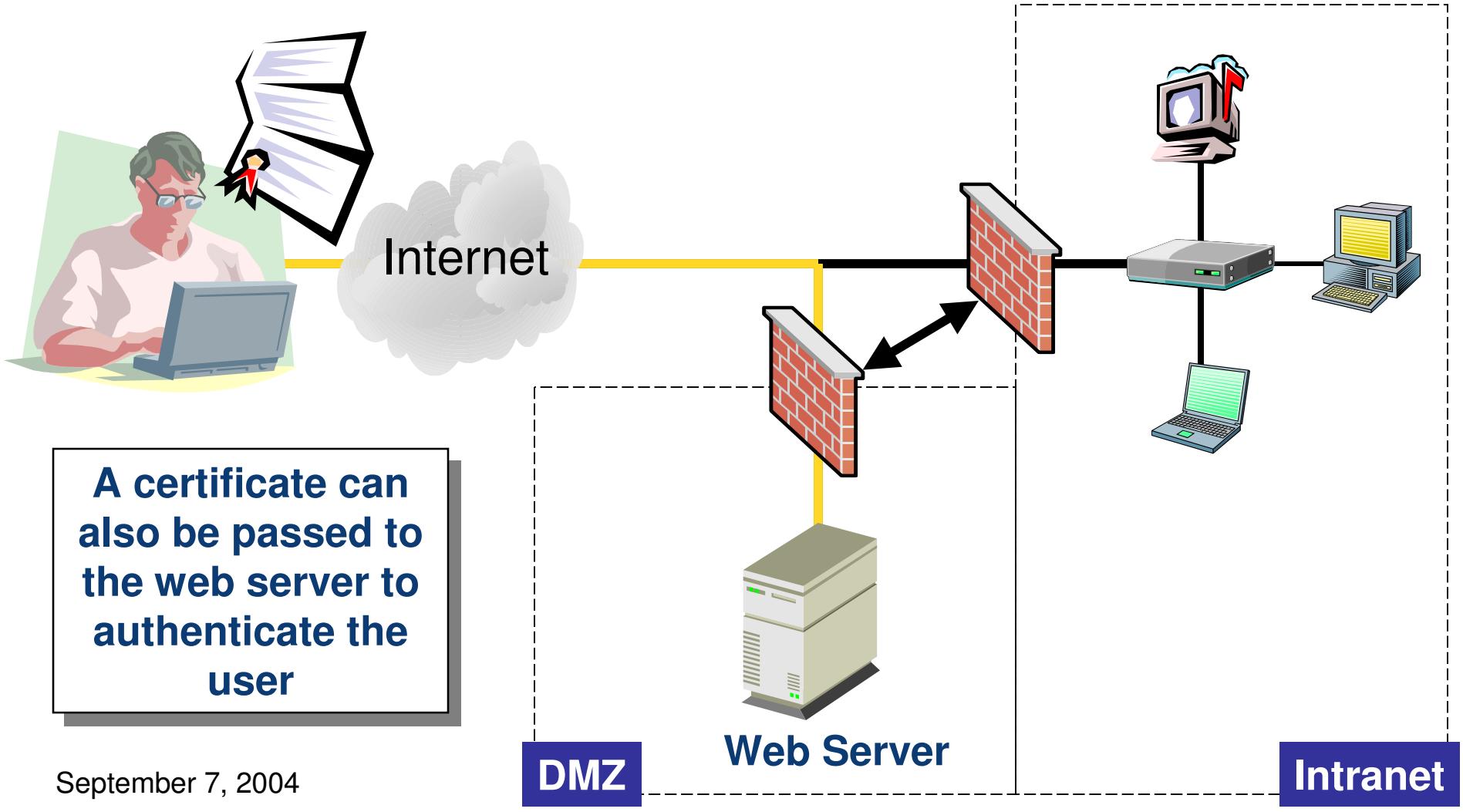
Protecting Confidential Transactions

- **Secure Socket Layer (SSL) using cryptographic certificates can be used to help deal with these issues**
  - **SSL enables encrypted communications that prevent confidential web traffic from being read**
  - **Certificates provide a level of authentication that you are really talking to the intended web server and not a imposter**
  - **A user certificate can also be used to authenticate who they are**

Secure Web Transactions



Secure Web Transactions



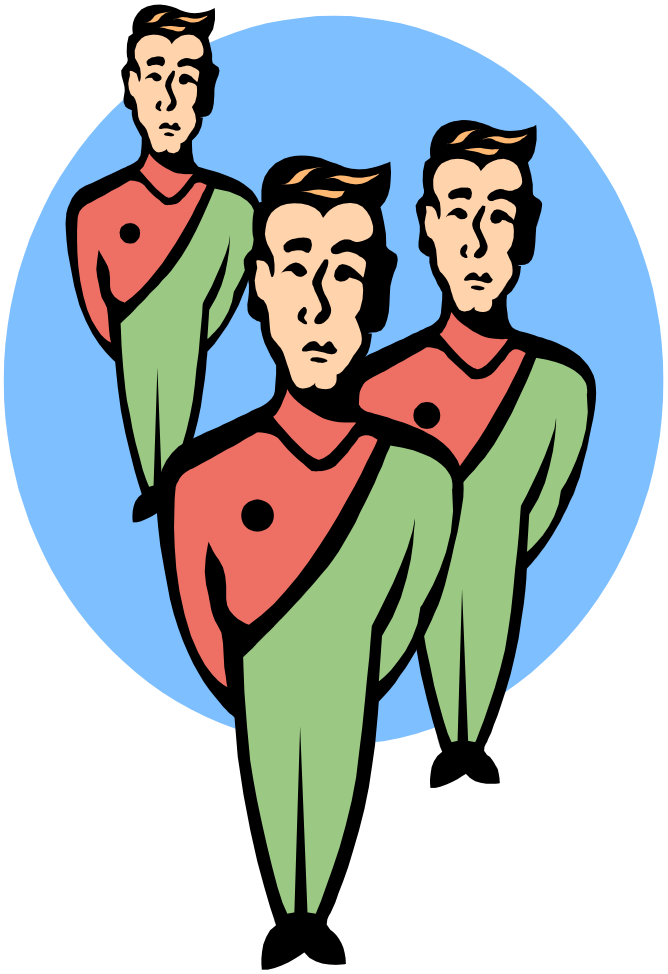
A certificate can also be passed to the web server to authenticate the user

Disaster Recovery

What if the Worst happens?

- **Security is not foolproof**
  - **Security should be balanced to your needs**
  - **0 Day attacks are becoming real**
  - **Insider attacks continue to haunt the world**
  - **System or hardware failures contribute**
- **A disaster recovery plan is needed**
  - **Identification of key systems**
  - **Redundancy build in**
  - **Regular backups**
  - **Incident correlation for due diligence**

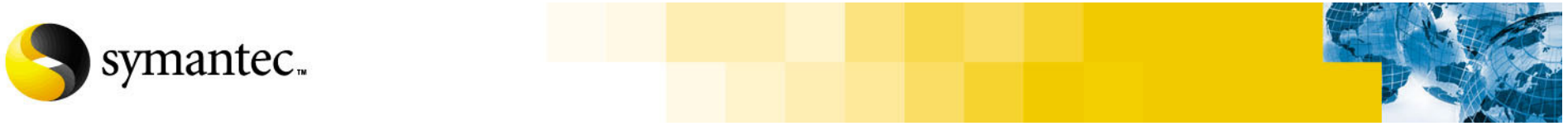
Redundancy



- **Server clusters**
- **Key system mirrors**
- **RAID Arrays**
- **Duel power supplies**
- **Multiple interfaces**
- **UPS**

Implement Comprehensive Backups Plan

- **All key systems**
  - **Web content**
  - **Database**
  - **Directory services (Samba, NFS)**
  - **Other**
- **User data**
- **Automate when possible**
  - **Monitor**
  - **Update**
- **Both full and incremental**
- **http://www.linux-backup.net/Full_Inc/**



Incident Correlation – Responding to a Break-in

- **Secure all longs (ids, network and system)**
- **Regain control of system**
  - **Disconnect from network**
  - **Copy an image of compromised system**
- **Analyze the intrusion**
  - **Look for modifications made to system software and configuration files**
  - **Look for modifications to data**
  - **Look for tools and data left behind by the intruder**
  - **Review log files**
  - **Look for signs of a network sniffer**
  - **Check other systems on your network**
  - **Check for systems involved or affected at remote sites**
- **Contact authorities**
- **Recover from the intrusion**
- **http://www.cert.org/tech_tips/root_compromise.html**
- **http://www.linux-forensics.com/ (forensics tools)**

Assessment: Finding Vulnerabilities

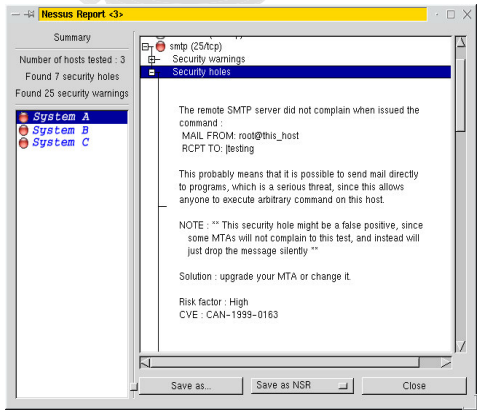
Find Vulnerabilities Before Others

- **Find vulnerabilities before they can be exploited**
- **Correct the problems that you find**
- **Use the tools that the attackers use**
- **Vulnerability scanners combine many of the exploits found in hundreds of attack tools into a easy to use interface**
  - **Detailed reports are created for review**
  - **Most include suggested procedures to remove the vulnerability**
- **Open source tools exist for small business and home users**
- **Commercial products generally provide a better assessment**
  - **Symantec ESM and NetRecon**
  - **…**

Scan For New Vulnerabilities

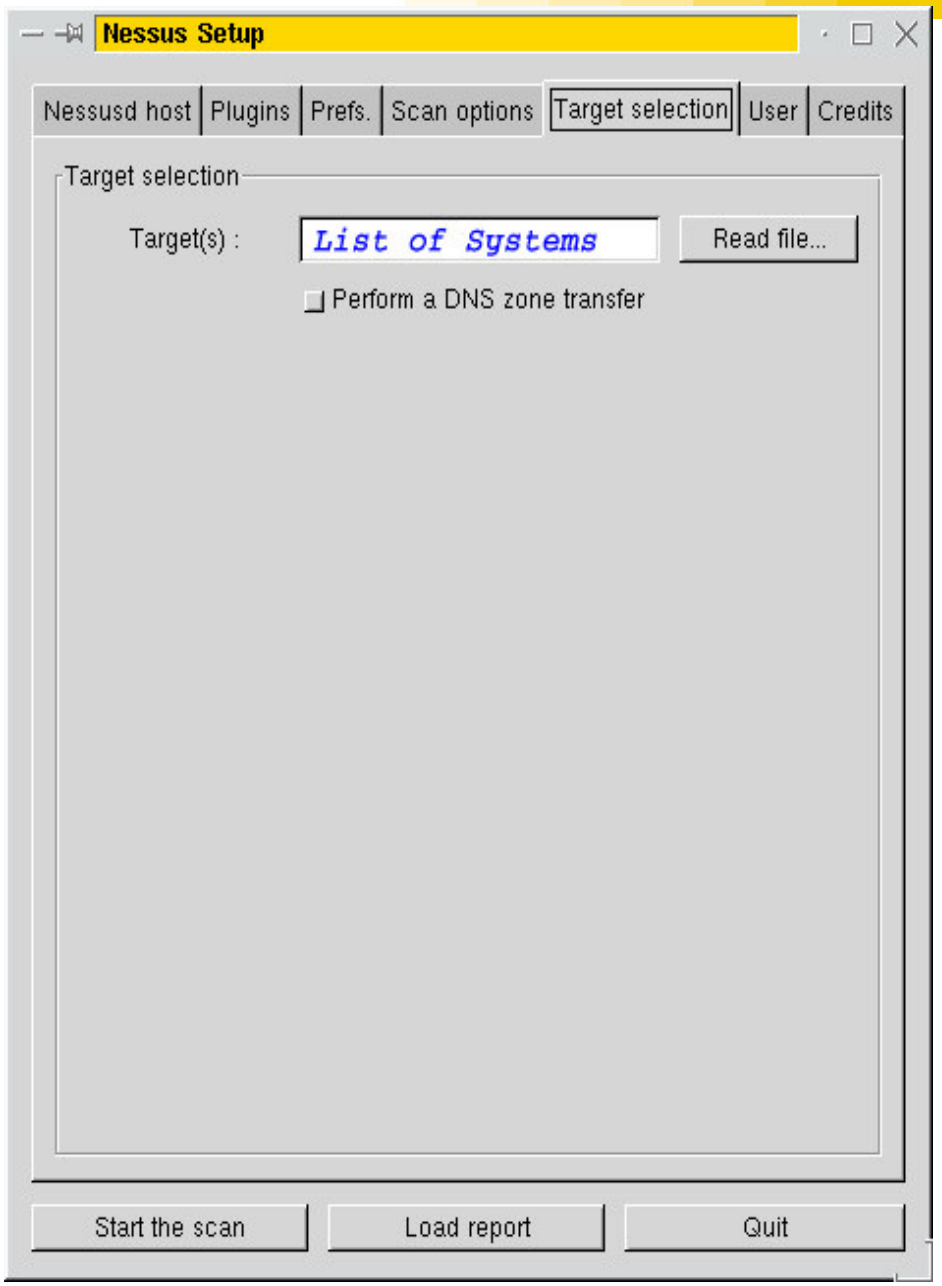
Actively Scan for Vulnerabilities

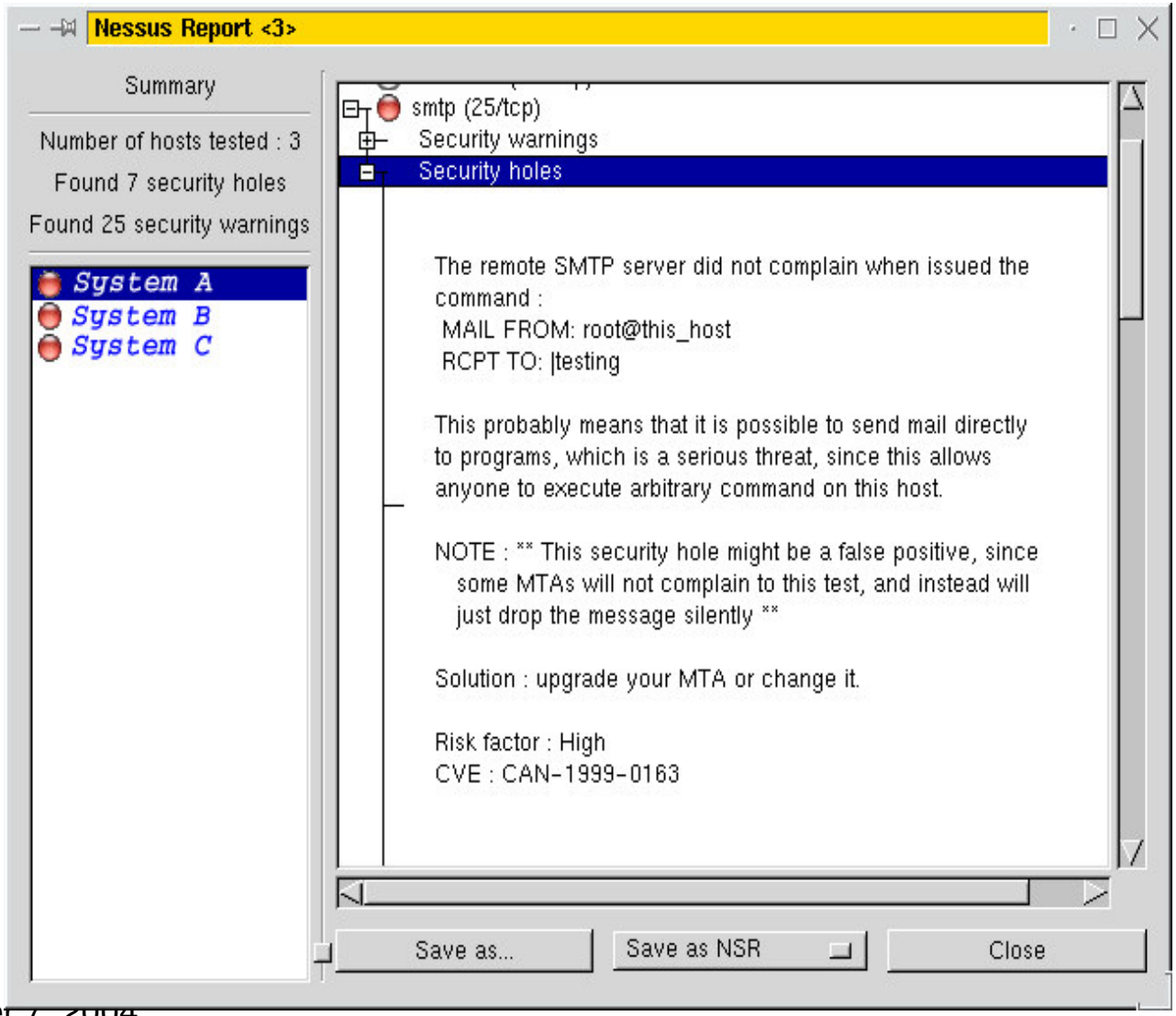
Internet



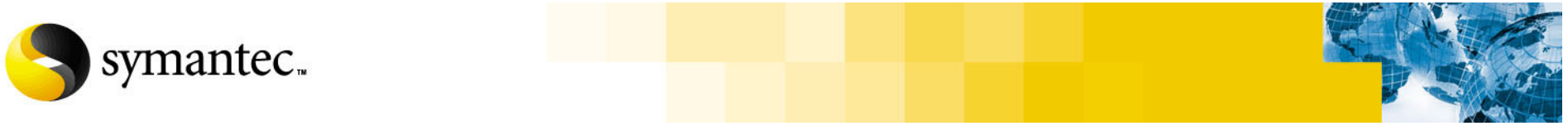
Hub

Policy Compliance


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
Credits
Target selection
Target(s) :
List of Systems
Read file...
Perform a DNS zone transfer
Start the scan
Load report
Quit


Nessus Report <3>
Summary
Number of hosts tested : 3
Found 7 security holes
Found 25 security warnings
System A
System B
System C
smtp (25/tcp)
Security warnings
Security holes
The remote SMTP server did not complain when issued the command :
MAIL FROM: root@this_host
RCPT TO: |testing
This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary command on this host.
NOTE : ** This security hole might be a false positive, since some MTAs will not complain to this test, and instead will just drop the message silently **
Solution : upgrade your MTA or change it.
Risk factor : High
CVE : CAN-1999-0163
Save as...
Save as NSR
Close

IV: Where Can I Find More Information?



Where You Can Find More Information

- **Symantec Corporation**
  - http://www.symantec.com
- **Security Focus (Home of BUGTRAQ) and now part of Symantec**
  - http://www.securityfocus.com
- **CVE (Common Vulnerability and Exposures)**
  - http://cve.mitre.org
- **SuSE Linux Internals**
  - http://www.bb-zone.com/SLGFG/
- **Red Hat Linux Security Guide**
  - http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide
- **Debian Security Information**
  - http://www.debian.org/security/

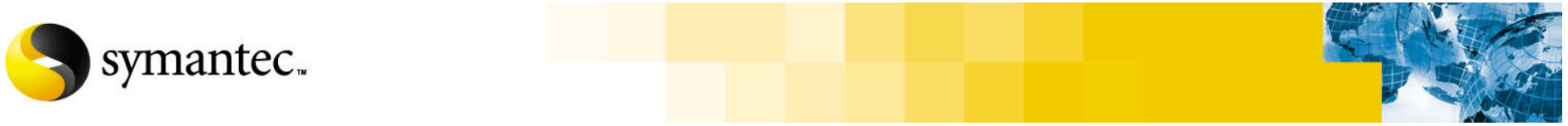
Where You Can Find More Information

- **SANS Institute**
  - http://www.sans.org
- **The Center for Internet Security**
  - http://www.cisecurity.org
- **Linux Security**
  - http://www.linuxsecurity.com
- **Network Security Library**
  - http://secinf.net
- **Virtual Private network daemon (vpnd)**
  - http://sunsite.dk/vpnd/
- **The Linux Documentation Project**
  - http://linuxdoc.org

Where You Can Find More Information

- **Linux Administrator's Security Guide**
  - http://www.seifried.org/lasg/
- **Securing & Optimizing Linux (online book)**
  - http://www.openna.com/products/books/sol/solus.php
- **Bastille Linux (Linux Hardening)**
  - http://www.bastille-linux.org/
- **Amanda (backup solution)**
  - http://www.amanda.org/
- **Linux-Sec.net**
  - http://www.linux-sec.net/
- **Packet Storm**
  - http://www.packetstormsecurity.com

V: Conclusion



Conclusion

- **The Linux Operating System (like others) is susceptible to security attacks**
- **Successful attacks can be a serious issue**
  - **Downtime**
  - **Embarrassment**
  - **Lost revenue**
- **You should consider security from the very beginning**
- **You have to understand the technical aspects to combat the threat**
- **Remember that the first step to securing your site should be the development of a security policy that fits your needs**

VI: Questions?