Firewall Design Issues

T.Rex

3/02/2000

Jim Livermore
Livermore Software Laboratories International
a division of Freemont Avenue Software, Inc.
2825 Wilcrest   Suite 160
Houston, TX 77042
(281)-759-3274
jim@lsli.com

Agenda

- I.   Nature of Attacks
- II. Firewall Architectures
- III. Design Goals
- IV. Implementation Specifics

Nature of Attacks

- There are hundreds of methods to attack a TCP/IP network
  - methods range from simple to complex
  - password sniffing
  - application weaknesses
  - trust based on IP address
  - low level attacks
  - application level attacks
  - …

Nature of Attacks - 2

- Rapid introduction of new applications and new functions create a fertile patch for hackers.
  - Applications developers are concentrating on solving business problems.
  - Insufficient consideration given to security.
    - Just because you can do something doesn’t mean you should
  - Programmers continue to make errors that have known solutions for > 25 years.
- New methods are being invented on a regular basis.

Nature of Attacks - 3

- Some applications are extremely vulnerable and difficult to defend.
    - Including software from large corporations

Nature of Attacks - 4

- Automated attack tools are readily available
    - lower skill required to mount an attack
    - Source code and executables available on the Internet
        - Satan
        - BackOrifice
        - BlueButton
        - SYN Flood

Nature of Attacks - 5

- **Nmap** network scanner
    - Vanilla TCP connect scan
    - TCP SYN (half open) scan
    - TCP FIN (stealth) scan
    - TCP ftp bounce attack
    - SYN/FIN scanning using packet fragments (bypass packet filters)
    - UDP raw ICMP port unreachable scan
    - ICMP (ping sweep)
    - TCP ping scanning
    - Remote OS Identification
    - Reverse-ident scanning
    - and more
    - www.insecure.org/nmap/index.html

Nature of Attacks - 6

- Firewalking
    - firewall protocol scan determines open ports
    - sending packets to every host behind a packet filter generates an accurate map of networks topology.
        - TTL ramping
        - scan TCP/UDP ports
    - Defenses
        - block ICMP TTL Exceeded messages from leaving private net
        - use proxy firewall
    - More info at:
        - www.es2.net/research/firewalk

Nature of Attacks - 7

- Many attacks depend on knowing host names, IP addresses, user IDs etc.
- Weak passwords
- Trojan horses

Nature of Attacks - 8

- Routing Attacks
  - enabling man in the middle
- Address spoofing
- SNMP
- ICMP Packet Magnification Attacks aka Smurf

Nature of Attacks - 9 Denial of Service

- SYN Flood Attacks
- Ping of Death
- Distributed Denial of Service Attacks
  - employ multiple machines (thousands) for the attack
  - –
- TRINOO/Tribal Flood Net
- Stacheldraht
  - appeared in August 1999
  - master
  - agents

Application Attacks

- The most serious network attacks rely on application data streams
  - exploit application server weaknesses
  - attack is buried deep within payload portion of packet.
  - these attacks pass through stateful packet filters, because they only examine protocol headers
- Application-specific content inspection is required to stop application level attacks

Application Attacks-2

- E-mail
  - – standards violations
    - lines longer than 1000 bytes can overrun E-mail servers buffer with unpredictable results.
  - – long filenames in MIME Attachments
    - buffer overruns in Netscape Communicator & MS Outlook
  - – Hackers exploit weaknesses in mail servers that allow passing of parameters and execution of commands imbedded in header information
    - Subject: something ; rm -r *
    - /usr/bin/mail < /etc/passwd

Application Attacks-3

- E-mail (continued)
- MS Word Macros
  - – Macros imbedded in MS Word attachments
- embedded links to Web pages
  - – Clicking on URL downloads page.
  - – If URL contains a JAVA program it can do anything the originator wishes
  - – Flaw has been used to install Back Orifice
  - – More than 18,000,000 copies of Eudora have this problem
  - – How many have installed the patch?

Application Attacks-4

- E-mail (continued)
- Denial of service attacks
  - – fill up disk space
  - – large files
  - – large number of recipients
- SPAM
- Sendmail
  - – large complex program with root authority
  - – dangerous combination
  - – major source of security alerts

Application Attacks - 4

- FTP exploits
  - – Complex state machine
    - requires proper setting and checking of state vectors
    - possible to execute commands prior to identification/authentication
    - Defense:
      - – create dual loop state machine
  - – FTP Bounce attack
    - FTP specification allow:
      - – control connections to come from anywhere and
      - – data connetions to go anywhere
    - Defense
      - – Only allow data connections to same host that the control connections originate from.
      - – Don’t allow control connections to originate from port 20

Application Attacks - 5

- FTP - continued
- FTP client executing downloaded file
  - If file name begins with pipe sign ftp client will try to execute it.
  - Defense:
    - block download of files when first character of filename is “|”.
- User ID and password travel in the clear
  - Hacker can sniff login packets and gain access
  - Defense
    - enforce strong user authentication for clients on un-trusted network

Application Attacks - 6

- **Exploiting Dangerous functions**
  - finger
  - showmount
  - RPC-info
  - rexec, rlogin, rsh, rwho
  - Netmeeting
  - tftp
  - NIS
    - password file access

Application Attacks - 7

- NFS
  - Remotely Exploitable Buffer Overflow Vulnerability in mountd
    - attacker can gain administrator authority (CA 98-12)
  - export passwd file
  - Fundamentally insecure and should not be made accessible form internet

Application Attacks - 8

- MS IE 4
- Untrusted Scripted Paste
  - aka Cuartango vulnerability
- malicious hacker can create a web site that, when visited, is able to use script to read a file on the user's system.
- MS patch available (VB98-12)
- Son of Curatango bypasses fix.
- Can’t trust ActiveX, or JavaScripts

Firewall Architectures

- Packet Filters
- Stateful Packet Filters
- Application Proxy
- Advanced Application Proxy
- Hybrids

Packet Filters

- Advantages
  - readily available on most routers
  - low overhead for simple networks

Packet Filters - 2

- Disadvantages
  - Security is based on trusted Source IP address
    - can be spoofed
  - No user authentication
    - who are you letting through?
  - Direct IP connectivity between external client and internal server
    - allows many application attacks through
  - Static filters leave permanent holes in the firewall
    - allow hacker entry
    - many applications are difficult to filter
  - Filters become complex and hard to manage
  - Complex filters often contain errors that open security holes
  - Significant burden is placed on systems administrator
  - Not application aware

Stateful Packet Filters

- Were developed to overcome the serious shortcomings of static filters
- For selected applications SPF can keep track of state and context of a session

SPF - 2

- **Advantages**
  - Unlike static filters, holes are opened on a temporary basis
    - It is significantly harder for a hacker to penetrate
  - It is easy to add filters for new services
  - Relatively low overhead for limited number of rules

SPF -3

- **Disadvantages**
  - Direct IP connectivity
    - hackers can exploit application weaknesses
    - ex. BO via UDP/53
  - No user authentication
    - requires a proxy
  - Proxies on top of SPF exhibit very poor performance
  - Can support any service
    - double edged sword
    - many un-secure applications have been granted access through SPF
  - Trust still based on IP address
  - Overhead increases with additional rules
  - Not scalable with SMP
  - Not application aware

Application Proxy

- Application proxies maintain separate connections with the client and the server preventing direct IP connectivity

Proxy -2

- **Advantages**
  - Proxies are fundamentally more secure than filters
  - There is no direct connectivity between client and server
  - Security is based on authenticated user ID
  - Proxies analyze application data streams and commands within the data portion of the payload.
  - Application specific proxies can check for attacks that exploit application weaknesses
    - proxies can detect and stop attacks that get past SPF firewalls
  - Proxies keep comprehensive logs of all activity

Proxy - 3

- **Disadvantages**
  - Slower than packets filters
    - do more work
    - often not optimized for system
  - they do not support every type of connection
    - RPC, UDP, …
  - client awareness

Advanced Application Proxy

- Advanced Application proxy firewalls extend proxy capabilities and overcome their disadvantages
  - generalized TCP, UDP, and RPC proxies
    - broadens application support
  - generic application level content filtering
  - sophisticated design can eliminate up to 90% of the systems overhead
  - Support SMP architecture
  - Support workload balancing across clusters of SMP firewalls
  - non-disruptive administrative changes as well as non-disruptive system upgrades
  - fault tolerant hardware/software architecture

Firewall Design Considerations

- There is no perfect solution for all problems
  - all designs involve tradeoffs
    - security, performance, reliability, availability, ease of administration, ease of use
- Pick design goals
  - Let goals dictate solution based on ability of architecture to meet goals

Primary Design Goals

- Provide highest level of security possible
- Provide the highest level of performance
  - scalable
  - parallelism
- Provide High Availability for Mission Critical Applications
  - up to 99.999% availability
  - < 6 minutes of unscheduled outage/year!
  - Non-disruptive administrative changes
  - Non-disruptive upgrades
  - fault tolerant hardware/software

Design Goals - 2

- Provide Cost effective Solution
  - Reduce Administrative costs
  - Reduce numbers of systems to manage
- Reduce risk of security breech due to human error
  - Deny all services except those which are explicitly permitted
  - Make interfaces simple to understand
  - do not provide risky options or defaults
- Support an organizations policy don't impose one.
- Accommodate new services
  - allowing application specific content inspection

Design Goals - 3

- User authentication
  - support multiple third party authentication servers
  - provide integrated authentication
  - support strong user authentication
  - support Out Of Band Authentication
- Permit filtering based on
  - source and destination IP address and port
  - user ID and group ID
- Log all activity
  - provide data reduction programs
- Issue Security Alerts
- Hide all information regarding internal network structure

Application Support

HTTP	SSL	SMTP	FTP	Telnet
tn3270	NNTP	POP3	IMAP	SQL
Oracle	Sybase	DB2	Lotus Notes	SNMP
Real Audio	Real Video	Java Filtering	SPAM blocking	HTTP Caching
UDP	RPC	URL Filtering	ActiveX Filtering	MS Exchange
NTP	Reverse HTTP	Log Analysis	Remote Admin	Encrypted Telnet
Out Of Band Auth	X11	WinFrame	NFS	Dual DNS
…				

Architecture determines Security & Intregity

- All hardware and software is subject to failure
- Packet filters run as part of the kernel
  - No error isolation
  - Errors in kernel code can cause catastrophic failures
- SPF's can and do fail wide open
  - Many customers will configure back to back SPF's to limit scope of failure
- Failures can impact all services

Architecture determines Security & Intregity (2)

- T.Rex is an advanced application proxy firewall
- Proxies run without root privileges in chrooted directories
  - hardware and software errors can not be used to access or alter the TCB.
  - Errors are isolated to a single process
  - Use of multiple processes rather than threads isolates instances of the same function from each other.
- Three levels error detection, reporting and recovery
  - extensive error checking and reporting in worker process
  - parent process simply monitors children and recovers from errors
  - Specialized system wide monitors that can detect errors in parent processes
- Cross system monitoring with redundant systems

High Availability

- Fault tolerant application proxies limit scope of a failure to a single transaction.
- Dynamic function recovery
  - prevent process depletion
  - automatic process retirement to prevent memory leaks
- Application proxies can be built in load balancing redundant configuration
  - complete hardware and software redundancy
  - cross system monitoring
  - dynamic take-over in event of failure
- Allows deployment of systems with 99.999% availability
  - less than 6 minutes of unscheduled outage per year!

Immunity to low level attacks

- The only way to transmit data through the firewall is via a secured proxy
  - disable IP packet forwarding
  - data is read into a buffer then sent to the target system
- Low level attacks depend on direct IP connectivity
- Low level attacks are never seen by hosts protected by an application proxy

Implementation Specifics

- SMTP
- FTP
- HTTP
- Reverse HTTP
- High Availability
- Reporting

Secure Mail Wrapper

- Provide a secure SMTP interface
- Separate receiving and sending programs
  - smwrap and smwrapd
  - store and forward
  - don’t forward mail until completely checked

- Smwrap receives mail
  - runs as an unprivileged program
  - change root directory to hermes
    - rest of file system inaccessible
  - unable to access or modify the TCB

Smwrap - 2

- Mail is checked for cracker signatures
  - long lines,
  - long names,
  - imbedded commands,
  - parameter passing
  - Bogus Helo
  - SMTP commands longer than 512 bytes
  - Excessive Mail Header Size > 32KB
  - Excessive number of recipients
  - Excessive number of “To:” lines in body
  - Use of VRFY & EXPN
  - Blocked Sender|Reciever
  - Unauthorized internal user

Smwrap - 3

- Block unauthorized mail relay
- SPAM blocking
  - deny from email4all@aol.com to *
  - deny from runnersssss@aol.com to *
  - deny from @bigfoot.com to *
- Complete scrubbing of out-bound headers
  - translate internal names to external
  - From:, To:, Cc:

Smwrap - 4

- Support multiple domains
- Support multiple mail servers
- Simple administration
  - @xyz.com @sys1.xyz.com
  - @abc.com @sys2.abc.com

Smwrapd

- Smwrapd is responsible for delivering mail
- Smwrapd
  - wakes up every minute
  - looks for complete messages
  - spawns multiple processes for parallel delivery
- Additional checking
  - excessive field lengths in MIME extensions
- If message can not be delivered to target
  - queue message and have sendmail deliver it.

FTP

- Ftproxy provides secure FTP access
- Runs as user hermes in a chrooted directory
  - can not be used to compromise TCB
- dual loop state machine
  - can not execute sub commands prior to
  - user ID and authentication
- prevent FTP Bounce Attack
  - data connections must go to the same hosta as the control connections.
- Protect FTP client from executing downloaded file
  - deny download of files when the first character of fn is a ‘|’.
  -

FTP - 2

- Safe but flexible user authentication rules
  - enforce strong user authentication for un-protected clients
    - avoid password sniffing
  - permit choice of authentication method for protected clients
    - optional user ID and password
- Special user Ids
  - transparent anonymous FTP
- Timed based rules
  - M-F 8am-6pm
- permit rules
  - user|group
  - from and to

HTTP Proxy

- High performance HTTP proxy
  - eliminate 90% of systems overhead
  - pre-forking
  - dynamic workload adjustment
  - automatic error recovery
  - process retirement
  - automatic error prevention
- Web caching
  - 40 - 80% of data found in cache
  - Significant reducing reduction in response time
  - conserve link bandwidth
  - automatic garbage collection
  - automated storage management
  - concurrent I/O to multi-drive cache

HTTP Proxy - 2

- Access control
  - stealth listening
- URL Content Filtering
  - integrated into proxy
  - improve user productivity
  - enforce organization policies
  - reduce legal exposures
  - improves performance
  - < 10 microseconds per decision
  - periodic list updates
  - multiple categories
  - exemption list
- FTP controls

HTTP Proxy - 3

- High Scalability
  - SMP support
  - distributed parallel processing
    - clustered SMP
- Workload balancing
- Dynamic non-disruptive system upgrades
- Hierarchical cache distribution

Reverse HTTP

- Webgate
  - protect one or more Web Servers from direct attack
  - high performance
  - workload balancing
    - round robin scheduling
    - hide server outages
  - centralized log management

High Availability

- Fault tolerant design
  - everything made by man will fail
- Redundant firewalls
  - hot load sharing firewalls
  - A monitors B and B monitors A
- fwpulse
  - periodically examine siblings interfaces
  - if not responding enter PD mode
    - isolate error
    - avoid un-necessary takeovers

Reporting

- Report programs produce 57 possible reports
- HTTP access log
  - large sites can get 1,000,000 hits per day
  - 200 MB of log data per day
  - logs contain IP address but meaningful reports require hostnames and domain names
  - 1 million DNS lookups could take > 24 hours!
- Parallel DNS lookups
  - 1000 at once
  - cache lookups to avoid redundant lookups