




Firewalls



Introduction


- Focus here is on securing network
 - Begin with description of company and policy
 - Network organization
 - Firewalls
 - DMZ and servers
 - Internal network
- 



A Company and its Security Policy



The Drib

- Builds and sells dribbles
 - Developing network infrastructure allowing it to connect to Internet to provide mail, web presence for consumers, suppliers, other partners
- 



Specific Problems

- Internet presence required
 - E-commerce, suppliers, partners
 - Drib developers need access
 - External users cannot access development sites
- Hostile takeover by competitor in progress
 - Lawyers, corporate officers need access to development data
 - Developers cannot have access to some corporate data



Goals of Security Policy

- Data related to company plans to be kept secret
 - Corporate data such as what new products are being developed is known on a need-to-know basis only
- When customer supplies data to buy a dribble, only folks who fill the order can access that information
 - Company analysts may obtain statistics for planning
- Lawyers, company officials must approve release of any sensitive data



Policy Development

- Policy: minimize threat of data being leaked to unauthorized entities
- Environment: 3 internal organizations
 - Customer Service Group (CSG)
 - Maintains customer data
 - Interface between clients, other internal organizations
 - Development Group (DG)
 - Develops, modifies, maintains products
 - Relies on CSG for customer feedback
 - Corporate Group (CG)
 - Handles patents, lawsuits, etc.



Users, Data, and Information Flow



Nature of Information Flow

- Public
 - Specs of current products, marketing literature
- CG, DG share info for planning purposes
 - Problems, patent applications, budgets, etc.
- Private
 - CSG: customer info like credit card numbers
 - CG: corporate info protected by attorney privilege
 - DG: plans, prototypes for new products to determine if production is feasible before proposing them to CG



Data Classes

- Public data (PD): available to all
- Development data for existing products (DDEP): available to CG, DG only
- Development data for future products (DDFP): available to DG only
- Corporate data (CpD): available to CG only
- Customer data (CuD): available to CSG only



User Classes

- Outsiders (O): members of public
 - Access to public data
 - Can also order, download drivers, send email to company
- Developers (D): access to DDEP, DDFP
 - Cannot alter development data for existing products
- Corporate executives (C): access to CD
 - Can read DDEP, DDFP, CuD but not alter them
 - Sometimes can make sensitive data public
- Employees (E): access to CuD only

Access Control Matrix for Policy

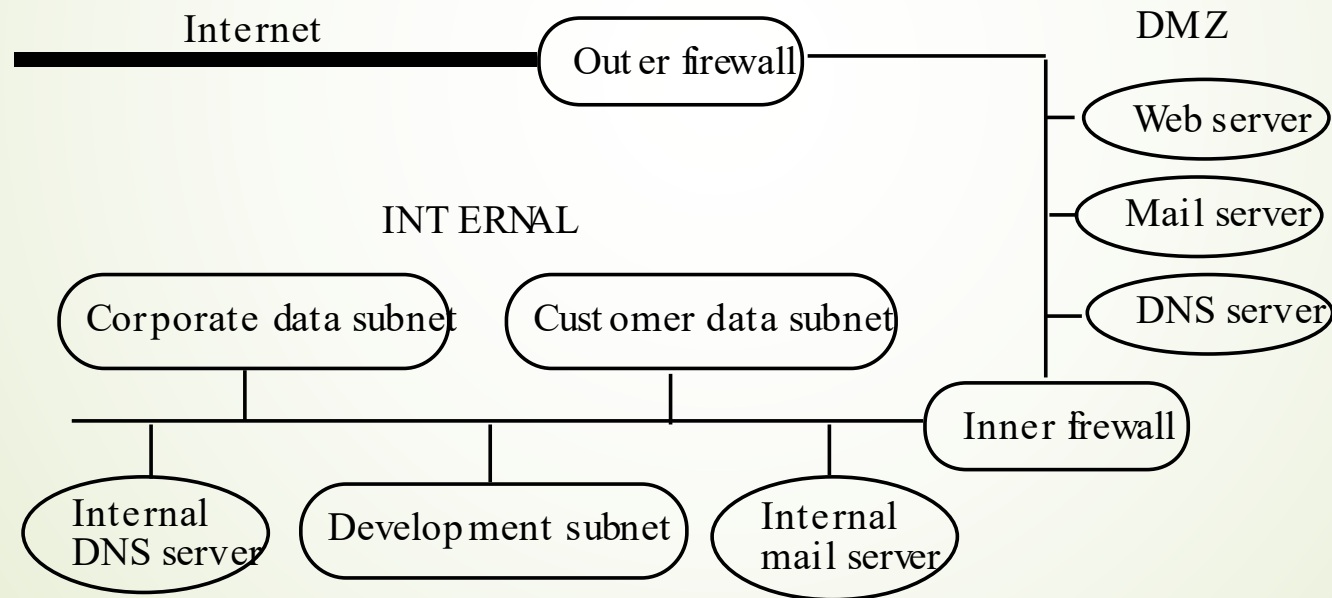
	O	D	C	E
PD	r	r	r	r
DDEP		r	r	
DDFP		r, w	r	
CpD		w	r, w	w
CuD	w		r	r, w



Network Organization

Network Organization

- Partition network into several subnets
- Guards between them prevent leaks





Components



DMZ

- Portion of network separating purely internal network from external network
 - Allows control of accesses to some trusted systems inside the corporate perimeter
 - If DMZ systems breached, internal systems still safe
 - Can perform different types of checks at boundary of internal,DMZ networks and DMZ,Internet network



Firewalls

- Host that mediates access to a network
 - Allows, disallows accesses based on configuration and type of access
- Example: block Back Orifice
 - BO allows external users to control systems
 - Requires commands to be sent to a particular port (say, 25345)
 - Firewall can block all traffic to or from that port
 - So even if BO installed, outsiders can't use it



Filtering Firewalls

- ▶ Access control based on attributes of packets and packet headers
 - ▶ Such as destination address, port numbers, options, etc.
 - ▶ Also called a *packet filtering firewall*
 - ▶ Does not control access based on content
 - ▶ Examples: routers, other infrastructure systems



Proxy

- Intermediate agent or server acting on behalf of endpoint without allowing a direct connection between the two endpoints
 - So each endpoint talks to proxy, thinking it is talking to other endpoint
 - Proxy decides whether to forward messages, and whether to alter them




Proxy Firewall

- Access control done with proxies
 - Usually bases access control on content as well as source, destination addresses, etc.
 - Also called an *applications level* or *application level firewall*
 - Example: virus checking in electronic mail
 - Incoming mail goes to proxy firewall
 - Proxy firewall receives mail, scans it
 - If no virus, mail forwarded to destination
 - If virus, mail rejected or disinfected before forwarding



Views of a Firewall

- ▶ Access control mechanism
 - ▶ Determines which traffic goes into, out of network
 - ▶ Audit mechanism
 - ▶ Analyzes packets that enter
 - ▶ Takes action based upon the analysis
 - ▶ Leads to traffic shaping, intrusion response, etc.
- 



Analysis and Implementation



Analysis of Drib Network

- Security policy: “public” entities on outside but may need to access corporate resources
 - Those resources provided in DMZ
- No internal system communicates directly with systems on Internet
 - Restricts flow of data to “public”
 - For data to flow out, must pass through DMZ



Implementation

- Conceal all internal addresses
 - Make them all on 10., 172., or 192.168. subnets
 - Inner firewall uses NAT to map addresses to firewall's address
 - Give each host a non-private IP address
 - Inner firewall never allows those addresses to leave internal network
- Easy as all services are proxied by outer firewall
 - Email is a bit tricky ...



Email

- Problem: DMZ mail server must know address in order to send mail to internal destination
 - Could simply be distinguished address that causes inner firewall to forward mail to internal mail server
- Internal mail server needs to know DMZ mail server address



DMZ Web Server

- In DMZ so external customers can access it without going onto internal network
 - If data needs to be sent to internal network (such as for an order), transmission is made separately and not as part of transaction



Application of Principles

- ▶ Least privilege
 - ▶ Containment of internal addresses
- ▶ Complete mediation
 - ▶ Inner firewall mediates every access to DMZ
- ▶ Separation of privilege
 - ▶ Going to Internet must pass through inner, outer firewalls and DMZ servers



Application of Principles

- ▶ Least common mechanism
 - ▶ Inner, outer firewalls distinct; DMZ servers separate from inner servers
 - ▶ DMZ DNS *violates* this principle
 - ▶ If it fails, multiple systems affected
 - ▶ Inner, outer firewall addresses fixed, so they do not depend on DMZ DNS



Outer and Inner Firewalls



Outer Firewall Configuration

- Goals: restrict public access to corporate network; restrict corporate access to Internet
- Required: public needs to send, receive email; access web services
 - So outer firewall allows SMTP, HTTP, HTTPS
 - Outer firewall uses its address for those of mail, web servers



Details

- Proxy firewall
- SMTP: mail assembled on firewall
 - Scanned for malicious logic; dropped if found
 - Otherwise forwarded to DMZ mail server
- HTTP, HTTPS: messages checked
 - Checked for suspicious components like very long lines; dropped if found
 - Otherwise, forwarded to DMZ web server
- Note: web, mail servers *different systems*
 - Neither same as firewall



Attack Analysis

- Three points of entry for attackers:
 - Web server ports: proxy checks for invalid, illegal HTTP, HTTPS requests, rejects them
 - Mail server port: proxy checks email for invalid, illegal SMTP requests, rejects them
 - Bypass low-level firewall checks by exploiting vulnerabilities in software, hardware
 - Firewall designed to be as simple as possible
 - Defense in depth



Defense in Depth

- Form of separation of privilege
- To attack system in DMZ by bypassing firewall checks, attacker must know internal addresses
 - Then can try to piggyback unauthorized messages onto authorized packets



Inner Firewall Configuration

- Goals: restrict access to corporate internal network
- Rule: block *all* traffic except for that *specifically* authorized to enter
 - Principle of fail-safe defaults
- Example: Drib uses NFS on some internal systems
 - Outer firewall disallows NFS packets crossing
 - Inner firewall disallows NFS packets crossing, too
 - DMZ does not need access to this information (least privilege)
 - If inner firewall fails, outer one will stop leaks, and vice versa (separation of privilege)



More Configuration

- Internal folks require email
 - SMTP proxy required
- Administrators for DMZ need login access
 - So, allow SSH through *provided*:
 - Destination is a DMZ server
 - Originates at specific internal host (administrative host)
 - Violates least privilege, but ameliorated by above
- DMZ DNS needs to know address of administrative host
 - More on this later



DMZ



DMZ

- Look at servers separately:
 - Web server: handles web requests with Internet
 - May have to send information to internal network
 - Email server: handles email with Internet
 - Must forward email to internal mail server
 - DNS
 - Used to provide addresses for systems DMZ servers talk to
 - Log server
 - DMZ systems log info here




Mail Server






DMZ Mail Server

- Performs address, content checking on *all* email
 - Goal is to hide internal information from outside, but be transparent to inside
 - Receives email from Internet, forwards it to internal network
 - Receives email from internal network, forwards it to Internet
- 



Mail from Internet

- Reassemble messages into header, letter, attachments as files
- Scan header, letter, attachments looking for “bad” content
 - “Bad” = known malicious logic
 - If none, scan original letter (including attachments and header) for violation of SMTP spec
- Scan recipient address lines
 - Address rewritten to direct mail to internal mail server
 - Forward letter there



Mail to Internet

- ▶ Like mail from Internet with 2 changes:
 - ▶ Step 2: also scan for sensitive data (like proprietary markings or content, etc.)
 - ▶ Step 3: changed to rewrite all header lines containing host names, email addresses, and IP addresses of internal network
 - ▶ All are replaced by “drib.org” or IP address of external firewall



Administrative Support



Administrative Support

- Runs SSH server
 - Configured to accept connections *only* from trusted administrative host in internal network
 - All public keys for that host fixed; no negotiation to obtain those keys allowed
 - Allows administrators to configure, maintain DMZ mail host remotely while minimizing exposure of host to compromise



Web Server





DMZ Web Server

- Accepts, services requests from Internet
- Never contacts servers, information sources in internal network
- Server itself contains no confidential data
- Server is www.drib.org and uses IP address of outer firewall when it must supply one



Updating DMZ Web Server

- Clone of web server kept on internal network
 - Called “WWW-clone”
- All updates done to WWW-clone
 - Periodically admin's copy contents of WWW-clone to DMZ web server
- DMZ web server runs SSH server
 - Used to do updates as well as maintenance, configuration
 - Secured like that of DMZ mail server



Internet Ordering

- Orders for Drib merchandise from Internet
 - Customer enters data, which is saved to file
 - After user confirms order, web server checks format, content of file and then uses public key of system on internal customer subnet to encipher it
 - This file is placed in a spool area not accessible to web server program
 - Original file deleted
 - Periodically, internal trusted administrative host uploads these files, and forwards them to internal customer subnet system



Analysis

- If attacker breaks into web server, cannot get order information
 - There is a slight window where the information of customers still on system can be obtained
- Attacker can get enciphered files, public key used to encipher them
 - Use of public key cryptography means it is computationally infeasible for attacker to determine private key from public key



DNS Server and Log Server



DMZ DNS Server

- Supplies DNS information for some hosts to DMZ:
 - DMZ mail, web, log hosts
 - Internal trusted administrative host
 - Inner firewall
 - Outer firewall
- Note: Internal server addresses not present
 - Inner firewall can get them, so DMZ hosts do not need them



DMZ Log Server

- DMZ systems all log information
 - Useful in case of problems, attempted compromise
- Problem: attacker will delete or alter them if successful
 - So log them off-line to this server
- Log server saves logs to file, also to write-once media
 - Latter just in case log server compromised
- Runs SSH server
 - Constrained in same way server on DMZ mail server is



Summary



Summary

- Each server knows only what is needed to do its task
 - Compromise will restrict flow of information but not reveal info on internal network
- Operating systems and software:
 - All unnecessary features, servers disabled
 - Better: create custom systems
- Proxies prevent direct connection to systems
 - For all services except SSH from internal network to DMZ, which is itself constrained by source, destination



Internal Network





Internal Network

- Goal: guard against unauthorized access to information
- Updating of DMZ web server, internal trusted administrative host
- Internal network organized into 3 subnets, each corresponding to Drib group
 - Firewalls control access to subnets



Internal Mail Server

- Can communicate with hosts on subnets
 - Subnet may allow mail to go directly to destination host
 - Internal DNS needs to know addresses of all destination hosts
- 



WWW-clone

- Provides staging area for web updates
- All internal firewalls allow access to this
 - WWW-clone controls who can put and get what files and where they can be put
- Used as testbed for changes in pages
 - Allows corporate review before anything goes public
 - If DMZ web server trashed or compromised, all web pages can be restored quickly



Trusted Administrative Host

- Access tightly controlled
 - Only system administrators authorized to administer DMZ systems have access
- All connections to DMZ through inner firewall must use this host
 - Exceptions: internal mail server, possibly DNS
- All connections use SSH
 - DMZ SSH servers accept connections from this host only



Analysis

- DMZ servers never communicate with internal servers
 - All communications done via inner firewall
- Only client to DMZ that can come from internal network is SSH client from trusted administrative host
 - Authenticity established by public key authentication
- Only data non-administrative folks can alter are web pages
 - Even there, they do not access DMZ



Analysis

- ▶ Only data from DMZ is customer orders and email
 - ▶ Customer orders already checked for potential errors, enciphered, and transferred in such a way that it cannot be executed
 - ▶ Email thoroughly checked before it is sent to internal mail server



Assumptions

- Software, hardware does what it is supposed to
 - If software compromised, or hardware does not work right, defensive mechanisms fail
 - Reason separation of privilege is *critical*
 - If component A fails, other components provide additional defenses
- Assurance is vital!



Key Points



Key Points

- Begin with policy
- Craft network architecture and security measures from it
- Assume failure will occur
 - Defend in depth
- Firewalls, filtering, and proxies
- DMZ and servers
- Internal network