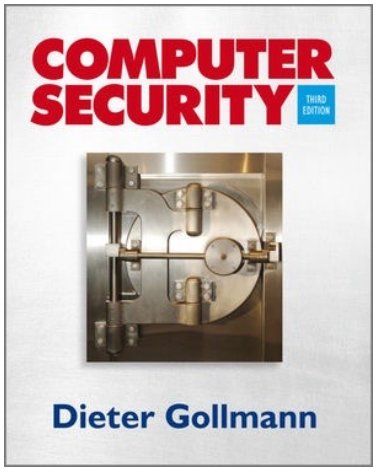
# Computer Security 3e

Dieter Gollmann






# Firewalls

# Introduction

- Cryptographic mechanisms protect data in transit (confidentiality, integrity).
- Authentication protocols verify the source of data.
- We may also control which traffic is allowed to enter our system (ingress filtering) or to leave our system (egress filtering).
- Access control decisions based on information like addresses, port numbers, ...



3

# Firewall

- Firewall: a network security device controlling traffic flow between two parts of a network.
- Often installed between an entire organisation's network and the Internet.
- Can also be installed in an intranet to protect individual departments.
- All traffic has to go through the firewall for protection to be effective.
  - Dial-in lines, wireless LANs, USB devices!?



4

# Purpose

- Firewalls control network traffic to and from the protected network.
- Can allow or block access to services (both internal and external).
- Can enforce authentication before allowing access to services.
- Can monitor traffic in/out of network.



5

# Types of Firewalls

- Packet filter
- Stateful packet filter
- Circuit-level proxy
- Application-level proxy



6

# Packet Filter

- Inspect headers of IP packets, also TCP and UDP port numbers.
- Rules specify which packets are allowed through the firewall, and which are dropped.
  - Actions: bypass, drop, protect (IPsec channel).
- Rules may specify source / destination IP addresses, and source / destination TCP / UDP port numbers.
- Rules for traffic in both directions.
- Certain common protocols are difficult to support securely (e.g. FTP).



7

# Example

- TCP/IP packet filtering router.
  - Router which can throw packets away.
- Examines TCP/IP headers of every packet going through the Firewall, in either direction.
- Packets can be allowed or blocked based on:
  - IP source & destination addresses
  - TCP / UDP source & destination ports
- Implementation on router for high throughput.



8

# Stateful Packet Filter

- Packet filter that understands requests and replies (e.g. for TCP: SYN, SYN-ACK, ACK).
- Rules need only specify packets in one direction (from client to server – the direction of the first packet in a connection).
- Replies and further packets in the connection are automatically processed.
- Supports wider range of protocols than simple packet filter (eg: FTP, IRC, H323).



9

# Stateful Packet Filter & FTP

- Client sends ftp-request to server
- Firewall stores connection state
  - FTP-Server Address
  - state of connection (SYN, ACK, ...)
- If correct FTP-server tries to establish data connection, packets are not blocked.



10

# Circuit-level proxy

- Similar to a packet filter, except that packets are not routed.
- Similar to gateway using IPsec in tunnel mode.
- Incoming TCP/IP packets accepted by proxy.
- Rules determine which connections will be allowed and which blocked.
- Allowed connections generate new connection from firewall to server.
- Similar specification of rules as packet filter.



11

# Application-level Proxy

- Layer-7 proxy server.
- “Client and server in one box”.
- For every supported application protocol.
- SMTP, POP3, HTTP, SSH, FTP, NNTP...
- Packets received and processed by server.
- New packets generated by client.



12

# Application-level Proxy

- Complete server & client implementation in one box for every protocol the firewall should handle.
- Client connects to firewall.
- Firewall validates request.
- Firewall connects to server.
- Response comes back through firewall and is also processed through client/server.
- Large amount of processing per connection.
- Can enforce application-specific policies.



13

# Firewall Policies

- Permissive: allow by default, block some.
  - Easy to make mistakes.
  - If you forget something you should block, it's allowed, and you might not realise for a while.
  - If somebody finds find a protocol is allowed, they might not tell you ....
- Restrictive: block by default, allow some.
  - Much more secure.
  - If you forget something, someone will complain and you can allow the protocol.



14

# Firewall Policies – Eexamples

- Permissive policies: Allow all traffic, but block ...
  - Irc
  - telnet
  - snmp
  - …
- Restrictive policies: block all traffic, but allow ...
  - http
  - Pop3
  - Smtp
  - ssh
  - …



15

# Rule Order

- A firewall policy is a collection of rules.
- Packets can contain several headers (→ IPsec).
- When setting a policy, you have to know in which order rules (and headers) are evaluated.
- Apply first matching entry in the list of rules.



16

# Typical Firewall Ruleset

- Allow from internal network to Internet:
  - HTTP, FTP, HTTPS, SSH, DNS
- Allow reply packets
- Allow from anywhere to Mail server:
  - TCP port 25 (SMTP) only
- Allow from Mail server to Internet:
  - SMTP, DNS
- Allow from inside to Mail server:
  - SMTP, POP3
- Block everything else



17

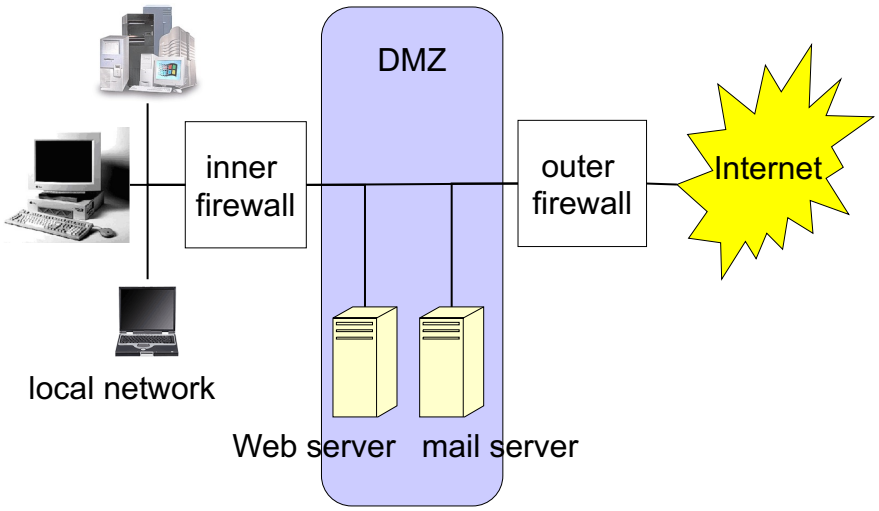
# Firewall Location

- Firewall can only filter traffic which goes through it.
- Where to put, for example, a mail server?
- Requires external access to receive mail from the Internet.
  - Should be on the inside of the firewall
- Requires internal access to receive mail from the internal network.
  - Should be on the outside of the firewall
- Solution: “perimeter network” (aka DMZ).



18

# DMZ






19

# Firewalls – Limitations

- Firewalls do not protect against insider threats.
- Blocking services may create inconveniences for users.
- Network diagnostics may be harder.
- Some protocols are hard to support.
- Protocol tunnelling: sending data for one protocol through another protocol circumvents the firewall.
  - As more and more administrators block almost all ports but have to leave port 80 open, more and more protocols are tunnelled through http to get through the firewall.
- Encrypted traffic cannot be examined and filtered.



20

# Intrusion Detection Systems



21

## Reminder: Security Strategies

- Prevention: take measures that prevent your assets from being damaged.
- Detection: take measures so that you can detect when, how, and by whom an asset has been damaged.
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets.



22

# Comment

- Cryptographic mechanisms and protocols make hard to prevent attacks.
- Perimeter security devices (e.g. firewalls) mainly prevent attacks by outsiders.
- Although it would be nice to prevent all attacks, in reality this is rarely possible.
- New types of attacks occur denial-of-service (where crypto may make the problem worse).
- We will now look at ways of detecting network attacks.



23

# Vulnerability Assessment

- Examines the “security state” of a network:
  - Open ports
  - Software packages running (which version, patched?)
  - Network topology
  - Returns prioritized lists of vulnerabilities
- Only as good as the knowledge base used.
  - Must be updated to handle new threats
- Vulnerability Assessment Methods.
  - Software solutions (ISS Scanner, Stat, Nessus etc.)
  - Audit Services (manual Penetration tests etc)
  - Web based solutions (Qualys, Security Point etc)



24

# Intrusion Detection Systems

- Passive supervision of network, analogue to intruder alarms.
  - Creates more work for personnel.
  - Provides security personnel with volumes of reports that can be presented to management …
- Two approaches to Intrusion Detection:
  - Knowledge-based IDS – Misuse detection
  - Behaviour-based IDS – Anomaly detection
- Network-based and host-based IDS.
- Given the (near) real-time nature of IDS alerts, an IDS can also be used as response tool.



25

# Knowledge-based IDS

- Knowledge-based IDS looks for patterns of network traffic or activity in log files that indicate suspicious behaviour, using information such as:
  - known vulnerabilities of particular OS and applications;
  - known attacks on systems;
  - given security policy.
- Example signatures might include:
  - number of recent failed login attempts on a sensitive host;
  - bit patterns in an IP packet indicating a buffer overrun attack;
  - certain types of TCP SYN packets indicating a SYN flood DoS attack.
- Also known as misuse detection IDS.



26

# Knowledge-based IDS

- Only as good as database of attack signatures:
  - New vulnerabilities not in the database are constantly being discovered and exploited;
  - Vendors need to keep up to date with latest attacks and issue database updates; customers need to install these;
  - Large number of vulnerabilities and different exploitation methods, so effective database difficult to build;
  - Large database makes IDS slow to use.
- All commercial IDS look for attack signatures.



27

# Behaviour-based IDS

- Wouldn't it be nice to be able to detect new attacks?
- Statistical anomaly detection uses statistical techniques to detect attacks.
- First establish base-line behaviour: what is "normal" for this system?
- Then gather new statistical data and measure deviation from base-line.
- If a threshold is exceeded, issue an alarm.
- Also known as behaviour-based detection.



28

# Behaviour-based IDS

- Example: monitor number of failed login attempts at a sensitive host over a period;
  - if a burst of failures occurs, an attack may be under way;
  - or maybe the admin just forgot his password?
- False positives (false alarm): attack flagged when none is taking place.
- False negatives: attack missed because it fell within the bounds of normal behaviour.
- This issue also applies to knowledge-based systems.



29

# Anomaly Detection

- IDS does not need to know about security vulnerabilities in a particular system:
  - base-line defines normality;
  - IDS does not need to know details of the construction of a buffer overflow packet.
- Anomalies are not necessarily attacks; normal and forbidden behaviour may overlap:
  - Legitimate users may deviate from baseline, causing false positives (e.g. user goes on holiday, works late in the office, forgets password, or starts to use new application).
  - If base-line is adjusted dynamically and automatically, a patient attacker may be able to gradually shift the base-line over time so that his attack does not generate an alarm.
  - There is no strong justification for calling anomaly detection "intrusion detection".



30

# IDS Architecture

- Distributed set of sensors – either located on hosts or on network – to gather data.
- Centralised console to manage sensor network, analyze data (→ data mining), report and react.
- Ideally:
  - Protected communications between sensors and console;
  - Protected storage for signature database/logs;
  - Secure console configuration;
  - Secured signature updates from vendor;
  - Otherwise, the IDS itself can be attacked and manipulated; IDS vulnerabilities have been exploited.



31

# HIDS & NIDS

- Host-based IDS (HIDS) looks for attack signatures in log files of hosts.
- Network-based IDS (NIDS) looks for attack signatures in network traffic.
- Trend towards host-based IDSs.
- Attacks a NIDS can detect but a HIDS cannot:
  - SYN flood, Land, Smurf,Teardrop, BackOrifice,…
- And vice-versa:
  - Trojan login script, walk up to unattended keyboard, encrypted traffic,…
- For more reliable detection, combine both IDS types.



32

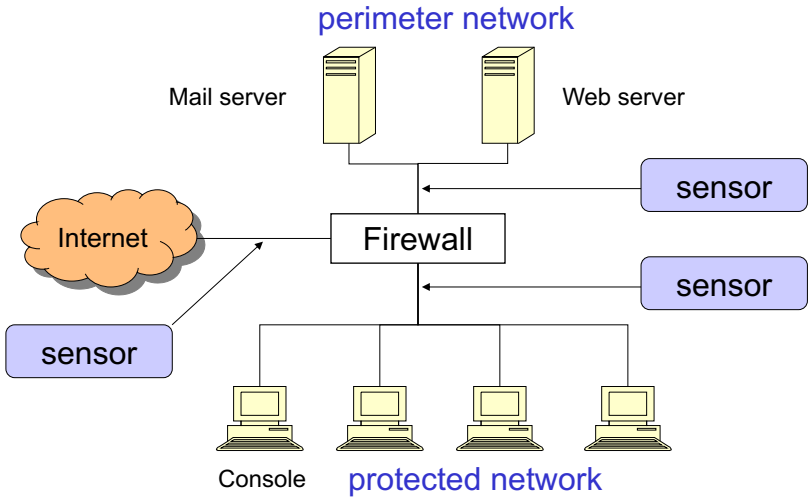
# Network-based IDS

- Uses network packets as data source.
- Typically, a network adapter running in promiscuous mode.
- Monitors and analyzes all traffic in real-time.
- Attack recognition module uses three common techniques to recognize attack signatures:
  - Pattern, expression or bytecode matching;
  - Frequency or threshold crossing (e.g. detect port scanning activity);
  - Correlation of lesser events (in reality, not much of this in commercial systems).



33

# Placement of NIDS






34

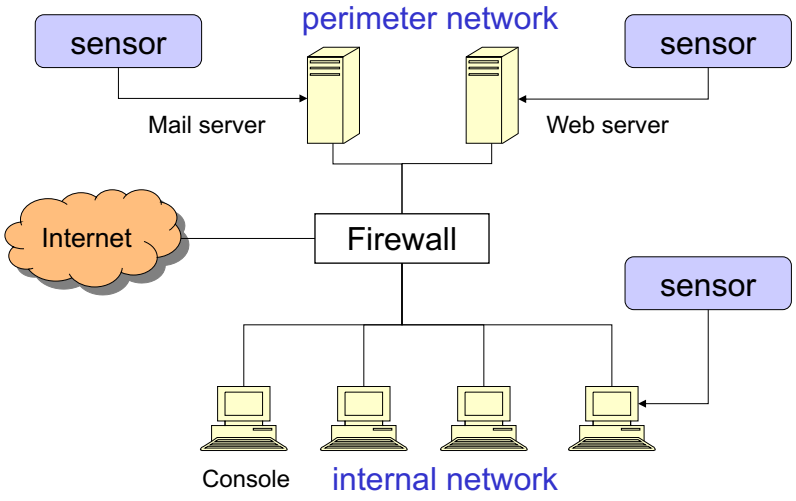
# Host-based IDS

- Typically monitors system, event, and security logs on Windows and syslog in Unix environments.
  - E.g., observe sequences of system calls to check whether a change from user to supervisor mode had been effected properly through a command like su.
- Verify checksums of key system files & executables at regular intervals for unexpected changes.
- Some products use regular expressions to refine attack signatures;
  - E.g., passwd program executed AND .rhosts file changed.
- Some products listen to port activity and alert when specific ports are accessed – limited NIDS capability.



35

# Placement of HIDS






36

# IDS Response Options

- Notify:
  - NIDS: alarm to console, email, SNMP trap, view active session
  - HIDS: alarm to console, email, SNMP trap
- Store:
  - NIDS: log summary, log network data
  - HIDS: log summary
- Action:
  - NIDS: kill connection (TCP reset), reconfigure firewall
  - HIDS: terminate user log in, disable user account, restore index.html



37

# Dangers of Automated Response

- Attacker tricks IDS to respond, but response aimed at innocent target (say, by spoofing source IP address).
  - Remember collateral spam?
- Users locked out of their accounts because of false positives.
- Repeated e-mail notification becomes a denial of service attack on sysadmin's e-mail account;
- Repeated restoration of index.html reduces website availability.



38

# IDS – Main Challenges

- Collecting and evaluating large amounts of data.
  - Combine events for more compact presentation.
- False positives, false negatives.
- Live intrusion detection systems generate lots of data.
  - E.g., DMZ with 60 hosts, monitored 7 days by NIDS with 244 signatures: 771,733 alerts created.
- Data mining applied for extracting useful information from such data collections.
- Context-aware systems filter out attacks that are irrelevant for the systems being monitored.
  - Ignore attacks on software or services you are not running.





# Honeypots

- How to detect zero-day exploits? There is no attack signature yet.
- How to "collect" new attacks for the knowledge base?
- Put systems online that mimic production systems but do not contain "real" data; anything observed on these systems is an attack.
- Honeypot: "… a resource whose value is being attacked or compromised"
  - Laurence Spitzner, "The value of honeypots", SecurityFocus, October 2001
- Honeypot: technology to track, learn and gather evidence of hacker activities.

# Honeypot Types

- Level of Involvement:
  - Low interaction: port listeners
  - Mid interaction: fake daemons
  - High interaction: real services
- Quality of information acquired increases with level of interaction.
- 'Intelligent' attackers will avoid obvious honeypots; tools for detecting honeypots exist.
- Risk that honeypot can be used as staging post in an attack increases with level of interaction.
- Pretending to be a honeypot has been proposed as a defence method.



41

# Honeynet

- Network of honeypots.
- Supplemented by firewalls and intrusion detection systems – Honeywall.
- Advantages:
  - "More realistic" environment
  - Improved possibilities to collect data



42

# Summary

- Apply prevention, detection and reaction in combination.
- IDS useful second line of defence (in addition to firewalls, cryptographic protocols, etc.).
- IDS deployment, customisation and management is generally not straightforward.
- Anomalies are not necessarily attacks.