Computer Security Foundations
Week 13: Network Security Threats and Countermeasures

Bernardo Portela

L.EIC - 24

Classes of Intruders - Cyber Criminals

- Individuals or members of an organized crime group, with the goal of financial reward
- Activities include, but not limited to
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming

- Information exchanged in underground forums to trade tips/data and coordinate attacks
- Anonymous networks (Tor et. al.) are very good for this

Classes of Intruders - State-Sponsored Organizations

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- A.k.a Advanced Persistent Threats
- Covert nature
- Persistence over extended periods

- Widespread nature and scope by a wide range of countries (China, Russia, USA, UK, and intelligence allies)

Classes of Intruders - Activists

- Individuals motivated by social or political causes
  - Working as insiders
  - Members of a larger group
- Also known as hacktivists
- Skill level often not high
- Goal is to promote and publicize their cause, typically through:
  - Website defacement
  - Denial-of-service attacks
  - Theft and distribution of data, resulting in negative publicity or compromise of their targets

Classes of Intruders - Others

- Hackers with motivations other than previously listed

- Include classic hackers/crackers
- Motivated by technical challenge or peer-group esteem and reputation
- Many responsible for discover new vulnerabilities

- Given the wide availability of toolkits, there is a pool of "hobby hackers" exploring system/network security challenges
  - **That's you guys!**

Intruder Skill Levels

- **Apprentice**
- **Journeyman**
- **Master**

Intruder Skill Levels

- **Apprentice**
  - Hackers with minimal technical skill, who primarily use existing attack toolkits
  - They likely comprise the largest number of attackers, including many criminal/activist attackers
  - Given their use of existing known tools, these attackers are the easiest to defend against
  - Also known as "script-kiddies" from plug-and-play usage
- **Journeyman**
- **Master**

Intruder Skill Levels

- **Apprentice**
- **Journeyman**
  - Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
  - They may be able to locate new vulnerabilities to exploit that are similar to some already known
  - Adapt tools for use by others
  - These hackers are found in all intruder classes
- **Master**

Intruder Skill Levels

- **Apprentice**
- **Journeyman**
- **Master**
  - Attackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
  - Write new powerful attack toolkits
  - Some of the better known classical hackers are at this level
  - Some are employed by state-sponsored organizations
  - Defending against these attacks is of the highest difficulty

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing a pirated software
- Using an unsecured AP to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Denial-of-Service

- A form of attack on the availability of services
- Is often done in a distributed fashion (DDoS)
- *Resource categories* that can be attacked:

- Network bandwidth
- System resources
- Application resources

Denial-of-Service

- A form of attack on availability of services
- Is often done in a distributed fashion (DDoS)
- *Resource categories* that can be attacked:

- Network bandwidth
  - Relates to the capacity of the network links connecting a server to the Internet
  - For most organizations, this is their connection to their ISP
- System resources
- Application resources

Denial-of-Service

- A form of attack on availability of services
- Is often done in a distributed fashion (DDoS)
- *Resource categories* that can be attacked:

- Network bandwidth
- System resources
  - Aims to overload or crash the network handling software
  - Consume resources in the system (e.g. buffers for arriving packets, tables of open connections)
- Application resources

Denial-of-Service

- A form of attack on availability of services
- Is often done in a distributed fashion (DDoS)
- *Resource categories* that can be attacked:

- Network bandwidth
- System resources
- Application resources
  - Propose several requests to a server within the target system
  - Each request consumes significant resources, limiting the server response ability

DoS Attacks - Flooding ping

The goal of the attack is to **overwhelm** the capacity of the network connection to the victim organization

- E.g. Internet Control Message Protocol echo request packets

DoS Attacks - Flooding ping

The goal of the attack is to **overwhelm** the capacity of the network connection to the victim organization

- E.g. Internet Control Message Protocol echo request packets

- Traffic can be handled by higher capacity links on the path, but packets are **discarded** as capacity increases
- Network performance is noticeably affected
- Source of the attack is clearly identified
  - ... unless a spoofed address is used
  - Zombie servers are very useful!

Botnets

A network of computers infected with malicious software (a.k.a. malware) that allows them to be controlled by an attacker (zombies)

- Botnets are used to commit a variety of cybercrimes
  - Spam; Scams; Hacks; DDoS

Botnets

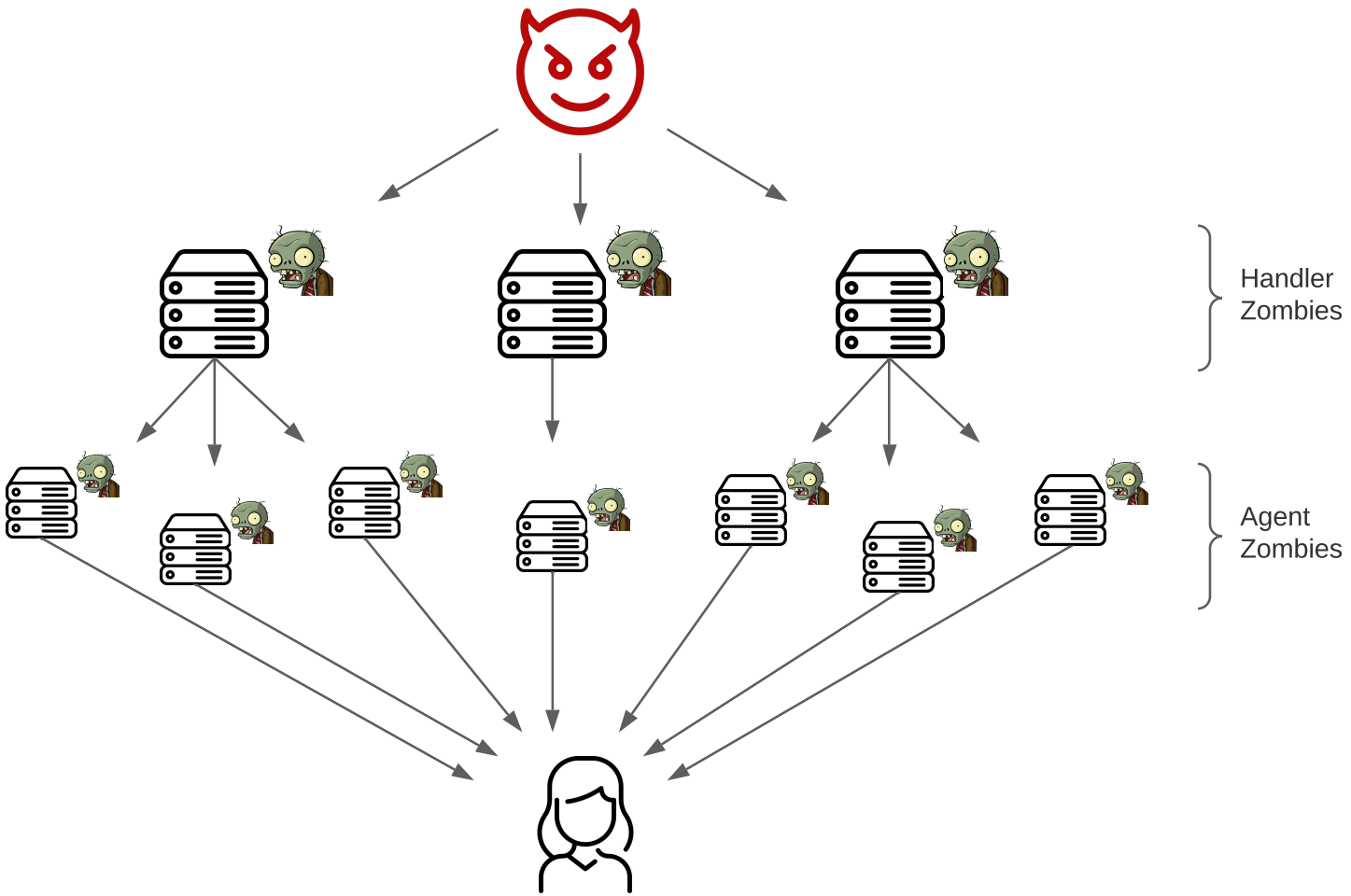
A network of computers infected with malicious software (a.k.a. malware) that allows them to be controlled by an attacker (zombies)

- Botnets are used to commit a variety of cybercrimes
  - Spam; Scams; Hacks; DDoS

Attack-as-a-Service

- Command and Control servers (C&C) are responsible for commanding infected computers
- Allows the attacker (bot-herder) to put the botnet to use
- Services of botnets can be provided to paying customers
  - The larger the botnet, the more powerful the cybercrime
  - More computational power; more messages can be sent in parallel

DDoS Control Hierarchy



Not rocket science

UPD Flood Attack

- Hacker sends UDP packets to a random port
- Generates illegitimate UDP packets
- Causes system to tie up resources sending back packets

Not rocket science

UPD Flood Attack

- Hacker sends UDP packets to a random port
- Generates illegitimate UDP packets
- Causes system to tie up resources sending back packets

Common tool for the job: diagnostic echo service (measure RTTs)

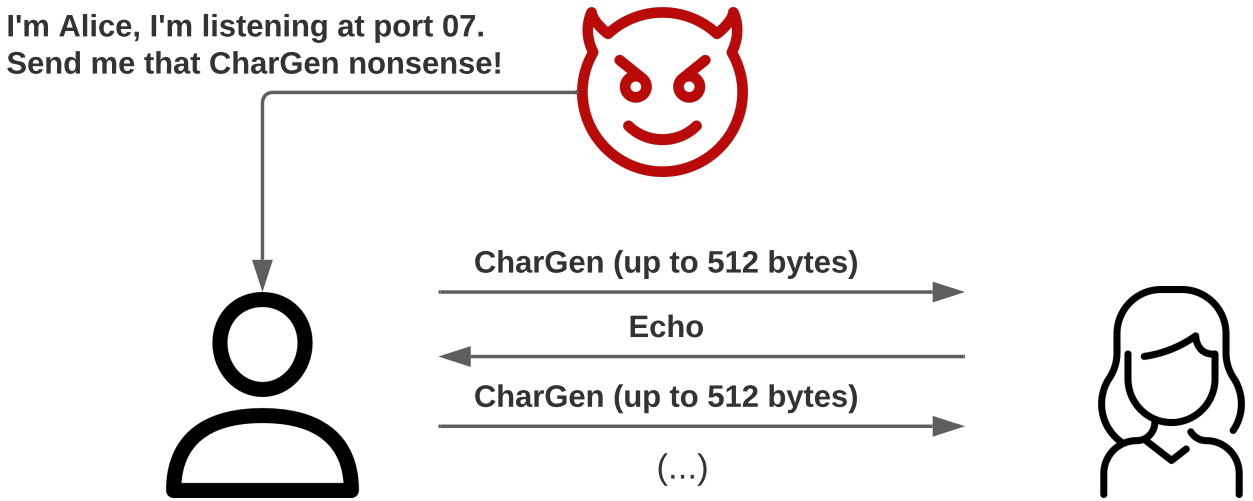
- Respond with UDP packet back to the source
- If service is not running, packet is discarded. ICMP destination unreachable packet returned to the sender
- Achieved its goal of occupying capacity on the link to the server!

Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a *spoofed* source address on the actual victim
- Intermediary responds to the victim
- "Reflects" the attack off the intermediary (reflector)

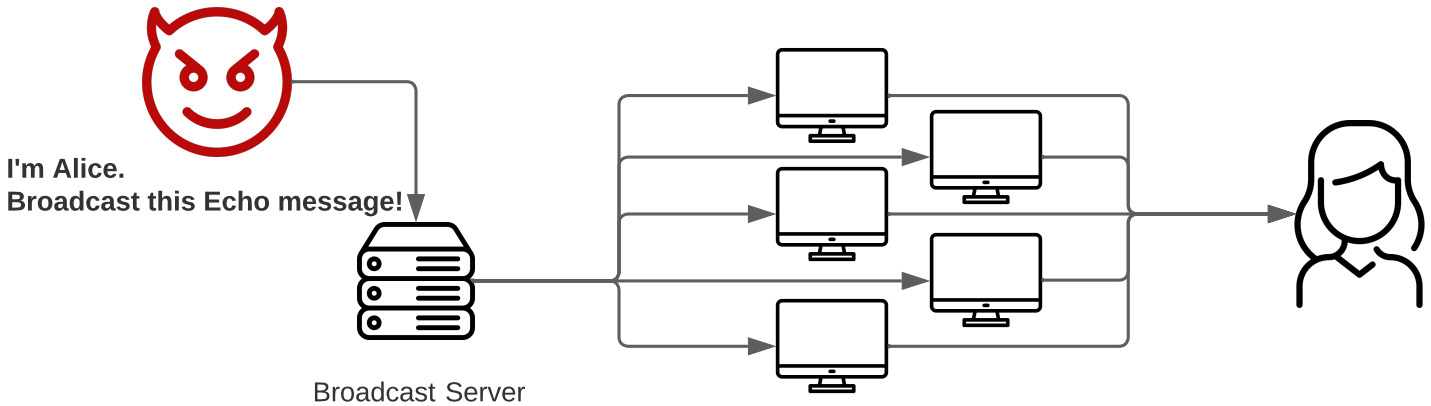
Goal: To generate enough volumes of packets to flood the link to the target system without alerting the intermediary

Echo-Chargen



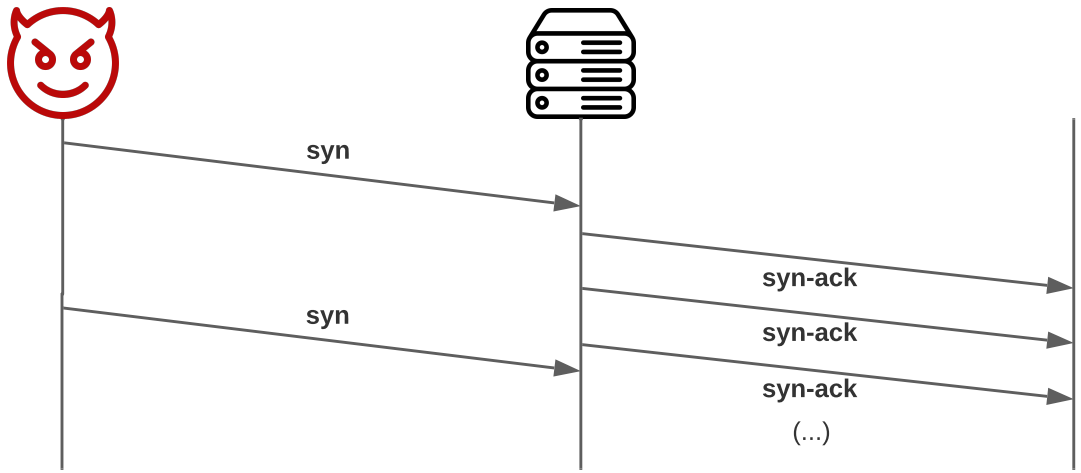
- *Requirement:* Source address spoofing (easy)
- Echo service (port 07) sends back whatever it receives
- CharGen is a character generation service
  - Used for debugging (of course...)
- Huge amounts of data form an endless loop!

Smurf Attack



- *Requirement:* Source address spoofing (easy)
- *Requirement:* Access to a server within the network
- Server broadcasts echo “from Alice” to the whole network
- Alice is blasted by echo messages from a bunch of machines

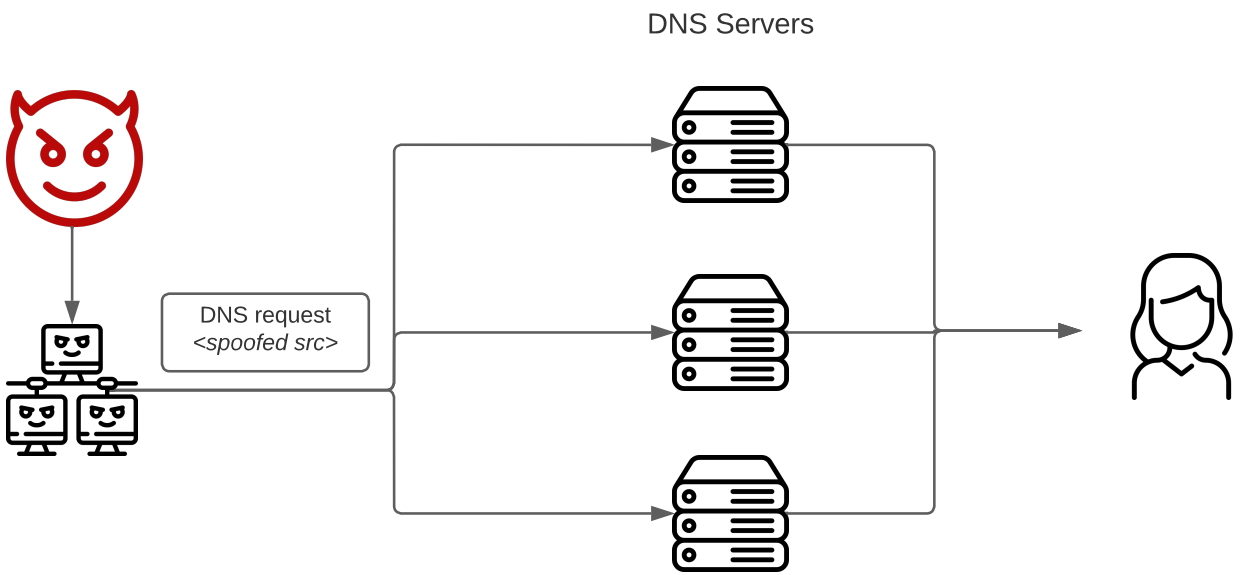
SYN Spoofing attack



- Attacker sends SYN with spoofed source
  - Source does not exist, will not reply
- Server replies with SYN-ACK
  - and after time out, sends another, and another...
- Eventually, connection request is assumed to fail
- Until that happens, these occupy table space
- Rinse and repeat

DNS Amplification Attack

- DNS requests with spoofed src IP address as the target
- Exploit DNS to convert small request to much larger response
  - Argument "ANY" produces large responses
  - 60 byte request can lead to a 512-4000 byte response
- Requests to multiple connected servers, flooding the target



Countermeasures

- DoS attacks cannot be prevented entirely
- High traffic volumes may be legitimate

1. Attack prevention and preemption
2. Attack detection and filtering
3. Attack source traceback and identification
4. Attack reaction

Countermeasures

- DoS attacks cannot be prevented entirely
- High traffic volumes may be legitimate

1. Attack prevention and preemption
   - Before the attack occurs
   - Enforce policies for resource consumption
   - Provide backup resources available on demand
2. Attack detection and filtering
3. Attack source traceback and identification
4. Attack reaction

Countermeasures

- DoS attacks cannot be prevented entirely
- High traffic volumes may be legitimate

1. Attack prevention and preemption
2. Attack detection and filtering
   - During the attack
   - Look for suspicious patterns of behavior
   - Filter packets likely to be part of the attack
3. Attack source traceback and identification
4. Attack reaction

Countermeasures

- DoS attacks cannot be prevented entirely
- High traffic volumes may be legitimate

1. Attack prevention and preemption
2. Attack detection and filtering
3. Attack source traceback and identification
   - During/after the attack
   - Identify sources of attack
   - Prepare whitelists/blacklists
4. Attack reaction

Countermeasures

- DoS attacks cannot be prevented entirely
- High traffic volumes may be legitimate

1. Attack prevention and preemption
2. Attack detection and filtering
3. Attack source traceback and identification
4. Attack reaction
   - After the attack
   - Eliminate effects of the attack
   - I.e. cleanup the system

Key Takeaways

- DoS - Denial of Service
  - Goal is to deny resources
  - Getting servers offline; or imposing delays

Key Takeaways

- DoS - Denial of Service
  - Goal is to deny resources
  - Getting servers offline; or imposing delays
- Multiple flavours of attacks
  - Flooding ping
  - Echo-Chargen
  - Smurf Attack
  - SYN Spoofing
  - DNS amplification

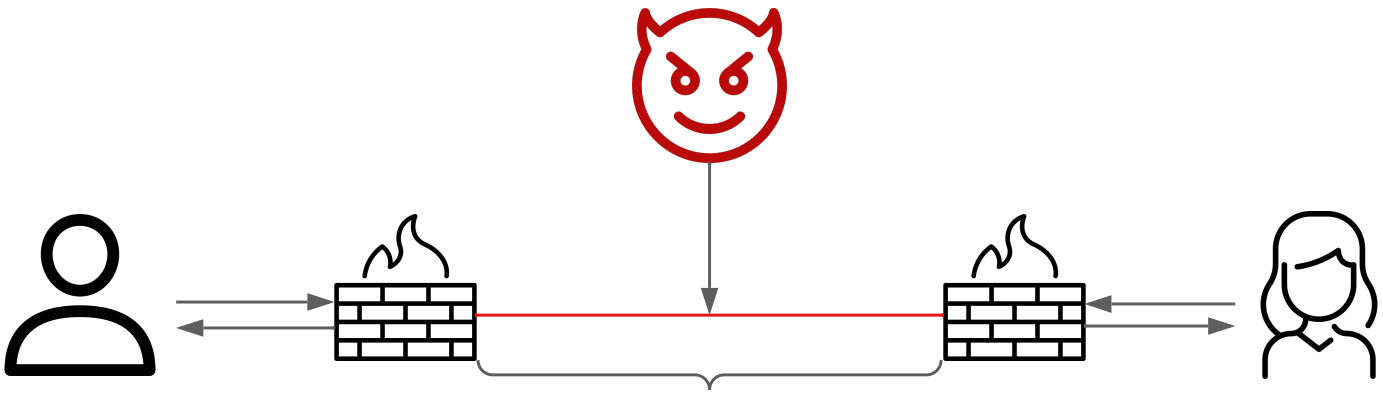
Key Takeaways

- DoS - Denial of Service
  - Goal is to deny resources
  - Getting servers offline; or imposing delays
- Multiple flavours of attacks
  - Flooding ping
  - Echo-Chargen
  - Smurf Attack
  - SYN Spoofing
  - DNS amplification
- Methodologies to bolster attack effectiveness
  - Botnets
  - Reflection attacks

Key Takeaways

- DoS - Denial of Service
  - Goal is to deny resources
  - Getting servers offline; or imposing delays
- Multiple flavours of attacks
  - Flooding ping
  - Echo-Chargen
  - Smurf Attack
  - SYN Spoofing
  - DNS amplification
- Methodologies to bolster attack effectiveness
  - Botnets
  - Reflection attacks
- Countermeasures entail a multitude of good practices:
  - Good access policies
  - Active monitoring for attacks
  - Mechanisms for traceback and identification
  - Blocking attacks and recovering systems

Firewalls



- Firewall decides what goes in and out of an internal network
- Access control for the network
- At a multitude of granularity levels

Managing what comes and and goes out

A firewall is like a **secretary**

- To meet with an executive:
  1. Contact the secretary
  2. Secretary will assess if the meeting is important
  3. Many requests are filtered according to relevance metrics
- If you want to meet the chair of CS department...
  - Secretary will do some filtering
- If you want to meet the President
  - Secretary will do a lot of filtering

Managing what comes and and goes out

A firewall is like a **secretary**

- To meet with an executive:
  1. Contact the secretary
  2. Secretary will assess if the meeting is important
  3. Many requests are filtered according to relevance metrics
- If you want to meet the chair of CS department...
  - Secretary will do some filtering
- If you want to meet the President
  - Secretary will do a lot of filtering

Criteria under which "meetings can be scheduled"

- Filtering done according to an access policy
- Types of traffic
- Address ranges and protocols
- Applications and content types

Capabilities and Limits

Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several internet functions that are not security related (e.g. NAT)
- Can serve the platform for IPSec (tunnel mode)

Capabilities and Limits

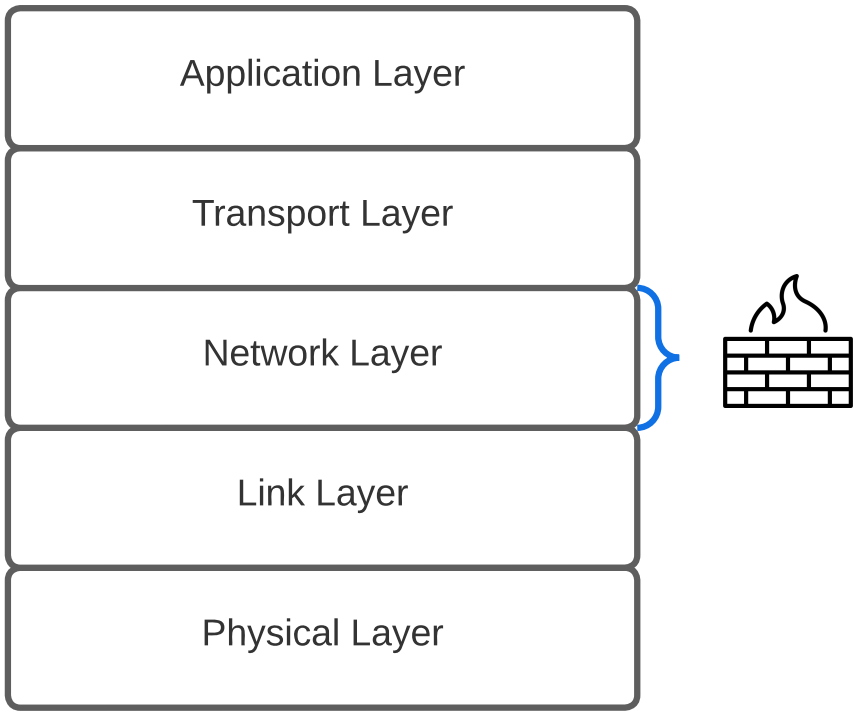
Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several internet functions that are not security related (e.g. NAT)
- Can serve the platform for IPSec (tunnel mode)

Limitations

- Cannot protect against attacks bypassing the firewall
- May not protect fully against internal threats
- Laptop, PDA, or portable storage device may be infected outside corporate network, and then used internally
- Improperly secured wireless LAN can be accessed outside the organization

Packet Filter- High-level view



- Operates at the network layer
- Observes IP packets and assesses their importance
- Why can this be incompatible with IPSec?

Packet Filter - Configuration

Configured via Access Control Lists (ACLs)

Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	>1023	HTTP	ACK
Deny	All	All	All	All	All	All

- Traffic is restricted to web browsing:
- Accept all outgoing HTTP traffic to port 80
- Accept all incoming HTTP ACK replies
- Reject everything else

Packet Filter - Strengths x Weaknesses

Advantages

- Speed
- Simplicity
- Transparent to users

Packet Filter - Strengths x Weaknesses

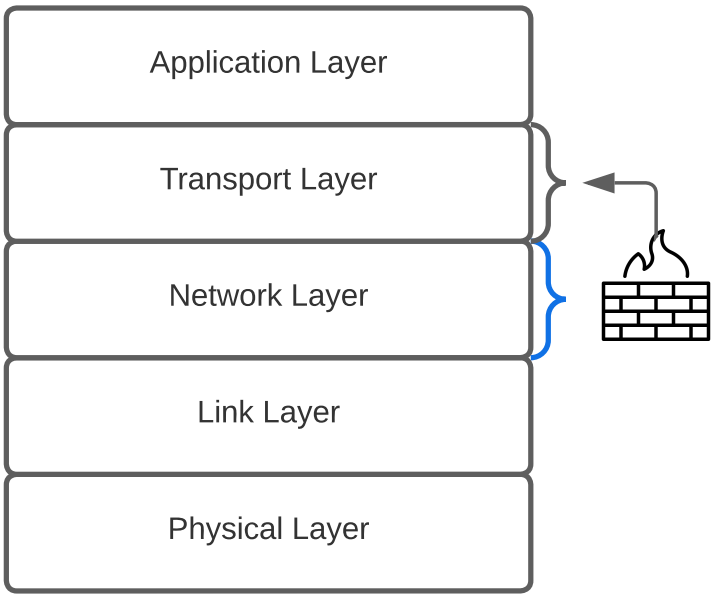
Advantages

- Speed
- Simplicity
- Transparent to users

Disadvantages

- No concept of state
- Vulnerable to attacks on TCP/IP bugs
- Cannot see TCP connections
- Unknowing of application data and context

Stateful Packet Filter



- Adds state to the packet filter
- Operates at the transport layer
- Remembers TCP connections (e.g. flag bits)
- Can even remember UDP packets (e.g. DNS requests)

Stateful Packet Filter

Advantages

- Can do everything a packet filter can
- Keeps track on ongoing connections
- Relies on protocol logic to detect misbehaviors

Stateful Packet Filter

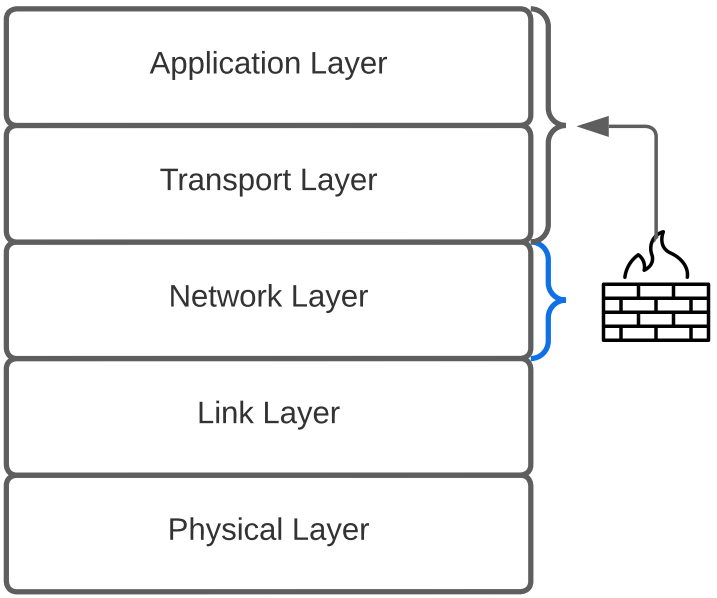
Advantages

- Can do everything a packet filter can
- Keeps track on ongoing connections
- Relies on protocol logic to detect misbehaviors

Disadvantages

- Cannot see application data
  - Lacks internal application logic
  - Cannot accurately detect deviations from expected behavior
- Slower than packet filtering

Application Proxy



- A proxy is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before allowing passage

Application Proxy

a.k.a. Application-Level Gateway

Additional security layer

- For every supported application protocol
  - SMTP, POP3, HTTP, SSH, ...
  - Create a new packet before sending to the lower layers
  - Validation done at the data granularity
  - Spoofing packet implies convincing proxy to accept

Application Proxy

a.k.a. Application-Level Gateway

Additional security layer

- For every supported application protocol
  - SMTP, POP3, HTTP, SSH, ...
  - Create a new packet before sending to the lower layers
  - Validation done at the data granularity
  - Spoofing packet implies convincing proxy to accept
- Large amount of processing per connection
- Can enforce application-specific policies
- Highly configurable

Application Proxy

Advantages

- Complete view of connections and application data
  - Can capture nuanced behavior
  - E.g. disable specific features, or specify execution criteria
- Filter bad data at application layer
  - Prevents software-level errors and vulnerability exploitation
  - E.g. macros allowing for SQL injection or buffer overflow

Application Proxy

Advantages

- Complete view of connections and application data
  - Can capture nuanced behavior
  - E.g. disable specific features, or specify execution criteria
- Filter bad data at application layer
  - Prevents software-level errors and vulnerability exploitation
  - E.g. macros allowing for SQL injection or buffer overflow

Disadvantages

- Performance takes a toll – yet another security layer
- Each application must have the associated proxy code

Firewall Policies

Permissive

Allow by default; block some

- Easy to make mistakes
- Mistakes can lead to security breaches
- Exploits can be covert, i.e. not obvious that they are occurring

Restrictive

Block by default; allow some

- Much more secure
- Mistakes can lead to availability problems
- Exploits depend on the security requirements and specifications

Firewall Policies

Permissive

Allow by default; block some

- Easy to make mistakes
- Mistakes can lead to security breaches
- Exploits can be covert, i.e. not obvious that they are occurring

Examples:

- IRC (messaging)
- Telnet
- SNMP (routing)
- Echo

Restrictive

Block by default; allow some

- Much more secure
- Mistakes can lead to availability problems
- Exploits depend on the security requirements and specifications

Examples:

- HTTP
- POP3
- SMTP (mail)
- SSH

A 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

Key Takeaways

- Firewalls monitor all traffic in a network
  - They can allow by default, and block some: permissive
  - They can block by default, and allow some: restrictive

Key Takeaways

- Firewalls monitor all traffic in a network
  - They can allow by default, and block some: permissive
  - They can block by default, and allow some: restrictive
- Multiple types of firewalls
- Packet filter
  - Stateless; lightweight
  - Coarse-grained control of traffic
- Stateful packet filter
  - Slightly more demanding
  - Can use protocol logic to understand if a certain set of interactions makes sense, or if it reflect malicious intent
- Application proxy
  - Quite more intrusive
  - Can use application logic to reason over payload contents

Intrusion Detection System

Requirements for an IDS:

- Availability
  - Run continuously
  - Provide graceful degradation of service

Intrusion Detection System

Requirements for an IDS:

- Availability
  - Run continuously
  - Provide graceful degradation of service
- Security
  - Be fault tolerant
  - Resist subversion

Intrusion Detection System

Requirements for an IDS:

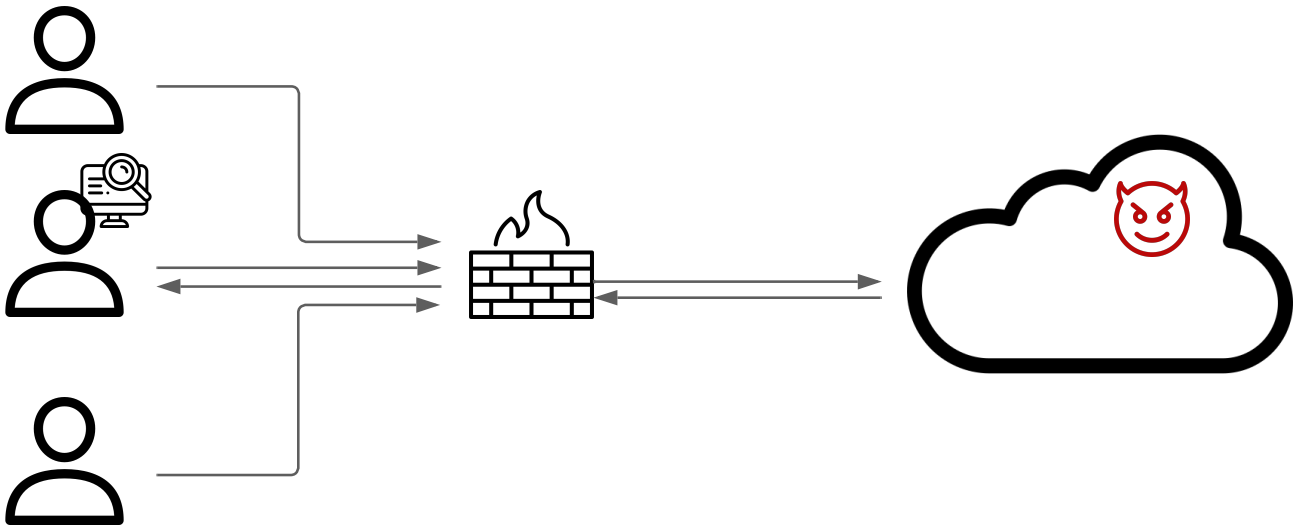
- Availability
  - Run continuously
  - Provide graceful degradation of service
- Security
  - Be fault tolerant
  - Resist subversion
- Performance
  - Impose a minimal overhead on a system
  - Scale to monitor large number of systems

Intrusion Detection System

Requirements for an IDS:

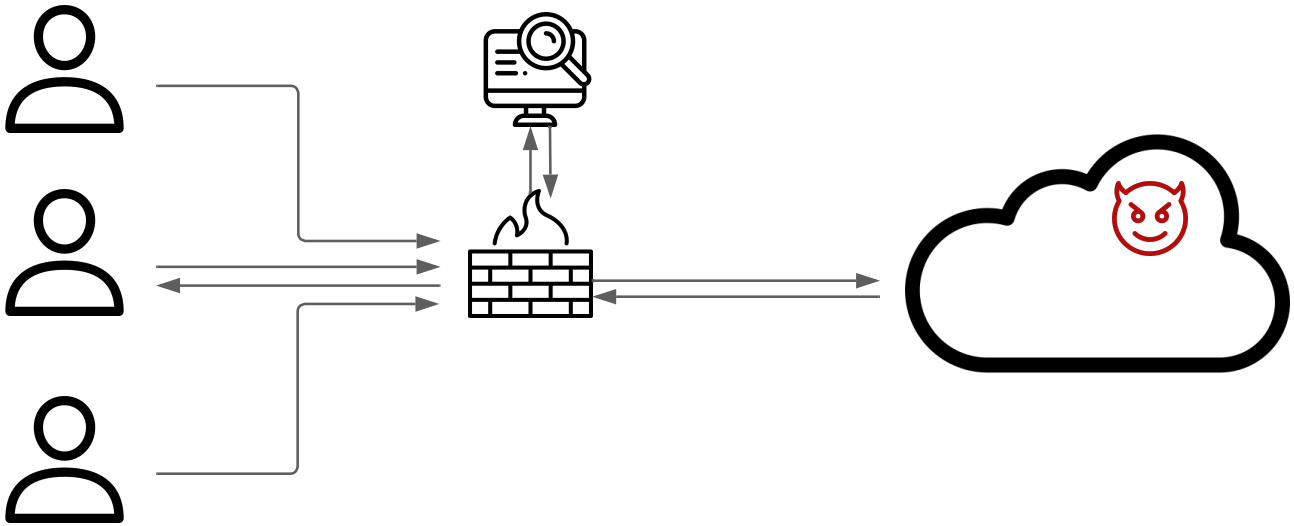
- Availability
  - Run continuously
  - Provide graceful degradation of service
- Security
  - Be fault tolerant
  - Resist subversion
- Performance
  - Impose a minimal overhead on a system
  - Scale to monitor large number of systems
- Adaptability
  - Configured according to system security policies
  - Adapt to changes in systems/users/attack patterns
  - Allow dynamic reconfiguration

Host-Based IDS



- Monitor activities on hosts for
  - Known attacks; Suspicious behavior
- Designed to detect attacks such as
  - Buffer overflow; Escalation of privilege
- Can detect both external and internal intrusions
- Little or no view of network activities

Network-Based IDS



- Monitor activity at selected points of the network for known attacks
- Examines network transport and application level protocols
- Designed to detect attacks such as:
  - Denial-of-service; network probes; malformed packets
- Some overlap with firewall
- Little to no view of host-based attacks

IDS Methodologies

Signature Detection

- Set of known malicious data patterns or attack rules
- Also known as misuse detection
- Only identifies known attacks for which it has patterns or rules

IDS Methodologies

Signature Detection

- Set of known malicious data patterns or attack rules
- Also known as misuse detection
- Only identifies known attacks for which it has patterns or rules

Anomaly Detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Observed behavior is analysed to determine whether it matches a legitimate user or an intruder
- Pattern recognition and machine learning approaches

Signature Detection

Example

- Failed login attempts may suggest a password cracking attack
- IDS sets rule *N failed login attempts in M seconds* as an attack signature. Listens for messages and looks for signatures
- A pattern identified as a signature triggers a warning
- A lot of specificity involved:
  - Administrator knows what attack triggered the system
  - Allows for timely responses...
  - ... Or a verification for false alarms

Signature Detection

Minutia

- Suppose IDS warns whenever N or more failed logins occur in M seconds
  - Define N and M to reduce false alarms
  - Do this based on "normal" behavior
  - But normal behavior can be neither easy to define
  - Nor static on the system lifecycle

Signature Detection

Minutia

- Suppose IDS warns whenever N or more failed logins occur in M seconds
  - Define N and M to reduce false alarms
  - Do this based on "normal" behavior
  - But normal behavior can be neither easy to define
  - Nor static on the system lifecycle

Adversary - An arms race

- An oblivious adversary can get caught
- But, knowing the signature, he can try $N - 1$ logins every M seconds
- Signature detection slows adversary, but doesn't stop it

Signature Detection

Advantages

- Simple
- Detects common, known threats
- Accurate identification of attacks upon detection
- Efficient (if we have a reasonable number of signatures)

Signature Detection

Advantages

- Simple
- Detects common, known threats
- Accurate identification of attacks upon detection
- Efficient (if we have a reasonable number of signatures)

Disadvantages

- Signature files must be kept up to date
- Number of signatures may become very large
- Can only detect known attacks
- Unexpected variations on known attacks may avoid detection

Detection of "Anomalies"

How can we measure the normal behavior of a system?

- Must measure during representative behavior
- Cannot be measured during an attack
- Normal is the statistical mean
- Must also allow for variance to know what is abnormal

Detection of "Anomalies"

How can we measure the normal behavior of a system?

- Must measure during representative behavior
- Cannot be measured during an attack
- Normal is the statistical mean
- Must also allow for variance to know what is abnormal

- On top of fancy modelling techniques:
  - Bayesian statistics
  - Linear discriminant analysis
  - Quadratic discriminant analysis

Anomaly Detection Issues

Constant evolution

- A static intrusion system places a huge burden on the admin
- But evolving IDS makes it possible to the attacker to manipulate the behavior and slowly convince IDS of an abnormal pattern
- Slow and steady can win the race

Anomaly Detection Issues

Constant evolution

- A static intrusion system places a huge burden on the admin
- But evolving IDS makes it possible to the attacker to manipulate the behavior and slowly convince IDS of an abnormal pattern
- Slow and steady can win the race

Types of IDS feedback

- Example: monitor failed login attempts
  - Burst of failures can occur - an attack?
  - ... or an admin that forgot his password?
- False positives (FP) - attack flagged when none is occurring
- False negatives (FN) - attack flagged as adequate behavior

Base-Rate Fallacy

- *Base-rate fallacy* probability of some conditional event is assessed without considering the "base rate" of that event

- Suppose an IDS is 99% accurate, 1% of FP/FN
- IDS generates 1,000,100 log entries
- Only 100 correspond to actual malicious events
- Because of the success rate, of the 100 malicious events, 99 will be detected as malicious = 1 **FN**
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious = 10,000 FP
- Out of all 10,099 expected alarms, 10,000 are false alarms, **roughly** 99% **of all flagged attacks**

Key Takeaways

- Intrusion detection systems complement firewalls
- Firewalls are the first line of defense
- IDSs monitor and detect more complex attacks

Key Takeaways

- Intrusion detection systems complement firewalls
- Firewalls are the first line of defense
- IDSs monitor and detect more complex attacks
- Host-based IDS:
  - Monitors the host for potential attacks
  - No context of network activity
- Network-based IDS:
  - Monitors network activity
  - No context of application logic

Key Takeaways

- Intrusion detection systems complement firewalls
- Firewalls are the first line of defense
- IDSs monitor and detect more complex attacks
- Host-based IDS:
  - Monitors the host for potential attacks
  - No context of network activity
- Network-based IDS:
  - Monitors network activity
  - No context of application logic
- Signature-based detection
  - Detects behavior given certain well-established patterns
  - Can evolve over time; requires expert design
- Anomaly-based detection
  - Develops a model for what constitutes "expected behavior"
  - Ideally automatic; can be very challenging to validate

Key Takeaways

- Intrusion detection systems complement firewalls
- Firewalls are the first line of defense
- IDSs monitor and detect more complex attacks
- Host-based IDS:
  - Monitors the host for potential attacks
  - No context of network activity
- Network-based IDS:
  - Monitors network activity
  - No context of application logic
- Signature-based detection
  - Detects behavior given certain well-established patterns
  - Can evolve over time; requires expert design
- Anomaly-based detection
  - Develops a model for what constitutes "expected behavior"
  - Ideally automatic; can be very challenging to validate
- IDSs require very low false positive rates – base rate fallacy

Computer Security Foundations
Week 13: Network Security Threats and Countermeasures

Bernardo Portela

L.EIC - 24