Network Security - Week 5

João Soares

DCC/FCUP

2023

Disruptive systems

Previously...

- Authentication schemes to withstand attacks
  - Authentication protocols
  - TLS/IPSec
- Encryption and MACs to protect data
  - Key exchange
  - Secure communication via TLS/SSH

Disruptive systems

Previously...

- Authentication schemes to withstand attacks
  - Authentication protocols
  - TLS/IPSec
- Encryption and MACs to protect data
  - Key exchange
  - Secure communication via TLS/SSH

Denial-of-Service (DoS)

NIST security incident handling guide defines DoS as:

"An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as CPU, memory, bandwidth and disk space"

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

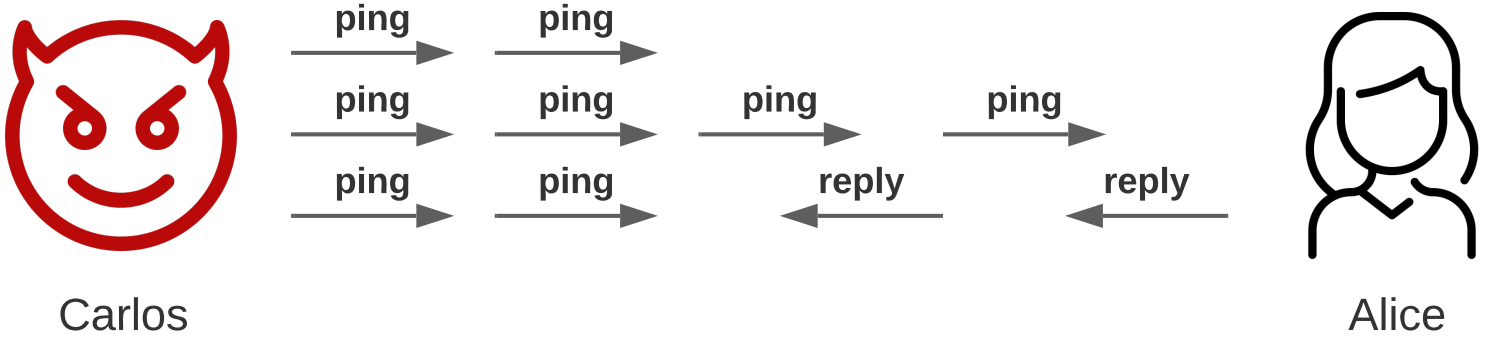
Denial-of-Service

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

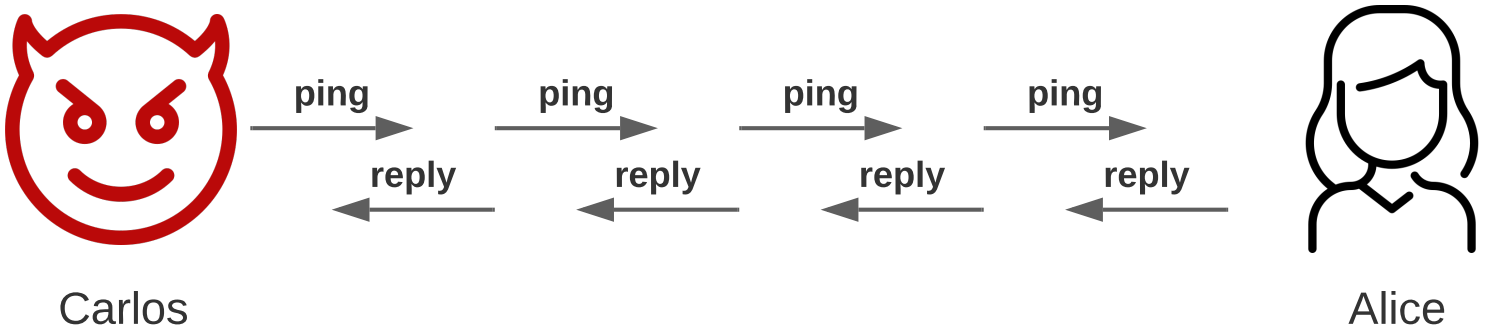
- Network bandwidth
- System resources
- Application resources
  - Propose several valid requests to a server within the target system
  - Each request consumes significant resources, limiting the server response ability

Ping Flood attack

Attacker with greater bandwidth...



Alice with greater bandwidth...



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!

Flooding Attacks - Truly a Classic

- Classified based on the network protocol used
- Goal: to overload the network capacity on some link to a server
- Virtually *any* type of network packet can be used

Flooding Attacks - Truly a Classic

- Classified based on the network protocol used
- Goal: to overload the network capacity on some link to a server
- Virtually *any* type of network packet can be used

ICMP flood

- Ping flood using ICMP echo request packets
- Traditionally, network admins allow these packets into their networks
- A good tool for diagnostics!

UDP/TCP flood

- Direct UDP packets to a specific port number on a system
- ... or TCP packets, depending on the systems of target victim!
- Brute force attack

Flooding Attacks - 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

Flooding Attacks - 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)

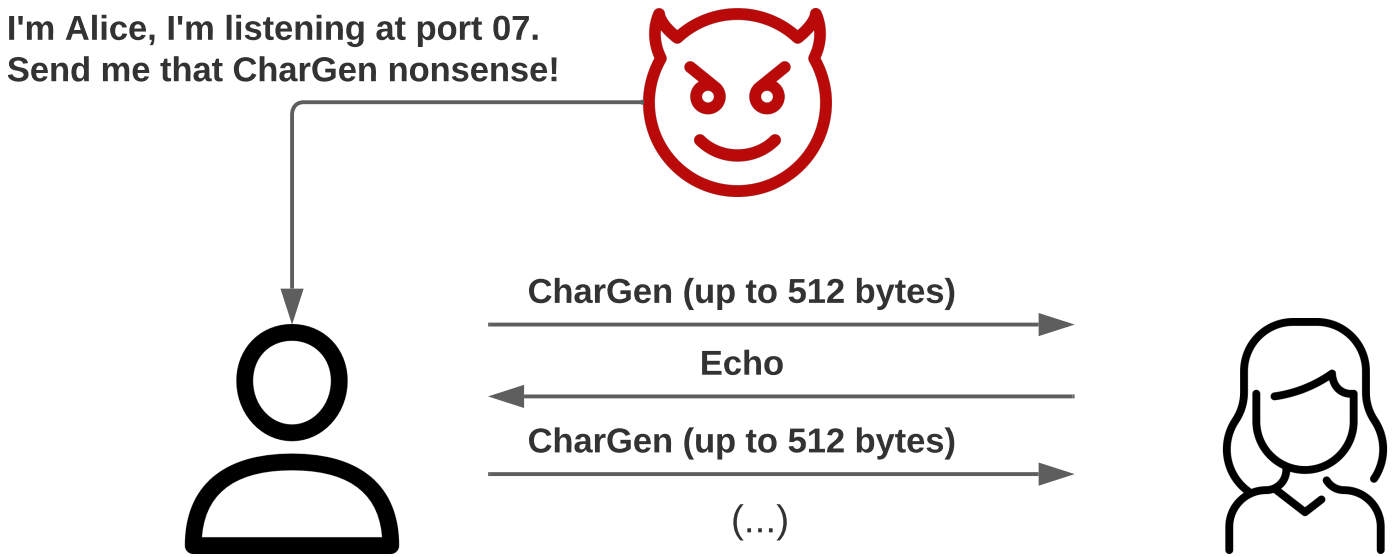
- Respond with UDP packet back to the source
- If service is not running, packet is discarded. ICMP destination unreachable packet returned to the sender
- Achieved its goal of occupying capacity on the link to the server!

Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a *spoofed* source address on the actual victim
- When the intermediary responds, the reply is sent to the victim
- “Reflects” the attack off the intermediary (reflector)

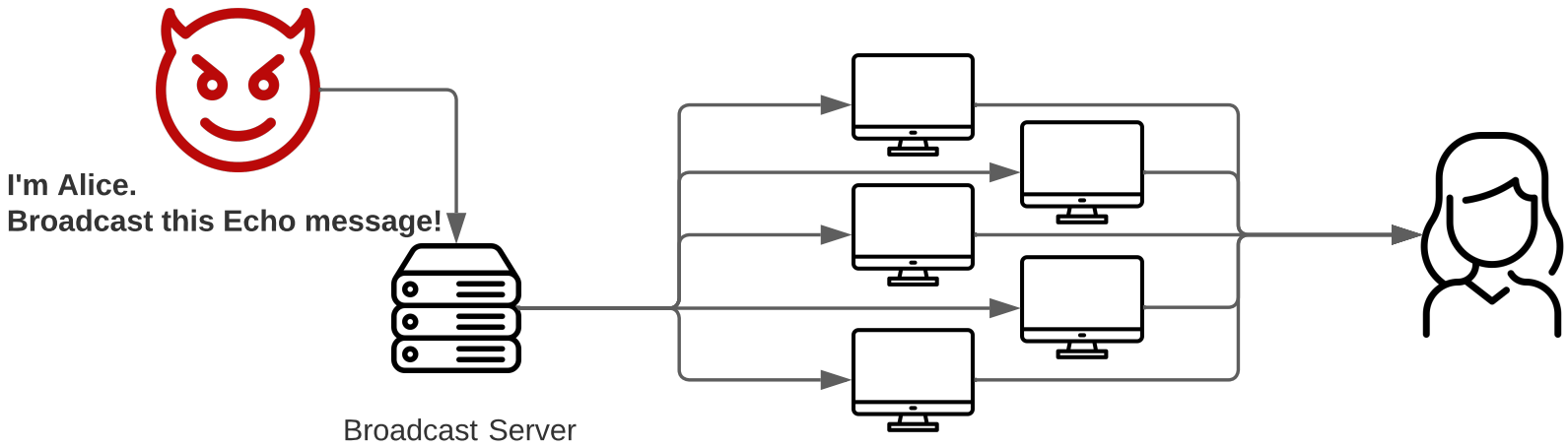
Goal: To generate enough volumes of packets to flood the link to the target system without alerting the intermediary

Echo-Chargen



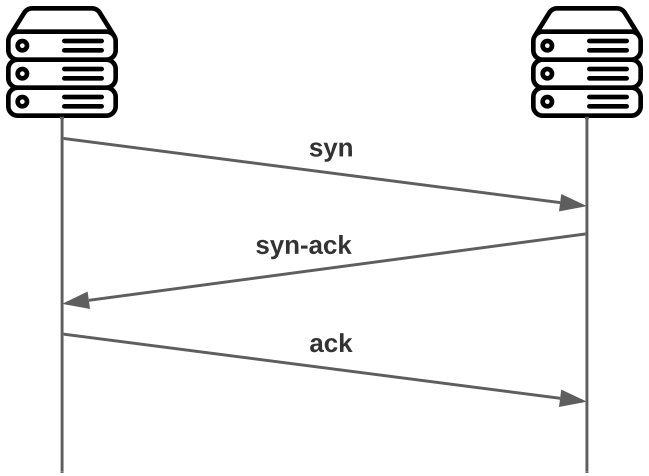
- *Requirement:* Source address spoofing (easy)
- Echo service (port 07) sends back whatever it receives
- CharGen is a character generation service
  - Used for debugging (of course...)
- Huge amounts of data form an endless loop!

Smurf Attack



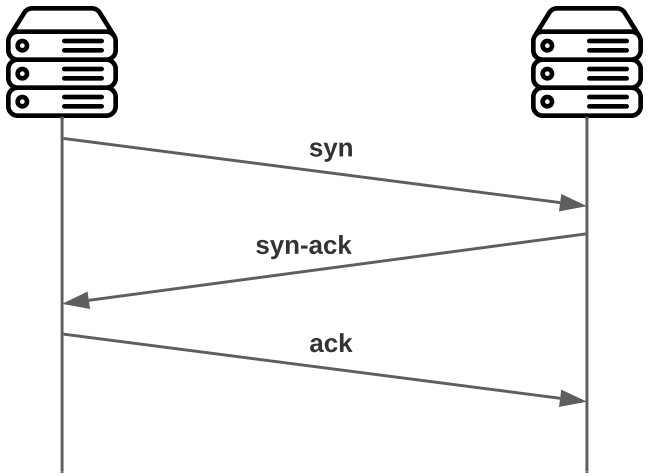
- *Requirement:* Source address spoofing (easy)
- *Requirement:* Access to a server within the network
- Server broadcasts echo “from Alice” to the whole network
- Alice is blasted by echo messages from a bunch of machines

TCP - Establish connection



1. A client sends a SYN (synchronize) message
2. The server replies with a SYN-ACK message
3. The client concludes with a ACK (acknowledge) message

TCP - Establish connection

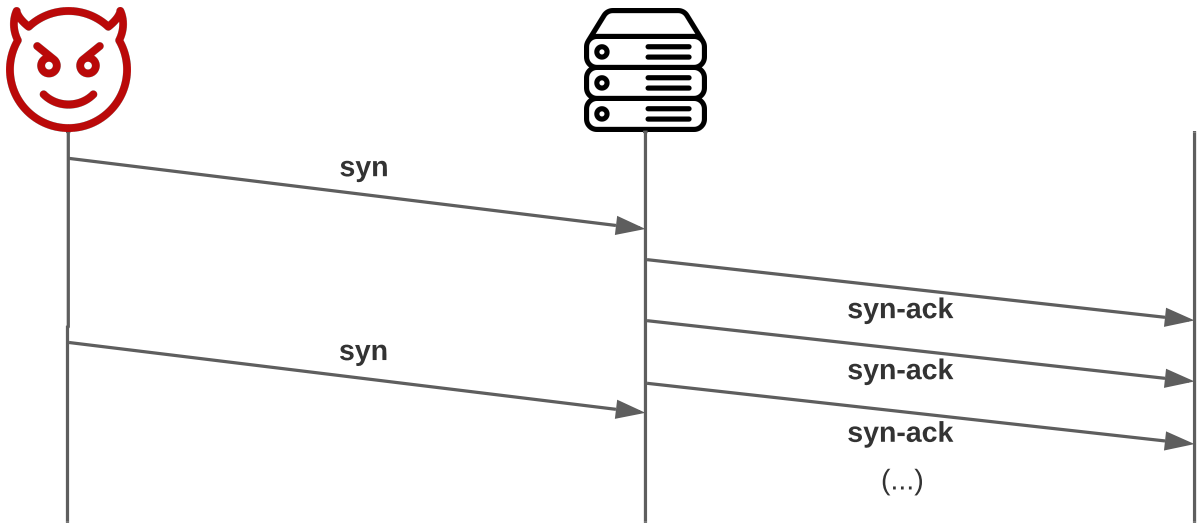


1. A client sends a SYN (synchronize) message
2. The server replies with a SYN-ACK message
3. The client concludes with a ACK (acknowledge) message
   - Channel is only established upon receiving the ACK message
   - Until then, the handshake is on-hold
   - Wasting resources...

SYN Spoofing attack

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests
  - Overflows tables used to manage TCP connections
- Legitimate users are denied access to the server
- An attack on *system resources*, specifically the network handling code in the operative system

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

Kaspersky DoS Report

Kaspersky regularly publishes reports statistical information[1]

Interesting titbits

- Attacks last longer
  - Average duration of an attack in Q1, 2021: 30 minutes
  - Average duration of an attack in Q2, 2022: 3000 minutes (2 days)

[1] Kaspersky 2022 Q2 Report

Kaspersky DoS Report

Kaspersky regularly publishes reports statistical information[1]

Interesting titbits

- Attacks last longer
  - Average duration of an attack in Q1, 2021: 30 minutes
  - Average duration of an attack in Q2, 2022: 3000 minutes (2 days)
- A rise of $\approx$ 50% of *smart* attacks
  - *Smart* attacks are defined as having sophisticated preparation
  - I.e. not trivial applications of known vulnerabilities

[1] Kaspersky 2022 Q2 Report

Kaspersky DoS Report

Kaspersky regularly publishes reports statistical information[1]

Interesting titbits

- Attacks last longer
  - Average duration of an attack in Q1, 2021: 30 minutes
  - Average duration of an attack in Q2, 2022: 3000 minutes (2 days)
- A rise of $\approx$ 50% of *smart* attacks
  - *Smart* attacks are defined as having sophisticated preparation
  - I.e. not trivial applications of known vulnerabilities
- New record duration of attack – 41441 minutes ($\approx$ 29 days)
  - Very expensive – machines wear-off and nodes fail
  - Experts wonder about expertise, affiliation and funding of attackers

[1] Kaspersky 2022 Q2 Report

Kaspersky DoS Report

Kaspersky regularly publishes reports statistical information[1]

Interesting titbits

- Attacks last longer
  - Average duration of an attack in Q1, 2021: 30 minutes
  - Average duration of an attack in Q2, 2022: 3000 minutes (2 days)
- A rise of $\approx$ 50% of *smart* attacks
  - *Smart* attacks are defined as having sophisticated preparation
  - I.e. not trivial applications of known vulnerabilities
- New record duration of attack – 41441 minutes ($\approx$ 29 days)
  - Very expensive – machines wear-off and nodes fail
  - Experts wonder about expertise, affiliation and funding of attackers
- Attacks are down from Q1 to Q2
  - Consistent with the decline of cryptocurrency
  - Stimulates the heating of the DDos market

[1] Kaspersky 2022 Q2 Report

Speaking of Distributed Denial of Service

Methodology

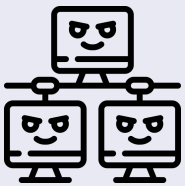
- Use multiple systems to generate attacks
- Attacker uses a flaw in operative system or in a common application to gain access and install a program on it (zombie)

Speaking of Distributed Denial of Service

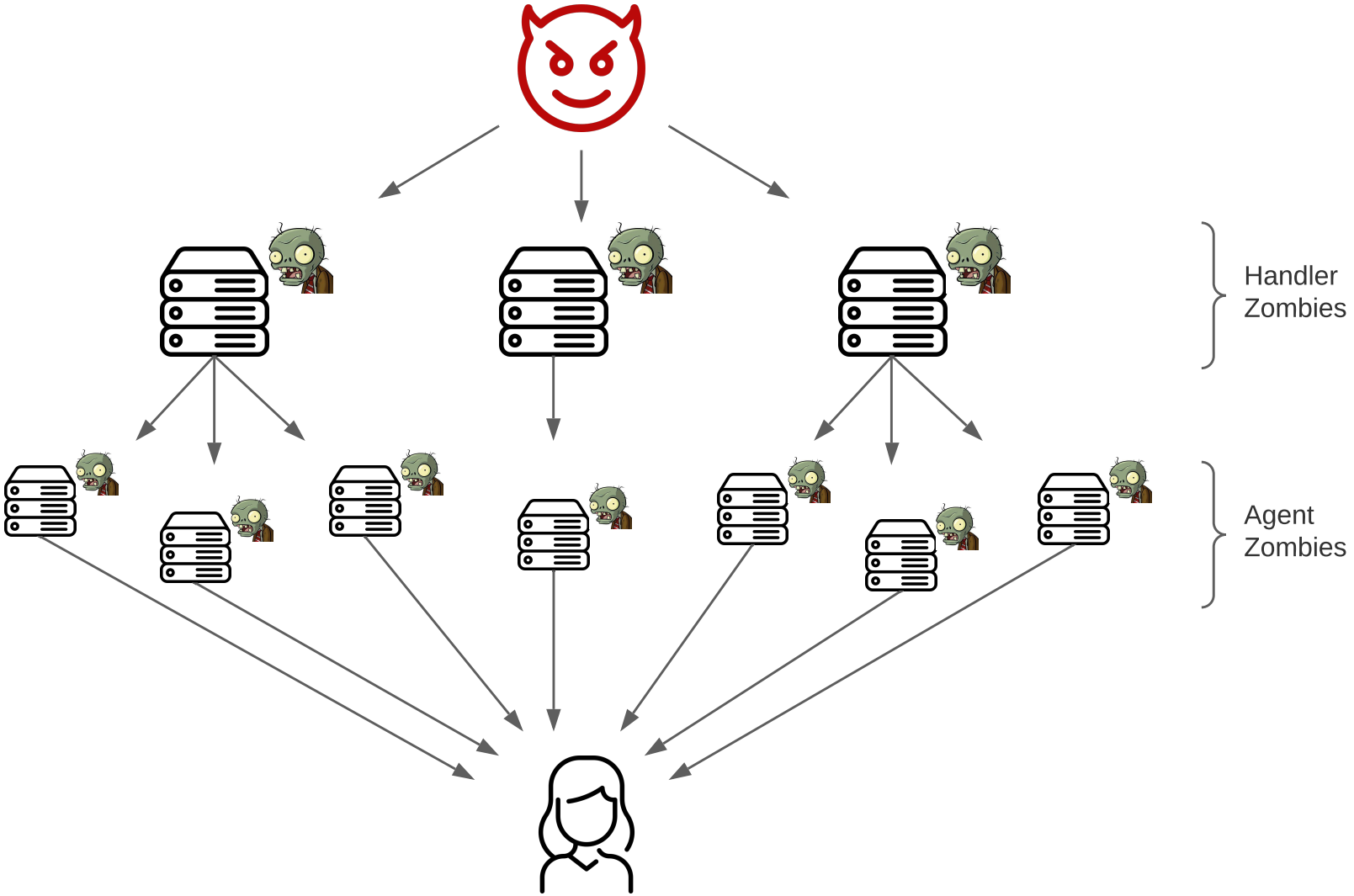
Methodology

- Use multiple systems to generate attacks
- Attacker uses a flaw in operative system or in a common application to gain access and install a program on it (zombie)

- This method can be applied to gain access to large collections of such systems, which are then used to perform attacks (*botnet*)



DDoS Control Hierarchy



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

Going back to attacks - HTTP

HTTP Flood

- Attack that bombards Web servers with HTTP requests
- Typically DDoS
  - Requests come from many different hosts
- Consumes considerable resources
- Spidering
  - Start from an HTTP link and follow all links on a Website recursively

Going back to attacks - HTTP

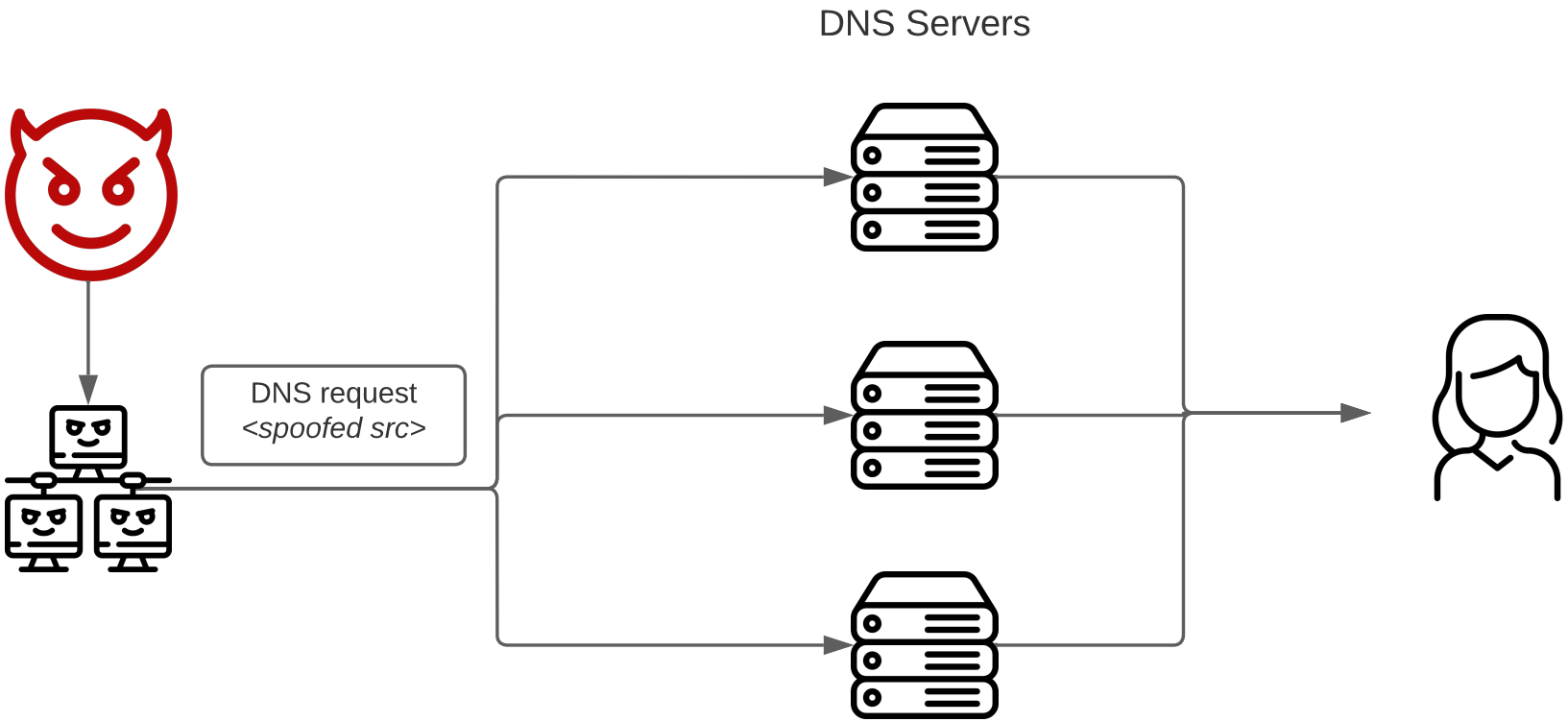
HTTP Flood

- Attack that bombards Web servers with HTTP requests
- Typically DDoS
  - Requests come from many different hosts
- Consumes considerable resources
- Spidering
  - Start from an HTTP link and follow all links on a Website recursively

Slowloris

- Send *legitimate* HTTP requests that never complete
- Exploits techniques to support parallel processing of requests
- Blocks all threads for establishing connections
- Current intrusion detection/prevention solutions relying on signatures do not recognize slowloris

DNS Amplification Attack



DNS Amplification Attack

- Use DNS requests with spoofed source IP address being the target
  - Alice, in the previous picture
- Exploit DNS behavior to convert a small request to a much larger response
  - Argument “ANY” produces large responses
  - 60 byte request can lead to a 512-4000 byte response
- Attacker sends request to multiple well connected servers, flooding the target
  - Only needs a moderate flow of request packets
  - ... Thus hard to detect
  - ... And also effective against DNS servers

Mitigating DNS Amplification

Not a lot of choices...

- A volumetric attack - large volumes of traffic are generated
  - Pressure is not only on the victim, but also on the surrounding infrastructure
- ISP may *blackhole* traffic (next!)

Mitigating DNS Amplification

Not a lot of choices...

- A volumetric attack - large volumes of traffic are generated
  - Pressure is not only on the victim, but also on the surrounding infrastructure
- ISP may *blackhole* traffic (next!)

Alternatives

- Reduce the total number of open DNS resolvers
- Restricting a DNS resolver to only respond to queries from *trusted* sources
- Have ISPs actively detect spoofed IP addresses
  - Ingress Filtering (Whitelist/Blacklist for IP addresses)
  - Collaborative ISP DDoS detection (not always possible...)

DDoS Blackhole Routing

- Traffic is routed into a null route and is lost.
  - From legitimate and illegitimate sources
  - The goal is to prevent a service from being flooded
- An aggressive countermeasure to blocking DDoS attacks
- Often **too severe a measure**

DDoS Blackhole Routing

- Traffic is routed into a null route and is lost.
  - From legitimate and illegitimate sources
  - The goal is to prevent a service from being flooded
- An aggressive countermeasure to blocking DDoS attacks
- Often **too severe a measure**

Shutting down Youtube

In 2008 Youtube was down after Pakistan Telecom's use of blackhole routing[a]

- Dutch cartoon depicting images deemed improper led to a government order to shut down a specific video
- Blackhole routing applied to *all* users trying to access Youtube.
- Pakistan Telecom shared this route with worldwide ISPs: all Youtube-bound traffic went through Pakistan telecom, which would then be dropped.

[a] https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/

Back to Amplification Attacks

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

- Commands to UDP protocols elicit very large responses
- Depending on the protocol, this is a nice way to upscale attacks
- Table based on the NCAS analysis (source)

NTP Amplification Attacks

An innocuous service for clock synchronization...

- Same MO as previous attacks:
  1. Find a service that has a good reply-to-request ratio
  2. Spoof source IP to forward packets to the victim
  3. Profit!

NTP Amplification Attacks

An innocuous service for clock synchronization...

- Same MO as previous attacks:
  1. Find a service that has a good reply-to-request ratio
  2. Spoof source IP to forward packets to the victim
  3. Profit!

Concretely...

- Use MONLIST to get the peers list
- Generates the last 600 IP addresses connected to the NTP
- Send those to Alice

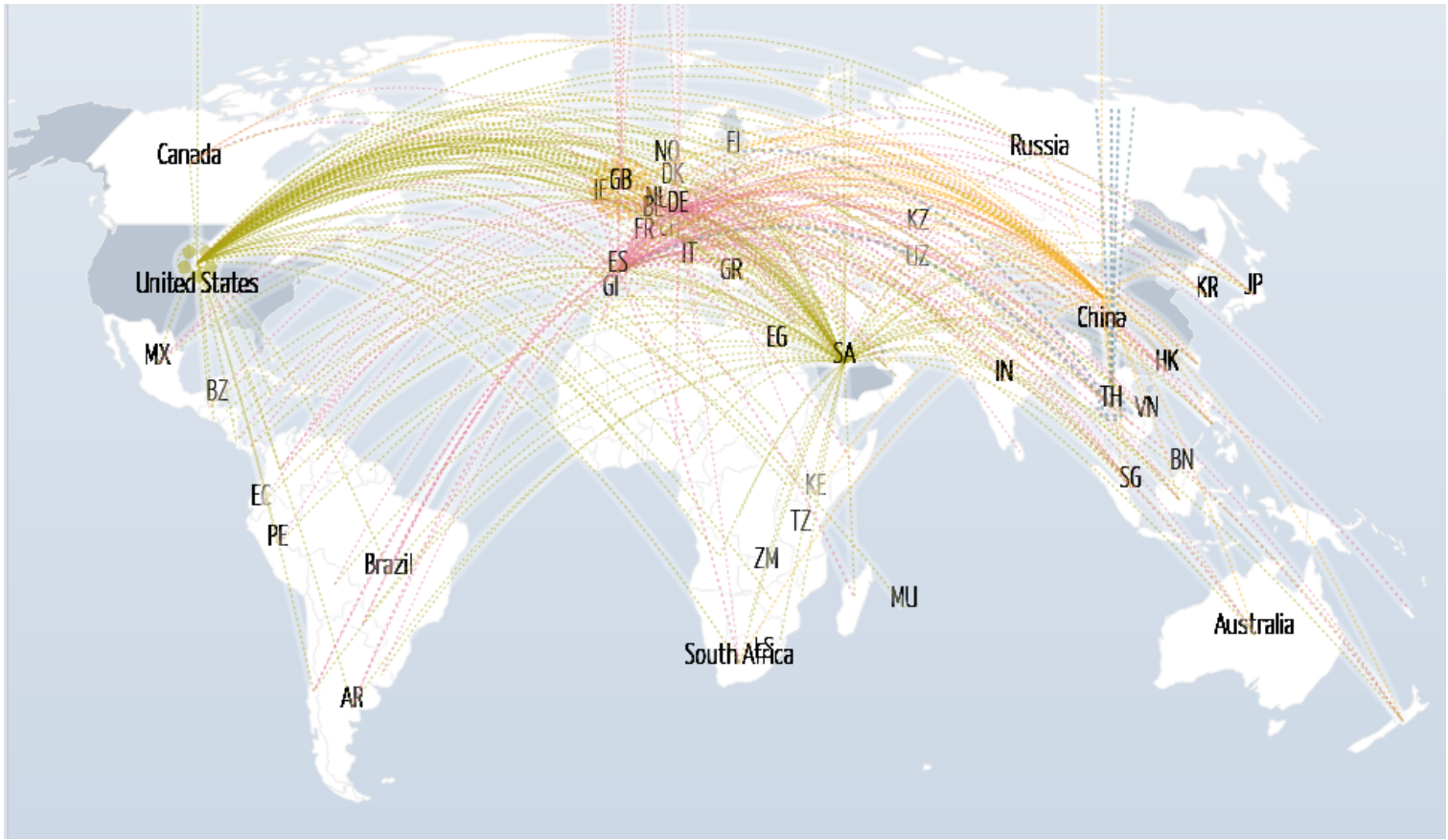
Simple Service Discovery Protocol

Used by Universal Plug and Play to advertise and search for services/devices over the network

- Attack is based on a UDP request over M-SEARCH
- Can request ssdp:all - i.e. all services that a given device offers
- Uses by default multicast address for destination, but can be set to use unicast
- Open on the WAN side (available over the internet)
- Post from Cloudfare describes how this “Stupidly Simple” attack can be used to generate a 100Gbps DDoS

Denial-of-Service Monitoring

Digital Attack Map presents data gathered and collected by the ATLAS system (330 ISP, over 130Tbps of global traffic)



Denial-of-Service Monitoring

Digital Attack Map presents data gathered and collected by the ATLAS system (330 ISP, over 130Tbps of global traffic)

According to the website and its references

- 150$ are sufficient to acquire a week-long DDoS attack on the black market
  - Attacks are cheaper and more powerful
- More than 2000 daily DDoS attacks can be observed world-wide
  - Sources, Destinations, Types and Duration all over the place
- 1/3 of all downtime incidents can be attributed to DDoS attacks
  - They may not be elegant, but they are effective

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

DoS Attack Prevention

Block Spoofed Source Addresses (RFC 2827)

- Ingress filtering
- On routers as close to the source as possible
- Still far too rarely implemented

DoS Attack Prevention

Block Spoofed Source Addresses (RFC 2827)

- Ingress filtering
- On routers as close to the source as possible
- Still far too rarely implemented

Rate control in upstream distribution nets

- Target specific packet types
- E.g. some ICMP, some UDP, TCP/SYN
- Leverage known amplification attacks

DoS Attack Prevention

Block Spoofed Source Addresses (RFC 2827)

- Ingress filtering
- On routers as close to the source as possible
- Still far too rarely implemented

Rate control in upstream distribution nets

- Target specific packet types
- E.g. some ICMP, some UDP, TCP/SYN
- Leverage known amplification attacks

Use modified TCP connection handling

- SYN cookies when table is full
- Selective/random drop when table is full
- Avoid a state where no further connections can be established

DoS Attack Prevention - High level

- Block IP directed broadcasts
- Block suspicious services and combinations
- Use mirrored and replicated servers when high-performance and reliability is required
- Manage application-level attacks with a form of graphical puzzle to distinguish legitimate human requests from bots

Responding to DoS Attacks

Having a good incident response plan...

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

Responding to DoS Attacks

Having a good incident response plan...

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

... and good proactive measures

- Antispoofing, directed broadcast and rate limiting filters
- Ideally, network monitors and Intrusion Detection Systems (soon) to detect and raise warnings over abnormal traffic patterns
  - How can we distinguish normal from abnormal?

Diagnosing DoS Attacks

- Identify the type of attack
- Have ISP trace packet flow back to the source
- Implement contingency plan
- Update incident response plan

Diagnosing DoS Attacks

- Identify the type of attack
  - Capture and analyse packets
    - Intrusion Detection Systems (soon)
  - Design filters to block attack traffic upstream
    - Firewalls (soon)
  - ... or identify and correct system application/bug
- Have ISP trace packet flow back to the source
- Implement contingency plan
- Update incident response plan

Diagnosing DoS Attacks

- Identify the type of attack
- Have ISP trace packet flow back to the source
  - May be difficult and time consuming
  - Necessary if planning legal action
  - Accountability is key
- Implement contingency plan
- Update incident response plan

Diagnosing DoS Attacks

- Identify the type of attack
- Have ISP trace packet flow back to the source
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan

Diagnosing DoS Attacks

- Identify the type of attack
- Have ISP trace packet flow back to the source
- Implement contingency plan
- Update incident response plan
  - Analyze the attack and the response for future handling
  - Attack strategies are not static
  - So neither can be the response plan

Wrap up

Denial of Service

- Denial of Service attacks aim to disrupt system resources
- The common tactic is to overwhelm the network
  - Flooding ping; Echo Chargen; Smurf Attack; SYN Spoofing

Wrap up

Denial of Service

- Denial of Service attacks aim to disrupt system resources
- The common tactic is to overwhelm the network
  - Flooding ping; Echo Chargen; Smurf Attack; SYN Spoofing

Botnets and Attacks

- Corrupted machines zombified to help with attacks
- Botnets are hierarchical systems of zombies
- Used to upscale attacks

Wrap up

Denial of Service

- Denial of Service attacks aim to disrupt system resources
- The common tactic is to overwhelm the network
  - Flooding ping; Echo Chargen; Smurf Attack; SYN Spoofing

Botnets and Attacks

- Corrupted machines zombified to help with attacks
- Botnets are hierarchical systems of zombies
- Used to upscale attacks

Countermeasures

- Hard to counteract
- Requires proactive policies and spoofing prevention
- And a good back-up plan for when they happen

Network Security - Week 5

João Soares

DCC/FCUP

2023