Internet Security

Introduction

1. Overview
   - Internet was not designed or built with security in mind
     - Afterthought after adversaries began misusing or abusing Internet services, resources, and infrastructure
   - Types of attacks
     - Misuse DNS protocol and infrastructure
     - Traffic attraction attacks based on BGP abuse
     - Techniques to infer network reputation
     - Denial of Service attacks
       * DDoS defense techniques offered at IXPs

Properties of Secure Communication

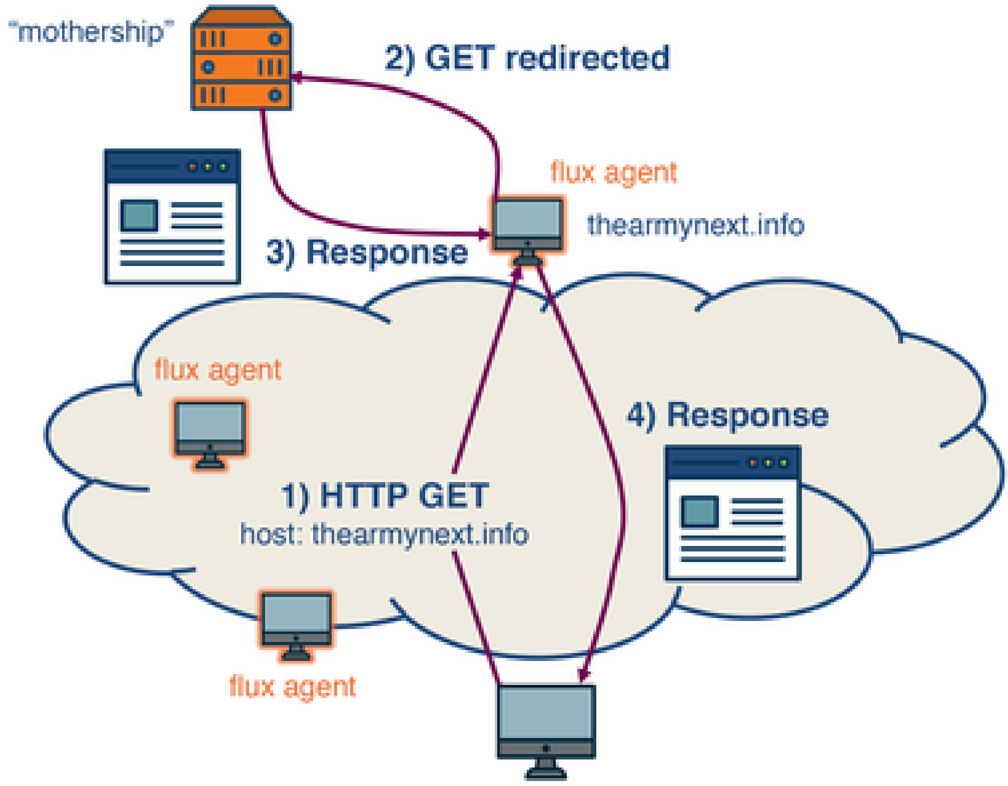
1. Establishing secure communication
   - Confidentiality: Ensure a message is only available to sender and receiver
   - Integrity: Ensure a message hasn't been modified while in transit
   - Authentication: Ensuring the two parties are who they say they are
   - Availability: Ensure multiple aspects of the communication channel are functioning appropriately and can cope with failures such as power outages, hardware failures, etc. or attacks that aim to render the system unavailable such as denial of service attacks

Quiz 1

1. Which property of secure communication ensures that people are who they say they are when communicating over the internet?
   - Authentication
2. Which property of secure communication ensures that a message is not modified before it reaches the receiver?
   - Integrity
3. Which property of secure communication is protected by encrypting the messages exchanged?
   - Confidentiality

DNS Abuse

1. Round Robin DNS (RRDNS)
   - Used by large websites to distribute the load of incoming requests to several servers at a single physical location
     - Cycles through DNS records in a round robin manner
     - Includes TTL for this mapping
2. DNS-based Content Delivery
   - CDNs use more complex strategies to distribute content using DNS
   - Distribute across servers around the world
3. Fast-Flux Service Networks
   - Previous two strategies provide reliability, scalability, and resilience
     - Vulnerable to spammers because if even one IP address is functional, the scam is still working
   - Fast-Flux Service Networks (FFSN) is an extension of the ideas behind RRDNS and CDN
     - Based on a rapid change in DNS answers, with a TTL lower than that of RRDNS and CDN
     - One key difference between FFSN and other methods is that after the TTL expires, it returns a different set of A records from a larger set of compromised machines
     - These machines act as proxies between the incoming request and control node, forming a resilient, one-hop overlay network



Fast-Flux Service Network

Quiz 2

1. Attackers tend to keep the uptime of domains used for malicious purposes as short as possible in order to avoid being detected.
   - False
2. Round Robin DNS is a mechanism used by large websites to distribute the load of incoming requests to several servers at a single physical location.
   - True
3. DNS-based content delivery aims to distribute the load amongst multiple servers at a single location, but also distribute these servers across the world.
   - True
4. DNS-based content delivery determines the nearest server, which results in increased responsiveness and availability.
   - True

How to Infer Network Reputation: Evidence of Abuse

1. FInding Rogue nEtworks (FIRE)
   - System that monitors the Internet for rogue networks
   - Rogue networks: Networks whose main purpose is malicious activity such as phishing, hosting spam pages, hosting pirated software, etc.
   - Uses three main data sources to identify hosts that likely belong to rogue networks
   - Legitimate networks are usually able to remove malicious content within a few days, rogue networks leave it up for weeks to a year

- FIRE looks at a list of malicious IP addresses and identifies malicious networks by finding those with the highest ratio of malicious to total IP addresses

2. Botnet command and control providers
    - Several botnets still rely on centralized command and control
    - Bot-master prefers to host their C&C on networks where it is unlikely to be taken down
    - Two main types
        - IRC-based botnets
        - HTTP-based botnets
3. Drive-by-download hosting providers
    - Drive-by-download is a method of malware installation without interaction with the user
    - Occurs when a victim visits a web page that contains an exploit for their vulnerable browser
4. Phish housing providers
    - Contains URLs of servers that host phishing pages
    - Phishing pages mimic authentic sites to steal login credentials, credit card numbers, and other personal information
    - Hosted on compromised servers and are transient

How to Infer Network Reputation: Interconnection Patterns

1. Data-plane monitoring
    - FIRE only flags a network as malicious after we have observed indications of malicious behavior for a long enough period of time
    - Monitoring traffic on all networks is infeasible
    - FIRE disadvantages
        - May take a very long time until a large fraction of IPs makes it to a blacklist
        - The approach does not differentiate well between networks that are legitimate but abused and those which are likely operated by cyberactors
2. ASwatch
    - Uses information exclusively from the control plane (routing behavior) to identify malicious networks
    - Attempts to differentiate between abused and malicious networks
        - Bulletproof: Malicious network
    - Bulletproof ASes have distinct interconnection patterns and overall different control plane behavior from most legitimate networks
3. Design of ASwatch
    - Monitor BGP routing activity to learn the control plane behavior of a network
    - Two phases
        - Training phase: Learn control-plane behavior typical of both types of ASes by computing statistical features of each AS
            - Rewiring activity: Based on changes in the AS connecting activity
            - IP space fragmentation and churn: Based on advertised prefixes
            - BGP routing dynamics: BGP announcements and withdrawals follow different patterns from legitimate ones
        - Operational phase: Given an unknown AS, it then calculates the features for this AS + Uses the model to assign a reputation score to the AS + Systems with low reputation scores for several days in a row are identified as malicious
    - Uses supervised learning to capture the known behaviors and patterns with a trained model

Quiz 3

1. Legitimate networks may let malicious content be up for weeks to more than a year.
    - False
2. How does FIRE identify the most malicious networks?
    - Analyzing the information given by data sources and searching for ASes with a large percentage of

malicious IP addresses.

3. ASwatch uses information exclusively from the data plane to infer network reputation.
    - False
4. ASwatch relies on the premise that “bulletproof” ASes have distinct interconnection patterns and overall different control plane behavior from most legitimate networks.

How to Infer Network Reputation: Likelihood of Breach

1. Prediction systems
    - Look at system to predict the likelihood of a security breach within an organization using only externally observable features
    - Allows model to scale to all organizations
2. Classes of features for this model
    - Mismanagement symptoms
        - Misconfigurations in a network indicate that there may not be policies in place to prevent such attacks or may not have the technological capability to detect these failures
            - Open Recursive Resolvers: Misconfigured open DNS resolvers
            - DNS Source Port Randomization: Many servers don’t implement this
            - BGP Misconfiguration: Short-lived routes can cause unnecessary updates to the global routing table
            - Untrusted HTTP Certificates: Can detect the validity of a certificate by TLS handshake
            - Open SMTP Mail Relays: Servers should filter messages so that only those in the same domain can send mails/messages
    - Malicious activities
        - How much malicious activity is originating from the organization’s network and infrastructure
            - Spam activity: CBL, SBL, SpamCop
            - Phishing and malware activity: PhishTank, SURBL
            - Scanning activity: Dshield, OpenBL
    - Security incident reports
        - Data based on actual security incidents give us the ground truth on which to train our machine learning model on
            - VERIS community database: Public effort to collect cybersecurity incidents, maintained by Verizon RISK team
            - Hackmageddon: Independently maintained blog that aggregates security incidents on a monthly basis
            - Web Hacking Incidents Database: Actively maintained repository for cyber security incidents
3. Model Design
    - Uses a random forest classifier and compares it to a baseline provided by a Support Vector Machine
        - Uses 258 features
        - Best combination of features give this model an accuracy of 90%

Traffic Attraction Attacks: BGP Hijacking

1. Classification by Affected Prefix
    - Concerned with IP prefixes that are advertised by BGP
    - Exact prefix hijacking: Two different ASes announce a path for the same prefix
        - Routes to the hijacker whenever the path is shortest, disrupting traffic
    - Sub-prefix hijacking: Works with a sub-prefix of the genuine prefix of the real AS
        - Exploits the characteristic of BGP to favor more specific prefixes
    - Squatting: Hijacking AS announces a prefix that has not yet been announced by the owner AS
2. Classification by AS-Path announcement
    - Illegitimate AS announces the AS-path for a prefix for which it doesn’t have ownership rights
        - Type-0 hijacking: AS announces prefix not owned by itself

    - Type-N hijacking: AS announces illegitimate path for a prefix it doesn't own to create a fake path between different ASes
    - Type-U hijacking: AS does not modify the AS-PATH but may change the prefix
3. Classification by Data-Plane traffic manipulation
    - Attacker hijacks and manipulates network traffic on its way to the receiving AS
        - Dropped: Never reaches the intended destination (blackholing)
        - Eavesdropped or manipulated (man-in-the-middle attack)
        - Impersonated: Victim is impersonated and response is sent back to the sender (imposture attack)

Traffic Attraction Attacks: Motivations

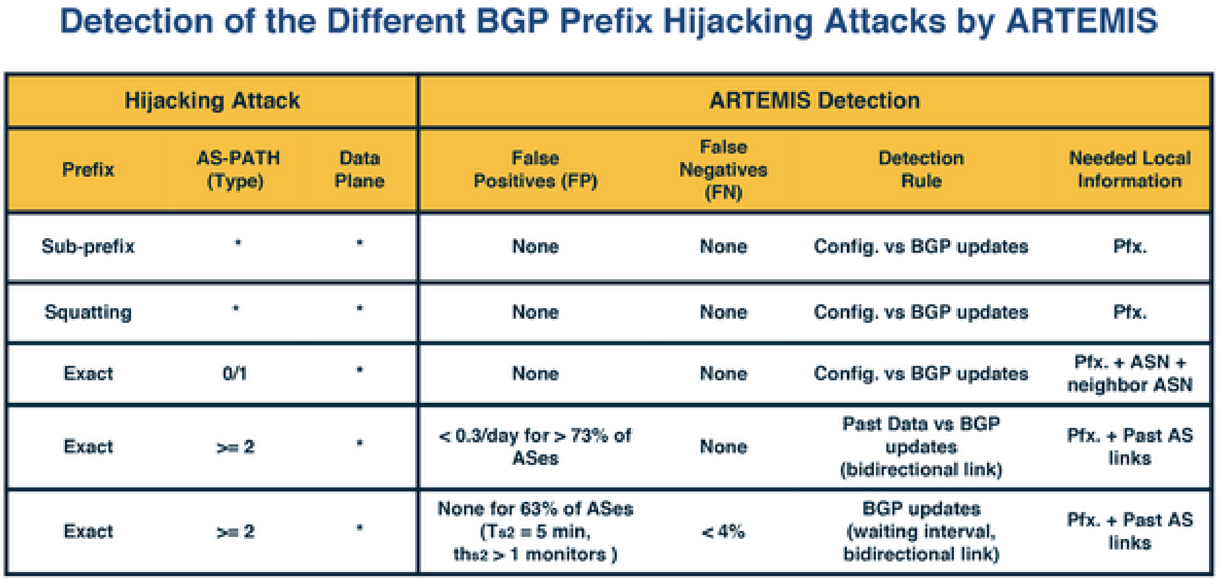
1. Human Error
    - Accidentaly routing misconfiguration due to manual errors
    - Can lead to large scale exact-prefix hijacking
    - Type-0 hijacking
2. Targeted Attack
    - Hijacking AS usually intercepts network traffic (MM attack) while operating in stealth mode to remain under the radar on the control plane
    - Type-N and Type-U hijacking
3. High Impact Attack
    - Attacker is obvious in their intent to cause widespread disruption of services

Example BGP Hijack Attacks

1. Hijacking a prefix
    - Attacker uses a router to send false announcements and hijack the prefix belonging to another AS
2. Hijacking a path
    - Attacker manipulates received updates before propagating them to neighbors

Defending Against BGP Hijacking: An Example Detection System

1. ARTEMIS
    - System run locally by network operators to safeguard its own prefixes against malicious BGP hijacking attempts
    - Key ideas
        - Configuration file: All prefixes owned by the network are listed for reference
        - Mechanism for receiving BGP updates: Allows receiving updates from local routers and monitoring services
    - Using local configuration as a reference, ARTEMIS can check for prefixes and AS-PATH fields and trigger alerts when there are anomalies
    - Important to consider false positive and false negative rates
    - ARTEMIS allows operator to choose between accuracy/speed and inconsequential false alarm rates



Detection of the Different BGP Prefix Hijacking Attacks by ARTEMIS

Hijacking Attack			ARTEMIS Detection			
Prefix	AS-PATH (Type)	Data Plane	False Positives (FP)	False Negatives (FN)	Detection Rule	Needed Local Information
Sub-prefix	*	*	None	None	Config. vs BGP updates	Pfx.
Squatting	*	*	None	None	Config. vs BGP updates	Pfx.
Exact	0/1	*	None	None	Config. vs BGP updates	Pfx. + ASN + neighbor ASN
Exact	>= 2	*	< 0.3/day for > 73% of ASes	None	Past Data vs BGP updates (bidirectional link)	Pfx. + Past AS links
Exact	>= 2	*	None for 63% of ASes (T_{s2} = 5 min, th_{s2} > 1 monitors)	< 4%	BGP updates (waiting interval, bidirectional link)	Pfx. + Past AS links

Example Defense Approach

Defending Against BGP Hijacking: Example Mitigation Techniques

1. Prefix deaggregation
   - Affected network can either contact other networks or simply deaggregate the prefixes that were targeted by announcing more specific prefixes of a certain prefix
   - YouTube advertised a different prefix when attacked
     - 208.65.153.0/24 -> 208.65.153.128/25 and 205.65.153.0/25
2. Mitigation with Multiple Origin AS (MOAS)
   - Third party organizations and service providers do BGP announcements for a given network
   - When a BGP hijacking event occurs, the following steps occur:
     - Third party receives a notification and immediately announces from their locations the hijacked prefix(es)
     - Network traffic from across the world is attracted to the third party organization, which scrubs it and tunnels it to the legitimate AS
3. ARTEMIS findings
   - Outsource the task of BGP announcement to third parties
     - Even a single external organization is highly effective
   - Comparison of outsourcing BGP announcements vs prefix filtering
     - Filtering is less optimal

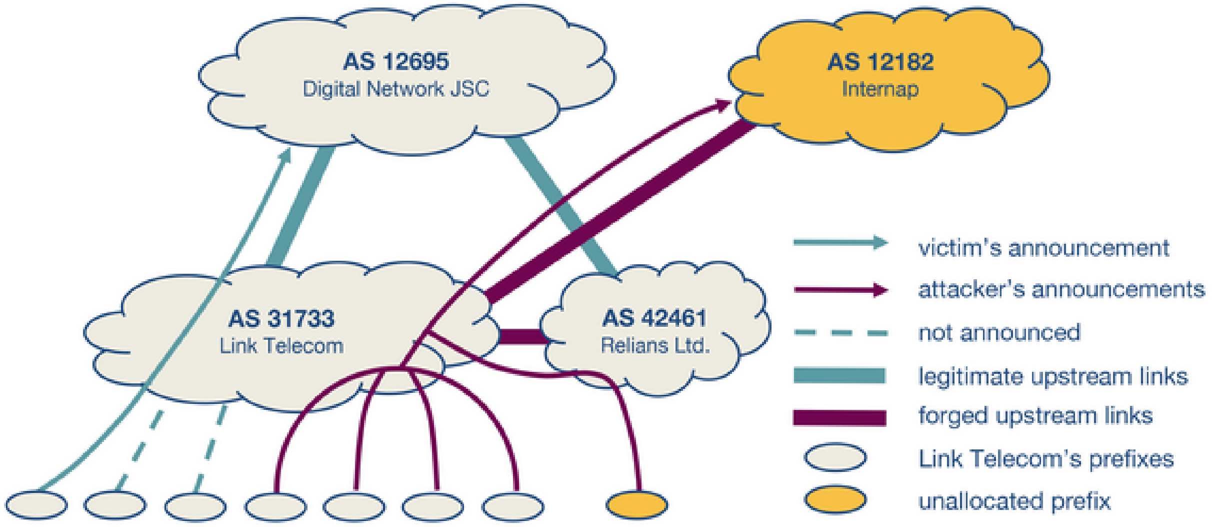
Quiz 4

1. In order to stop a prefix or AS-Path announcement attack, we need access to the control plane data, such as IP prefixes and AS-paths.
2. In attacks where network traffic is dropped, manipulated or impersonated, the data accessed is located at the data plane.
3. Which attack disrupts the BGP characteristic to favor more specific prefixes?
   - Sub-prefix hijacking
4. ARTEMIS uses a configuration file and a mechanism for receiving BGP updates from routers and monitoring services to detect BGP hijacking attacks.
   - True
5. Prefix deaggregation and mitigation with Multiple Origin AS (MOAS) are independent from ARTEMIS.

- False

A Hijacking Case Study - Background

1. Linktel Incident
   - Linktel, a Russian ISP under attack (AS31733, figure below) sent a distress mail (SOS) to North American Network Operators' Group (NANOG) about a prefix hijacking in August 2011.
   - The Russian ISP had gone through financial struggles, and thus had not renewed its DNS domain, which allowed administrative take-over of its Internet resources.
   - The attacker took over the Internet resources and forged a letter of authorization to announce prefixes of AS31733 from a customer's AS (AS12182, figure below).
   - The attacker uses a second attack to hijack AS42461 (Relians Ltd., figure below) to announce an unallocated prefix.



Resulting AS Topology after the Hijacking Phase

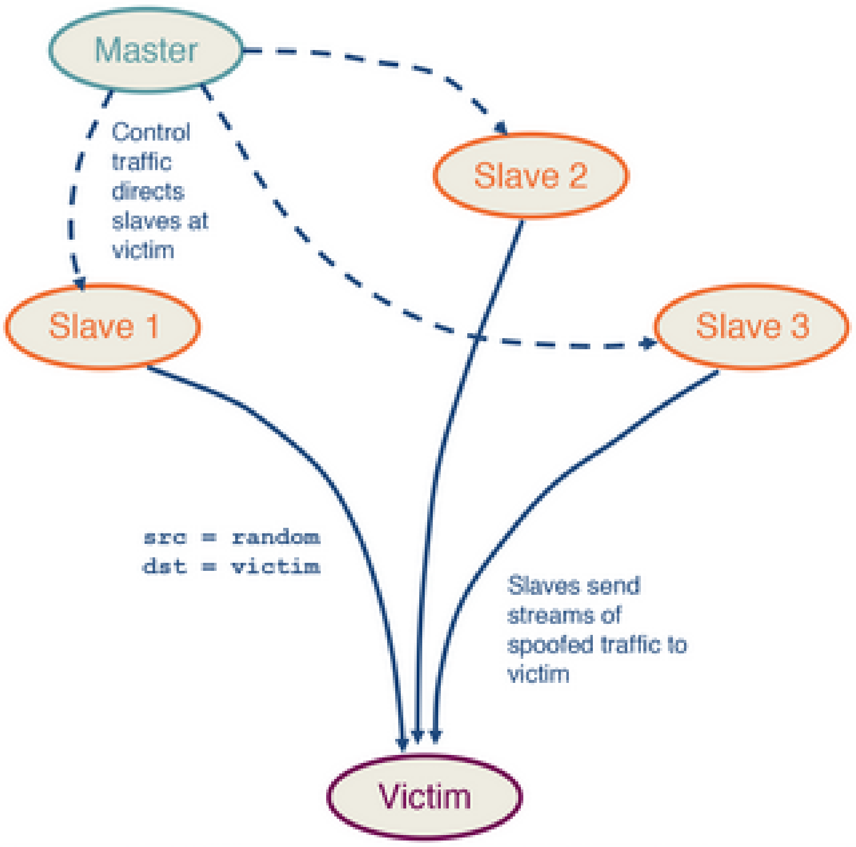
A Hijacking Case Study - Attack Progression

1. Hijacking Phase
   - Linktel let its DNS domain expire which allowed it to be taken over by anyone and used maliciously
2. Productive Phase
   - Attacker stopped announcing the unallocated prefix
3. Recovery Phase
   - Upstream ISPs redelgate reverse DNS entries and announces more specific prefixes
     - Withdraw routes from hijacked prefixes

DDoS: Background and Spoofing

1. Denial of Service Attacks
   - Distributed Denial of Service (DDoS): Attempt to compromise a server or network resources with a flood of traffic
     - Compromise and deploy flooding servers
     - Attacker instructs flooding servers to send a high volume of traffic to the victim
   - Difficult to block attack traffic because it comes from multiple sources
2. Spoofing

- IP Spoofing: Act of setting a false IP address in the source field of a packet with the purpose of impersonating a legitimate server
- Two forms
  - Source IP address is spoofed (send to a different client, DDOS)
  - Use same IP address for source and destination (server sends replies to itself, causing it to crash)


Master
Control traffic directs slaves at victim
Slave 2
Slave 1
Slave 3
src = random
dst = victim
Slaves send streams of spoofed traffic to victim
Victim

Structure of a DDoS Attack

DDoS: Reflection and Amplification

1. Reflection attack
   - Attackers use a set of reflectors to initiate an attack on the victim
   - Reflector: Any server that sends a response to a request
   - Master commands the three slaves to send spoofed requests to the reflectors, which in turn sends traffic to the victim
     - Contrast to previous DDoS attack where slaves send traffic directly to the victim
2. Reflection and Amplification Attack
   - If the requests are chosen in a way that the reflectors send large responses to the victim

Quiz 5

1. A Distributed Denial of Service Attack consists on the attacker sending a large volume of traffic to the victim through servers (slaves), so that the victim host becoming unreachable or in exhaustion of its bandwidth.
   - True

2. IP spoofing is the act of setting a false IP address in the source field of a packet with the purpose of impersonating a legitimate server.
    - True
3. In a reflection attack, the attackers use a set of reflectors to initiate an attack on the victim.
    - True
4. During a Reflection and Amplification attack, the slaves set the source address of the packets to the victim's IP address.
5. What is the difference between a conventional DDoS and a Reflection and Amplification attack?
    - In a DDos attack, the slaves send traffic directly to the victim as opposed to a reflector sending the traffic to the victim.

Defenses Against DDoS Attacks

1. Traffic Scrubbing Services
    - Scrubbing service diverts incoming traffic to a specialized server where the traffic is "scrubbed" into either clean or unwanted traffic
    - Only clean traffic is sent to the destination
    - Limitations
        - Setup and recurring costs
        - Reduced effectiveness due to per packet processing
        - Challenges in handling Tbps level attacks
        - Possibility of decreased performance
2. ACL Filters
    - Access Control List filters are deployed by ISPs or IXPs at their AS broder routers to filter out unwanted traffic
    - Effective when the hardware is homogenous and the deployment of the filters can be automated
    - Limitations
        - Limited scalability
        - Can exhaust bandwidth to neighboring AS because filtering does not occur at ingress points
3. BGP Flowspec
    - Flowspec: Flow specification feature of BGP that helps mitigate DDoS attacks by supporting the deployment and propagation of fine-grained filters across AS domain borders
        - Can be designed to match a specific flow or be based on packet attributes like length and fragment
        - Can be based on drop rate limit
    - BGP Flowspec is an extension to the BGP protocol which allows rules to be created on the traffic flows and take corresponding actions
        - Can help BGP mitigate DDoS attacks by specifying appropriate rules
    - Actions
        - Discard traffic
        - Rate limiting
        - Redirecting
        - Filtering
        - Default rule is to accept the incoming traffic
    - Seen to be effective in the intra-domain environment, but not so popular in the inter-domain environments as it depends on trust and cooperation among competitive networks

DDoS Mitigation Techniques: BGP Blackholing

1. Blackholing
    - Countermeasure to mitigate a DDoS attack
    - All attack traffic to a targeted DDoS destination is dropped to a null location
    - Implemented with the help of an upstream provider or IXP
    - Victim AS uses BGP to communicate the attacked destination prefix to its upstream AS, which

then drops the attack traffic towards this prefix

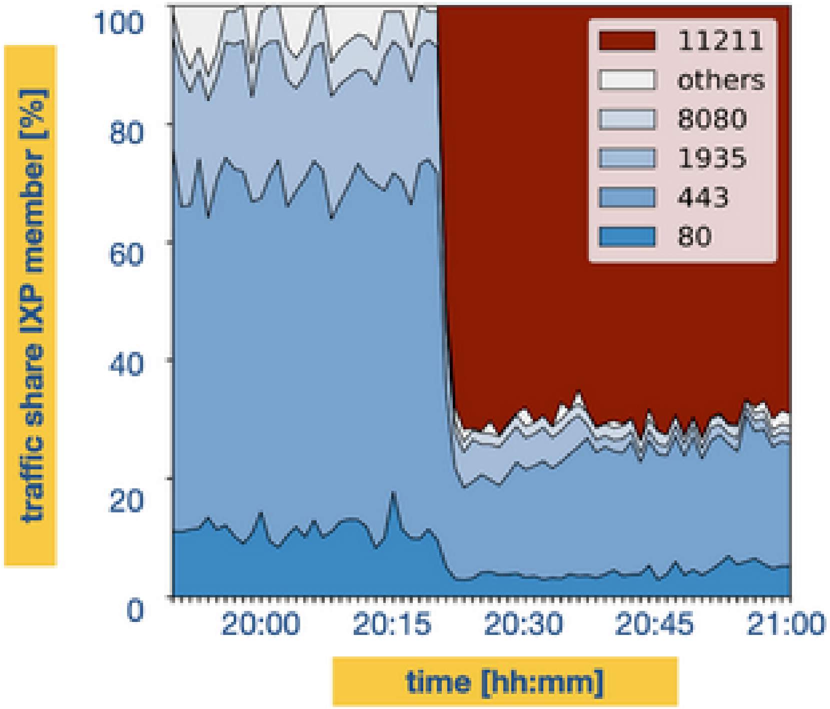
  - Provider will advertise a more specific prefix and modify the next-hop address that will divert the attack traffic to a null interface
  - Blackhole messages are tagged with a specific BGP blackhole community attribute, usually publicly available, to differentiate it from the regular routing updates

Quiz 6

1. Which mitigation technique uses fine-grained filters across AS domain borders, and attributes such as length and fragment can be used to match traffic?
   - BGP Flowspec
2. Which defense mechanism consists on a service that diverts the incoming traffic to a specialized server, where traffic is divided in either clean or unwanted traffic, and clean traffic is then sent to its original destination?
   - Traffic Scrubbing Services
3. BGP Blackholing stops the traffic closer to the destination of the attack.
   - False
4. BGP Blackholing is used to mitigate DDoS attacks.
   - True

DDoS Mitigation Techniques: BGP Blackholding Limitations and Problems

1. Limitations
   - Major drawback of BGP blackholing is that the destination under attack becomes unreachable since all the traffic including the legitimate traffic is dropped



Collateral Damage of Blackholing