FIT5037: Network Security
Denial of Service Attacks and Countermeasures

Faculty of Information Technology
Monash University

Copyright Notice

Lecture 12: Denial of Service Attacks and Countermeasures

Lecture Topics:

- Symmetric key cryptography
- Asymmetric key cryptography
- Pseudorandom Number Generators and hash functions
- Authentication Methods and AAA protocols
- Security at Network layer (IPsec)
- Security at Network layer (firewalls and wireless security)
- Security at Transport layer
- Security at Application layer
- Computer system security and malicious code
- Computer system vulnerabilities and penetration testing
- Intrusion detection
- **Denial of Service Attacks and Countermeasures / Revision**

Outline

- Denial of Service Definition and Classes
- Examples of DoS/DDoS attack
  - OS Vulnerability
  - Application Layer
  - Protocol Feature
- Volumetric DDoS
- Protection against Source Address Spoofing
  - BGP Vulnerability and Mitigation Techniques
  - Source Address Validation Techniques

Denial of Service (DoS) Attack

- RFC 4949 defines Denial of Service as: "The prevention of authorized access to a system resource or the delaying of system operations and functions."
- Specifies four types of solutions:
  - Awareness of vulnerabilities and security threats
  - Detection of attacks on systems and networks
  - Prevention by following defensive practices
  - Response according to a contingency plan
- Distributed DoS is a coordinated DoS attack often using a set of compromised devices
  - compromised devices are referred to as *botnet* or *zombies*
    - usually infected with malware that installs backdoor
- Spoofed source IP address are used in DDoS attack
  - to avoid detection
  - to perform a UDP-based reflect and amplify attack

DoS/DDoS Attack Classes

- Operating System
  - exploit vulnerability in the operating system host of a server or network device leading to crash
- Application layer
  - consume the application layer service resources by creating many open connections
  - exploit application layer vulnerability by sending malformed messages leading to crash of the service
- Protocol feature
  - sending malformed or forged messages to consume resources of the target system
  - sending malformed or forged messages to disrupt legitimate communications
- Volumetric
  - a generic classification based on the outcome of the attack
  - consumes available bandwidth of the network or server by sending large amount of data
- US National Cybersecurity and Communications Integration Center provides a simple guide for classifying DoS attacks based on OSI layer

DoS/DDoS Attack Example: OS Vulnerability

- CVE-2019-11683
  - a vulnerability in Linux kernel 5.x before 5.0.13 in UDP Generic Receive Offload (GRO)
    - UDP GSO (Generic Segmentation Offload) and GRO are techniques to use a virtual MTU that reduces processing time for network communications
  - vulnerability exists in `net/ipv4/udp_offload.c` in `udp_gro_receive_segment`
  - allows attacker to cause a DoS attack via UDP packet with 0 payload
    - mishandled padded packets: "GRO packet of death"
  - Current CVSS score: 10.0
    - Confidentiality: total information disclosure, resulting in all system files being revealed
    - Integrity: a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised
    - Availability: There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.
    - Access Complexity: Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.
    - Authentication: not required
  - to find out if a metasploit module exists for this vulnerability search using CVE code
- for a list of reported DoS vulnerabilities in 2019 (various types): CVE Details: Security Vulnerabilities Published In 2019(Denial Of Service)

DoS/DDoS Attack Examples: Application Layer

- Slowloris (fragmented HTTP)
  - attacker creates many HTTP connections with the target server (using botnest)
  - keeps the connection open for as long as possible with minimum bandwidth
    - attacker sends partial request
    - before the connection is timed out sends another partial request (for instance 1 byte at a time)
    - attacker continues the process: wait long enough and just before connection times out sends another byte
  - attack succeeds when the server runs out of resources or maximum number of concurrent connections is reached
- HTTP Flood
  - attacker sends many HTTP GET or POST requests using botnet to consume server's processing power
- DNS Flood
  - attacker sends many DNS queries with many spoofed source IP addresses
  - attack succeeds if response is much larger than queries and results in consumption of available bandwidth
- Application Layer DDoS mitigation
  - application layer firewall to detect particular attacks
  - use of shorter connection timeouts that does not affect legitimate users
  - dynamically scaling up resources to deal with attack in progress until attack is stopped
    - e.g. use of cloud-based or in-house scrubbing centres
  - prevent DNS recursive queries and limit external views only to required RRs

DoS/DDoS Attack Examples: Protocol Feature

- SYN flood attack is a classic DDoS attack
  - according to Kaspersky Lab report[1] 58% of DDoS attacks in Q4 2018 were TCP SYN flood
- SYN flood can be classified as a protocol feature DDoS
  - attacker sends many TCP SYN request to the target server with spoofed IP addresses
    - for each received SYN the server sets aside resources (e.g. RAM)
    - the queue of of half-open connections is incremented
    - the attack succeeds if the server runs out of resources or the queue of half-open connections is filled
- Ping of Death
  - in a local network sending an echo request with spoofed source IP address and broadcast destination address
  - results in all receivers to send an echo reply to the victim
- ICMP flood or Ping flood
  - sending echo request from a botnet to a target system
    - the request for individual senders is small
    - the collection of all ICMP messages will consume target system's bandwidth
- Reflected ICMP
  - sending TCP/UDP messages with spoofed source IP address of a victim to a range of addresses with closed ports
  - results in ICMP port unreachable messages to be sent back to the victim (usually combined with other attacks)

[1] ;persky Lab report

SYN and ICMP Flood Mitigation

- use of SYN cookies on the server
  - for each received SYN the server sends back SYN/ACK
  - calculates a SYN cookie as: `t mod 32 || MSS`$_3$ `||` s_{24}
    - `t` is a timestamp (current time shifted right 6 positions)
    - MSS is Maximum Segment Size (3 bits)
    - `s` is the cryptographic hash of the server IP, server port, client IP, client port (24 bits)
  - server sends the SYN cookie as the TCP initial sequence number and throws away the SYN request (no queue and no resource allocation)
  - client must respond with final ACK where sequence number is `n+1` (`n`: server's sequence number)
  - server verifies
    - that `t` has not expired
    - recalculates and verifies `s`
    - decodes `m`
- use of circuit-level gateway firewall
  - the firewall creates connections on behalf of the server
    - for each received SYN request the firewall sends back SYN+ACK
    - sets a timer for the received SYN
    - if the firewall receives the client's final ACK then creates connection with server
- block ICMP echo request and reply
- disable ICMP directed broadcast on hosts

DoS/DDoS Attack Examples: Volumetric

- use of UDP and or ICMP flood to consume target network's bandwidth
- particularly takes advantage of reflection and amplification method
  - each node in a botnet sends a set of UDP messages to a UDP-based server (e.g. DNS, NTP, SSDP, etc.)
  - the UDP requests are small in size
  - the requests have spoofed source IP address of the target host/network
  - the UDP response will be larger in size and will be sent to the spoofed address
    - hence amplifies the effect by reflecting it off other servers
- the reflection and amplification techniques in latest DDoS attacks have reached TeraBytes per second bandwidth consumption

Examples

- Asymmetric request response (in size)
  - DNS `ANY` query generally results in a large response
    - DNS query: `dig @8.8.8.8 ANY monash.edu` is 81 bytes whereas the response in this case is 867 bytes (10x)
    - DNS query `dig @8.8.8.8 ANY nist.gov` is 79 bytes whereas the response is 2993 bytes (37x)
  - NTP `monlist` returns a list of recent clients that made a time query
    - using `nmap` script: `nmap -sU -pU:123 -Pn -n --script=ntp-monlist <target>`
    - to manually check on an ubuntu: `ntpdc -n -c monlist <target>`

Protection against Source Address Spoofing

- source IP address spoofing is used in reflect and amplify DDoS attacks
  - the request is small however the large response is sent to the spoofed address
- various protective measures can be used
  - Control Plane and BGP Security
    - preventing attacks against BGP that performs routing in Internet Backbone
  - Source Address Validation (SAV)
    - performed at the network edge by ISPs or large enterprises to prevent consumers/users systems use spoofed source IP
  - Monitor vulnerable applications to reflect and amplify attacks
    - limit access, rate limit, or disable certain features of the protocol

Appendix 1: BGP Attacks and Countermeasures

BGP Vulnerability: Prefix Hijack[2]

- when an Autonomous System (AS) accidentally or maliciously originates a prefix that it is not authorised to do
- in the following example the AS64510 is not authorised to announce the prefix `192.0.2.0/24`
  - this is referred to *prefix hijack* or *false-origin announcements*
- AS64500 is the authorised AS for `192.0.2.0/24` prefix

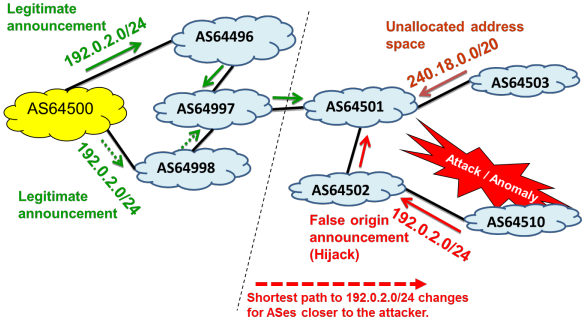


Figure 1: Illustration of Prefix Hijacking and Announcement of Unallocated Address Space.

- another issue is unauthorised announcements of unallocated address space
  - AS64503 originates `240.18.0.0/24` which is part of reserved address range `240.0.0.0/8`
  - an allocated but not yet used address space can also be announced by an unauthorised AS
    - this is referred to as *prefix squatting*

BGP Security[3]

Registration of Route Objects

- register all Internet Number Resources in appropriate Regional Internet Registries (RIR) registration database and POC information
  - e.g. address blocks, ASNs
  - should also reflect all sub-allocations to entities operating their own network services
    - e.g. enterprises, branch offices operating their Internet access, DNS etc.
- register and maintain route objects corresponding to BGP routes in appropriate RIR
  - Internet Routing Registries (IRRs) information must include all IP address space used by an enterprise (directly or outsourced)

Certification of Resources in Public Key Infrastructure

- Resource Public Key Infrastructure (RPKI) provides cryptographically-secured registries of Internet resources and routing authorisation
  - RFC 6480: An Infrastructure to Support Secure Internet Routing
  - RFC 6482: A Profile for Route Origin Authorizations (ROAs)

[3] Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation

Certification of Resources in RPKI[4]

- the IPv4/IPv6 address and AS numbers are allocated hierarchically
  - Internet Assigned Numbers Authority (IANA) allocates resources to RIRs (ARIN, RIPE, etc.)
    - RIRs sub-allocate to ISPs and enterprises
  - RPKI is a global CA and registry service offered by all RIRs
  - certificate chain then follows the same hierarchy

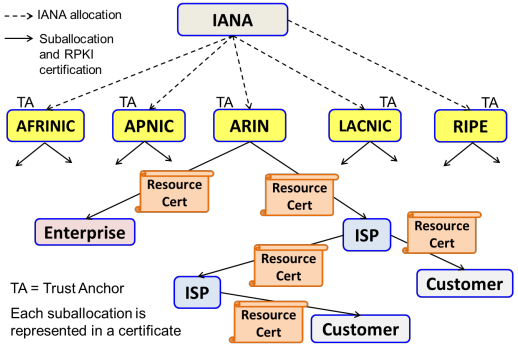


Figure 4: Illustration of resource allocation and certificate chain in RPKI.

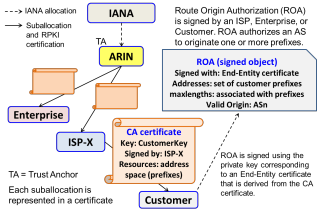
- The resource (IPv4/IPv6 addresses and ASNs) holders should obtain a certificate for their resources
- Transit providers should create, publish, and manage subordinate resource certificates for their customers

[4] S. Sriram et al. "Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation

RPKI is based on X.509 standard and RFC 3779 extension that defines a special certificate [RFC5280] to bind Internet number resources (prefixes and ASN numbers) [RFC6487] [RFC5771]. As shown in Figure 4, the RIRs issue resource certificates, called Certificate

BGP Origin Validation (BGP-OV)[5]

- prefix owner uses the obtained certificate to generate an End-Entity (EE) certificate
  - the associated private key of the EE certificate is used to digitally sign Route Origin Authorisation (ROA)
    - RFC 6482: A Profile for Route Origin Authorizations (ROAs)
    - RFC 6811: BGP Prefix Origin Validation
    - RFC 8481: Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)
  - the ROA declares an AS as an authorised originator of BGP announcements for that prefix
    - ROA can also be generated by an ISP for its customer (as part of their service agreement)
- RPKI validating servers can access RPKI data from repositories
  - a BGP router accesses ROA data from RPKI validating (cache) servers
    - this mitigates the risk of prefix hijack as announcements can be verified



the complete list of security recommendations discussed in NIST SP 800-189 for BGP-OV is rather complex (3 out of 36 security recommendations are discussed here)

[5] Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation

Source Address Validation (SAV) Techniques

Using ACL

- is performed in network edge devices such as the perimeter router, DSLAMs, Packet Data Network gateways
- Ingress/egress Access Control List are employed to detect and drop spoofed source addresses
  - check the source addresses against either acceptable or unacceptable prefixes
  - e.g. compromised customers of an ISP
    - Mirai botnat[6] of compromised IoT devices and home routers etc. were used to attack Dyn services in 2016[7]
  - ACLs need to be kept up to date
    - can be operationally expensive/difficult

Using a variant of Unicast Reverse Path Forwarding (uRPF)

- a Forwarding Information Base (FIB) is maintained by the border router
- the source address of an ingress packet at border router is checked using one of the various uRPF methods
  - Strict, Feasible-Path, Loose, Enhanced Feasible-Path

[6] Mirai: what you need to know about the botnet behind recent major DDoS attacks

[7] Analysis Summary Of Friday October 21 Attack

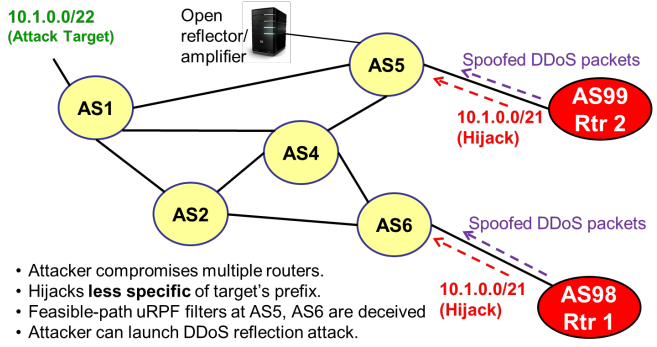
uRPF Methods[8]

- **Strict uRPF**: (ingress) packet at (border) router is accepted if the best routing path in FIB for the source address of the packet points to the interface the packet is coming from
  - creates problem with multi-homed customers (connected to two or ISPs)
- **Feasible-Path uRPF**: similar to strict however instead of having only one entry in FIB there will be additional entries for multi-homed customers
  - packet source address matches one of the entries
- **Loose uRPF**: packet is accepted if a route is found in FIB
  - not effective against IPv4 as almost all addresses appear in global routing table
- **Enhanced Feasible-Path**: is a work in progress
  - checks the source address against all authorised prefixes

[8] Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation

Combination of BGP-OV and SAV[9]

- combining BGP-OV and SAV (uRPF) techniques provides a stronger defence against source address spoofing
  - an (skilled) attacker can subvert uRPF techniques by performing prefix hijack and then perform source address spoofing using the hijacked prefix



- BGP-OV will prevent the prefix hijacking
- feasible-path uRPF will prevent source address spoofing

[9] Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation

References

The materials in this document are reproduced, at times without modification, from the following sources:

- NIST SP 800-189-draft: Secure Interdomain Traffic Exchange, BGP Robustness and DDoS Mitigation
- Dyn Analysis Summary Of Friday October 21 Attack
- DDoD Quick Guide
- CVE-2019-11683

Other Articles

- Amplification Hell: Revisiting Network Protocols for DDos Abuse
- Alert (TA14-017A) UDP-Based Amplification Attacks