Service: Denied!

CMSC 414

November 20, 2017

What is Denial-of-Service?

Any restriction of *access to a resource* by *legitimate principals*

Violates the property of *Availability*

Might be a single server

Might be a large part of the network infrastructure

Not excluding unauthorized principals

Does not require authentication

Motivation

Why does someone launch a denial-of-service?

- Laughs
  Hey, look what I can do!
- Spite/Revenge
  MegaCorp made me mad!
- Competitive advantage
  Our sales are down—let's kill our competitor's webstore!
- Extortion
  We'll let you do business again if you pay us...1 million dollars!
- Political/social statement
  GreedCo stands for greed!
- Civil disruption
  Our enemies will be in a panic without their search engine!

Types of DoS

Any attack on Availability is a Denial-of-Service attack

Targets vary:

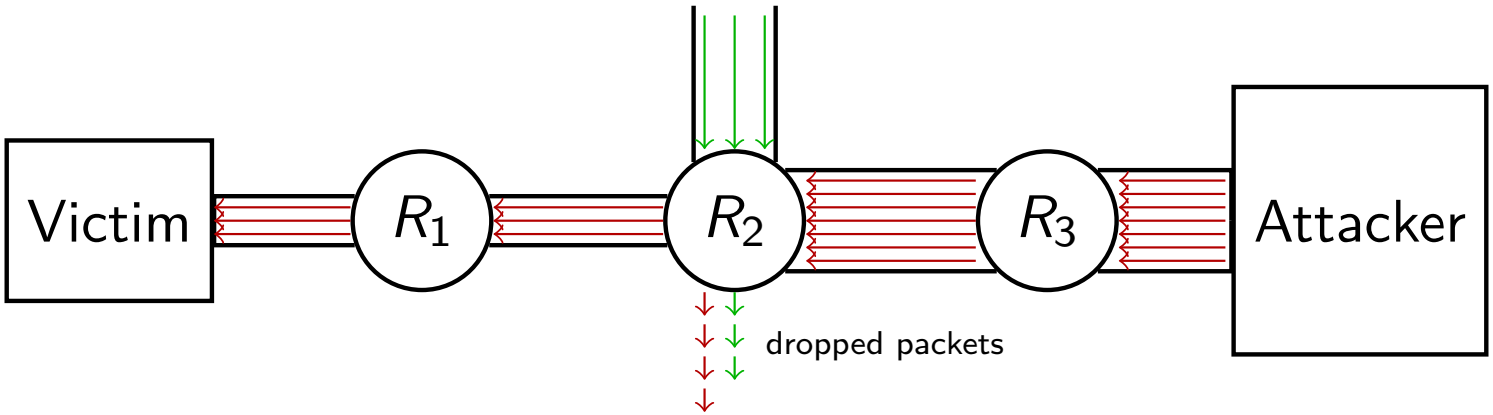
- Single user
  Send bad passwords enough times to get account locked
- Single service/host
  Crash a server or process; Exhaust disk/memory
- Entire subnet/network
  Incapacitate routers, switches, or links

Techniques also vary:

- Low-volume $\Rightarrow$ *Single/few messages*
- High-volume $\Rightarrow$ *Flooding*

How Does Flooding Work?

[The] Internet is not something that you just dump something on. It's not a big truck. It's a series of tubes. —Sen. Ted Stevens



Attacker overwhelms some node on the path towards a victim

Legitimate traffic through that node can't get through

Internet Control Message Protocol

Used for error messages and network status signalling

IP protocol 1

Ping is ICMP types 8 (Echo Request) and 0 (Echo Reply)

Traceroute uses type 11 (Time Exceeded) to learn routers

ICMP has an 8-byte header and variable-sized payload

Popular vector for DoS attacks

Ping Flood

Simple idea ⇒ Send lots of ping packets to victim

Don't bother waiting for responses
⇒ Spoof the source, and responses won't come back to you

Requires attacker having more bandwidth than the victim
⇒ *No amplification factor*

Can still be useful, as we'll see

A lot of networks block external pings
⇒ *Other ICMP types can't be blocked, though!*

General spoofed ICMP floods often called *Twinge attacks*

Group Exercise 1

We'll use the `spoof` repo from a previous class, but now you're going to *have* to work with other people at your table. Run `git pull upstream master` to get the new version of the README.

Poison Packets

A **Poison Packet** is a malformed IP packet designed to disrupt a host or service

Exploits specific implementations

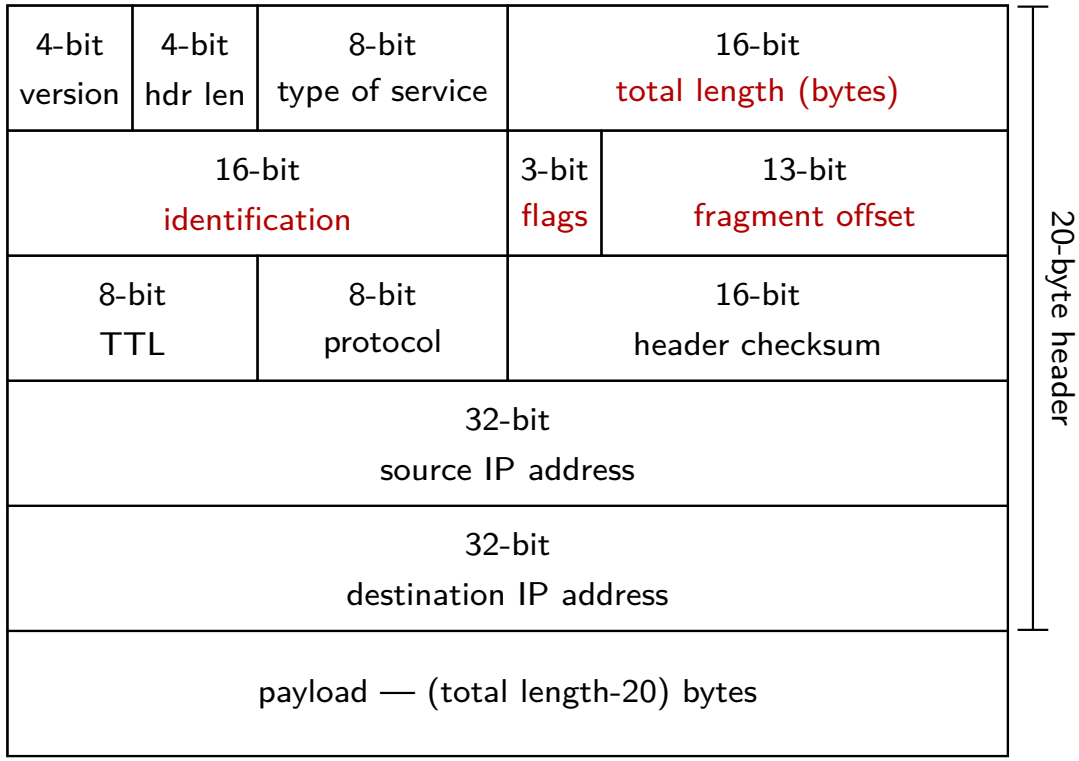
- Poor assumptions
- Bugs

Different protocols vulnerable

Before we look at some, a brief digression...

IP Packet Fragmentation

Our old friend:



Packets can be up to $2^{16} - 1$ bytes

Most links can't handle more than 1500 bytes

$\Rightarrow$ Maximum Transmission Unit (MTU)

IP Packet Fragmentation

Router R receives a packet p on interface a

Forwarding table indicates interface b as next hop

b has an MTU less than the length of p

R has to break p into **fragments** no larger than b's MTU

All fragments have same *identification* header

More Fragments in packet indicated in *flags* header

First payload byte specified by *fragment offset*

Ping of Death

The fragment offset isn't actually in bytes

It's really in 8-byte chunks

We can have $2^{13} - 1$ as the maximum offset value, but this means byte $(2^{13} - 1) \times 8 = 65528$

The largest (reconstructed) packet can be $2^{16} - 1 = 65535$ bytes
$\Rightarrow$ Last fragment can be at most 7 bytes of payload

If we make this fragment 8 bytes or longer $\Rightarrow$ reconstructed packet size exceeds max value

Can cause buffer overflows in network stack!

Local Area Network Denial (LAND)

IP payload starts with TCP header

⇒ First two bytes are *source port*, next two are *destination port*

Spoofed SYN packet (ignoring everything after ports):

<table>
<tr><td>4-bit
version</td><td>4-bit
hdr len</td><td>8-bit
type of service</td><td colspan="2">16-bit
total length (bytes)</td></tr>
<tr><td colspan="3">16-bit
identification</td><td>3-bit
flags</td><td>13-bit
fragment offset</td></tr>
<tr><td colspan="2">8-bit
TTL</td><td>6 (TCP)</td><td colspan="2">16-bit
header checksum</td></tr>
<tr><td colspan="5">source IP address
1.2.3.4</td></tr>
<tr><td colspan="5">destination IP address
1.2.3.4</td></tr>
<tr><td colspan="3">souce port
80</td><td colspan="2">destination port
80</td></tr>
</table>

Victim tries to handshake with itself ⇒ Overwhelms network stack!

INVITE of Death

Voice-over-IP (VoIP) increasingly popular

- Individuals can make long-distance calls cheaper
- Companies can have more features and configurability

Session Initiation Protocol (SIP) establishes connections between VoIP endpoints

Via field of SIP INVITE message vulnerable to buffer overflow
$\Rightarrow$ Bug in popular implementation (since fixed)

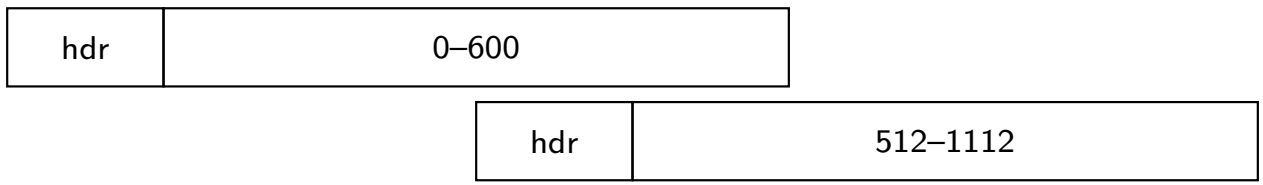
Other fields vulnerable in other implementations

Can cause DoS, as well as potentially other problems

IP Fragmentation Attacks

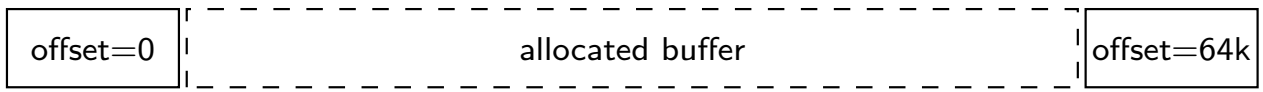
In addition to the Ping of Death, other attacks can employ packet fragmentation

Overlapping fragments might trigger bugs in reconstruction logic



⇒ *Teardrop attack*

Incomplete packets due to missing fragments consume buffer space, which might exhaust memory



⇒ *Rose attack*

Distributed Denial-of-Service

Single-source DoS has limited power

Can send poison packets, but flooding expensive for attacker
$\Rightarrow$ Also requires a very good network connection

Distributed Denial-of-Service (DDoS) uses **zombies** for attack
$\Rightarrow$ Attacker doesn't need to actually send attack traffic

Gives attacker massive *amplification factor*

Attack can come from all over the Internet
$\Rightarrow$ Much harder to filter out

As Internet grows, pool of potential zombies grows
$\Rightarrow$ Poorly secured gadgets make this even worse
(cf. *Viruses and Other Malware*)

Smurf Attack

Simple ICMP Echo DDoS

Uses spoofed pings, flooding victim

Exploits networks responding to broadcast pings
$\Rightarrow$ Every host in network receives ICMP Echo Request

Popular in late 1990's

Can be mitigated by rejecting broadcast ICMP Echo Request at gateway

Individual hosts can also ignore these

LOIC/HOIC

Low Orbit Ion Cannon and **High Orbit Ion Cannon**

Bots added voluntarily

Typically uses TCP and UDP, not ICMP

Used to stress-test networks

Used by Anonymous in DDoS attacks

Project Chanology Attacks against Church of Scientology and Recording Industry Association of America

Operation Payback Attacks against opponents of WikiLeaks

Operation Megaupload Retaliation attack for shutdown of Megaupload

Group Exercise 2

In the same repository, look at Denial-of-Service Exercise 2. We're going to extend the previous exercise to perform a DDoS against the Victim!