Kapitel 7: DoS

7: Denial of Service (DoS) Angriffe

- Angriff versucht, das Zielsystem oder Netzwerk für berechtigte Anwender unbenutzbar zu machen, z.B. durch
  - Überlastung
  - Herbeiführen einer Fehlersituation
  - Ausnutzung von Programmierfehlern
  - Ausnutzung von Protokollschwächen

- (Asymptotischer) Aufwand des Angreifers **A**, ist signifikant kleiner als der des Ziels **Z**.

- Häufige Arten von DoS-Angriffen
  - Anforderung bzw. Nutzung beschränkter Ressourcen (CPU-Zeit, RAM, Plattenplatz, Bandbreite, . . .)
  - Zerstörung oder Veränderung der Konfiguration
  - Physische Zerstörung oder Beschädigung

DoS Angriffe: E-Mail und Fax

- E-Mail Bombing
  Überflutung der Inbox mit Mails.
- Mailstorm
  Konfigurierte "out of office" Mail mit CC: an interne Mailingliste, und aktiviere die automatische Bestätigung durch Empfänger.
- E-Mail Subscription Bombing
  Opfer wird auf hunderten Mailinglisten registriert.
- Fax Bombing
  (Schwarzes Papier zu einer Rolle zusammenkleben und faxen.)

Beispiele für einfache DoS Angriffe

- Membomb

```
while(malloc(long int));
pause();
```

- Forkbomb

```
while(1) fork();
```

- Floodping

```
# sudo ping -f <ip-address>
```

Java Beispiel

```
import java.util.List;
import java.util.LinkedList;
import java.lang.Thread;
import java.lang.OutOfMemoryError;

class Foo {
  static  List<Integer> l;

  public static void main(String args[]) throws Exception{
    try {
      l = new LinkedList<Integer>();
      int i=0;
      while(true) l.add(i++);
    } catch(OutOfMemoryError e) {
      Thread.currentThread().join();
    }
  }
}
```

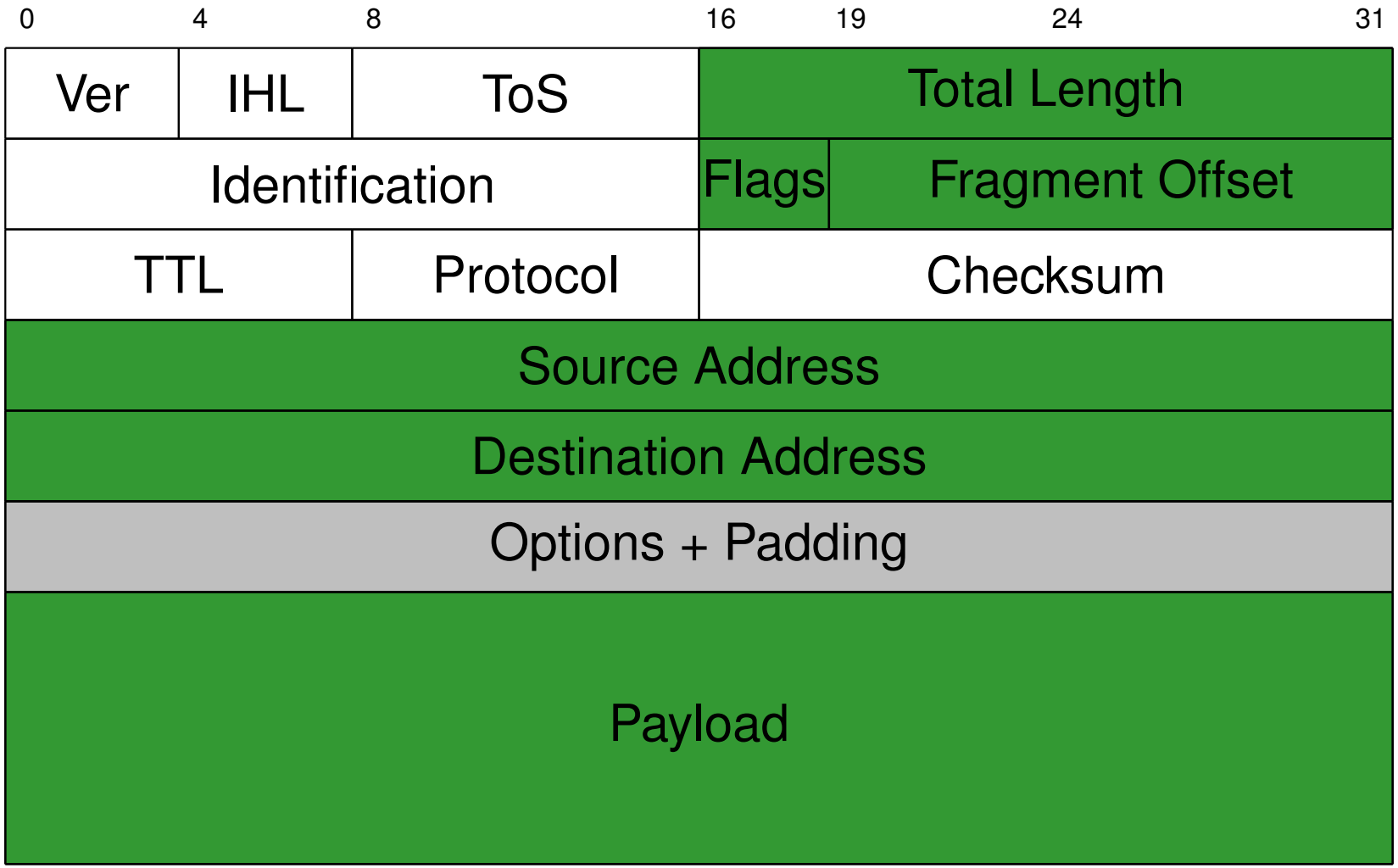
7.1: Mini-Exkurs: Netzwerkprotokolle

- Internet Protokol (IP, Netzwerkschicht (L3))
- Zur Übemittelung eines Datenpaketes an einen Host.

- Internet Control Messages Protocol (ICMP, Netzwerkschicht (L3))
- Kontrollnachricht für einen Host

- Transmission Control Protocol (TCP, Transportschicht (L4))
- Datenverbindung zu einer bestimmten Anwendung auf einem Host

IP-Header


0
4
8
16
19
24
31
Ver
IHL
ToS
Total Length
Identification
Flags
Fragment Offset
TTL
Protocol
Checksum
Source Address
Destination Address
Options + Padding
Payload

IP-Pakete und Fragmentierung

- Die Maximale Größe eines IP-Paketes ist $2^{16} - 1$ bytes.
- **Warum?**
- Die Maximale Paketgröße der Vermittelungsschicht (Layer 2) ist meist kleiner.
  - Ethernet MTU: 1500 bytes
  - 802.11: 2312 bytes
- Größe des IP-Paketes $>$ Max. Paketgröße des Layer 2 Protokols.
- $\Longrightarrow$ das IP-Paket wird fragmentiert oder verworfen.
- Maximum Transmission Unit (MTU)
- Maximale Größe eines IP-Paketes, das ohne Fragmentierung zugestellt wird.

Vorgehensweise bei der IP-Fragmentierung

- Bei der Fragmentierung wird ein IP-Paket in mehrere kleine aufgeteilt
- Alle Fragmente haben die ID des orginal IP-Pakets
- Bis auf das letzte Fragment haben alle das More Fragment (MF) Flag gesetzt.
- Der Offset wird in 8 byte (64 bit) Blöcken angegeben.
  - Länge es Payloads eines Fragmentes: Vielfaches von 8 Bytes.
  - Ausnahme: Letztes Fragment.

Beispiel: IP-Fragmentierung

Aufgrund der MTU ist die Größe das Payloads auf 50 Bytes beschränkt.

Orignalpaket

ID	Offset	MF	Payload
123	0	0	100

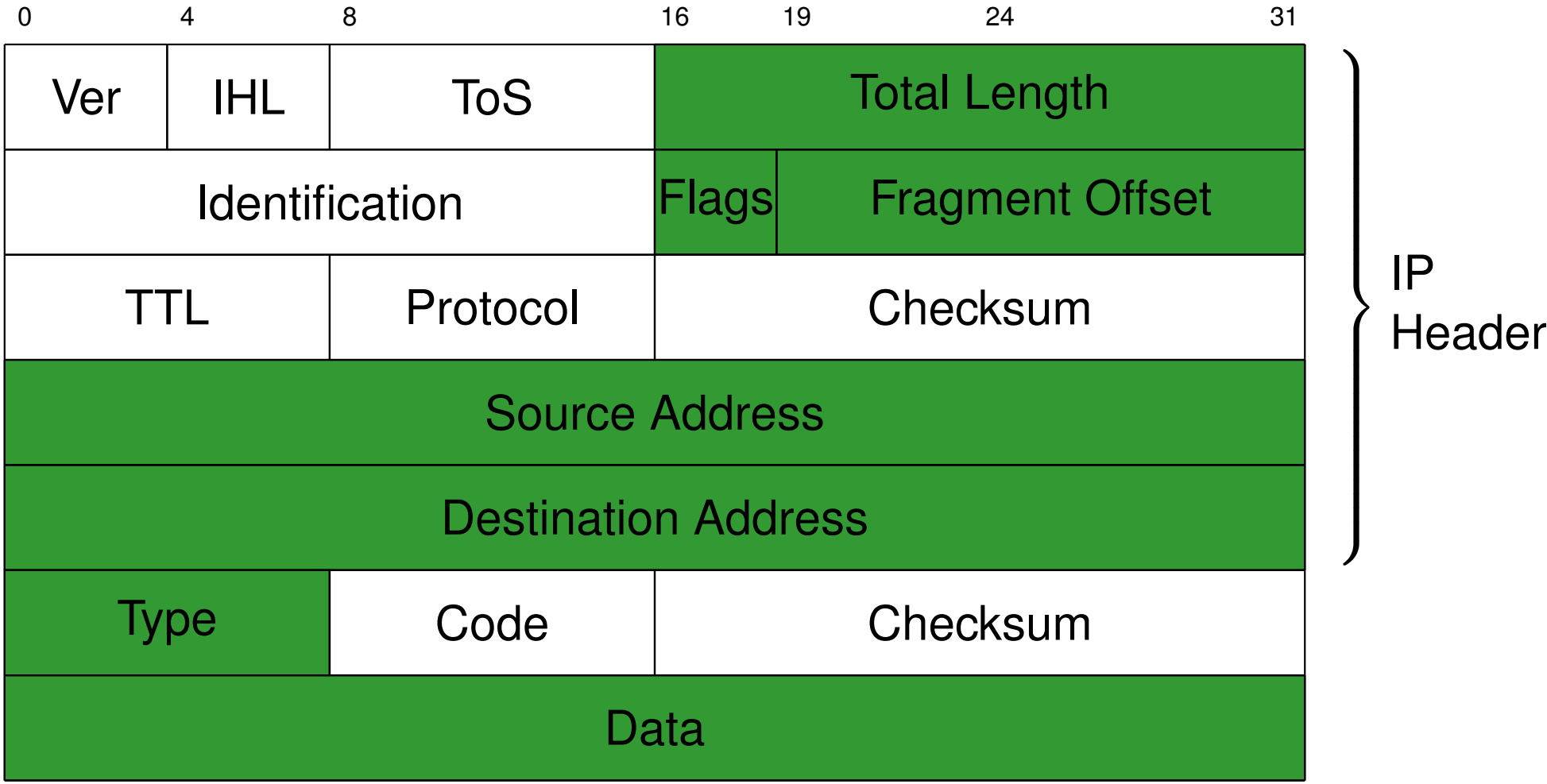
Fragmente

ID	Offset	MF	Payload
123	0	1	48

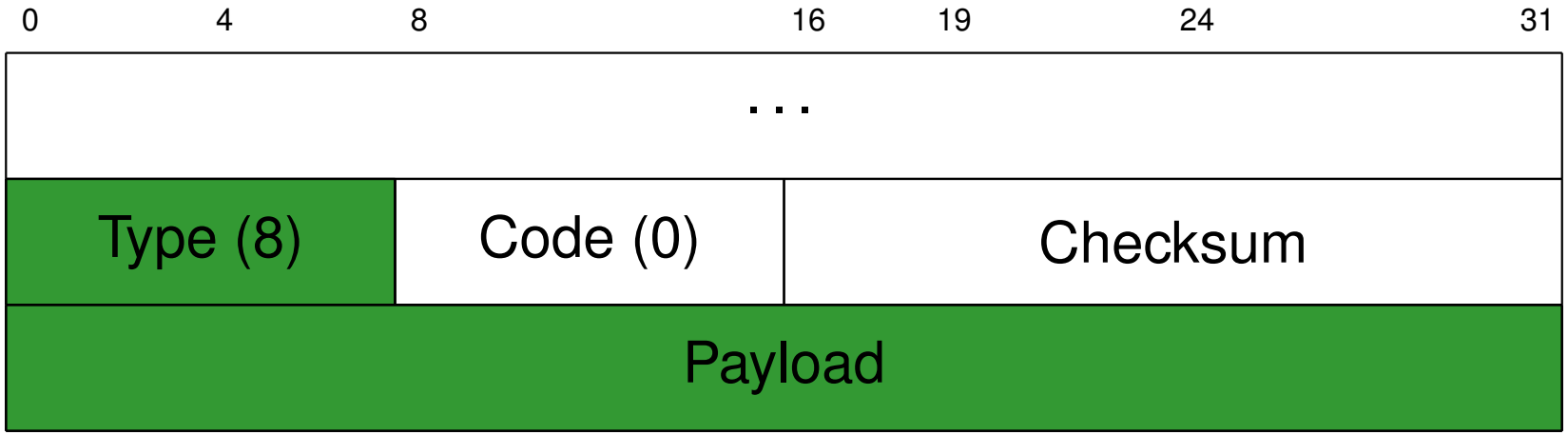
ID	Offset	MF	Payload
123	6	1	48

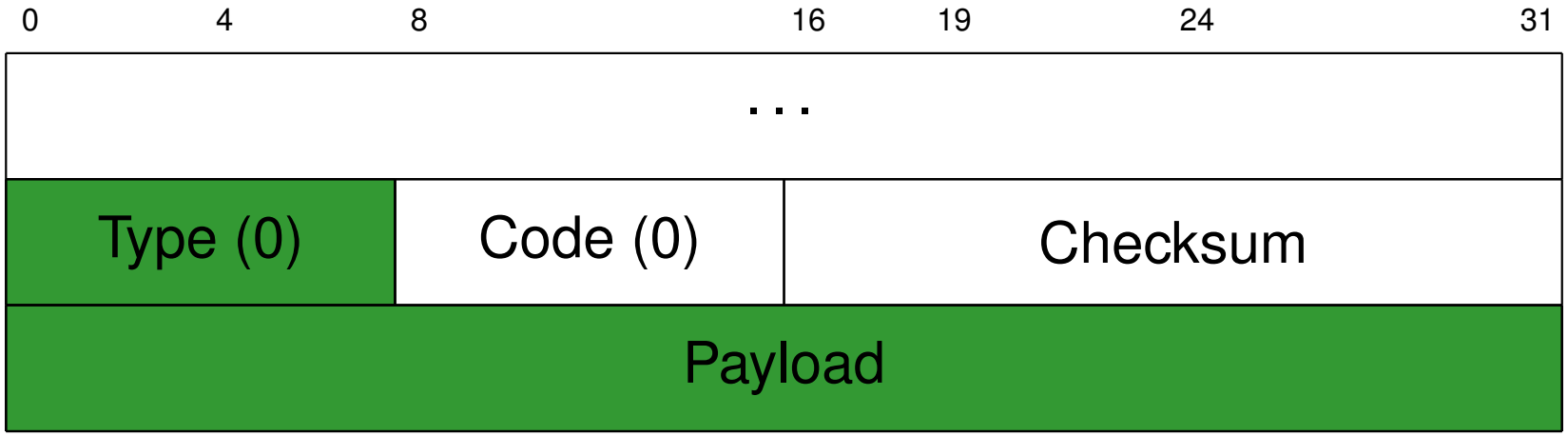
ID	Offset	MF	Payload
123	12	0	4

ICMP-Header

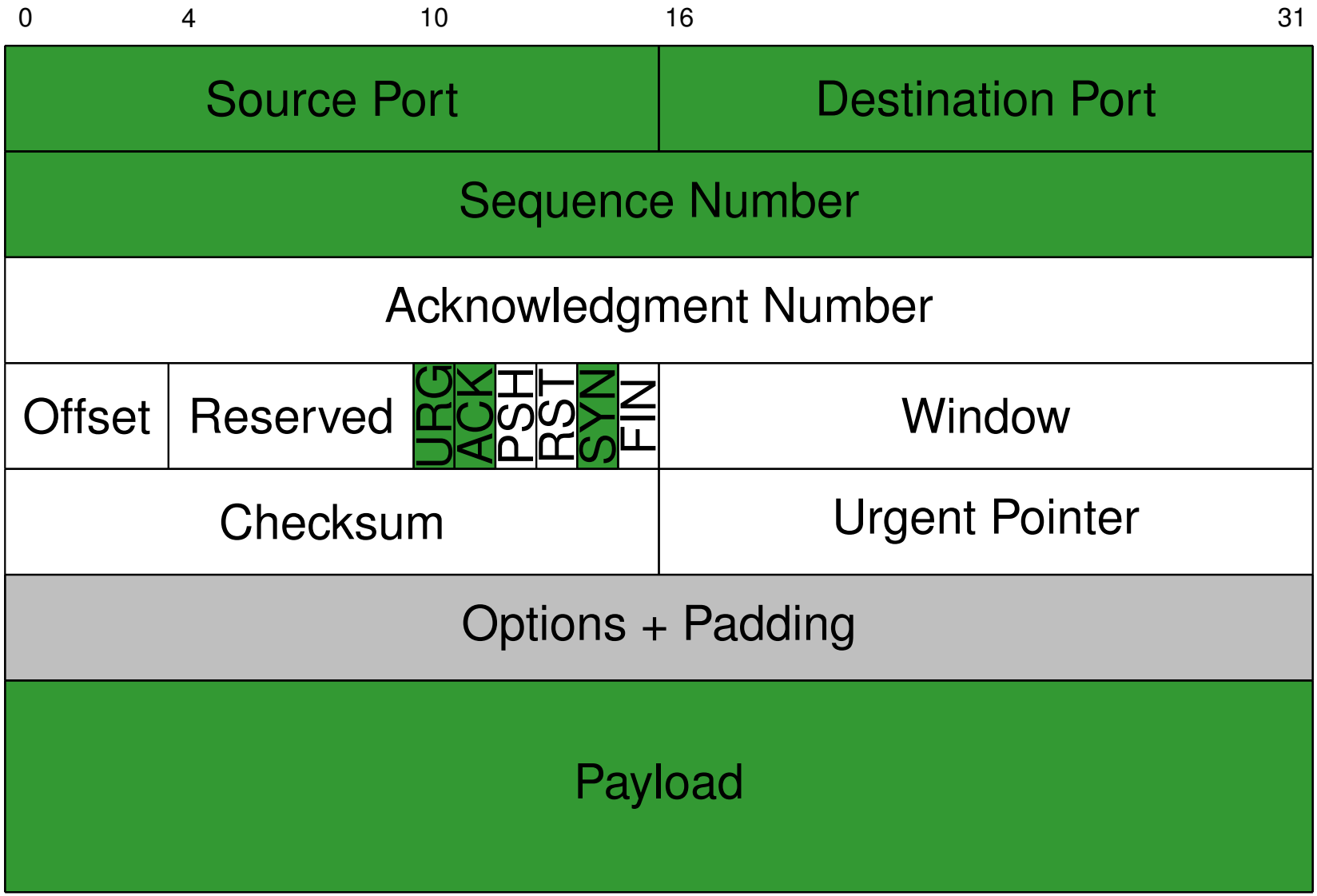

0
4
8
16
19
24
31
Ver
IHL
ToS
Total Length
Identification
Flags
Fragment Offset
TTL
Protocol
Checksum
Source Address
Destination Address
Type
Code
Checksum
Data
IP Header

Beispiel: ICMP-Echo Request und Reply (Ping)

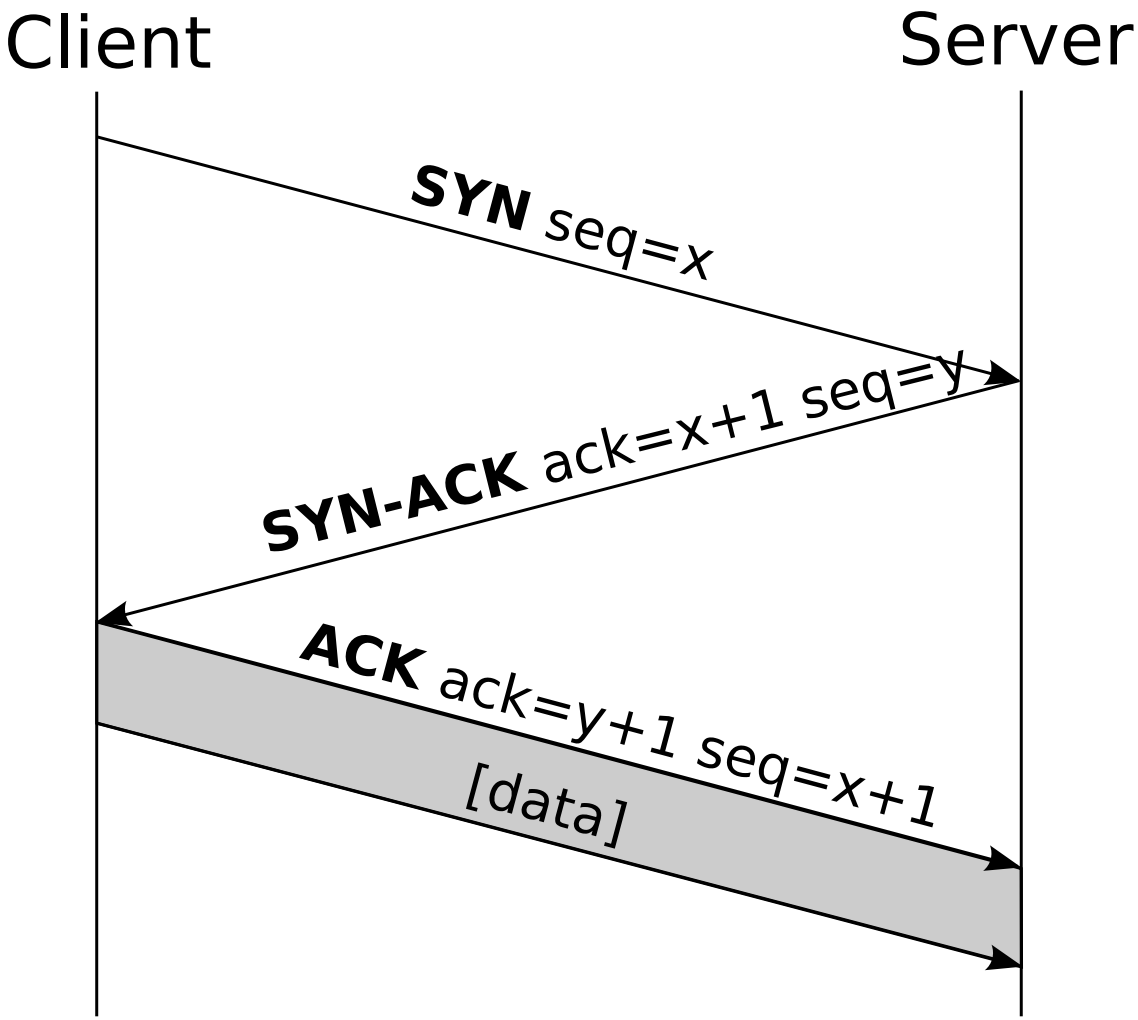




TCP-Header

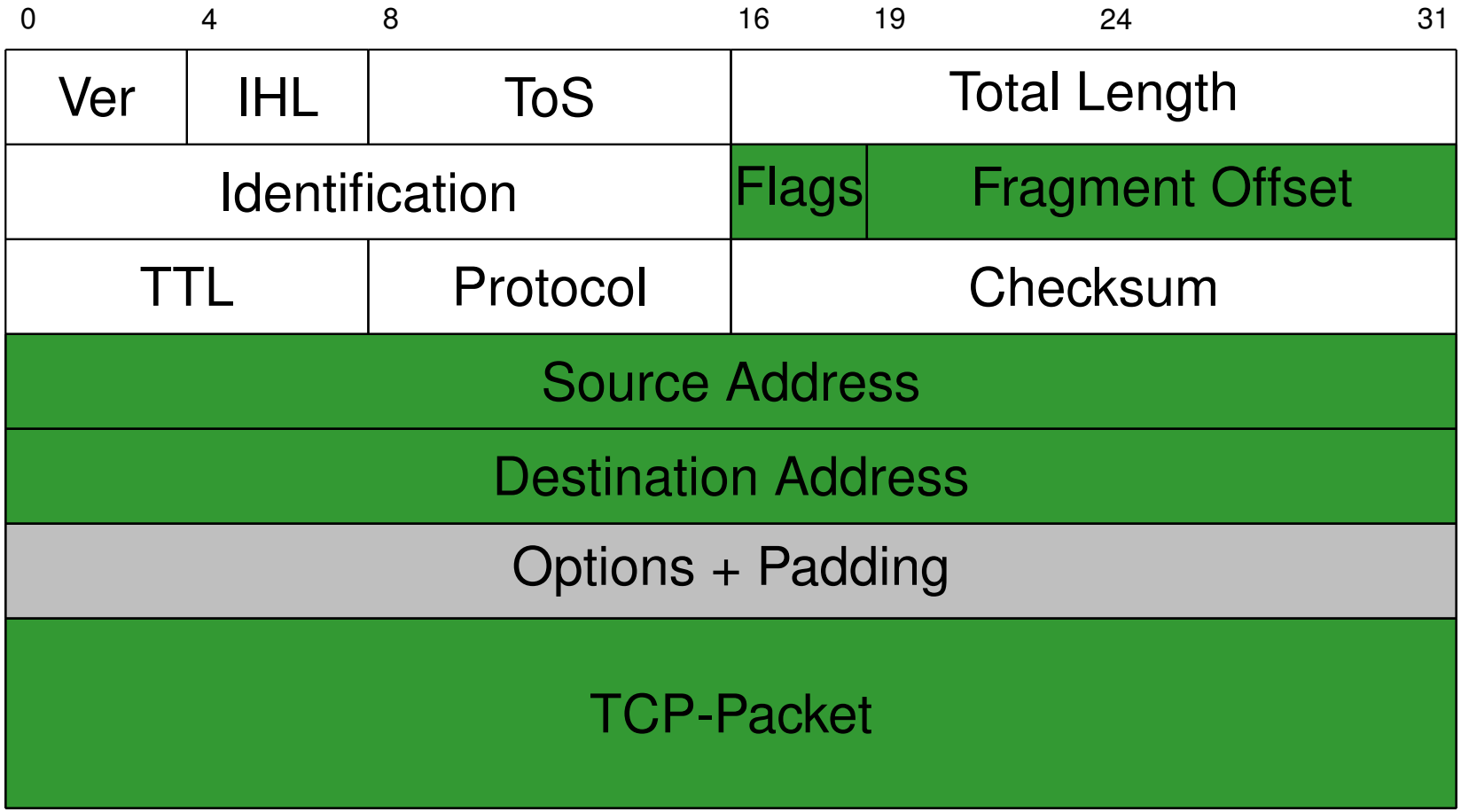

0
4
10
16
31
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window
Checksum
Urgent Pointer
Options + Padding
Payload

TCP-Verbindungsaufbau



Quelle: `https://de.wikipedia.org/wiki/Transmission_Control_Protocol`

TCP/IP Paket



Ein TCP/IP-Paket ist ein Netzwerkpaket bei dem der Payload des IP-Paketes ein TCP-Paket ist.

LAND (Local Area Network Denial, 97)

- Schwachstelle betraf viele Betriebssysteme
  (AIX, FreeBSD, Mac OS, NetBSD, SunOS, Windows, . . .)
- Schwachstelle betraf auch einige Cisco Router.
- Senden eines gefälschten TCP/IP SYN-Paket mit
  - Source Address = Destination Address und
  - Source Port = Dest. Port.
- Rechner antwortet sich selbst mit einem SYN-ACK-Paket.
- Durch Fehler wird dieses Paket als SYN-Paket betrachtet.
- Folge: 100% CPU Last.
- Gegenmaßnahme: Firewall-Regel um LAND-Pakete zu blockieren.

Teardrop, 97

- Schwachstelle betraf Windows NT 4.0, Win95 und Linux bis 2.0.32
- Überlappende IP-Fragmente durch Manipulation des Fragment Offset.
- Erstes IP-Fragment mit *N* Bytes Nutzdaten
- Weiter IP-Fragmente mit wenig Nutzdaten und einem Offset zu kleinen Offset.
- Ursprüngliches IP-Paket konnte nicht mehr rekonstruiert werden.
- Folge: Absturz oder Reboot des Betriebssystems.
- Gegenmaßnahme: Entsprechenden Patch einspielen.

Beispiel: Teardrop

ID	Offset	MF	Payload
456	0	1	48

ID	Offset	MF	Payload
456	2	1	48

ID	Offset	MF	Payload
456	5	0	2

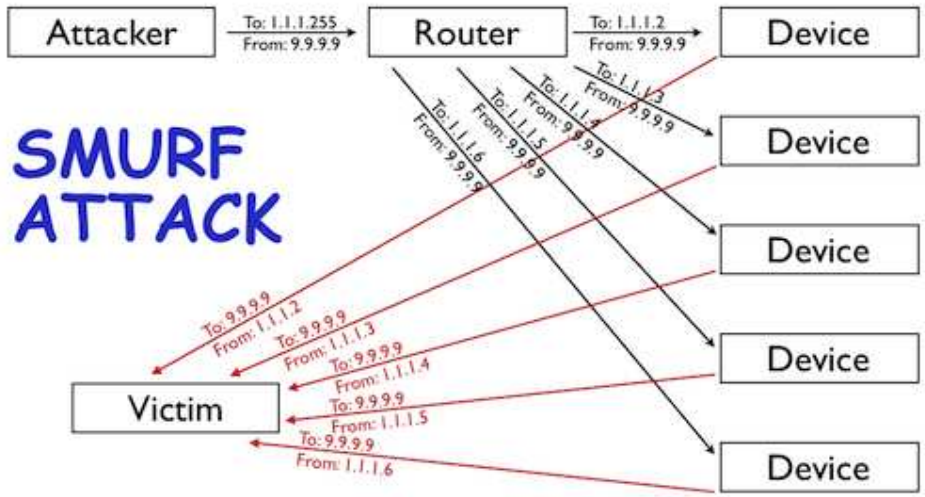
WinNuke, 97

- Schwachstelle betraf Windows 3.x/95/NT.
- Verbindung zu TCP-Port 139 (NetBIOS)
- Sende eine Out-Of-Band (OOB) Paket.
  (TCP-Paket bei dem das `URG`-Flag gesetzt ist.)
- Folge: Blue Screen of Death.

Ping of Death, 98

- IP-Paket das größer als die max. erlaubte 2^{16} (65.536) Bytes ist.
- `C:\\ping -l 65510 <hostname or ip>`
- IP Header + ICMP-Header + Payload $> 2^{16}$.
- Schwachstelle betraf viele Betriebssysteme
  (AIX, Mac OS, Linux, HP-UX, NEXTSTEP, Solaris, Windows, . . .)
- Übertragen in mehreren Fragmenten; andernfalls würden die Router das Paket verwerfen.
- Reassemblieren der Fragmente im Zielsystem führt zu Überlauf des internen Puffers im IP-Stack.
- Folge: Absturz oder Reboot des Betriebssystems.
- Gegenmaßnahme: Firewall-Regel die ICMP-Request blockiert.

Smurf Angriff

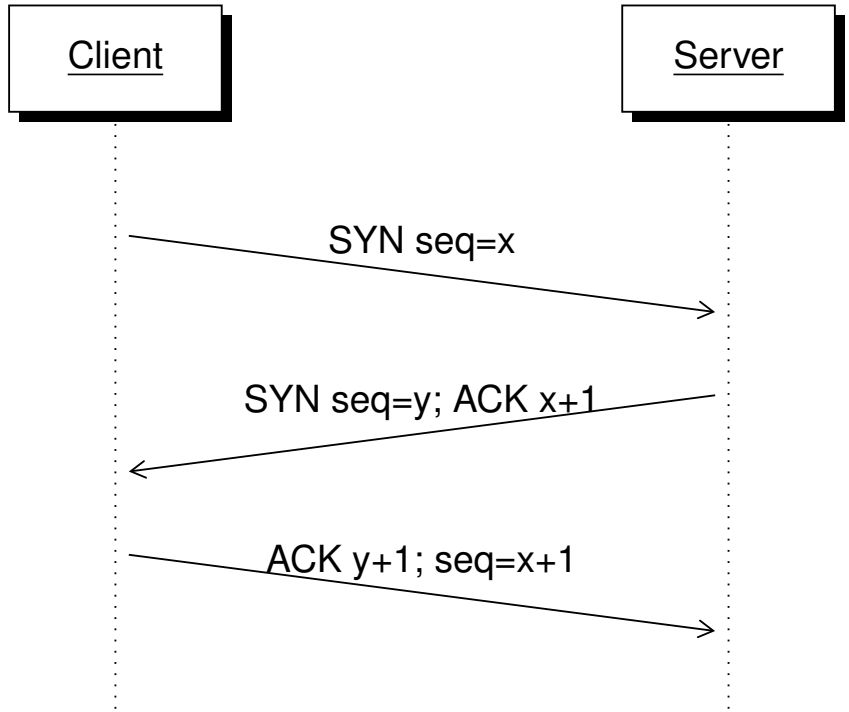


- **A** sendet *ICMP-Echo Request*-Paket (Ping), mit Absender IP von **Z**, an die Broadcast-Adresse eines Netzwerkes.
- Alle Rechner des Netzwerkes antworten mit *Echo-Reply*.
- Bei Netzwerken mit vielen aktiven Rechnern kann eine Flut von solchen Broadcast-Pings Netzwerk oder OS von **Z** überlasten.
- Gegenmaßnahme: Firewall Regel die Broadcast-Pings blockiert.

TCP-Verbindungsaufbau

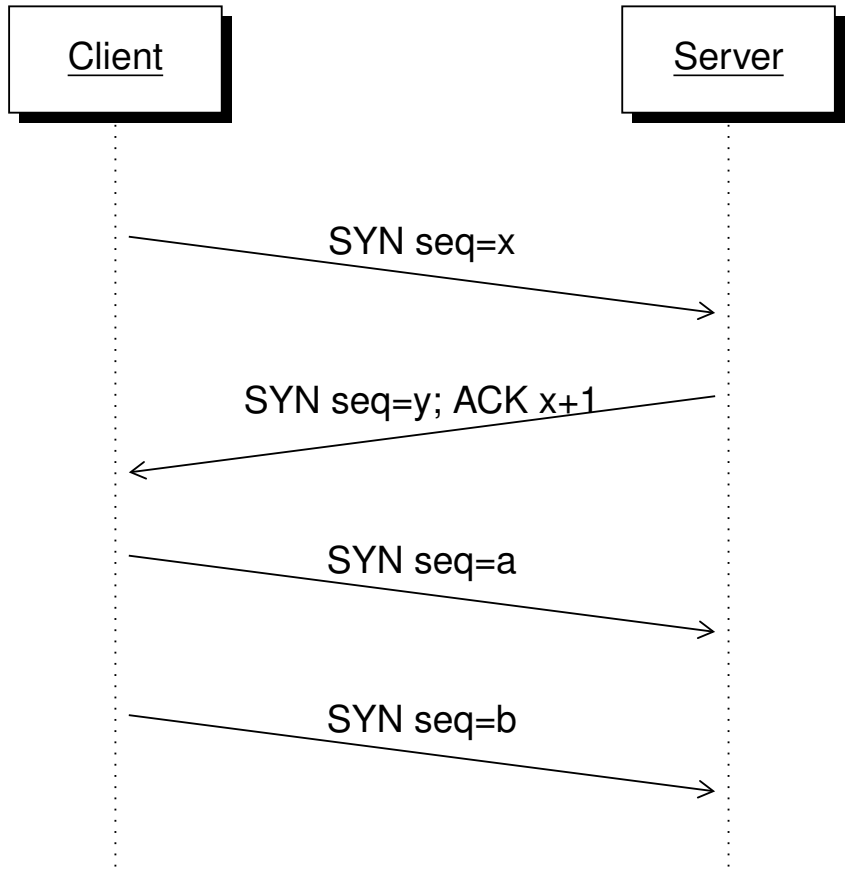
Drei-Wege-Handschlag

1. Der Client möchte eine Verbindung aufbauen und schickt ein SYN-Pakete an den Server.
2. Der Server allokiert die entsprechenden Ressourcen und stimmt dem Verbindungsaufbau mittels einem SYN-ACK-Paketes zu.
3. Durch das Senden eines ACK-Paketes bestätigt der Client den Aufbau der Verbindung.



SYN-Flooding

- "Halboffene" TCP-Verbindungen so lange aufbauen, bis Ressourcen des Servers erschöpft sind.
- Der Server kann dann keine weiteren Netzverbindungen mehr aufbauen.



SYN-Flooding: Gegenmaßnahmen

- Falls ACK nicht innerhalb einer bestimmten Zeitspanne erfolgt, werden die Ressourcen wieder freigeben.
- Falls alle Ressourcen belegt sind, wird zufällig eine halboffene Verbindung geschlossen.
- Maximale Anzahl gleichzeitig halboffener Verbindungen pro Quell-Adresse festlegen.

Die Gegenmaßnahmen sind nur von bedingtem Nutzen.

SYN Cookies, (Dan Bernstein, 1996)

Sequenz Nummer y des Servers „kodiert“ Adressinfo des Clients. Dadurch ist der Server in der Lage Ressourcen zu allokieren nachdem das ACK $y + 1$ des Clients eingeht.

7.2: Distributed Denial of Service (DDoS)

Grundidee eines DDoS-Angriffes

DoS-Angriffswerkzeuge werden auf mehrere Maschinen verteilt und führen auf Befehl eines Masters Angriff durch.

Terminologie

- Intruder oder Attacker: Angreifer (Person)
- Master oder Command & Control (C&C) Server: Koordinator des Angriffs (Software)
- Daemon, Agent, Client, Zombie, Bot oder bcast-Programm: Einzelkomponente, die Teil des DDoS durchführt (Software)
- Victim oder Target: Ziel des Angriffs

Historie

- Aug. 99: 227 Clients greifen eine Maschine der Uni Minnesota an.
- Schaden: 2 Tage Down-Zeit
- Feb. 2000: Mafiaboy (15 Jahre) startet DDoS-Angriff auf Yahoo!, Amazon, CNN und andere.

  Schaden: Mehrere Stunden Down-Zeit.
- Sep. 2016: Mehr als 145.000 "gehackten" Überwachungskameras (ca. 620 Gbps) greifen den Blog KrebsOnSecurity an.
- Feb. 2018: Mehrere Tausend Hosts (1.35 Tbps) greifen Github an.

  Schaden: ca. 5 Minuten Down-Zeit.
- 2017: Amazon nimmt in 5 Minuten ca. 1,4 Million EUR ein.

DDoS as a Service

- Ox-booter bietet am 17. Oktober 2018 DDoS als Service (Webapp) an.
- Behauptung: 500 GB/s Traffic mit 20.000 Bots.
- Preise (inklusive 24/7 Support)
  - 1 x 15 Minuten DDoS Angriff: 20 USD
  - 2 x 60 Minuten DDoS Angriff: 100 USD
  - 2 x 120 Minuten DDoS Angriff: 150 USD
- Testergebnisse: 424.825 GB/s mit 16.993 Bots.

Quelle: `https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet-.html`

DDoS: Grundsätzlicher Ablauf

Dreistufiges Verfahren

1. Intruder kompromittiert initialen Server und installiert Hacking-Werkzeuge, Scanner, Rootkits und DoS/DDoS-Tools.
   $\Longrightarrow$ Rechner wird Master.

2. Master versucht automatisiert, weitere Maschinen zu kompromittieren, um DDoS-Software (Daemon) zu installieren, bzw. schiebt anderen Nutzern Malware unter.

3. Intruder startet Programm auf Master, das allen Daemonen mitteilt, wann und gegen wen der Angriff zu starten ist. Zum vereinbartem Zeitpunkt startet jeder Daemon DoS-Angriff

Trinoo – Ein Verteilter UDP Flooding Angriff, 1999

- Der Master ist in C geschrieben (430 LOC)
- Lauscht auf UDP-Port 31335 auf Daemon Nachrichten.
- Steuerung über TCP-Port 27665 (Passwort `betaalmostdone`.)
- Die wichtigstens Master-Commands:
  `die`, `mtimer <T>`, `mdie <pwd>`, `mdos <ip1:ip2:ip3>`, `msize <S>`, `killdead`, `bcast`,
- Der Trinoo daemon is ebenfalls in C geschrieben (166 LOC).
- Lauscht auf UDP-Port 27444.
- Eingehende Befehle werden mit dem Passwort "44adsl" autorisiert.
- Beim Start wird eine `*HELLO*` Nachricht an den Master gesandt.
- Keep-Alive-Kommunikation:
  - Master $\rightarrow$ Daemon: `png`
  - Daemon $\rightarrow$ Master: `PONG`
- Wenn aktiv, bombadiert der Daemon das Opfer mit einer Flut an UDP-Pakete (zufällige Ports, default 120 sec).

Tribe Flood Network (TFN), 1999

- Master kompromittiert UNIX-Systeme über RPC-Buffer-Overflow
- Unterstützt SYN-, ICMP-, UDP-Flooding und den SMURF-Angriff.
- Master wird per Kommandozeile bedient.
- Kommunikation wird vollständig in *ICMP-Echo* und *ICMP-Replay* Nachrichten *versteckt*.
- Beispielsweise werden Kommandos im Identifier-Feld eines ICMP Paketes kodiert,
  - 345 $\rightarrow$ SYN-Flooding.
  - 890 $\rightarrow$ UDP-Flooding.
- Die Tribe FloodNet 2k edition
  - Flooding mit gefälschter Absenderadresse.
  - Protokoll wird zufällig ausgewählt.
  - Decoy Pakete um Master zu verschleiern.
  - Passwort Authentisierung mittels AES.

Stacheldraht, 2000

- Stacheldraht ist eine Kombination von Trinoo und TFN
- Verschlüsselte Kommunikation
- Auto-Update des Agenten
- Inzwischen hunderte Derivate und Weiterentwicklungen... mit GUI/ Weboberfläche/Chat steuerbar.

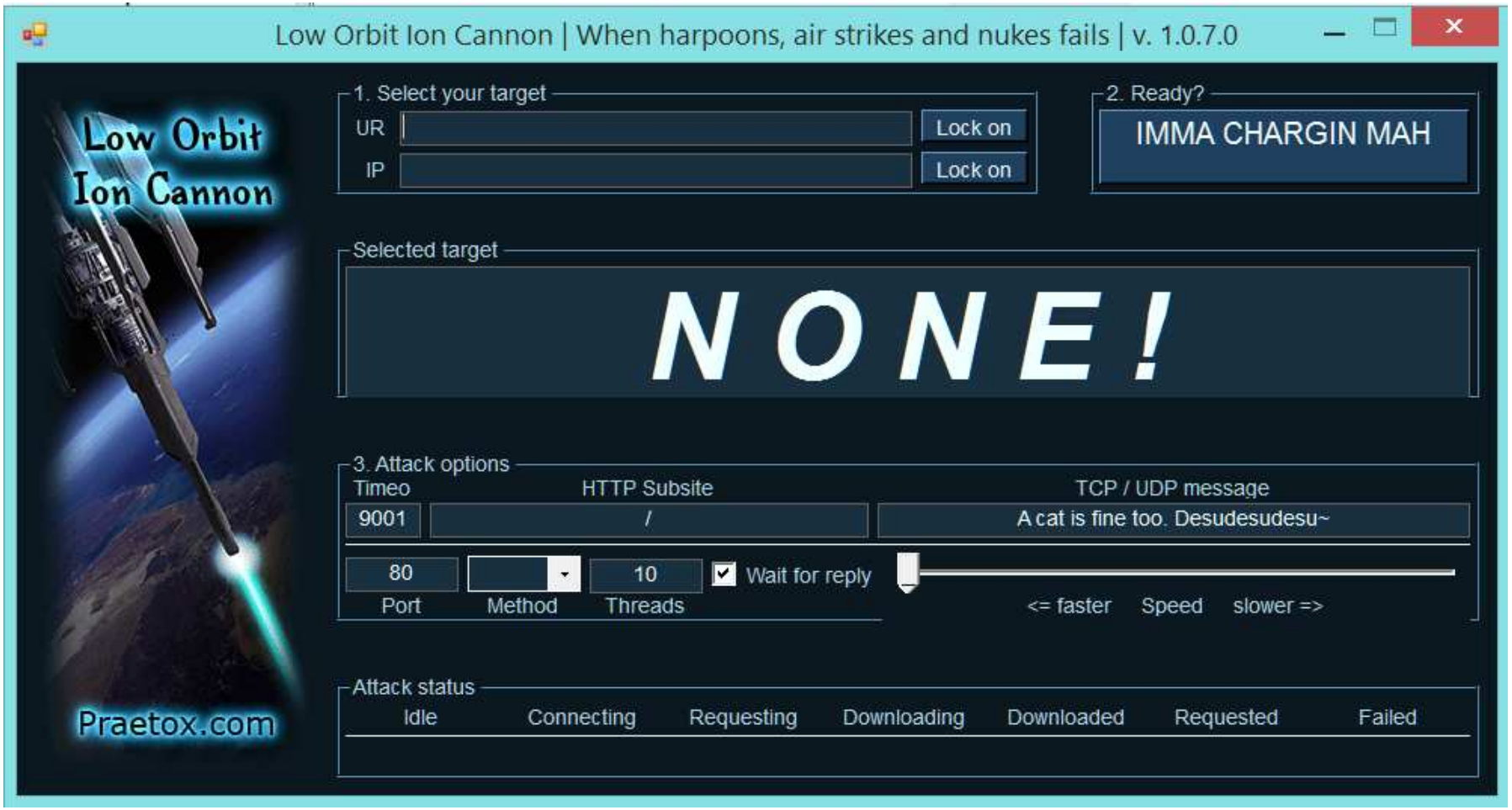
Anmerkungen zum Thema Botnetze

- Ungefähr 7-25% aller Rechner sind Teil eines Botnetzes.
- Einsatzzwecke
  - DDoS und Spamming (ca. 135 Millarden SPAM-Mails pro Tag).
  - Datendiebstahl und Betriebsspionage
  - Verbreitung von Malicious Software.
  - Manipulation von Online Wahlen.
  - Rent-a-Botnet
  - ...

Low Orbit Ion Cannon (LOIC), 2010

- Open Source „Network Stress Testing Application“. :)
- Naives Flooding mit TCP- oder UDP-Paketen.
- Weltweit in den Massenmedien bekannt geworden Ende 2010 im Rahmen der „Operation Payback“.
  - DDoS-„Racheakt“ an VISA, Mastercard, PayPal und Amazon wegen Stop der Diensterbringung für WikiLeaks.
  - Tausende Internet-Nutzer beteiligten sich „freiwillig“ durch Installation der Software bzw. Nutzung einer JavaScript-Variante per Web-Browser.

LOIC-GUI, 2010



Beteiligung an DDoS-Angriffen ist vielerorts illegal

- LOIC verschickt Pakete mit echter Quell-IP-Adresse.
- Opfer protokolliert Quell-IP-Adressen der LOIC-Angreifer.
- Internet-Provider können IP-Adressen Nutzern zuordnen.
- Operation Payback: Festnahmen in England, Spanien und Türkei.
- Drakonische Gesetzgebung
  - Deutschland: Computersabotage nach §303b StGB.
    (Freiheitsstrafe bis zu 3 Jahren + zivilrechtliche Ansprüche)
  - Holland: bis zu sechs Jahre Haftstrafe.

Erpressungsversuch mit DDoS-Drohung, 2011

Erpressungsversuche richten sich gegen zahlreiche Firmen und auch mehrere bayerische Hochschuleinrichtungen

```
Betreff: DDOS www.zhs-muenchen.de
Datum: Mon, 5 Sep 2011 02:50:02 -0600
Von: <amiliaivgspopek@yahoo.com>
An: <hostmaster@lrz.de>
Your site www.zhs-muenchen.de will be subjected to DDoS attacks
100 Gbit/s. Pay 100 btc(bitcoin) on the account
17RaBqjGLisGzLRaAUVqdA2YHgspdkD1rJ Do not reply to this email
```

Bei ausbleibender Zahlung finden tatsächlich DDoS- Angriffe statt; DDoS-Botnet besteht aus ca. 40.000 Maschinen welche die folgende HTTP-Anfrage stellen.

```
GET / HTTP/1.1\nAccept: */*
Accept-Language: ru
...
Connection: Keep-Alive
```

Filter-Kriterium: `Accept-Language ru` (bei dt./eng. Website)

DDoS-Erpressungsversuche: sipgate, 2014

- Test-Angriff am 23.10.2014 ab 3:35 Uhr.
- Erpresserschreiben am Vormittag, Lösegeldforderung in Bitcoins.
- Drei Angriffswellen über mehrere Tage.
- sipgate-Kunden können während dieser Zeit nicht mehr telefonieren
  Es werden sehr hohe Schäden bei Firmenkunden vermutet
- sipgate-Hotline wird überrannt, diverse Presseberichte
- Beschreibung des Ablaufs von sipgate: `https://medium.com/@sipgate/ddos-attacke-auf-sipgate-a7d18bf08c03`

DDoS-Erpressungsversuche: Fidor Bank, 2014

Fidor Bank München

- DDoS-Angriff am Freitag 24.10.2014 ab 18:30 Uhr.
- Erpresserschreiben ist veröffentlicht.
  `https://www.facebook.com/fidorbank/posts/1015285962771841 7`
- Laut Erpresserschreiben war es ein SYN-Flood-Angriff.
- Bank erstattet Anzeige, schaltet Webseite temporär ab.
- Zahlungskarte kann nicht mehr genutzt werden.

(D)DoS: Schutz- und Gegenmaßnahmen

- Pauschaler Schutz gegen (D)DoS-Angriffe ist praktisch fast unmöglich. Aber Overprovisioning durch Content Delivery Network (CDN) hilft. (Akamai, CloudFront, Cloudflare, . . .)
- Schutz gegen Brute-Force-(D)DoS-Angriffe
  - Firewall-Regeln, ggf. basierend auf Deep-Packet-Inspection.
  - Aussperren von Angreifern möglichst schon beim Uplink.
  - Zusammenarbeit mit den Internet-Providern der Angriffsquellen.
  - Anzahl Verbindungen und Datenvolumen überwachen.
  - Bug- und Sicherheitswarnungen (z.B. CERT) verfolgen.
  - Nur Software aus vertrauenswürdigen Quellen installieren.
  - Ad- und Scriptblocker installieren.
  - *Schattige Internetseiten* meiden.
  - Intrusion Detection System (IDS).
  - Sicherheitsupdates einspielen.
  - Nicht auf alles klicken.

Zusammenfassung

Sie sollten . . .

- . . . den LAND Angriff verstanden haben.
- . . . den Teardrop Angriff verstanden haben.
- . . . wissen wie der Ping-of-Death-Angriff funktioniert.
- . . . wissen wie der SMURF-Angriff funktioniert.
- . . . wissen was SYN-Flodding ist.
- . . . wissen was ein (D)DoS-Angriff ist.
- . . . wissen was man gegen (D)DoS-Angriffe tun kann.