UNIVERSIDADE DA CORUÑA

[D]DoS
[Distributed] Denial of Service

LSI - 2016/2017

José Manuel Vázquez Naya
jose@udc.es

DENEGACIÓN DE SERVICIO

Denegación de Servicio

- Definición
  - *CERT - "Ataque caracterizado por un intento explícito de denegar a los usuarios legítimos el uso de un servicio o recurso"*

- *¿Por qué los servicios son vulnerables?*
  - *Los protocolos suelen estar diseñados para ofrecer servicios, no para prevenir o evitar estos ataques*

Denegación de Servicio

- **Legislación aplicable**
  - Ley Orgánica 10/1995, de 23 de Noviembre, del **Código Penal**

- **Implicaciones jurídicas**
  - Tras la reforma del Código Penal por la Ley Orgánica 5/2010, el Ataque de Denegación de Servicio ha pasado a ser considerado un **delito** pudiendo llegar las penas hasta los **3 años de prisión** según el Art. 264 del mismo.

Denegación de Servicio

- Tipos de ataques DoS
  1. Semánticos o lógicos
     - Aprovechan una vulnerabilidad del protocolo, aplicación o sistema
  2. Fuerza bruta o inundación (*flooding*)
     - Se intenta desbordar a los sistemas mediante un uso legítimo pero desmedido del envío de paquetes

  - Clasificación clásica
    - Algunos ataques presentan características de ambos tipos

Denegación de Servicio

- Ataques **semánticos o lógicos**
  - ¿En qué consisten?
    - Enviar al equipo remoto paquetes mal construidos (o mal intencionados) para aprovechar vulnerabilidades
  - ¿Cómo pueden evitarse?
    - Actualización de servicios (parcheo de vulnerabilidades)
    - Definición de reglas en firewall

Ping of Death (PoD)

- Tipo de ataque que implica enviar un ping malformado a una computadora
- Un ping normalmente son 56 bytes (+20 bytes fijos de la cabecera IP, + 8 bytes de la cabecera ICMP, haciendo un total de 84 bytes)
- Muchos sistemas no podían soportar un paquete ping de mayor tamaño que el tamaño máximo de paquete IPv4 (65.535 bytes)
  - Enviar un paquete ping superior a este tamaño podría hacer que la computadora objetivo se quedase colgada
  - Realmente, enviar un paquete > 65.535 bytes viola el protocolo IP (RFC 791)
    - Se puede enviar el paquete fragmentado. Cuando la máquina lo reensambla se cae
- Los sistemas operativos "modernos" (posteriores a 1997/1998) no son vulnerables a este ataque

Teardrop

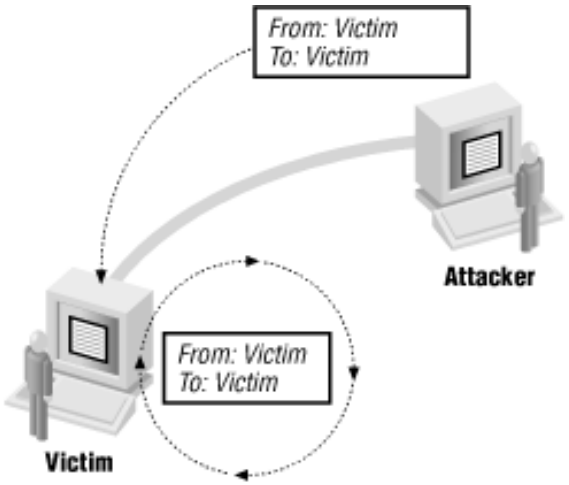
- Ataque basado en **fragmentación**
- Cuando se envían datos por red, se fragmentan en origen y se reensamblan en destino
- Por ejemplo, para enviar 3000 bytes, en lugar de enviar un único paquete, se generarían los siguientes paquetes:
  - paquete 1 que contiene bytes 1-1000.
  - paquete 2 que contiene bytes 1001-2000.
  - paquete 3 que contiene bytes 2001-3000.

Teardrop

- En el ataque teardrop:
  - Se envía un paquete fragmentado a la máquina objetivo
  - Los fragmentos están mal formados, de forma que se solapan
    - (bytes 1-1500) (bytes 1001-2000) (bytes 1500-2500)
  - Cuando la máquina objetivo intenta reensamblar los datos se queda colgada o se reinicia
- Windows NT, Windows 95, y versiones de Linux anteriores a la versión 2.1.63 son vulnerables a este ataque

LAND - Local Area Network Denial

- Ataque basado en **spoofing**
- Pasos
  - Envío de un paquete TCP SYN a la máquina objetivo
  - Además, se establece como IP origen (falsa) la dirección de la propia máquina objetivo
  - Consecuencia: la víctima se responde a sí misma continuamente. Se crea un bucle infinito y la máquina se queda colgada



- Windows NT antes del Service Pack 4 era vulnerable a este ataque

Denegación de Servicio

- Ataques de fuerza bruta o **inundación (*flooding*)**
  - ¿En qué consisten?
    - En *inundar* un sistema con un flujo continuo de tráfico
    - Acaban por consumirse todos sus recursos propios y el ancho de banda

Ping flood

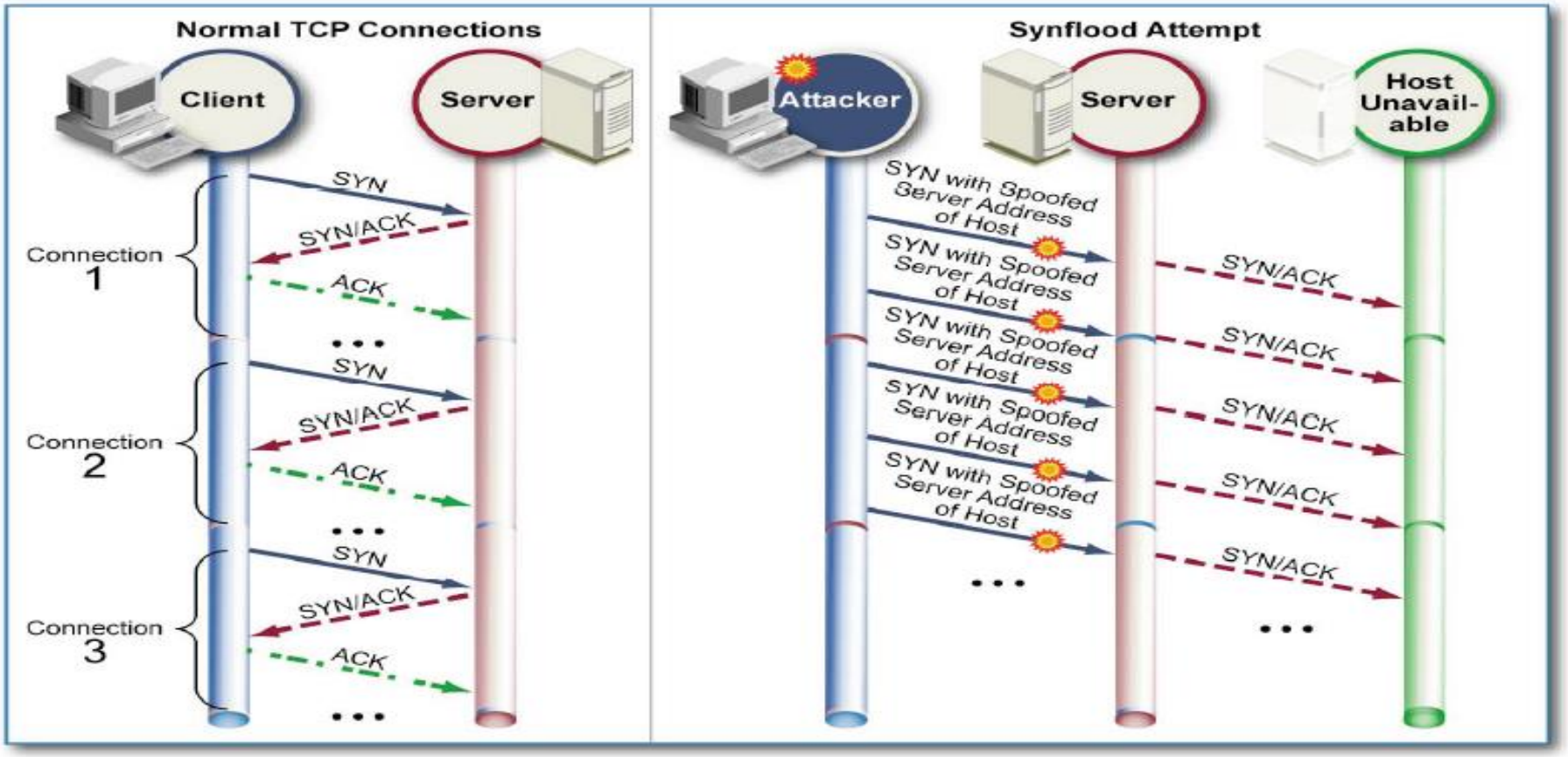
- ICMP Echo Request (***Ping flood***)
  - Envío masivo de paquetes ICMP Echo

TCP SYN Flood

- Atacante envía paquetes TCP con flag SYN al servidor, reemplazando la IP origen por una IP legal pero inalcanzable

- Servidor, al recibir el mensaje,
  - Reserva espacio para la conexión (buffer, sockets, …)
  - Responde a una dirección inalcanzable (nadie responderá)
  - Debe esperar a que venza el *timeout* (e.g. 75s) con socket abierto, reserva de buffers, etc.
  - Si recibe muchas peticiones se agotan los recursos

TCP SYN Flood



TCP SYN Flood

- Explota una debilidad intrínseca del protocolo TCP
  - Complejo de evitar
- Algunas contramedidas
  - SYN Cookies
  - SYN Caches

SYN Cookies

- La idea de las SYN Cookies es aprovechar el número de secuencia para codificar datos
  - Permite al servidor, evitar el rechazo de nuevas conexiones cuando la cola SYN se llena
  - El servidor descarta la petición SYN original y crea un "SYN cookie challenge". Encapsula una parte de la solicitud original y se devuelve al cliente como un número de serie largo
  - Si el cliente responde, el servidor puede reconstruir la petición SYN original
  - Esto permite reservar espacio para la conexión (buffer, sockets, ...) únicamente cuando se recibe el mensaje de confirmación final
  - Las SYN cookies se pueden activar en caso de ataque (no tienen por qué estar siempre activadas).

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

sysctl -w net.ipv4.tcp_syncookies=1
```

SYN Caches

- La Transmission Control Block (TCB) es una estructura de datos que mantiene toda la información de una conexión
- La idea de las SYN Caches es usar una una estructura de datos independiente de la TCB, con un tamaño limitado y en la que se guarda sólo un subconjunto de datos de los que se guardarían normalmente en la TCB
- Si se completa el handshake y se recibe el ACK, estos datos se copian a la TCB
- En la estructura de datos de la SYN Cache, se pueden reutilizar los *slots* más antiguos
- Implementado por defecto en FreeBSD

UDP Flood

- Al contrario que TCP, el protocolo UDP no está orientado a conexión
  - Ataques por inundación UDP ¿En qué consisten?
    - Envío masivo de paquetes a puertos UDP aleatorios
    - Destinatario (víctima)
      - Comprueba si alguna aplicación está escuchando en ese puerto
      - Puerto aleatorio -> ninguna aplicación estará a la *escucha*
      - Respuesta con un paquete ICMP Destination Unreachable
    - Si el número de paquetes enviados (puertos analizados) es suficientemente elevado el destino será incapaz de responder

Denegación de Servicio

- Herramientas de generación de paquetería
  - packit
  - hping3
  - …

Denegación de Servicio

- **Packit** (apt-get install packit)
  - Herramienta para la captura e inyección de paquetes
  - Permite personalización paquetes
    - TCP, UDP, ICMP, IP, ARP, RARP, Ethernet header

Denegación de Servicio

```
packit  -m inject [-t protocol] [-options] [-i interface]

Opciones básicas de inyección de paquetes:
-t protocolo      TCP (defecto),  UDP, ICMP, ARP
-c número         Número de paquetes a inyectar (0: continuo)
-w número         Intervalo (en seg.) entre cada ráfaga de paquetes
                  (def. 1)
-b número         Número paquetes a inyectar en cada intervalo (0:
                  máximo)
-h                Host Response: salida por pantalla
-i interface      especifica la interfaz desde la que transmitir
-s dirección      IP origen (spoofing)
-sR               Establece dirección IP origen aleatoria
-d dirección      IP destino
-dR dirección     Establece una dirección destino aleatoria
-S puerto         Indica puerto origen en TCP y/o UDP
-D puerto         Indica puerto destino en TCP y/o UDP
-F flags          Flags TCP : S(SYN), F(FIN), A(ACK), P(PSH), U(URG),
                  R(RST)
```

1) http://linux.die.net/man/8/packit

Denegación de Servicio

- Packit. Ejemplos:
  - Envío 2 paquetes udp al puerto 7 (UDP-Echo), falseando IP origen (aleatoria) y mostrando salida por pantalla

```
packit -t udp -D 7 -sR -d 172.30.0.20 -c 2 -h
```

Denegación de Servicio

- Packit. Ejemplos
  - Envío 2 paquetes tcp con el flag SYN al puerto 22 (ssh), falseando IP origen (aleatoria) y mostrando salida por pantalla

```
packit -t tcp -D 22 -sR -FS -d 172.30.0.20 -c 2 -h
```

Denegación de Servicio

- hping3 (apt-get install hping3)
  - Añade funcionalidades a ping
    - spoofing, inyección paquetes, etc.
    - http://www.hping.org/hping3.html
  - Ejemplo

```
root@debian:/home/lsi# hping3 www.google.com
HPING www.google.com (eth0 173.194.34.241): NO FLAGS are set, 40 headers + 0 data
bytes
len=46 ip=173.194.34.241 ttl=255 id=10222 sport=0 flags=RA seq=0 win=0 rtt=0.4 ms
len=46 ip=173.194.34.241 ttl=255 id=10223 sport=0 flags=RA seq=1 win=0 rtt=0.4 ms
```

Denegación de Servicio

- hping3 [opciones] host
- Opciones básicas
  - -c número paquetes
  - -i intervalo espera en segundos o microsegundos (u)
    - -i 1 1 paguete/segundo
    - --fast alias -i u10000
    - --faster alias -i u1
    - --flood envío de paquetes sin espera (lo más rápido posible)
  - Modo funcionamiento (si no se especifica, default mode TCP)
    - -0 --rawip RAW IP mode
    - -1 --icmp ICMP mode
    - -2 --udp UDP mode
    - -8 --scan SCAN mode
    - -9 --listen listen mode
  - -a --spoof spoof dirección origen
  - --rand-source especificar dirección de origen aleatoria
  - UDP/TCP
    - -s --baseport puerto de origen
    - -p --destport puerto destino
    - -S --syn flag SYN
    - -R --rst flag RST

Denegación de Servicio

- hping3 . Ejemplos
  - Envío paquetes TCP con el flag SYN al puerto 80 de <ipVictima> todo lo rápido que puede (--flood) y desde direcciones IP origen aleatorias (--rand-source)

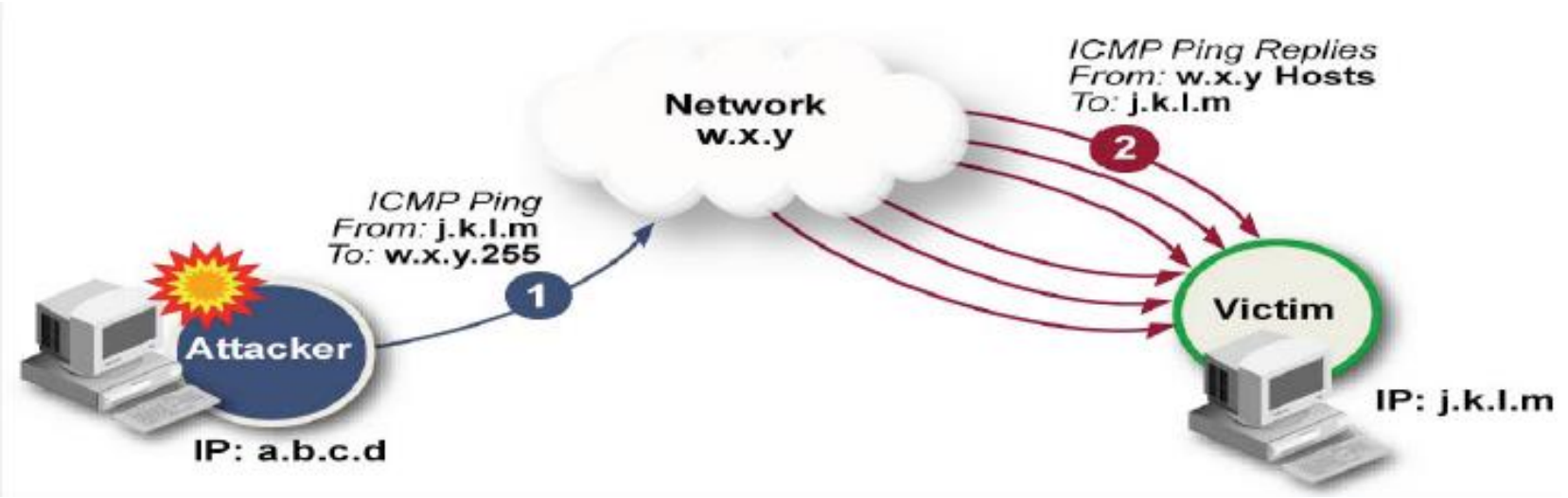
```
hping3 --rand-source -p 80 -S --flood <ipVictima>
```

Denegación de Servicio

- Ataques semánticos/lógicos vs ataques inundación/fuerza bruta
- Otra posible clasificación
  - Ataques Directos
    - Envío masivo de paquetes de manera directa a la víctima
      - Eg. Ping of Death, TCP SYN Flood, …
    - Dirección origen generalmente falsificada
  - Reflector Attacks
    - Uso nodos intermedios como amplificadores
      - Routers, Servidores Web , DNS, NTP, …
    - Atacante envía paquetes que requieren respuesta a un amplificador con la dirección de la víctima como dirección origen
      - Eg. Smurf, Fraggle, …

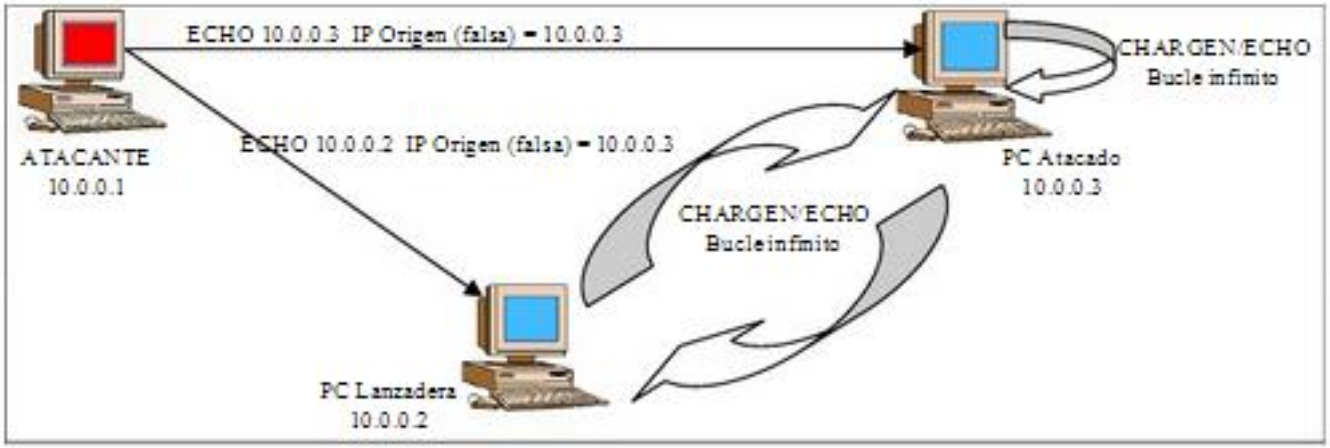
SMURF

- Usa paquetes ICMP Echo-Request
  - IP origen : máquina atacada (spoofing)
  - IP destino: dirección broadcast de la red
- Todos los equipos de la red responderán mediante paquete ICMP Echo-Reply, consumiendo ancho de banda y recursos de la víctima



FRAGGLE

- Usa protocolo UDP
- Envío de mensaje broadcast UDP con IP origen = IP victima (*spoofing*) y destino generalmente al servicio chargen (puerto 19) o echo (puerto 7) de la víctima
- Inundación
  - Equipos con *echo* inactivo responderán ICMP Error
  - Equipos con *echo* activo reenviarán paquete a la víctima
  - Si la víctima tiene servicio *chargen* activo, entrarán en un bucle infinito con los servidores de echo activo.



Denegación de Servicio

- **Factor de amplificación**
  - Relación entre las tramas recibidas por la víctima por cada trama transmitida por el atacante
  - Eg. TCP SYN Flood directo
    - Por cada paquete enviado, la víctima recibe un paquete.
    - Factor Amplificación: 1
  - Eg. Smurf
    - Por cada paquete enviado por atacante se generan n paquetes hacia la víctima (n: número de máquinas activas en la red):
    - Factor Amplificación: n

DDOS
DENEGACIÓN DE SERVICIO DISTRIBUIDA

DDoS

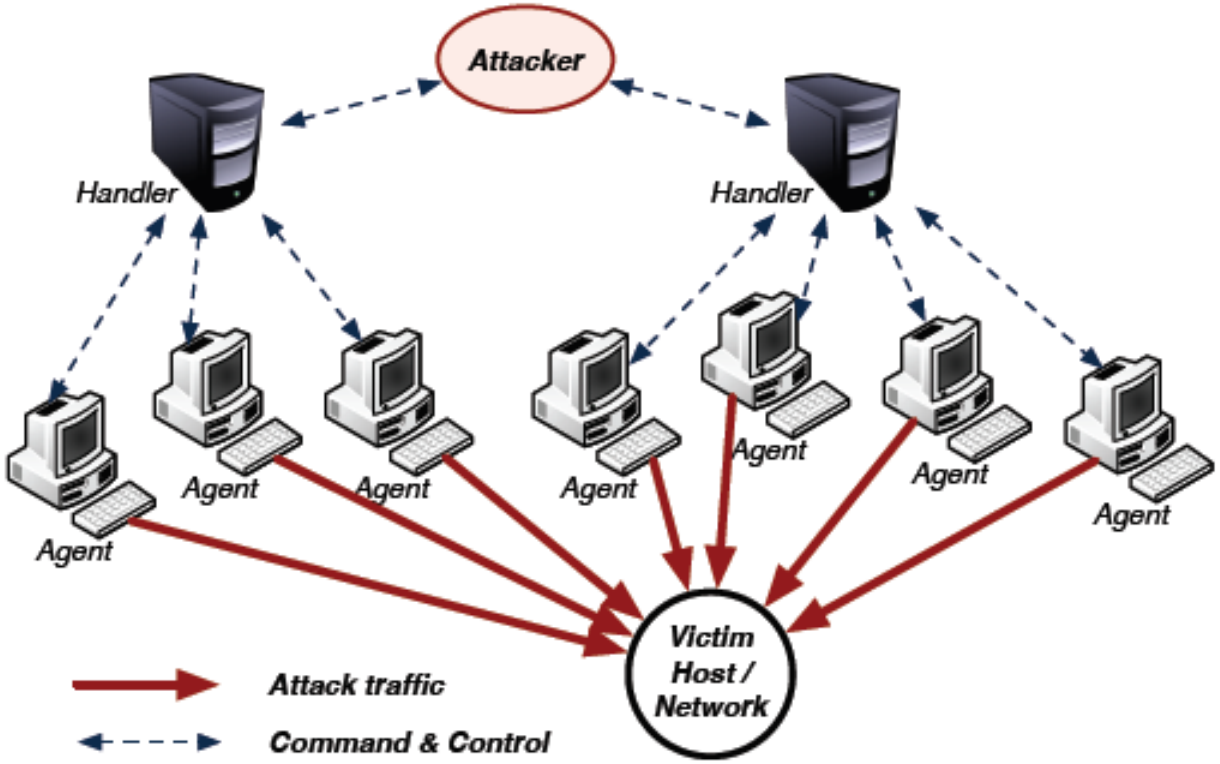


Imagen extraída de *Internet Denial of Service Attacks and Defense Mechanism, M. Abliz*

DDoS

- Participantes principales
  - Agentes (bots, zombies)
    - Máquinas intermediarias
    - Equipos que tras su infección (e.g. malware) son usados por una tercera persona como medio para lanzar un ataque
      - DDoS, Distribución material, envío de spam, robo de datos, etc.
  - Handlers o manejadores
    - Programa/servicio encargado del control de los agentes
    - Especifica a quien atacar, cuando atacar y cómo atacar

DDoS

- Dimensión Botnets
  - “Mariposa” (2010) – 13 millones equipos
  - “TDL” (2011) – 4.5 millones equipos
  - “Rustock” (2011) – 2.4 millones de equipos

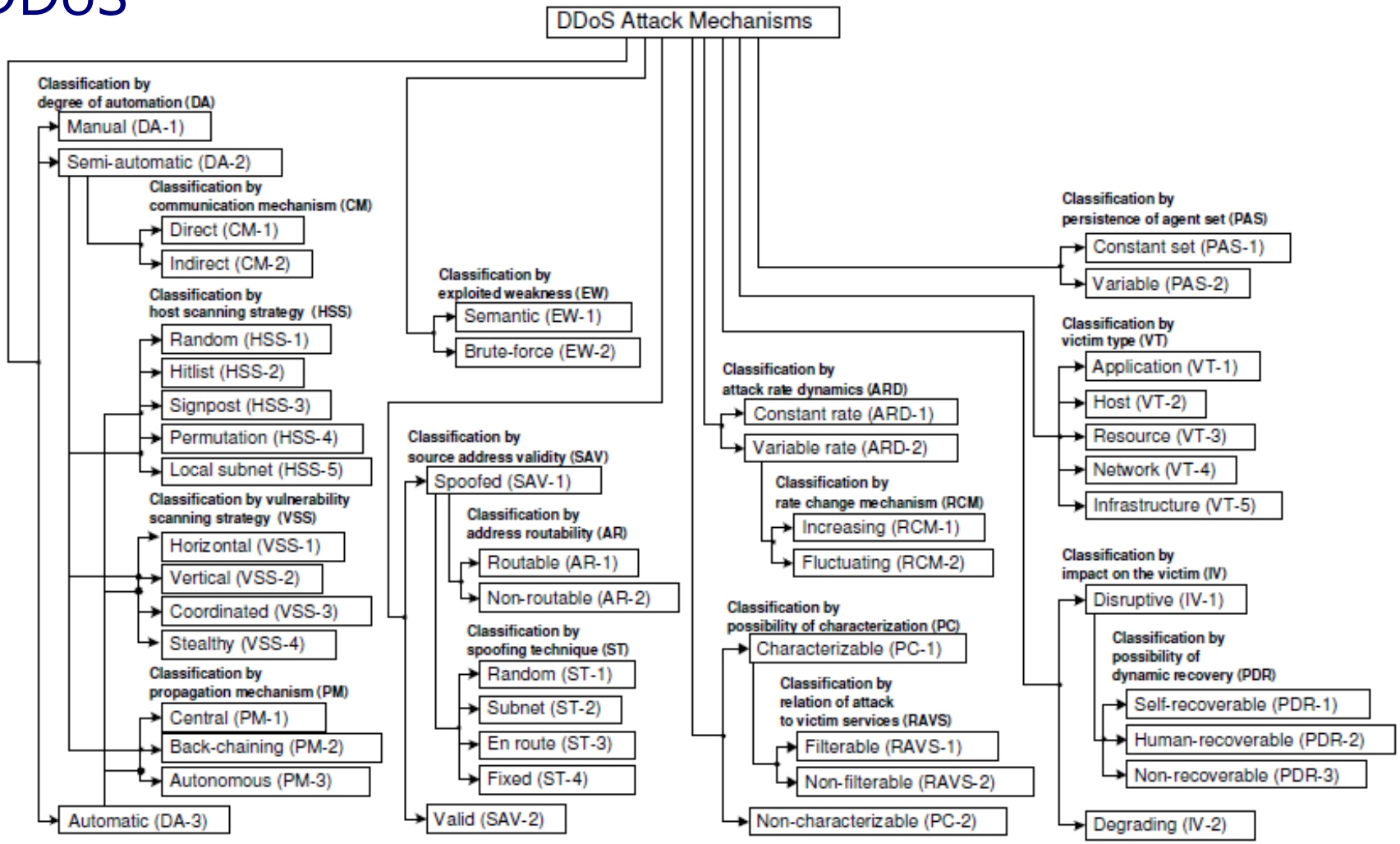
DDoS

- Fases
  - 1) Reclutamiento agentes
    - Escaneo de puertos, búsqueda de vulnerabilidades, etc.
    - Troyanos, Spam, etc.
  - 2) Explotación / infección
    - Generalmente automatizada
    - Máquinas infectadas serán utilizadas para nuevos reclutamientos
  - 3) Ataque
    - Tras la orden del manejador, los agentes serán los encargados del lanzamiento de paquetes

Internet's largest 1Tbps DDoS Attack was conducted using 145k hacked cameras

By Waqas on September 29, 2016 *Email* *@hackread* CYBER ATTACKS CYBER CRIME

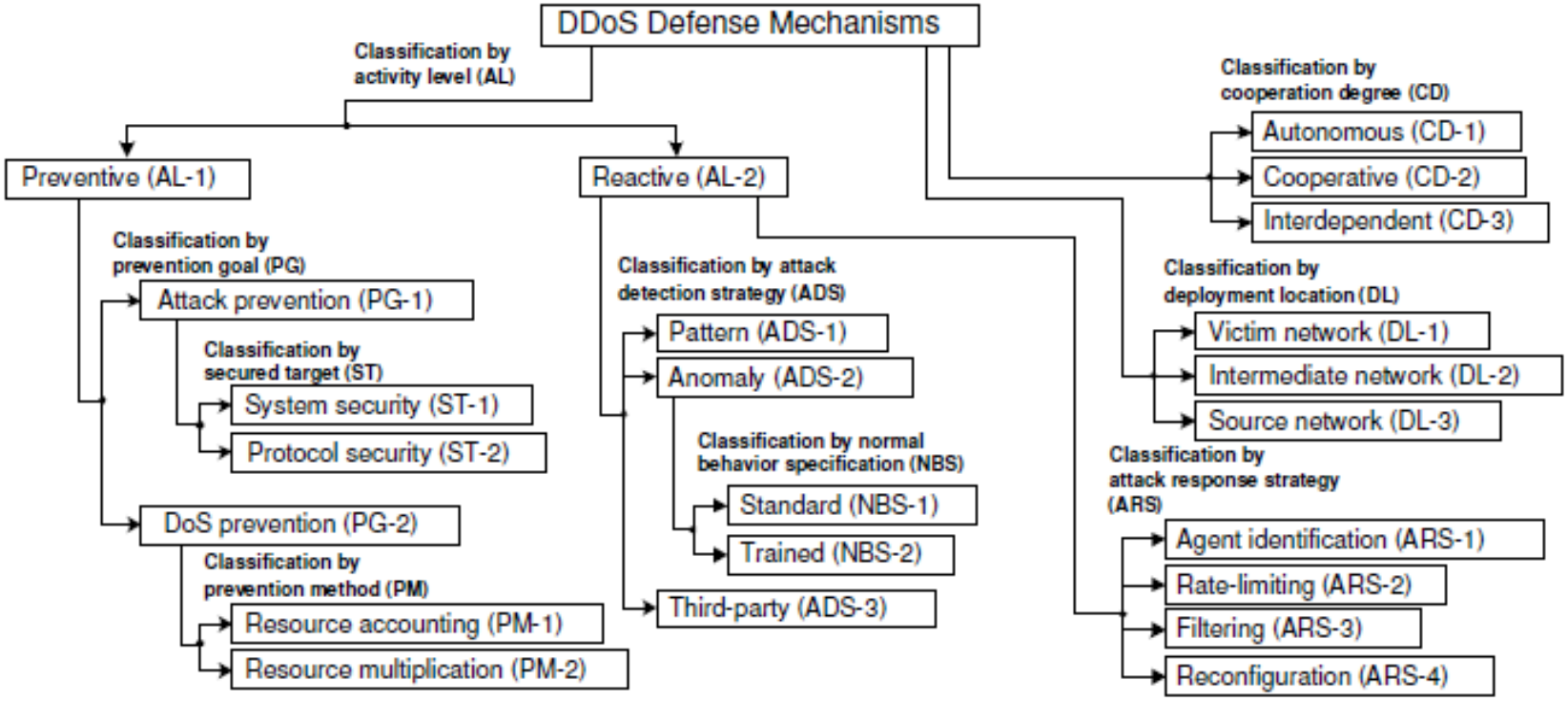
DDoS



Taxonomía de los mecanismos de ataque en DDoS

(imagen extraída de A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, J. Mirkovic)

DDoS



Taxonomía de los mecanismos de defensa en DDoS

(imagen extraída de A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, J. Mirkovic)

Bibliografía recomendada

- CERT. (2001) ***Denial of Service Attacks***. Software Engineering Institute. Carnegie Mellon. Disponible en: www.cert.org/tech_tips/denial_of_service.html
- Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2010) ***Botnets ¿Qué es una red de ordenadores zombis?***. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Articulos/Articulo_botnet
- Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher (2004). Internet Denial of Service. Attack and Defense Mechanisms. ISBN: 0-13-147573-8. Prentice Hall.
- Santos del Riego, A (2016). ***DDoS***. ***Legislación [Protección] y Seguridad de la Información***. Disponible en: http://psi-udc.blogspot.com.es/search/label/DDoS.