CAPITULO 1

Ubicación de la tesis sobre DDOS

En este primer capítulo presentaremos el contexto social de Internet y su relevancia actual en la sociedad del siglo XXI. Introduciremos muy brevemente los conceptos de ataques de denegación de servicio (*Deny Of Service o DOS*) y ataques de denegación de servicio distribuido (*Distributed Deny Of Service, DDOS*) justificando su importancia y relevancia actual.

Como ilustración de su presencia en la sociedad digital actual analizaremos el caso del famoso virus MyDoom, dónde podremos observar cómo cientos de miles de ordenadores domésticos pueden ser utilizados para desencadenar un terrible ataque que obligó a la empresa SCO a cesar todo servicio por Internet durante varios días y puso en graves dificultades el servicio WWW de Microsoft Corporation.

También realizaremos una breve descripción de la trayectoria curricular que se ha seguido hasta este momento acreditando los conocimientos necesarios para proceder al estudio en la tesis doctoral de los ataques de denegación de servicio distribuidos o DDOS.

Este estudio se centrará únicamente en la versión 4 del protocolo IP, ya que aunque actualmente se está trabajando en la versión 6 [Hui98][Ver00] esta es aún experimental y no se encuentra implantada de forma mayoritaria en Internet.

1.1 Redes IP

El protocolo de comunicaciones IP (*Internet Protocol*) facilita un sistema **sin conexión** (*connectionless*) y **no fiable** (*unreliable*) de entrega de datagramas o paquetes de información entre dos ordenadores cualesquiera conectados a Internet.

Esta simplicidad de funcionamiento del protocolo IP permite que sea utilizado como base para la definición de otros protocolos de comunicación utilizados comúnmente en la red Internet. A continuación se detallan los más comunes junto a sus características principales:

- **ICMP** (*Internet Control Message Protocol*) es un protocolo no fiable encargado de regular el flujo de las comunicaciones.

- **UDP** (*User Datagram Protocol*) es un protocolo no fiable de transmisión de datos sin conexión.

- **TCP** (*Transmission Control Protocol*) es un protocolo fiable de transmisión de datos con conexión.

Definiremos las **redes IP** como aquellas redes que utilizan los protocolos TCP/IP para su funcionamiento. Internet es una red IP.

"Las familias de protocolos TCP/IP permiten la comunicación entre diferentes tipos de ordenadores con independencia del fabricante, red a la que se encuentren conectados y sistema operativo utilizado." [Ric98-1]

Las redes IP se caracterizan por haber sido construidas siguiendo un esquema de capas (*layers*). Cada capa es la responsable de cada una de las diferentes facetas de la comunicación. De esta forma, se puede definir la familia de protocolos TCP/IP como una combinación de cuatro capas (ver figura 1-1) según el modelo OSI [Ric98-1].

En este esquema, la capa superior accede únicamente a los servicios prestados por la capa situada justo en el nivel inferior a ella. De esta forma, independizamos una capa del resto de capas inferiores, lo que nos permite tener un esquema modular.

APLICACIONES (Applications)	WWW, SSH, FTP...
TRANSPORTE (Transport)	TCP, UDP, ICMP...
RED o Interconexión de redes (Network)	IP
ENLACE o Red real (Link)	IEEE 802.2, 802.3...

FIG. 1-1: Estructura de cuatro capas.

Este sistema incremental en su construcción permite una independencia entre las diferentes capas y obliga a que la comunicación entre dos ordenadores se realice mediante una comunicación entre las capas del mismo nivel de los dos ordenadores.

De este modo, la comunicación en Internet se produce mediante el intercambio de paquetes de información entre los distintos ordenadores. Estos paquetes de información, también denominados **datagramas,** viajan por los diferentes ordenadores que están conectados a Internet hasta que alcanzan su destino o son descartados por algún motivo (ver figura 1-2).

De esta forma, en la comunicación de dos ordenadores por Internet podemos diferenciar dos tipos de funciones que pueden desempeñar los ordenadores por los cuales se transmiten los paquetes de información:

1. Ordenador ***emisor/receptor*** (*end-system o end-host*): Aquí se englobaría el ordenador origen o destinatario de la comunicación.

2. Ordenador ***intermedio*** *(intermediate-system, router o gateway*): Serían todos los ordenadores por los que van pasando los datagramas o paquetes de información hasta el ordenador destino de la comunicación o hasta el origen (en el caso de una respuesta).

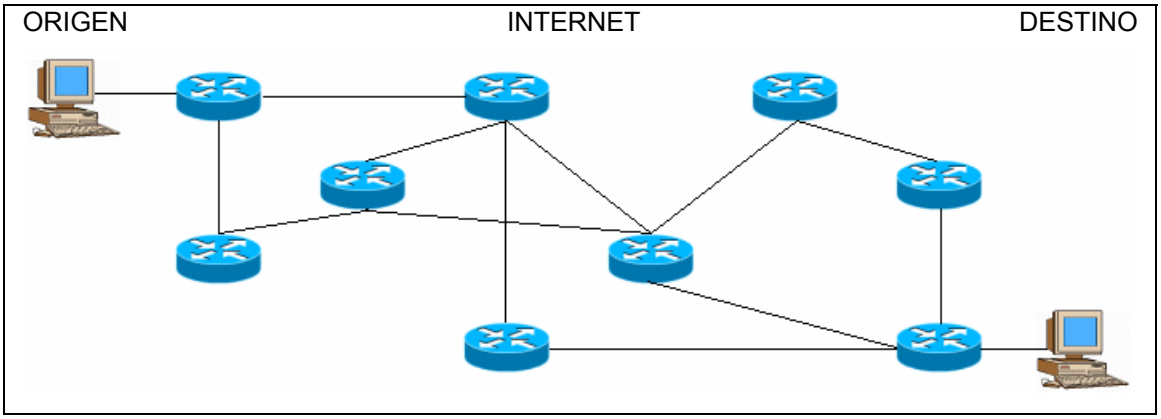

FIG. 1-2: Rutado de paquetes en Internet.

1.2 La importancia de Internet

Pese a la mal llamada "*crisis de las .com*" Internet se ha convertido en la última década en el nuevo santo grial de la civilización. Nadie puede ignorar actualmente expresiones como *email*, *router, buscador, on-line* o *servidor*.

En septiembre de 2002 ya había más de 600 millones de personas conectadas a Internet [WWW3] así como 171 millones de sitios Web [WWW4].

La explicación fundamental a este éxito sin precedentes es la capacidad única de aunar en un mismo medio ocio y negocio. Por otro lado, la disponibilidad de los servicios 24 horas al día, su interactividad total así como su accesibilidad desde cualquier punto del mundo, no hacen más que acrecentar su éxito sin límites.

El impacto tecnológico de Internet en nuestra sociedad ha sido tan fuerte que ha trascendido su propio ámbito natural (la red Internet) y es muy extraño no observar referencias suyas casi a diario en otros medios de comunicación masiva (televisión, prensa, radio…).

Para observar hasta que punto está absorbiendo a los medios de comunicación tradicionales, simplemente podemos destacar cómo todos los diarios importantes del mundo tienen sus equivalentes en edición digital (La Vanguardia, El periódico, El país, New York Times, Le Monde…) que son consultadas diariamente por cientos de miles de usuarios. Incluso las cadenas de televisión han llegado a simultanear la transmisión de programas por la red.

Análogamente, en la actualidad todas las empresas importantes disponen de servicios "*on-line*" que abarcan desde simples catálogos de sus productos hasta la posibilidad de realizar compras desde cualquier sitio del mundo.

Las empresas únicamente digitales (Yahoo, Google, Amazon…) empiezan a tener una relevancia y peso económico considerable, ya que actualmente cotizan en bolsa y mueven cientos de millones de euros al igual que hacen otras empresas más tradicionales como bancos, eléctricas o petroleras.

Sin embargo, estas mismas características que lo hacen único e "imprescindible" actualmente pueden condenarlo a "**morir de éxito**". El envío de *spam* o publicidad indiscriminada, las apariciones regulares de virus, las acciones judiciales en contra de la red (desde cánones por royalties a CD-ROM hasta persecuciones a usuarios de programas *peer-to-peer* o P2P pasando por atentados a la privacidad de los usuarios) hacen que la realidad de Internet diste mucho de ser idílica.

Por todos estos motivos, Internet es actualmente el medio masivo "de moda" y su gran importancia a corto y medio plazo está fuera de toda duda.

1.3 Ataques en redes IP

Desde un punto de vista sociológico, en cualquier grupo social un pequeño porcentaje de su población es malévolo [CZ95]. Con los datos de utilización de Internet anteriormente comentados, podemos observar como si tan sólo el 1 por cien de la población pertenece a este sector tenemos casi 6 millones de posibles atacantes.

Incluso suponiendo sólo un uno por mil tenemos la cantidad de casi seiscientos mil peligros potenciales. Cabe notar que esta cifra aumenta progresivamente con la propia expansión de Internet.

Los ataques en redes IP son aquellos perpetrados por usuarios de la propia red que utilizan los protocolos o servicios existentes con el objetivo de conseguir algo de forma ilegal y/o ilegítima.

De esta forma, podemos observar como a diferencia de lo que ocurre en otros medios masivos ¡la propia tecnología que lo sustenta puede utilizarse en su contra!.

La gran variedad de protocolos, tecnologías y servicios que sustentan Internet hacen que la posibilidad de realizar un ataque a cualquiera de estos elementos sea elevada, ya que entre otros problemas, la seguridad nunca fue un elemento clave del diseño inicial de Internet.

En las estadísticas anuales de organismos oficiales como el CERT [WWW6] podemos observar como desde 1988 hasta el año 2003 se ha pasado de 6 a más de 137.000 incidentes registrados (ver figura 1-3), es decir un aumento del 23.000% en quince años.

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988-2003): **319,992**

FIG. 1-3: Desglose de incidentes registrados en el CERT.

De la gran cantidad de ataques posibles [Sch00][GP01][Ver03] nos centraremos en aquellos denominados ataques de denegación de servicio distribuido o DDOS (*Distributed Deny Of Service*).

Podemos definir un **ataque de denegación de servicio** (*DOS Attack*) como *"la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso*" [WWW7].

Una vez de definidos los objetivos de un ataque de denegación de servicio realizaremos una ampliación del concepto sumándole la capacidad de acceso simultáneo y desde cualquier punto del mundo que ofrece Internet.

De esta forma definiremos los ataques de denegación de servicio distribuido o DDOS como "*un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino* [Dit99][WWW8]".

Una vez más una de las características fundamentales de la red, el acceso universal entre dos puntos cualesquiera conectados a Internet, es utilizado en su contra. En la figura 1-4 podemos observar de forma simplificada un esquema de los ataques DDOS.

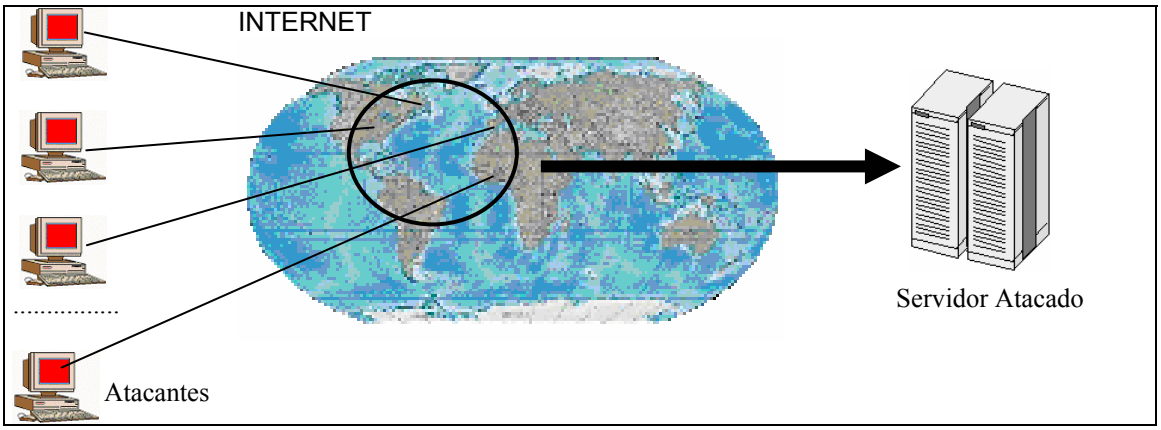

FIG. 1-4: Ataque típico de DDOS.

1.4 Virus y ataques DDOS: El caso MyDoom

La primera quincena de febrero de 2004 marcó el inicio de una nueva tendencia en los ataques de denegación de servicio distribuido. Hasta la fecha, el procedimiento de preparación de un ataque DDOS quedaba circunscrito a un grupo selecto de hackers ya que pese a la existencia de herramientas más o menos sofisticadas, el sistema continuaba siendo mayoritariamente artesanal.

1. **Conseguir acceso a un ordenador vulnerable**. Este paso conlleva la comprobación de cientos de *exploits* para cada una de las posibles víctimas. Pese a existir programas semi-automàticos encargados de las comprobaciones, este no deja de ser un método de fuerza bruta (prueba y error) que consume mucho tiempo y no siempre garantiza resultados.

2. **Instalación del kit de DDOS**. Una vez que se ha conseguido el acceso al ordenador, se debe instalar/compilar (y este paso si que es manual) los programas necesarios para que el atacante tome en control del ordenador y lo integre en su red de ataque.

Estos dos puntos se han de repetir una y otra vez para cada ordenador que se añada a la red de los atacantes. De esta forma, en los ataques observados hasta la fecha raramente existían más de dos o tres decenas de ordenadores implicados.

El virus **MyDoom** [WWW20][WWW21] original, cabe notar que han salido varias mutaciones posteriormente que modifican su comportamiento [WWW23], se propaga a través del correo electrónico y afecta únicamente a sistemas operativos Windows.

En la actualidad más del 90% de los ordenadores existentes utilizan la plataforma Microsoft como sistema operativo [WWW22], lo que nos lleva potencialmente a varios cientos de millones de ordenadores.

El comportamiento de este virus consistía en lanzar desde el ordenador infectado un ataque de denegación de servicio a la dirección www.sco.com [WWW24] que finalizaba el día 12 de febrero de 2004. SCO es una empresa propietaria de un sistema operativo Unix que actualmente se encuentra en varios juicios por patentes de software contra Linux, IBM y comunidades de software libre.

Se hace prácticamente imposible determinar de forma exacta la cantidad de peticiones realizadas por los ordenadores infectados. En cualquier caso, el éxito de este ataque fue tan rotundo que la dirección www.sco.com permaneció fuera de uso durante más de una semana.

La desesperación de esta compañía les llevó a ofrecer públicamente el día 30 de enero de 2004 la cantidad de 250.000 dólares [WWW25][WWW26] para cualquier pista que llevase a la identificación del autor o autores de este virus. De hecho, la compañía SCO ante la imposibilidad de absorber el ataque realizado por MyDOOM tuvo que dar de baja su dominio del sistema de DNS y comprar un nuevo dominio http://www.thescogroup.com/ hasta que pasado el día 12 de febrero el virus dejó de lanzar el ataque.

Para recalcar la gran trascendencia e importancia de este hecho, mostraremos unas cifras que permitirán ubicar la potencia de este nuevo sistema de ataque.

La compañía de sistemas antivirus Messagelabs registró hasta el 12 de abril de 2004 en las empresas que utilizan sus antivirus más de 54 millones de emails infectados [WWW27]. Teniendo en cuenta que los emails que filtra esta compañía no son ni un 1‰ del total mundial, la envergadura que ha alcanzado este nuevo sistema de DDOS revela que no es posible actualmente parar este tipo de ataques.

Independientemente del hecho puntual del ataque a SCO, cabe destacar que se ha producido un cambio tecnológico importante pasando de un sistema semi-manual dónde apenas decenas de ordenadores colaboraban en un ataque DDOS bajo las órdenes directa de una o varias personas, a un sistema de ataque totalmente automático con millones de ordenadores distribuidos por todo el mundo.

Hasta la fecha en gran problema de los virus se centraba en los estragos o problemas que pudieran causar en nuestro ordenador infectado y su capacidad de propagación. A partir de MyDoom, el problema deja de circunscribirse a nuestro ordenador y pasa a afectar a terceros (SCO en este caso y al resto de usuarios de Internet debido al consumo de ancho de banda que ralentiza toda la red) lo que abre una puerta a un inquietante peligro

Por otro lado, ya no son necesarios conocimientos tan específicos y tiempo para realizar ataques de fuerza bruta. Cualquier persona que simplemente modifique en el código del virus el destino de su ataque (a su colegio, empresa, universidad...) puede fácilmente lanzar DDOS siendo prácticamente imposible demostrar su implicación en el hecho.

Otro efecto colateral a tener en cuenta de este tipo de sistemas, es que los ordenadores con fechas erróneas estarán creando continuamente tráfico que permanecerá ralentizando la red y consumiendo ancho de banda, lo que conllevará una degradación de los servicios de Internet.

El peligro del sistema híbrido que inició MyDoom no es únicamente que se pueda conseguir la parada real de cualquier sistema conectado a Internet, sino que además podemos conseguir un colapso de toda la red inundándola de tráfico espurio o atacando sus zonas más sensibles (DNS, routers intercontinentales…).

1.5 Justificación de la tesis sobre ataques DDOS

El objetivo de nuestra tesis se centrará precisamente en el análisis de los ataques de denegación de servicio así como de los nuevos mecanismos de seguridad que pueden adoptarse para la minimización o neutralización de los estragos que pueden producir a los servicios on-line de Internet.

La elección del tema de seguridad en redes IP para nuestra tesis se basa en la importancia de la propia Internet y la necesidad básica de proporcionar un entorno seguro y libre de peligros a los usuarios (tanto particulares como empresas) inexistente actualmente.

Como ya se ha comentado anteriormente, la cantidad de protocolos y servicios existentes en Internet es muy grande y no deja de aumentar. Podemos encontrarnos desde servicios sencillos como resolver nombres (DNS) hasta complejos sistemas de multiconferencia en tiempo real o video a la carta.

Análogamente, las posibilidades de ataque a estos protocolos o servicios son múltiples y aumentan cada día. De esta forma, nosotros nos centraremos concretamente en los ataques de denegación de servicio distribuido principalmente por los siguientes motivos:

- Los ataques distribuidos aprovechan la universalidad de conexión en Internet, lo que hace que proliferen y aumenten su virulencia a medida que crezca el acceso de la sociedad a la red. Cuantos más nodos se conecten, más posibilidades existirán de verse envueltos en ataques. Ya sea como orígenes (un atacante toma el control y lo usa contra un tercero) o como destino de algún ataque.

- Este tipo de ataques continua siendo válido, generalmente, con nuevos protocolos y servicios al igual que lo es con los ya existentes.

- El carácter mundial y descentralizado de Internet implica que nos encontramos ante distintos países con distintas leyes y desarrollos tecnológicos distintos. La protección ante ataques en Internet es un tema complicado y de difícil solución debido a la gran cantidad de piezas que implica.

- Actualmente no existe ninguna solución universalmente aceptada contra este tipo de ataques.

- De la posibilidad de conseguir una red "segura" para todos sus usuarios depende en gran medida el éxito o fracaso a medio y largo plazo de Internet.

Desde el punto de vista curricular se han realizado los siguientes cursos del programa de doctorado en informática dentro de la unidad de combinatoria y comunicación digital (CCD) de la universidad autónoma de Barcelona (UAB):

Nombre del curso	***Calificación***
Esquemas de seguridad sobre redes de ordenadores	Excelente
Seminario de combinatoria y comunicación digital	Excelente
Técnicas avanzadas en criptografía	Excelente
Técnicas de combinatoria en computación	Excelente
Técnicas de compresión de información	Excelente
Trabajo de investigación "Seguridad en redes IP"	Excelente

También se ha obtenido el título de diploma de estudios avanzados (**DEA**) al calificar el tribunal correspondiente como APTO la suficiencia investigadora realizada.