Tesis Doctoral

ATAQUES DE DENEGACIÓN DE SERVICIO A BAJA TASA CONTRA SERVIDORES

Autor: Gabriel Maciá Fernández
Directores: Jesús E. Díaz Verdejo
Pedro García Teodoro

Departamento de Teoría de la Señal, Telemática y Comunicaciones
(Universidad de Granada)

RESUMEN DE LA TESIS DOCTORAL

1. Descripción del trabajo

En este apartado se describirán las motivaciones por las que se ha realizado la tesis doctoral. Seguidamente se presentan los objetivos de la misma y el desarrollo seguido en los diferentes trabajos realizados. Finalmente se resumirán las principales conclusiones obtenidas en la tesis doctoral.

La presentación de la información se realiza, en esta síntesis, de forma didáctica y resumida, tratando de simplificar la comprensión del alcance del trabajo. Para una profundización en los aspectos técnicos, motivaciones y detalles de la investigación se recomienda la lectura de la versión completa de la tesis doctoral.

1.1. Origen y motivación del problema

La seguridad en las redes de comunicación

El campo de la seguridad es una disciplina muy extensa que abarca muchos ámbitos. Estos ámbitos van desde la seguridad física de una instalación, en la que se tienen en cuenta aspectos tan diversos como los accesos físicos a la misma, riesgo de fallos de los sistemas por causas tales como inundaciones, altas temperaturas y demás, hasta aspectos de la seguridad en cada uno de los componentes de dichas instalaciones.

En este sentido, las redes de comunicaciones son un componente esencial de las instalaciones y tecnologías en el presente y también para el futuro y, por tanto, garantizar su seguridad es vital para el desarrollo de la sociedad de la información. Para ello, es preciso desarrollar ciertas *políticas de seguridad*, que no son más que normas o criterios que, directa o indirectamente, permiten discernir los eventos y acciones permitidos o prohibidos para un sistema, desde el punto de vista de su seguridad [Carracedo, 2004].

Aunque no existe una terminología ampliamente aceptada y establecida, existen ciertos términos cuya consideración es importante a la hora de evaluar o discutir acerca de la seguridad de un sistema. En primer lugar, algunos autores definen el concepto de amenaza a la seguridad como cualquier violación potencial de la política de seguridad establecida [Carracedo, 2004]. Partiendo de este concepto, se define también un *ataque* como la instanciación de una amenaza, es decir, como el hecho de que una amenaza se haya materializado. Mientras que la amenaza es una violación potencial de la política de seguridad, el ataque es una violación cierta de dicha política. También es necesario definir el concepto de *vulnerabilidad*, entendiéndose por tal una debilidad inherente a un diseño, configuración o implementación de un sistema, que hace que sea susceptible a sufrir una amenaza.

Algunos autores han tratado de realizar una clasificación de los ataques que pueden sufrir las comunicaciones entre una fuente y un destino a través de una red de comunicación, obteniendo como grandes grupos los siguientes tipos [Stallings, 2003]:

- *Ataques de intercepción:* un elemento o parte no autorizada consigue el acceso a la información a proteger.
- *Ataques de modificación:* en este caso, el atacante no sólo consigue el acceso a la información proporcionada por la fuente sino que, además, la modifica.
- *Ataques de fabricación:* una parte no autorizada inserta cierta información en la comunicación.
- *Ataques de interrupción:* en este caso, el objetivo del ataque es la fuente de información, el canal de comunicación, o el destino. Como consecuencia, un activo del sistema queda inutilizable.

Por el papel jugado en el estudio que se realiza en esta tesis, tienen importancia los ataques de interrupción. Estos son ataques contra el servicio de disponibilidad, es decir, estos ataques impiden el uso normal de los sistemas o de las comunicaciones. Por esta razón, a estos tipos de ataque se los denomina típicamente ataques de denegación de servicio (DoS, del inglés *Denial of Service*).

Los ataques de denegación de servicio (DoS)

Los ataques de denegación de servicio son diferentes en su objetivo, forma y efecto a la mayoría de ataques que se efectúan contra redes de comunicaciones y sistemas informáticos. Este efecto de denegación de servicio se realiza enviando determinados mensajes hacia uno de los destinatarios o el propio canal de la comunicación de forma que se interfiera en su funcionamiento, impidiendo acceder total o parcialmente al servicio ofertado.

Existen dos métodos básicos para la realización de un ataque de denegación de servicio: la explotación de una vulnerabilidad descubierta en una máquina objetivo, o el envío hacia la víctima de un amplio número de paquetes de apariencia legítima. El primer tipo se denomina usualmente *ataque de vulnerabilidad*, mientras que el segundo es conocido como *ataque de inundación* [Mirkovic et al., 2004].

Los ataques de vulnerabilidad funcionan enviando a una aplicación que posee una determinada vulnerabilidad uno o varios paquetes construidos de forma especial. La vulnerabilidad consiste, generalmente, en un fallo en la implementación del software de la aplicación o en una deficiencia en la configuración del recurso/utilidad. Los paquetes maliciosos procedentes del atacante pueden provocar en una determinada aplicación un estado que el programador no previó en el momento de su diseño. De esta forma, la llegada de dichos paquetes puede generar un bucle infinito, ralentizar gravemente la velocidad de ejecución de la aplicación, hacer que ésta deje de funcionar, provocar el reinicio de la máquina o consumir grandes cantidades de memoria, generando, en todos los casos, la denegación del servicio ofertado a los usuarios legítimos.

Por otro lado, los ataques de inundación funcionan enviando un número amplio de mensajes hacia un destino que se convierte en víctima del ataque, de forma que su procesamiento supone el agotamiento de determinados recursos críticos en dicha víctima. Por ejemplo, el procesamiento de peticiones complejas puede requerir un amplio tiempo de CPU, la transmisión de mensajes largos puede agotar el ancho de banda disponible para las comunicaciones y la recepción de mensajes que inician comunicaciones con nuevos clientes puede agotar la memoria disponible. Una vez que un recurso está agotado, los clientes legítimos no podrán hacer uso del servicio.

La principal característica de los ataques de inundación consiste en que su fortaleza reside más en el volumen de tráfico que en su contenido. Esto tiene dos implicaciones principales:

- Los atacantes pueden enviar una gran variedad de paquetes. El tráfico de ataque se puede hacer incluso similar al legítimo y adoptar, dentro de ciertos márgenes, una estructura y estadística arbitraria, lo cual facilita en gran medida la ocultación del ataque.
- El flujo de tráfico del ataque debe ser tan elevado como para consumir los recursos del destinatario.

Los ataques DoS a baja tasa

Una mejora significativa, desde el punto de vista del atacante, para un ataque DoS es utilizar de forma conjunta la técnica del ataque de vulnerabilidad y el de inundación con el objetivo de ejecutar ataques de inundación pero que precisen del envío de una tasa no elevada de mensajes hacia la víctima. En este caso, se aprovecha cierta información aportada por una vulnerabilidad en la víctima y se construye de forma inteligente el ataque DoS.

Dos son las principales ventajas que esta modalidad de ataque presenta:

- La cantidad de recursos necesarios para realizar el ataque se reduce drásticamente, facilitando de este modo su ejecución.
- Es más sencillo, para el atacante, la ocultación del ataque, especialmente para aquellos detectores que se basan en la observación de patrones de tráfico consistentes en tasas elevadas.

En este sentido, el único ataque DoS de baja tasa descubierto con anterioridad a esta tesis es el ataque DoS a baja tasa contra el protocolo TCP [Kuzmanovic and Knightly, 2003]. Este ataque ha sido objeto de mucha atención en los últimos años por parte de investigadores que han centrado sus esfuerzos en combatirlos, entre los cuales se pueden citar como los más importantes los presentados en [Yang et al., 2004] [Sun et al., 2004] [Shevtekar et al., 2005].

La existencia reciente de este elevado número de trabajos de investigación en torno a este tipo de ataques muestra la relevancia que la comunidad investigadora ha dado a la necesidad de contrarrestar este tipo de amenazas. En este marco aparece el trabajo de investigación realizado en esta tesis.

1.2. Objetivos de la tesis doctoral

La aparición de los ataques DoS a baja tasa plantea numerosas cuestiones desde el punto de vista de la investigación. En primer lugar, es necesario explorar el alcance de dicho tipo de ataques. Además, también es preciso el estudio y desarrollo de mecanismos de detección, prevención y respuesta a los mismos, con el fin de asegurar el funcionamiento de los sistemas.

En esta línea, la tesis doctoral trata de explorar, desde el punto de vista del atacante, las posibilidades que existen de utilizar las técnicas de ataques DoS a baja tasa para su ejecución contra servidores en Internet o cualquier red de comunicaciones.

El trabajo de investigación de esta tesis tiene como objetivo aportar una visión de las posibilidades y alternativas que el atacante dispone para la ejecución de estos ataques. Su finalidad es la de poner a disposición de la comunidad investigadora una guía de referencia que permita abordar la elaboración de mecanismos de defensa, como la detección, prevención y respuesta.

1.3. Desarrollo del trabajo

Metodología seguida en la investigación

Para el desarrollo de la investigación se ha seguido una metodología que ha dividido el trabajo en diferentes fases de estudio:

1. Estudio en un escenario simple: servidores iterativos. En este estudio primero se ha pretendido explorar si se pueden aplicar técnicas que permitan la ejecución de ataques DoS a baja tasa contra servidores iterativos, considerándolos como los escenarios más sencillos posibles.

2. Definición de un marco de evaluación de la eficiencia. Esta fase consiste en la elaboración de indicadores que permiten medir el rendimiento del ataque en términos de la indisponibilidad que generan en el servidor víctima del ataque, y de la cantidad de tráfico necesaria para provocar esta denegación del servicio.

3. Definición de un modelo matemático. A continuación se ha desarrollado un modelo matemático que representa el comportamiento del sistema servidor bajo las condiciones del ataque. Este modelo permite obtener los valores de los indicadores de rendimiento definidos en la fase anterior en función de los parámetros de diseño del ataque.

4. Extensión a servidores concurrentes. A continuación se realizado la extensión del ataque a sistemas de tipo concurrente, es decir, aquellos en los que el procesado de las peticiones se realiza de forma paralela, ya sea de forma virtual mediante varias hebras o procesos, o real mediante varios procesadores. En esta fase se ha realizado tanto la adaptación de las técnicas exploradas en la fase 2, como también de las herramientas de medición y evaluación del ataque, es decir, del modelo matemático.

5. Mejoras del ataque. La última fase de la investigación ha consistido en explorar las diferentes alternativas que el atacante puede explorar para mejorar, por un lado, el rendimiento del ataque, en términos de eficiencia y también de nivel de tráfico necesario y, por otro, en evaluar las técnicas que se pueden utilizar para la ocultación del ataque.

Fundamentos básicos del ataque a baja tasa contra servidores

A continuación se presenta un resumen de las técnicas de ataque DoS a baja tasa contra servidores que, detalladamente, se desarrollan en la tesis doctoral.

El servidor víctima del ataque (Fig. 1) se modela como un sistema compuesto por M máquinas posibles y un balanceador de carga cuya función es redirigir las peticiones que llegan al servidor a alguna de las M máquinas disponibles, siguiendo una determinada política. Cada una de las máquinas se compone de una cola de servicio de tamaño finito en la que se almacenan las peticiones conforme van llegando, y un módulo de servicio, en el que se produce el procesado de las peticiones por parte de ciertos elementos de procesamiento (típicamente hebras o procesos).

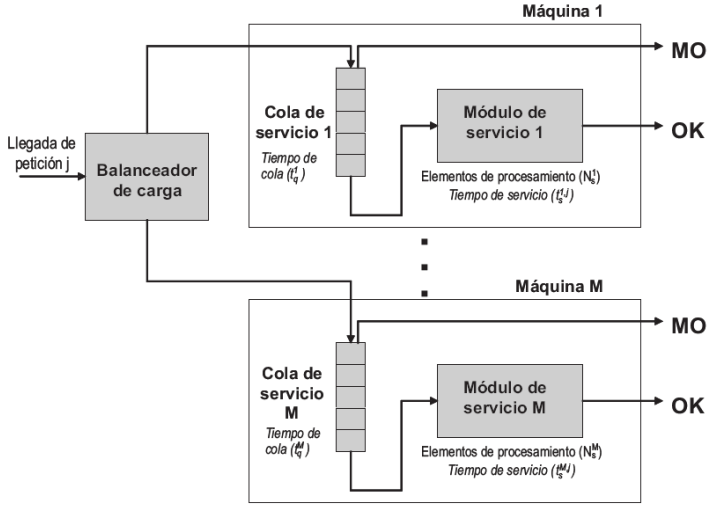

Fig. 1. Modelo del servidor.

El camino que, en funcionamiento normal, sigue cualquier petición será, en primer lugar, el almacenamiento en la cola de servicio, para posteriormente ser procesado en el módulo de servicio. Sin embargo, hay que tener en cuenta que, si al llegar una nueva petición a una máquina, su cola de servicio está completamente llena, la petición que llega será descartada (evento MO de la figura).

La estrategia que el ataque DoS a baja tasa sigue es la de, en primer lugar, conseguir que el servidor tenga todas las colas de servicio llenas de peticiones para, en segundo lugar, mantener esta situación mediante el envío inteligente de un tráfico cuya tasa no sea precisamente elevada. Existe un hecho que permite realizar esta tarea. Consiste en la constatación de que cada vez que se produce una respuesta en el servidor, alguna cola libera una posición. Por tanto, la estrategia del atacante será la de capturar dicha posición antes que cualquier usuario legítimo. Aunque esta tarea se podría hacer mediante el envío de una tasa elevada de tráfico, es posible hacerlo con una tasa reducida si se eligen adecuadamente los

instantes en los que hay que enviar el tráfico al servidor. Precisamente éste es el aspecto fundamental en el que se basan las técnicas desarrolladas en esta investigación. El atacante tratará de predecir los instantes en los que se producen las respuestas en el servidor para así enviar el tráfico únicamente en torno a dichos instantes, maximizando así la probabilidad de capturar las posiciones de las colas de servicio y, consecuentemente, provocando la denegación de servicio.

En la tesis se proponen varias técnicas para la predicción de los instantes en los que se producen las respuestas en el servidor. En el caso de servidores iterativos, se muestra cómo la observación de los tiempos entre respuestas en el servidor permite predecir con bastante exactitud los instantes de las respuestas futuras. En el caso más complejo de los servidores concurrentes, se proponen varias alternativas. En primer lugar, realizar la predicción del tiempo de servicio para determinadas peticiones y utilizar la técnica utilizada para servidores iterativos. En segundo lugar, utilizar la información aportada por el propio funcionamiento de la aplicación o servidor víctima y determinar la existencia de comportamientos cuasi-deterministas que permiten predecir los instantes en los que se producen las respuestas.

Precisamente para este último tipo de técnicas, es decir, las que aprovechan comportamientos deterministas en el servidor, en la tesis se propone el método de ataque para un tipo de servidor de uso ampliamente extendido en Internet, el servidor HTTP1.1 con característica de conexiones persistentes. Se detalla el procedimiento que un potencial atacante seguiría para conseguir predecir los instantes en los que se producen las respuestas en el servidor.

Una vez que se han predicho los instantes en los que se producen las respuestas, el ataque DoS a baja tasa contra servidores se ejecuta, por parte del atacante, mediante el envío al servidor de ondas de tráfico de tipo ON/OFF, denominadas periodos de ataque, consistentes en secuencias de inactividad (durante un tiempo $t_{offtime}$) seguidos de periodos de actividad (tiempo t_{ontime}) (Fig. 2). Durante los períodos de actividad, el atacante envía mensajes al servidor a una tasa $1/\Delta$. Los parámetros $t_{offtime}$, t_{ontime} y Δ son los que permiten el diseño del ataque, y deben elegirse de modo que la llegada al servidor de los mensajes de ataque se produzca en torno al instante estimado de ocurrencia de las respuestas o salidas.

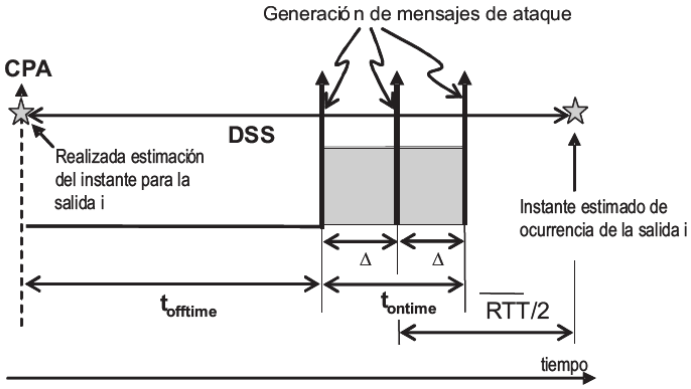

Fig. 2. Estructura de la onda de ataque

Esta forma de onda se debe repetir para cada uno de los instantes estimados de respuesta. La implementación de este mecanismo conlleva ciertas dificultades y se produce la aparición de ciertos problemas que se abordan en la tesis. Los más destacados son los siguientes:

- La existencia de variaciones en los tiempos de servicio del servidor hace que la estimación de los instantes de aparición de las respuestas presente un error.
- Existen variaciones adicionales provocadas por la existencia de un tiempo de ida y vuelta entre el servidor y el atacante. Este tiempo es variable incluso para cada servidor considerado independientemente, y dicha variación depende, entre otras causas, de las condiciones de la red, el encaminamiento seguido por los mensajes de ataque, etc.

- La aparición de numerosas respuestas en el servidor hace difícil un diseño que permita al atacante generar de forma sincronizada, incluso de manera distribuida, los diferentes periodos de ataque.
- El ataque se debe llevar a cabo de modo robusto, de forma que se consideren situaciones en las que los periodos de ataquen no tengan éxito en la captura de posiciones en las colas. Esto produce numerosas situaciones diversas que se deben abordar con un diseño común.
- Es deseable, para el atacante, poder controlar la cantidad de tráfico enviado al servidor e, incluso, establecer mecanismos que permitan, gradualmente, ir elevando el nivel de tráfico enviado en función del grado de denegación de servicio requerido.

En la tesis se plantean las soluciones a estos problemas mediante la propuesta de un diseño software multihebra. Se aportan las soluciones para el dimensionamiento del número de hebras de ataque que se deben utilizar según las condiciones que se deseen para el ataque, el comportamiento que cada hebra de ataque debe tener en cada caso, y se muestran diferentes soluciones para la comunicación entre hebras de ataque y sus problemas asociados.

1.4. Conclusiones

En resumen, el trabajo de investigación realizado:

- Presenta un estudio exhaustivo de las posibles técnicas de ataque DoS a baja tasa contra servidores, considerando la problemática asociada a la ejecución de los servidores en entornos con condiciones variables en los que se complica la ejecución del ataque.
- Se ha propuesto un diseño para el ataque, que se ha contrastado ampliamente con una base experimental mediante su implementación en entornos de simulación y entornos reales (ver apartado de resultados).
- Se ha desarrollado un modelo matemático de gran complejidad que permite la evaluación del rendimiento del ataque.

Los principales hallazgos de esta tesis son:

- Se ha detectado que numerosos sistemas actuales poseen vulnerabilidades que permiten la ejecución de ataques DoS de baja tasa. Más concretamente, se ha mostrado detalladamente cómo se pueden llevar a cabo contra servidores del tipo HTTP1.1 con conexiones persistentes.
- Se ha encontrado que el conocimiento del tiempo entre salidas o respuesta en un servidor iterativo permite la ejecución de los ataques DoS a baja tasa contra servidores de tipo iterativo.
- Se ha evidenciado el peligro de exhibir comportamientos deterministas en los diseños de las aplicaciones. Este tipo de comportamientos son una fuente de riesgo ante este tipo de ataques.
- Se ha mostrado que es factible la ejecución de los ataques DoS a baja tasa, tanto contra servidores iterativos como concurrentes. Además, se ha verificado la versatilidad de estos ataques, en el sentido de que permiten al atacante adoptar una amplia variedad de configuraciones y alternativas.
- Se ha modelado el comportamiento de este tipo de ataques, aportando un conocimiento detallado de su operación y funcionamiento.

Este trabajo, en conclusión, precisamente por facilitar la comprensión de las posibilidades que el ataque DoS a baja tasa posee, debe ser el punto de partida para la generación de mecanismos de defensa frente a este tipo de ataques, ya sea en el campo de la detección, como también en su prevención y respuesta.

2. Resultados obtenidos

La experimentación realizada en esta tesis ha ido enfocada a la evaluación del rendimiento que los diferentes diseños propuestos para el ataque permiten obtener al atacante. De este modo, el rendimiento se ha medido en base a tres indicadores:

- *Disponibilidad (D)*: Se define como la ratio, en porcentaje, entre el número de peticiones procedentes de usuarios legítimos que son efectivamente atendidas por el servidor y el número total de peticiones enviadas por éstos.

- *Porcentaje de tiempo disponible* (T_D): En un escenario en el que no existe tráfico de usuarios, se define el porcentaje de tiempo disponible, T_D, para un tiempo de observación fijado, como el porcentaje de dicho tiempo de observación durante el cual existe al menos una posición libre en el servidor de modo que una nueva petición entrante pueda ser aceptada.

- *Sobrecarga (S)*: Se define como la ratio, en porcentaje, entre la tasa de tráfico generada por el atacante y la máxima tasa de tráfico aceptada por el servidor.

En esta tesis doctoral se ha seguido la evaluación de los diseños propuestos para el ataque en base a tres bases experimentales: simulación, entornos reales y modelos matemáticos.

Evaluación en entorno de simulación

Para ello, se ha utilizado el simulador de redes NS2, en el cual se ha procedido a la implementación de un módulo que actúa como servidor concurrente o iterativo, de un generador de tráfico legítimo, y de un objeto atacante que genera el tráfico de ataque.

En estos experimentos se ha constatado que el rendimiento obtenido por el ataque es muy alto (baja disponibilidad (D) del servidor y baja sobrecarga). Además, se ha observado que el atacante tiene múltiples posibilidades en la configuración del ataque para obtener diferentes valores tanto de D como de S. Esto se puede observar en la Fig. 3, donde se representan los valores de disponibilidad y sobrecarga para 18 configuraciones diferentes del ataque DoS a baja tasa.

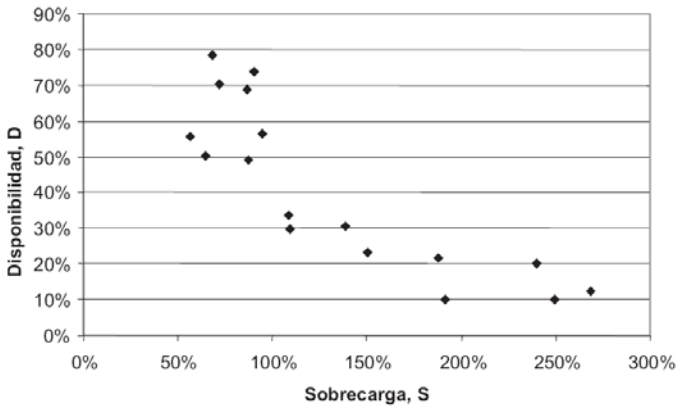

Fig 3. Disponibilidad, *D*, *vs.* sobrecarga, *S*, para 18 configuraciones diferentes de ataque.

Además, también se han realizado numerosos experimentos encaminados a comprobar la mejora que los diseños propuestos para el ataque suponen cuando se compara su rendimiento con el obtenido de una estrategia en la que se manda la misma carga de mensajes al servidor, pero enviados de forma aleatoria, siguiendo una distribución de Poisson (estrategia *naïve*). Estos experimentos han demostrado que existe una considerable mejora con los diseños propuestos en la tesis. Algunos de estos resultados se muestran en la Fig. 4. En ella se observa que los valores de disponibilidad del servidor obtenidos por el ataque propuesto (serie

con int.) siempre son mejores (más bajos), que los de la estrategia *naïve*, incluso usando sobrecargas más bajas en el ataque propuesto.

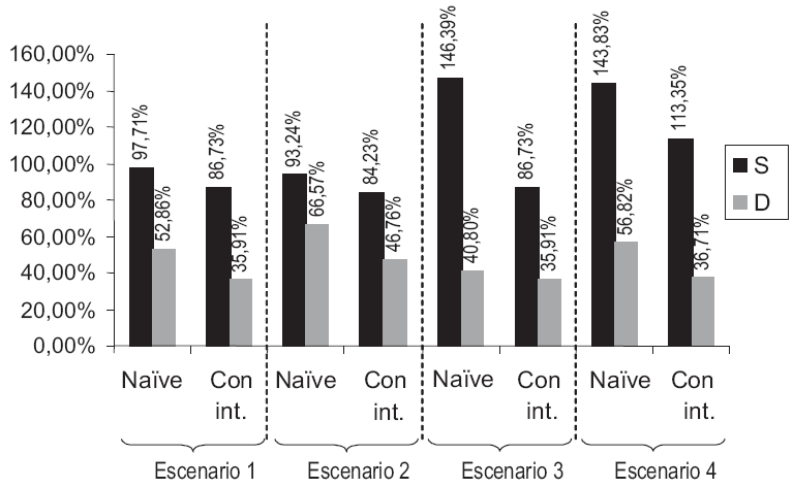

Fig 4. Comparación entre la estrategia inteligente y la *naïve* para tres configuraciones de ataque diferentes.

Evaluación en entorno real

Se ha procedido a la implementación del software de ataque en una plataforma Win32. Además, el ataque se ha llevado a cabo en una red real en la que se ha ubicado un servidor Web apache 2.0.52 instalado en una plataforma WinXP.

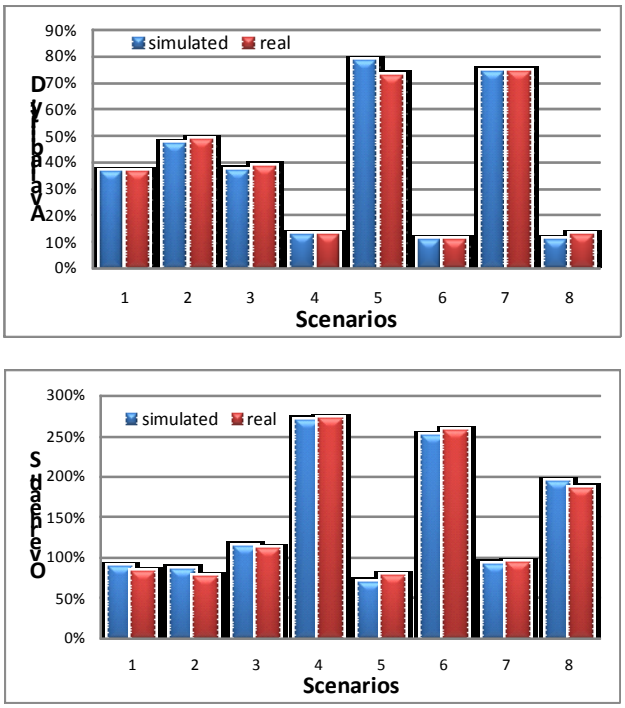

Fig 5. Resultados obtenidos en el entorno real comparados con los obtenidos en simulación, para 8 escenarios de ataque diferentes: (a) valores de disponibilidad, D y (b) de sobrecarga, S.

Algunos de los resultados obtenidos se representan en la Fig. 5, en la que se realiza una comparación entre los valores de los indicadores de rendimiento obtenidos en un entorno de simulación, y aquellos que se producen en un entorno real. Como se puede observar y se muestra de forma más detallada en la versión completa de la tesis, los valores obtenidos en

simulación y en entorno real son muy similares. El hecho de que los resultados obtenidos de las simulaciones no difieran considerablemente del comportamiento real permite extrapolar las conclusiones obtenidas a estos últimos entornos.

Evaluación mediante el modelo matemático

El modelo matemático permite la obtención de los valores para los indicadores de rendimiento a partir de expresiones analíticas que relacionan dichos indicadores con los parámetros de diseño del ataque. Las expresiones finales obtenidas para los indicadores son las siguientes:

$$T_D = 100 \cdot \frac{C}{T} \cdot \int_0^{\infty} T_D(s) \cdot g(s) ds \qquad T_D(s) = \sum_{i \in \mathcal{I}} T_D^i(s)$$

$$\begin{aligned} T_D^i(s) \quad = \quad & \int_a^b t_D^U(t)\big|_b \cdot P_j^U(t)\big|_a^b \cdot f_j(t)dt + \int_a^b t_D^U(t)\big|_b \cdot P_{j+1}^U(t)\big|_a^b \cdot f_{j+1}(t)dt + \\ & \int_a^b t_D^{\overline{U}}\big|_a^b \cdot P_{j+1}^{\overline{U}}(t)\big|_a^b \cdot f_{j+1}(t)dt \end{aligned}$$

$$D = 100 \cdot \frac{P_u \cdot C}{\lambda \cdot T} \qquad P_u = \int_0^{\infty} P_u(s) \cdot g(s) ds \qquad P_u(s) = \sum_{i \in \mathcal{I}} \left(1 - e^{-\lambda T_D^i(s)}\right)$$

$$S = 100 \cdot \frac{C'}{C} \cdot \left(floor \left[\frac{t_{ontime}}{\Delta} \right] + 1 + (1 - P_u) \right)$$

El modelo matemático propuesto ha permitido, fundamentalmente, extender las conclusiones obtenidas mediante simulación a cualquier tipo de escenario. La existencia del modelo matemático permite obtener el rendimiento del ataque en cualquier configuración proporcionada a sus parámetros de diseño y también a los que definen el comportamiento del servidor y la red de comunicación.

Finalmente, hay que señalar que los resultados obtenidos del modelo se han contrastado con los extraídos de las simulaciones, realizando una comparativa que indica que el ajuste del modelo es aceptable para su utilización como herramienta de estimación del rendimiento. Como ejemplo, la Fig. 6 muestra una comparación realizada para el indicador T_D. En ella se aprecia que los valores del modelo y los de la simulación no presentan desviaciones considerables.

En resumen, las conclusiones extraídas de estas evaluaciones son las mostradas en el apartado de conclusiones anteriormente expuesto.

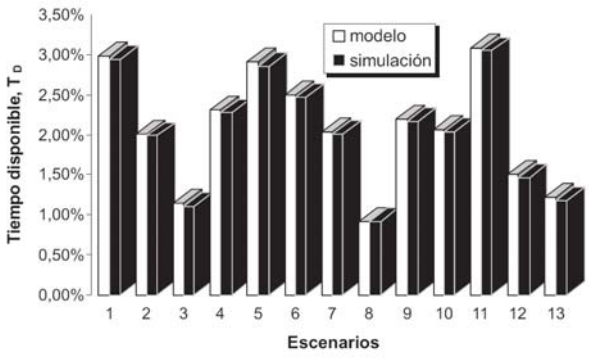

Fig. 6. Comparación del valor T_D obtenido mediante la simulación y a través del modelo matemático, para 13 escenarios de ataque diferentes.

3. Aplicabilidad práctica en el área

Considerando que el efecto del ataque de denegación de servicio solamente tiene lugar mientras el ataque se está llevando a cabo, podría pensarse el impacto que la denegación de servicio produce, en comparación con otro tipo de ataques, no es muy importante. Sin embargo, para muchos usuarios de la red puede ser devastador. En efecto, el uso de servicios de *Internet* se ha convertido en una parte importante de nuestras vidas diarias. *Internet* se está utilizando de forma creciente para realizar negocios y proporcionar servicios críticos. Algunos ejemplos de los efectos e impacto que pueden producir los ataques de denegación de servicio son los siguientes:

- Los sitios de *Internet* que ofrecen servicios a usuarios a través de peticiones *on-line* solamente ganan dinero cuando los usuarios pueden acceder a dichos servicios. Por ejemplo, una compañía de aviones que vende sus billetes por *Internet* dejará de hacer negocio mientras dure el ataque. Además, si los ataques son de corta duración pero frecuentes, se puede afectar a la imagen de la compañía.

- Los sitios que ofrecen noticias y los buscadores están subvencionados por la publicidad que ofrecen al público. Sus beneficios dependen del número de usuarios que visitan dichas páginas.

- Los ataques de denegación de servicio a dichos sitios afectan directamente al número de usuarios que visitan las páginas y, por tanto, al beneficio obtenido. Además, la pérdida de popularidad de dichos sitios debido a su vulnerabilidad a este tipo de ataques afecta a la financiación que reciben procedente de publicidad.

- Muchos sitios ofrecen servicios críticos de forma gratuita a los usuarios de internet. Por ejemplo, el servicio de resolución de nombres de dominio (DNS) [TVS03], que proporciona la información necesaria para traducir direcciones Web en formato legible (como www.ejemplo.com) en direcciones IP (como 12.35.37.123). Todos los navegadores Web y otras muchas aplicaciones se apoyan en este servicio para ejecutar las acciones solicitadas por los usuarios. Si los servidores DNS son atacados mediante DoS o DDoS, muchos sitios quedarán indisponibles debido a que no se podrán traducir sus direcciones, aunque los recursos de dichos sitios estén perfectamente disponibles y en condiciones de dar servicio.

- Muchos negocios dependen de *Internet* para la realización de actividades críticas. Un ataque DoS podría interrumpir una reunión en conferencia o un gran pedido que se intenta realizar por parte de un cliente. Puede impedir que una compañía envíe un documento importante en una fecha límite o puede interferir en su puja por un contrato.

- *Internet* se está utilizando cada vez más para facilitar la gestión de los servicios públicos, como la sanidad, gestión de impuestos, y también para envío de información importante, como informes de tiempo y tráfico para barcos. Los ataques DoS hacia este tipo de servicios pueden afectar a entidades cuya actividad no está directamente relacionada con los ordenadores o *Internet*.

Todos estos ejemplos aportan una idea de la importancia que pueden adquirir los efectos de un ataque de denegación de servicio actualmente. De hecho, este tipo de ataques están siendo objeto de cuantiosos esfuerzos por parte no solo de las principales compañías en el campo de la seguridad en redes, sino también por parte de la comunidad científica.

Por ello, la aplicación inmediata de este trabajo es la aportación de un conocimiento sobre el método de ejecución de los ataques DoS a baja tasa de modo que se permite extraer conclusiones para la elaboración de mecanismos de defensa, tanto en el campo de la prevención, como para la detección y respuesta.

Por otro lado, hay que señalar el fuerte impacto que la descripción de estos ataques tiene a la hora de desarrollar mecanismos que protejan infraestructuras críticas, tales como controladores

de redes de alta tensión, mecanismos de control de infraestructuras civiles, sistema SCADA, o cualquier mecanismo de control que dependa de un servidor y que esté conectado a una red de comunicaciones. De hecho, una de las publicaciones extraídas de esta tesis se ha realizado en la 2nd International Workshop on Critical Infrastructures Security (CRITIS'2007) (ver bibliografía y anexo para la publicación).

Por último, hay que destacar que los estudios realizados en la tesis doctoral se han aplicado a entornos reales, en los que se ha demostrado que es relativamente sencillo conseguir la denegación de servicio de un servidor Web Apache mediante las técnicas propuestas en este trabajo.

4. Originalidad del trabajo

El trabajo presentado presenta tres aspectos fundamentales en cuanto a su originalidad:

a) Objeto de estudio.
b) Enfoque del trabajo.
c) Metodología aplicada.

En primer lugar, considerando el objeto de estudio, los ataques de baja tasa se han estudiado con respecto al protocolo TCP, por lo que su aplicación a servidores y sistemas finales se considera un aspecto novedoso.

En cuanto al enfoque del trabajo, se puede decir que, tradicionalmente, el estudio en este tipo de aspectos de seguridad ha dedicado sus esfuerzos al desarrollo de sistemas de defensa frente a problemas que han aparecido y se han detectado, principalmente originados por la comunidad hacker. En contra, este estudio pretende profundizar en el enfoque que un atacante aplicaría a la hora de estudiar este tipo de ataques. Esto conlleva la realización de un profundo análisis de los métodos de ataque y partir de la mentalidad de quien trata de infligir normas, más que de la de aquél que trata de protegerse. Este enfoque del problema es novedoso en sí mismo.

Por último, la metodología aplicada en el trabajo de investigación también presenta aspectos novedosos. Más concretamente, hay que señalar el desarrollo de un modelo matemático como el aspecto más relevante en este punto. Tradicionalmente, la fase experimental de todos estos estudios de investigación se ha basado en la realización de experimentos en plataformas reales o de simulación. Sin embargo, en el ámbito de los ataques de denegación de servicio, el autor no puede constatar la existencia de trabajos que aborden la evaluación de la eficiencia del ataque en términos de un modelo matemático.

En resumen, los tres aspectos más novedosos que presenta esta tesis están relacionados en primer lugar con su objeto de estudio, en segundo lugar con el enfoque que se hace del trabajo, y por último, en la metodología aplicada para la consecución de resultados.

5. Anexos y otras referencias

Se indica a continuación algunas referencias para la evaluación de la calidad de la tesis.

1. Publicaciones relacionadas con la tesis: 5 publicaciones en revistas indexadas JCR y una publicación en congreso internacional de reconocido prestigio.

    - Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro, On the Design of a Low-Rate DoS Attack Against Iterative Servers. Proceedings of the SECRYPT 2006, pp.149-156, Setúbal (Portugal), August, 2006.

- Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro: Low Rate DoS Attack to Monoprocess Servers. Lecture Notes on Computer Science (SPC 2006), vol. 3934, pp. 43-57, 2006

- Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro: Mathematical Foundations for the Design of a Low-Rate DoS Attack to Iterative Servers (Short Paper). Lecture Notes on Computer Science (ICICS 2006), vol. 4307, pp. 282-291, 2006

- Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro: Assessment of a Vulnerability in Iterative Servers Enabling Low-Rate DoS Attacks. Lecture Notes on Computer Science (ESORICS 2006), vol. 4189, pp. 512-526, 2006

- Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro: Evaluation of a low-rate DoS attack against iterative servers. Computer Networks 51(4): 1013-1030 (2007)

- Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Pedro Garcia-Teodoro: LoRDAS, a low-rate DoS Attack against Application Servers, in Pre-proceedings of the 2nd International Workshop on Critical Infrastructures Security (CRITIS'07). To appear in Lecture Notes on Computer Science. 2007.

2. Referencias por parte de otros investigadores a la tesis doctoral, certificando el grado de calidad de la misma (se adjuntan como anexos a este resumen).

    - Carta de la Dra. Emilia Rosti, associate professor del Dipartimento di Informatica e Comunicazione de la Università degli Studi di Milano

    - Carta del Dr. Mattia Monga, associate professor del Dipartimento di Informatica e Comunicazione de la Università degli Studi di Milano

    - Pese a la reciente aparición de la tesis, los trabajos que se derivan de ella ya han sido citados en alguna revista internacional:

      Nadarajah, S. and Kotz, S. 2007. On the convolution of Pareto and gamma distributions. *Comput. Networks* 51, 12 (Aug. 2007), 3650-3654. DOI= http://dx.doi.org/10.1016/j.comnet.2007.03.003

3. Financiación para el trabajo de la tesis:

    - La financiación para la realización de esta tesis se ha obtenido del proyecto CYCIT con código TSI2005-08145-C02-02 del Ministerio de Educación y Ciencia de España.

6. Bibliografía

[Carracedo, 2004] Carracedo, J. (2004). *Seguridad en redes telemáticas*. Mc Graw Hill. ISBN: 84-481-4157-1.

[Kuzmanovic and Knightly, 2003] Kuzmanovic, A. and Knightly, E. (2003). Low-rate TCP-targeted denial of service attacks (The shrew vs. the mice and elephants). In *Proc. ACM SIGCOMM'03*, pp. 75-86.

[Mirkovic et al., 2004] Mirkovic, J., Dietrich, S., Dittrich, D., and Reiher, P. (2004). *Internet Denial of Service. Attack and Defense Mechanisms*. Prentice Hall. ISBN: 0-13-147573-8.

[Shevtekar et al., 2005] Shevtekar, A., Anantharam, K., and Ansari, N. (2005). Low rate TCP denial-of-service attack detection at edge routers. *IEEE Communications Letters*, 9:363-365.

[Stallings, 2003] Stallings, W. (2003b). *Network Security Essentials*. Prentice Hall, 2nd edition. ISBN: 0-13-035128-8.

[Sun et al., 2004] Sun, H., Lui, J., and Yau, D. (2004). Defending against low-rate TCP attacks: Dynamic detection and protection. In *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP04)*, pp. 196 - 205.

[Yang et al., 2004] Yang, G., Gerla, M., and Sanadidi, M. Y. (2004). Defense against low-rate TCP-targeted denial-of-service attacks. In *Proc. IEEE Symposium on Computers and Communications (ISCC'04)*, pp. 345 - 350, Alexandria, Egypt.

Report on the doctoral thesis
"Low rate DoS attacks against servers"
by Ph.D. Candidate Gabriel Maciá-Fernández
Advisors: Jesús E. Díaz Verdejo, Pedro García Teodoro

This dissertation focuses on the problem of denial of service (DoS) attacks that use the minimum resources to keep the victim server busy, thus unavailable to legitimate users. Such a type of DoS attack is called low-rate since the rate at which malicious requests are sent is usually much lower than that used in a flooding attack. As a consequence, it is easier for an attacker to go undetected by an intrusion detection system.

The problem investigated in this dissertation is fairly novel and not much work exists about it. The dissertation describes very clearly how the attack works, both when the victim is a serial server and a concurrent one and presents various interesting results. The major contributions/strengths of this thesis are in the following:

1. the detailed description and formalization of the attack mechanism, conditions under which it can succeed, and its consequences;

2. the development of an analytical model for the analysis of the system parameters, both from the attacker and server points of view, for both serial and concurrent servers;

3. the presentation of results of extensive simulations that validate the analytical model; and

4. the presentation of experimental results conducted on a real system.

The quality of contributions is very good, and so is the quality of the writing. These are results that have the potential to be widely used and cited by the community, and sparkle a whole new activity related to the identification of such attacks by intrusion detection systems. Several of the chapters of the dissertation have appeared as contributions in good quality journals and conferences in the area of computer and network security. Nonetheless, all chapters relate to each other very smoothly, a not-so-common characteristic in Ph.D. dissertations which often tend to be a collection of articles the candidate has presented during the years as Ph.D student.

Overall, it is my opinion that this is a high quality dissertation on network security. I congratulate the candidate for original and exciting contributions in a young research field.

Prof. Emilia Rosti
Associate Professor
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39, 20135 - Milano, Italy
April 6, 2007.

Università degli Studi di Milano
Dipartimento di Informatica e Comunicazione
Via Comelico 39/41
I 20135 – Milano

To whom it may concern

Milano, 25th April 2007

Subject: Report on PhD thesis

Dear Sirs,

please find enclosed my report on the thesis "Low-rate DoS Attack against Servers" ("*Ataques de denegación de servicio a baja tasa contra servidores*"), authored by Gabriel Maciá-Fernández.

Summary

The thesis studies Denial of Service attacks carried out by exposing servers to a low rate malicious traffic. A novel attack is proposed that exploits the vulnerability intrinsic in the fact that malicious users might be able to foresee when a slot in the service queue will become available by observing the output rate of the service. This information can be used to keep the server busy mostly with malicious requests, while neglecting legitimate customers.

Comments on the approach

The system under attack is modelled as an iterative server which consumes requests coming from a service queue to produce outputs. The attacker is supposed to be able to measure inter output intervals between identical requests. Attacker's observations are then used to characterized a random process, representing the service time, used to derive the optimal time to send a malicious request. The analyzed attack scenario seems to me quite reasonable, however in some real world cases some difficulties may

arise:

- To identical requests might correspond fairly different service times; this not only due to the variations in the operating environment, but it could be a specific property of the service, as in the case of cached computations. In these cases a bimodal distribution could be more appropriate for modelling service time.
- Identical requests could be queued together, thus effectively countering the attack, or at least forcing it to be analogous to a high rate flooding.

The evaluation of the predicting model is mathematically sound and simulations are backed up by experiments with off-the-shelf applications. The assessment of the approach shows that in fact the approach is effective in reducing the perceived user performance, *with respect to a blind attack employing the same effort.* In other words, *ceteris paribus*, a given rate of malicious traffic is able to produce a greater decrease of the service level with respect to blind flooding. However, the lower level of the traffic could be high enough to be noticeable by intrusion detectors.

Thesis evaluation

The thesis presents solid research work, as witnessed by two articles describing the approach published in the proceedings of relevant international conferences (ESORICS, SECRYPT) and an international peer reviewed journal (Computer Networks). The research contributes to the study of information security both by describing a novel approach to application-level denials of service, and by proposing analytical means to the assessment of the effectiveness of the attack effort and the possible countermeasures.

Yours faithfully,

dr. Mattia Monga