Mejoras de seguridad en el protocolo TCP

Fernando Gont

Universidad Tecnológica Nacional

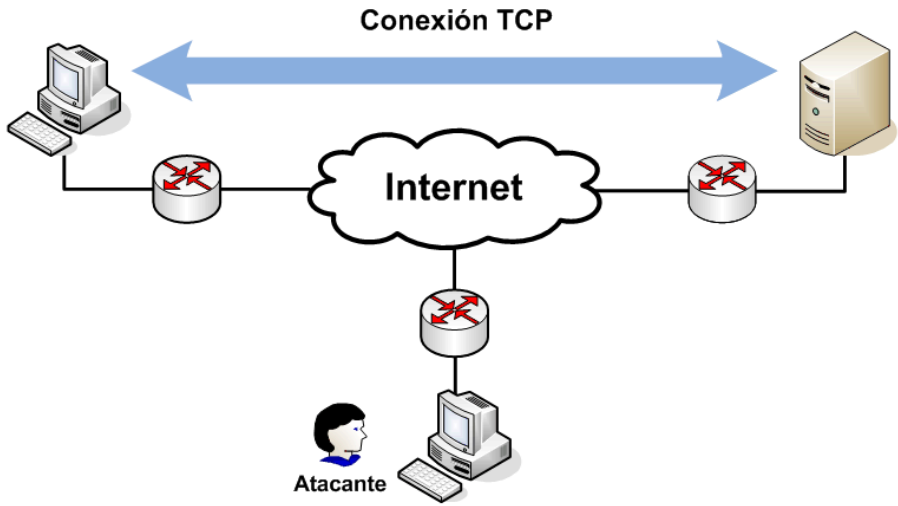
Facultad Regional Haedo

Argentina

LACNIC X, Mayo 21-25, 2007. Isla Margarita, Venezuela

Ataques ciegos contra TCP

- En los últimos años se han divulgado dos familias de ataques “ciegos” contra TCP
  - “**Slipping in the Window**”: Ataques basados en segmentos TCP falsificados (NISCC vulnerability advisory #236929)
  - “**ICMP attacks against TCP**” : Ataques basados en paquetes ICMP falsificados (NISCC vulnerability advisory #532967)
- Estos ataques pueden ser realizados sin la necesidad de acceder a los paquetes pertenecientes a la conexión atacada.



- Afortunadamente, existen en la IETF algunas iniciativas para mitigar estas vulnerabilidades

Ataques “Slipping in the Window”

- Esta familia de vulnerabilidades se basan en la falsificación de segmentos TCP.
  - Segmentos RST: Permiten la realización de ataques de reseteo de conexión.
  - Segmentos SYN: Permiten la realización de ataques de reseteo de conexión.
  - Segmentos de “datos”: Permiten la realización de ataques de inyección de datos.
- Requieren que el atacante conozca (o pueda adivinar) los valores {client IP, client TCP port, server IP, server TCP port}, así como también un número de secuencia (TCP sequence number) válido.
- La gran disponibilidad de ancho de banda, así como el uso de ventanas TCP grandes (entre otros), hacen que estos ataques sean viables.

Actividad relevante en la IETF

En el área de estas vulnerabilidades, la IETF ha trabajado en los siguientes documentos:

- Soluciones generales
  - “Improving TCP’s Robustness to Blind In-Window attacks”, Ramaiah, A., Stewart, R., Dalal, M. 2007. (draft-ietf-tcpm-tcpsecure-07.txt)
  - “Port randomization”, Larsen, M., Gont, F. 2007. (draft-larsen-tsvwg-port-randomization-01.txt)
- Soluciones específicas (orientadas a BGP)
  - “The Generalized TTL Security Mechanism”. Gill, V., Heasley, J. Meter, D. 2004. (RFC 3682)
  - Reemplazo de la opción TCP MD5:
    - “The TCP Simple Authentication Option”, Touch, J., Mankin, M. 2006. (draft-touch-tcpm-tcp-simple-auth-02.txt)
    - “Authentication for TCP-based Routing and Management Protcols”. Bonica, R. et al. 2007.(draft-bonica-tcp-auth-04.txt)

Improving TCP's Robustness to Blind In-Window Attacks (draft-ietf-tcpm-tcpsecure-07.txt) (I)

Propone modificaciones a la máquina de estados TCP para dificultar la realización exitosa de estos ataques.

- Procesamiento de segmentos SYN
  - En los estados sincronizados se responde con un ACK ("challenge ACK"), sin importar el número de secuencia del segmento TCP en cuestión.
- Procesamiento de segmentos RST
  - La conexión se aborta únicamente si SEG.SEQ == RCV.NXT. Si esto no se cumple, pero SEG.SEQ está dentro de la ventana de recepción, se responde con un ACK ("challenge ACK"). En caso contrario, se descarta el segmento RST.
- Procesamiento de los segmentos de "datos"
  - Ahora: Se requiere que SEG.SEQ esté dentro de la ventana de recepción, y que (SND.UNA - MAX.SND.WND) <= SEG.ACK <= SND.NXT

Improving TCP's Robustness to Blind In-Window Attacks (draft-ietf-tcpm-tcpsecure-07.txt) (II)

Estado actual

- El draft se adoptó como WG document del TCPM WG en 2004, existiendo sobre el mismo una patente pendiente (IPR) de Cisco.
- El TCPM WG se encuentra discutiendo la categoría bajo la cual debería publicarse este draft (Standards track, Informational, etc) y el nivel de requerimiento de las modificaciones introducidas (MAY/SHOULD/MUST, etc).
- Se prevee su publicación como RFC en 2007.

Port randomization (I) (draft-larsen-tsvwg-port-randomization-01.txt)

- La mayoría de las implementaciones actuales de TCP eligen los puertos efímeros de un rango de puertos innecesariamente pequeño (por ej., 1024-4999). Adicionalmente, utilizan una misma secuencia incremental para las conexiones “salientes” realizadas con cualquier nodo/servicio, lo cual hace que los puertos TCP utilizados por los diversos clientes sean predecibles.
- Dado que los ataques **ciegos** requieren que el atacante conozca o pueda adivinar los valores {client IP, client TCP port, server IP, server TCP port}, eligiendo el client port de forma “aleatoria” se puede dificultar la tarea del atacante.
- Este documento propone, especificamente:
  - Utilizar para los puertos efímeros el rango 1024-65535.
  - La utilización de un algoritmo de selección de puertos efímeros basado en la idea introducida en RFC 1948 por Steven Bellovin para la selección de ISNs.

Port randomization (II) (draft-larsen-tsvwg-port-randomization-01.txt)

Estado actual

- El draft fue publicado para su discusión en el TSV WG.
- Fue discutido brevente en la lista de correo correspondiente, pero todavía no se a discutido su adopción como elemento de trabajo del TSV WG.
- En materia de implentaciones, el algoritmo propuesto ha sido implementado en Linux, y planea incorporarse en (al menos) FreeBSD.

The Generalized TTL Security Mechanism (GTSM) (RFC 3682)

- Limita la cantidad de sistemas que en principio pueden realizar ataques exitosos mediante la falsificación de segmentos TCP, estableciendo rangos aceptables para el TTL de los paquetes recibidos.
- El sistema que transimite información inicializa el campo TTL, (idealmente) con el valor 255. El sistema receptor del paquete comprueba que el TTL esté dentro un rango de valores aceptable. De no estarlo, descarta el paquete en cuestión.
- Este mecanismo particularmente útil en aquellas aplicaciones cuyos peers usualmente se encuentran en el mismo segmento de red, o a algunos pocos hops. En tal caso, el sistema transmisor puede inicializar el TTL en 255, y el receptor admitir solamente aquellos paquetes que tengan un TTL de 255.
- Este mecanismo apunta a ser utilizado por aplicaciones como BGP, ya que en el caso general no se tiene control ni sobre la inicialización del campo TTL, ni sobre la cantidad de hops entre los dos peers (ó cliente y servidor).
- Esta propuesta fue publicada como RFC Experimental en 2004.

Reemplazo de la opción TCP MD5

- Se publicaron dos internet-drafts, con el objetivo de reemplazar la opción TCP MD5 (RFC 2385), con el fin de solucionar algunas flaquezas de la misma.
  - “The TCP Simple Authentication Option”, Touch, J., Mankin, M. 2006. (draft-touch-tcpm-tcp-simple-auth-02.txt)
  - “Authentication for TCP-based Routing and Management Protcols”. Bonica, R. et al. (draft-bonica-tcp-auth-04.txt)
- El TCPM WG decidió formar un equipo de diseño, dirigido por Steven Bellovin, que se encuentra trabajando en un documento inicial sobre el cual trabajará el TCPM WG.
- Todavía no se ha publicado el documento inicial producido por el equipo de diseño.

ICMP attacks against TCP

- Se basan en el envío de mensajes ICMP falsificados
- Requieren **únicamente** que el atacante conozca (o pueda adivinar) los valores {source IP, source port, Dest. IP, Dest. Port}
- Tres tipos de vulnerabilidades:
  - Reseteo de conexión: Mediante el envío de ICMP “hard errors”
  - Degradación de tasa de transferencia: Mediante el envío de ICMP Source Quench
  - Degradación de performance: Mediante el envío de mensajes ICMP “fragmentation needed and DF bit set”
- La solución **no** es filtrar ICMP (se rompe el mecanismo Path-MTU Discovery, se pueden producir grandes delays al establecer conexiones TCP, etc.)
  - “TCP Problems with Path-MTU Discovery”. Lahey, K. 2000. (RFC 2923)
  - “TCP’s Reaction to Soft Errors”, Gont, F. 2007. (draft-ietf-tcpm-tcp-soft-errors-05.txt)
- Ni IPsec ni TCP MD5 eliminan (*per se*) estas vulnerabilidades.

ICMP attacks against TCP

En el área de estas vulnerabilidades, la IETF ha trabajado en los siguientes documentos:

- “ICMP attacks against TCP”, Gont, F. 2007. (draft-ietf-tcpm-icmp-attacks-02.txt):
- “Port randomization”. Larsen, M. and Gont, F. 2007.

ICMP attacks against TCP (I) (draft-ietf-tcpm-icmp-attacks-02.txt)

Modificaciones introducidas por el draft:

- Reacción a ICMP hard errors
  - Antes: Se abortaba la conexión
  - Ahora: Para conexiones en los estados sincronizados (>= ESTABLISHED) se almacena la información recibida, pero **no** se aborta la conexión
- Reacción a ICMP Source Quench
  - Antes: Se reducía la tasa de transferencia (se ponía a la conexión TCP en el estado Slow Start)
  - Ahora: Se ignoran los mensajes ICMP Source Quench
- Reacción a ICMP “frag needed and DF bit set”
  - Antes: Se modificaba la información del Path-MTU al recibir el mensaje ICMP
  - Ahora: Se modifica la información sobre el Path-MTU únicamente si no existe progreso en la conexión

ICMP attacks against TCP (II) (draft-ietf-tcpm-icmp-attacks-02.txt)

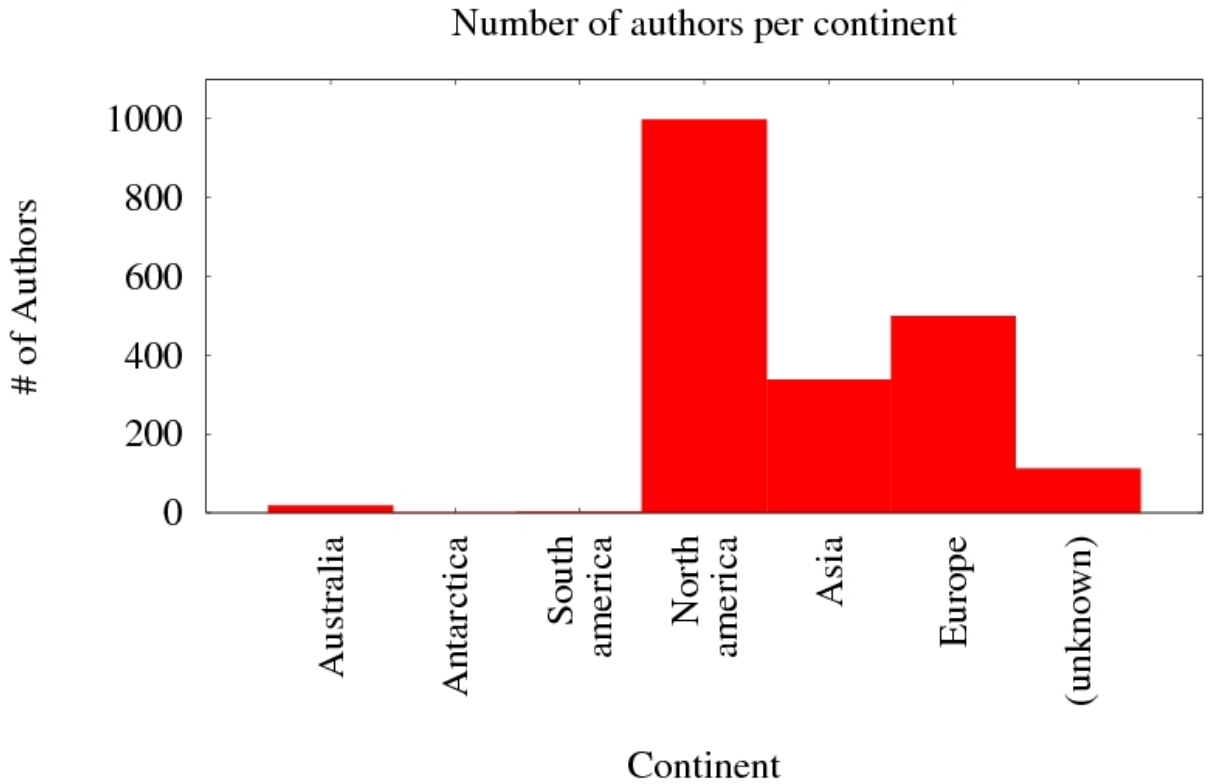
Estado del documento

- Aceptado como WG document del TCPM WG en 2005, para ser publicado con categoría **Informational**. Esto significa que las especificaciones continuarán recomendando la implementación de las vulnerabilidades descriptas.
- El documento se encuentra en proceso de revisión, con la idea de ser publicado como RFC durante este año.
- Pese a la lentitud del proceso en el ámibito de la IETF, el documento es un “industry standard”, estando casi la totalidad de su contenido implementado en la gran mayoría de las pilas TCP/IP.

Algunas “reflexiones”

- La gran mayoría de los problemas de seguridad en TCP radican en que el mismo fue diseñado sin considerar cuestiones de seguridad (por ej., SYN flood).
- Sin embargo, el hecho de que TCP no haya sido diseñado teniendo en cuenta consideraciones de seguridad no implica que no debamos mantener vulnerabilidades… en particular aquellas simples de mitigar.
- Si bien se han publicado una gran cantidad de reportes de vulnerabilidad referidos a TCP, no han habido muchos esfuerzos para documentar las vulnerabilidades (y sus respectivas soluciones) en el ámbito de la IETF (por ej., recién en 2007 tendremos un RFC documentando los ataques SYN-flood, y las posibles técnicas para mitigarlos)
- Mientras que las especificaciones no se modifiquen para solucionar las vulnerabilidades identificadas, se incrementa el riesgo de:
  - Que se sigan produciendo equipos con vulnerabilidades
  - Que las vulnerabilidades se reinventen en nuevos protocolos (por ej., reinvención de IPv4 source routing en IPv6 mediante el RH0)

(Shameless) Plug-in



- Hay muy poca participación latinoamericana activa en la IETF (3 autores, de acuerdo a http://www.arkko.com/tools/stats/countrydistr.html), muy probablemente por falta de apoyo de compañías, instituciones educativas, y organizaciones.
- Posiblemente sea algo para considerar por quienes estén en la posición de hacer algo al respecto.

Agradecimientos

- LACNIC
- Carlos M. Martinez, Florencia Bianchi y Ruth Puente @ LACNIC

…. y a Uds., los asistentes a esta presentación

Fernando Gont

e-mail: fernando@gont.com.ar

web: http://www.gont.com.ar