

Resultados de una evaluación de la seguridad del Transmission Control Protocol (TCP)

Fernando Gont

proyecto realizado para

UK Centre for the Protection of National Infrastructure

4to Evento de Seguridad en Redes de América Latina y el Caribe, LACNIC XII
Ciudad de Panamá, Panamá. Mayo 24-29, 2009

Enunciado del problema

- Durante los últimos veinte años, el descubrimiento de vulnerabilidades en implementaciones de los protocolos TCP/IP, y en los propios protocolos, han llevado a la publicación de un gran número de reportes de vulnerabilidad por parte de fabricantes y CSIRTs.
- Si bien hubo bastante trabajo en el área de seguridad de TCP, el mismo siempre estuvo esparcido en un sinnúmero de documentos y sitios web, muchos de los cuales proponen contramedidas a las mencionadas vulnerabilidades, sin realizar un análisis minucioso de las implicancias de las mismas sobre la interoperabilidad de los protocolos.
- Asimismo, el trabajo de la comunidad en esta área no ha reflejado cambios en las especificaciones correspondientes de la IETF.
- Es conocido en la comunidad que no puede realizarse una implementación segura del protocolo TCP a partir de las especificaciones de la IETF. Sin embargo, nunca se había hecho un esfuerzo en cambiar esta situación.

Descripción del proyecto

- En los últimos años, UK CPNI (Centre for the Protection of National Infrastructure) – antes UK NISCC (National Infrastructure Security Co-ordination Centre) – se propuso llenar este vacío.
- El objetivo fue producir documentos que sirvieran de complemento a las especificaciones de la IETF, con el fin de que, mínimamente, nuevas implementaciones no posean vulnerabilidades ya conocidas, y que las implementaciones existentes puedan mitigar estas vulnerabilidades.
- Finalmente, se esperaba llevar este material al ámbito de la Internet Engineering Task Force (IETF), para promover cambios en los estándares correspondientes.

Algunos resultados

- En febrero de 2009 CPNI publicó el documento “Security Assessment of the Transmission Control Protocol (TCP)” – consistente en 130 paginas, que incluyen los resultados del análisis de seguridad del protocolo TCP. El mismo se encuentra disponible en:
<http://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>
- Seguidamente, publicamos el mismo material como IETF I-D (draft-gont-tcp-security-00.txt). El mismo se encuentra disponible en:
<http://www.gont.com.ar/drafts/tcp-security/index.html>
- Hemos involucrado a distintos fabricantes para que revisen el documento en cuestión, lo analicen, y apliquen cambios en sus implementaciones de los protocolos en caso de considerarlo necesario.



Algunas áreas de trabajo

Obfuscación de puertos efímeros

- Propusimos la “obfuscación” de los puertos efímeros en base al esquema propuesto por “Port randomization” (Larsen & Gont), basado en el esquema definido para la generación de ISNs por RFC 1948).
- Asimismo, hemos propuesto la ampliación del rango de puertos utilizados para dichos puertos.
- Estas recomendaciones ya han sido implementadas en algunos sistemas (Linux implementó el esquema de obfuscación propuesto, y FreeBSD amplió el rango de los puertos efímeros).

Opciones TCP

- Existen más de 30 números de opción de TCP asignados por IANA.
- Resultó bastante complicado identificar la relevancia de las distintas opciones TCP en la actualidad
 - Algunas de ellas son popularmente conocidas, y estandarizadas por la IETF (por ej., MSS)
 - Algunos números de opción habían sido asignados hace muchos años atrás, pero nunca fueron utilizadas en ambientes de producción (por ej., Skeeter, Bubba, etc.)
 - Algunas opciones TCP han sido estandarizadas fuera de la IETF, y son utilizadas actualmente en ambientes de producción (por ej., SCPS Capabilities, Record boundaries, etc.)
- En todos los casos propusimos “chequeos de sanidad” para los contenidos de las distintas opciones.

TCP timestamps option

- Las opciones TCP timestamps se utilizan para la medición del Round-Trip Time (RTT) de una conexión, y Protection Against Wrapped Sequence Numbers (PAWS)
- Si los valores utilizados para los timestamps son predecibles, se hace más simple la realización de ataques contra conexiones TCP, y potencialmente se puede averiguar el “system uptime” del sistema en cuestión.
- Propusimos un esquema de obfuscación de los timestamps que mitiga dichas vulnerabilidades, y asimismo permite evitar problemas de interoperabilidad en TCP (fallos en el establecimiento de conexiones cuando ocurren colisiones de connection-id’s).
- La propuesta realizada será adoptada en la revisión actual del estandar correspondiente (RFC 1323).
- Asimismo, ha sido incorporada en Linux.

Remote OS detection via TCP/IP fingerprinting

- La técnica consiste en identificar el sistema operativo utilizado en un sistema remoto analizando la respuesta del mismo a distintos paquetes de prueba.
- ¿No es **demasiada** la precisión de nmap? ¿Realmente necesita cada versión de un sistema operativo de cada fabricante hacer algo distinto? ¿No se pueden unificar criterios?
- Unificamos criterios para la respuesta a tecncas de fingerprinting tales como:
 - FIN probe
 - Bogus flag test
 - RST sampling
 - Port-0 probe
- Todavía pendiente:
 - Unificar el uso y *framing* the opciones TCP

Urgent mechanism

- El “urgent mechanism” provee un medio para que una aplicación pueda marcar un “punto interesante” en el flujo de datos (sualmente un punto al cual el receptor de la información debería “saltar”).
- Hemos encontrado una variedad de inconsistencias en la implementación de este mecanismo, con el potencial de:
 - Evasión de NIDS (por ambigüedades ene l flujo de datos resultante)
 - Denegación de Servicio (DoS)
- Asimismo hemos generado recomendaciones en estos aspectos, para mitigar las implicancias de seguridad mencionadas.
- La IETF ya ha adoptado estas propuestas para su publicación en Std. Track (draft-ietf-tcpm-urgent-data)

“The new TCP bug”

SEGURIDAD/INTERNET

Expertos advierten de una vulnerabilidad de amplio alcance en TCP/IP

[Versión para imprimir](#)

Investigadores de la firma de seguridad finlandesa Outpost24 aseguran haber descubierto un fallo en el protocolo de Internet (IP) que puede interrumpir el funcionamiento de cualquier ordenador o servidor conectado a la red.

<http://www.idg.es/pcworld/Expertos-advierten-de-una-vulnerabilidad-de-amplio/doc71996-Seguridad.htm>

- Probablemente hayan escuchado del “nuevo bug de TCP” (Slashdot, The Register, y otros).
- E líneas generales, son el conocido Naphta o Netkill, o variantes de lo mismo
- UK CPNI, proveyó asesoramiento a fabricantes sobre las distintas alternativas para mitigar las mismas.
- Nuestro documento incluye una discusión de dichas vulnerabilidades, y de posibles maneras de mitigarlas

Siguientes pasos

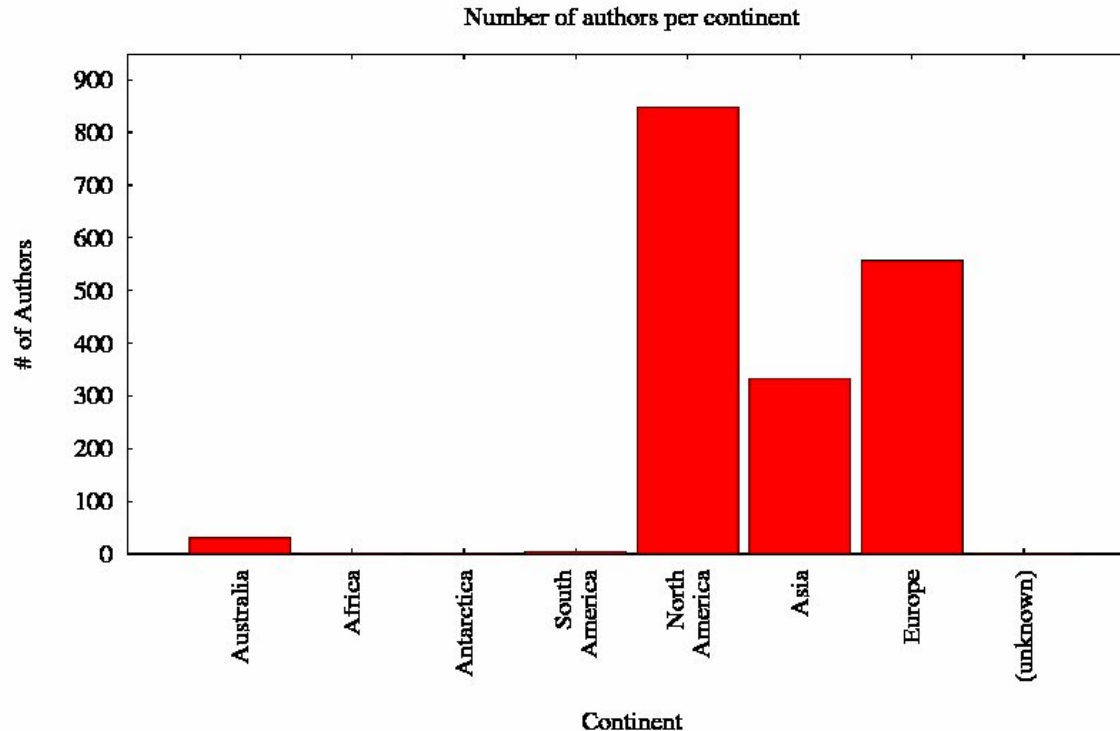
- Se encuentra en discusión en la IETF el I-D draft-gont-tcp-security.
Posibles caminos:
 - Ser adoptado en el opsec wg para el track Informational
 - Ser adoptado en el tcpm wg para el track Std. Track
 - No hacer absolutamente nada.
- Sería interesante que se involucren en el proceso de decisión en la IETF (listas de correo del opsec wg, tcpm wg, y lista general de la IETF).
- Asimismo, serán bien recibidas sugerencias y revisiones del documento en cuestión.

Algunas conclusiones

- Usualmente se asume que, debido a la antigüedad de los protocolos “core” de la suite TCP/IP, todas las implicancias negativas de seguridad del diseño de los mismos han sido resueltas, o solo pueden resolverse mediante uso de IPsec.
- Las vulnerabilidades publicadas incluso en los últimos cinco años parecen indicar lo contrario.
- Curiosamente, este es el primer proyecto que, en 25 años de utilización de los protocolos TCP e IP, intenta hacer un análisis completo de las implicancias de seguridad de los mismos.
- La respuesta de la comunidad a este proyecto ha sido variada.
- Estamos en conocimiento de una variedad de esfuerzos en la comunidad de fabricantes para mejorar la seguridad de las implementaciones de TCP. Salvo en el caso de proyectos “open source”, a la fecha no ha habido resultados concretos.

Shameless plugin (version 3.0) (I)

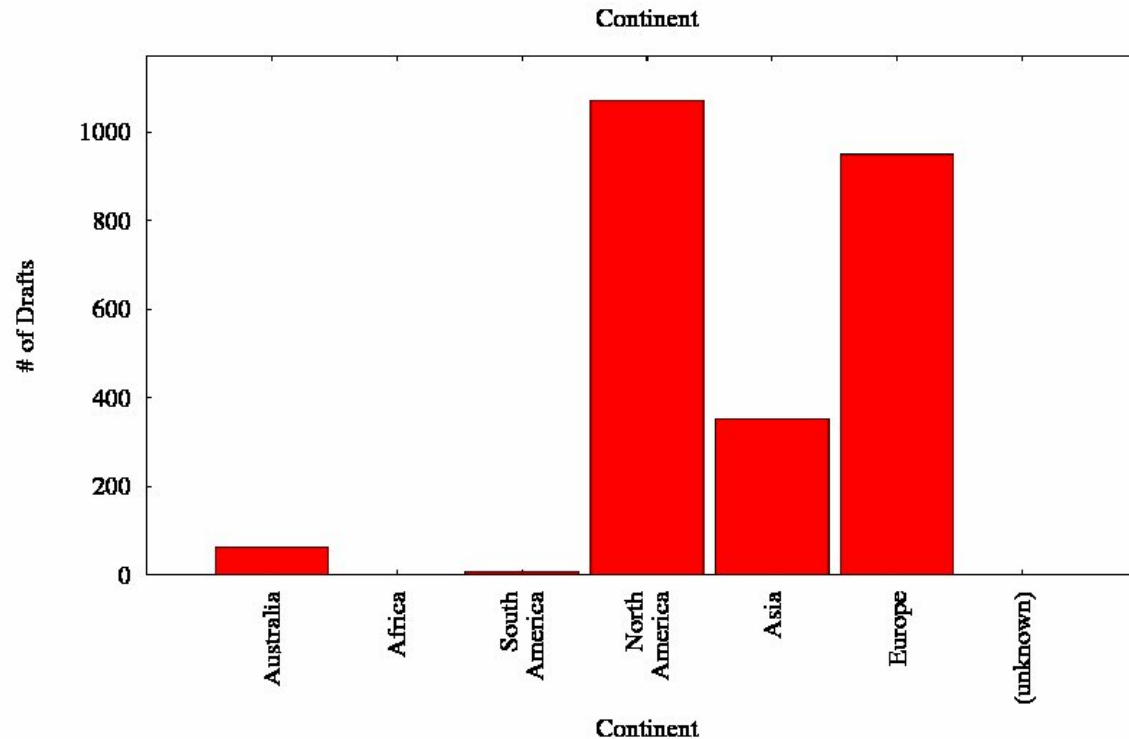
Cantidad de autores de IETF I-Ds de Sudamérica



- Ha habido un incremento del 100% en la cantidad de autores de I-Ds de la IETF con respecto al 2008.
- Ok, eramos 3, ahora somos 6. ☹
- Todavía no hay una solución concreta a la problemática de participación en las reuniones presenciales.

Shameless plugin (version 3.0) (II)

Cantidad de IETF I-Ds con autores de Sudamérica



- Sudamérica tiene 6 Internet-Drafts
- En los últimos meses ha publicado 2 RFCs.



Preguntas?

Agradecimientos

- UK CPNI, por su soporte en este proyecto.
- Carlos M. Martínez, por todo su trabajo para este evento de seguridad, y en la lista de seguridad de LACNIC.
- LACNIC, por su soporte para la presentación de los resultados de este proyecto en este evento.

Fernando Gont

fernando@gont.com.ar

<http://www.gont.com.ar>