

Resultados de una evaluación de seguridad del Protocolo de Internet (IP)

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 IPv4, 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 IPv4 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 para los protocolos TCP e IP.
- 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 julio de 2008 CPNI publicó el documento “Security Assessment of the Internet Protocol” – consistente en 63 paginas, que incluyen los resultados del análisis de seguridad del protocolo IPv4. El mismo se encuentra disponible en: <http://www.cpni.gov.uk/Products/technicalnotes/3677.aspx>
- Seguidamente, publicamos el mismo material como IETF I-D (draft-gont-opsec-ip-security-00.txt). El mismo se encuentra disponible en: <http://www.gont.com.ar/drafts/ip-security/index.html>
- El I-D fue adoptado por el opsec wg de la IETF a finales del 2008, para ser publicado en la categoría *Informational*.
- 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.



Ejemplo:

Implicancias de seguridad del campo Identification

El campo Identification (ID)

- Es utilizado por el mecanismo de fragmentación y reensamble
- El grupo de valores {Source Address, Destination Address, Protocol, Identification} identifica los fragmentos que corresponden a un determinado paquete original (sin fragmentar). Por tal motivo, el mismo grupo de valores **no** puede estar siendo utilizado para los fragmentos de mas de un paquete original.
- Si esto ocurriese, los fragmentos podrían ser reensamblados incorrectamente, con la consecuente pérdida del paquete resultante.
- Estas “colisiones de IP ID” tradicionalmente han sido evitadas utilizando un contador global para la inicialización del campo IP ID, incrementando dicho contador una vez por cada paquete IP enviado.
- De este modo, un determinado valor de IP ID se reutilizaba unicamente luego de que todos los otros valores hubieran sido utilizados.

Implicancias de seguridad

- La utilización de un contador global para la generación de los valores del IP ID permite que el campo en cuestión sea explotado para:
 - Obtener la cantidad de paquetes transmitidos por un sistema remoto en un determinado período de tiempo
 - Contar la cantidad de dispositivos físicos detrás de un middle-box tal como un NAT.
 - Realizar un port-scanning the tipo stealth.

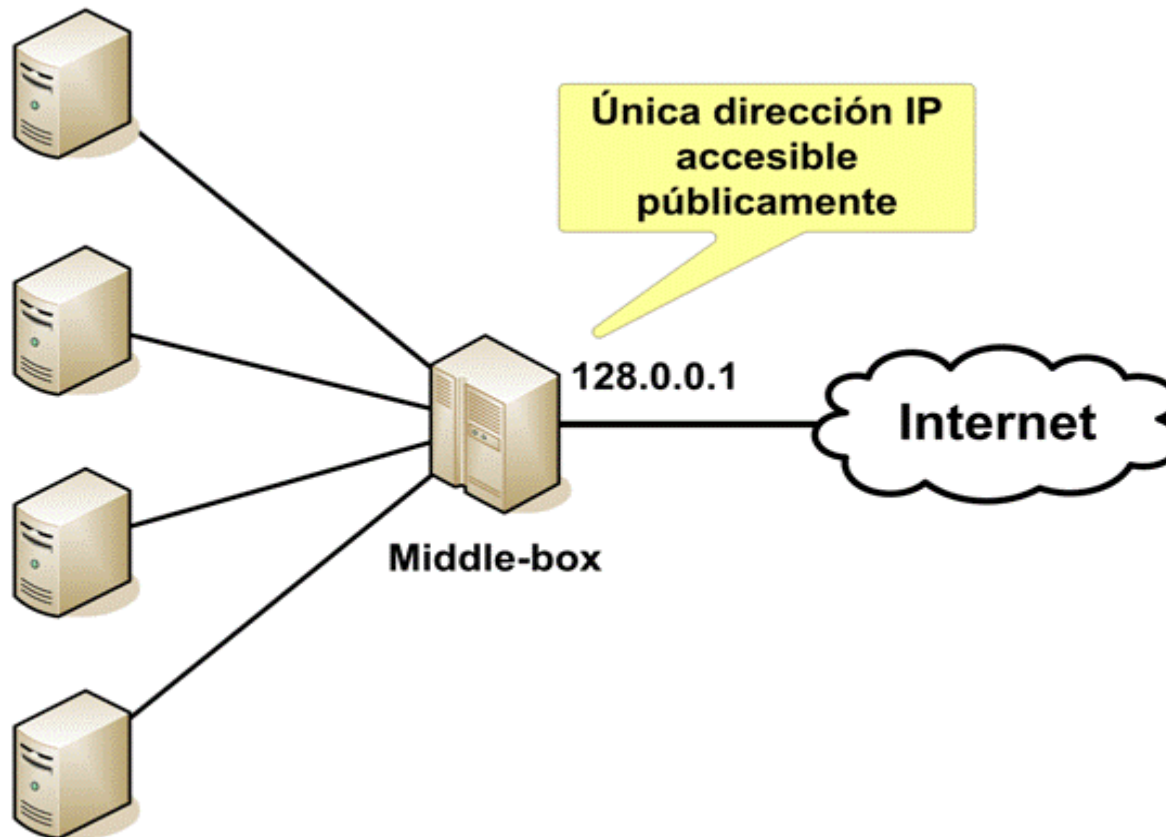
Determinando la cantidad de paquetes transmitidos

- El ataque envía un “paquete de prueba” (por ej., un ICMP echo request) a la víctima, y anota el IP ID de la respuesta obtenida (“IPID_1”).
- Luego envía un segundo paquete de prueba, y anota el IP ID de la respuesta obtenida (“IPID_2”).
- Así, la cantidad de paquetes transmitida por el sistema víctima será de:

$$\text{num_packets} = \text{IPID_2} - \text{IP_1} - 1$$

Contando sistemas detrás de un middle-box (I)

- Un posible escenario:



Contando sistemas detrás de un middle-box (II)

- Utilizando una herramienta como hping:

```
# hping2 -c 10 -i 1 -p 80 -S 128.0.0.1
```

```
HPING 128.0.0.1 (eth0 128.0.0.1): S set, 40 headers + 0 data bytes
```

```
46 bytes from 128.0.0.1: flags=SA seq=0 ttl=56 id=57645 win=16616 rtt=21.2 ms
```

```
46 bytes from 128.0.0.1: flags=SA seq=1 ttl=56 id=57650 win=16616 rtt=21.4 ms
```

```
46 bytes from 128.0.0.1: flags=RA seq=2 ttl=56 id=18574 win=0 rtt=21.3 ms
```

```
46 bytes from 128.0.0.1: flags=RA seq=3 ttl=56 id=18587 win=0 rtt=21.1 ms
```

```
46 bytes from 128.0.0.1: flags=RA seq=4 ttl=56 id=18588 win=0 rtt=21.2 ms
```

```
46 bytes from 128.0.0.1: flags=SA seq=5 ttl=56 id=57741 win=16616 rtt=21.2 ms
```

```
46 bytes from 128.0.0.1: flags=RA seq=6 ttl=56 id=18589 win=0 rtt=21.2 ms
```

```
46 bytes from 128.0.0.1: flags=SA seq=7 ttl=56 id=57742 win=16616 rtt=21.7 ms
```

```
46 bytes from 128.0.0.1: flags=SA seq=8 ttl=56 id=57743 win=16616 rtt=21.6 ms
```

```
46 bytes from 128.0.0.1: flags=SA seq=9 ttl=56 id=57744 win=16616 rtt=21.3 ms
```

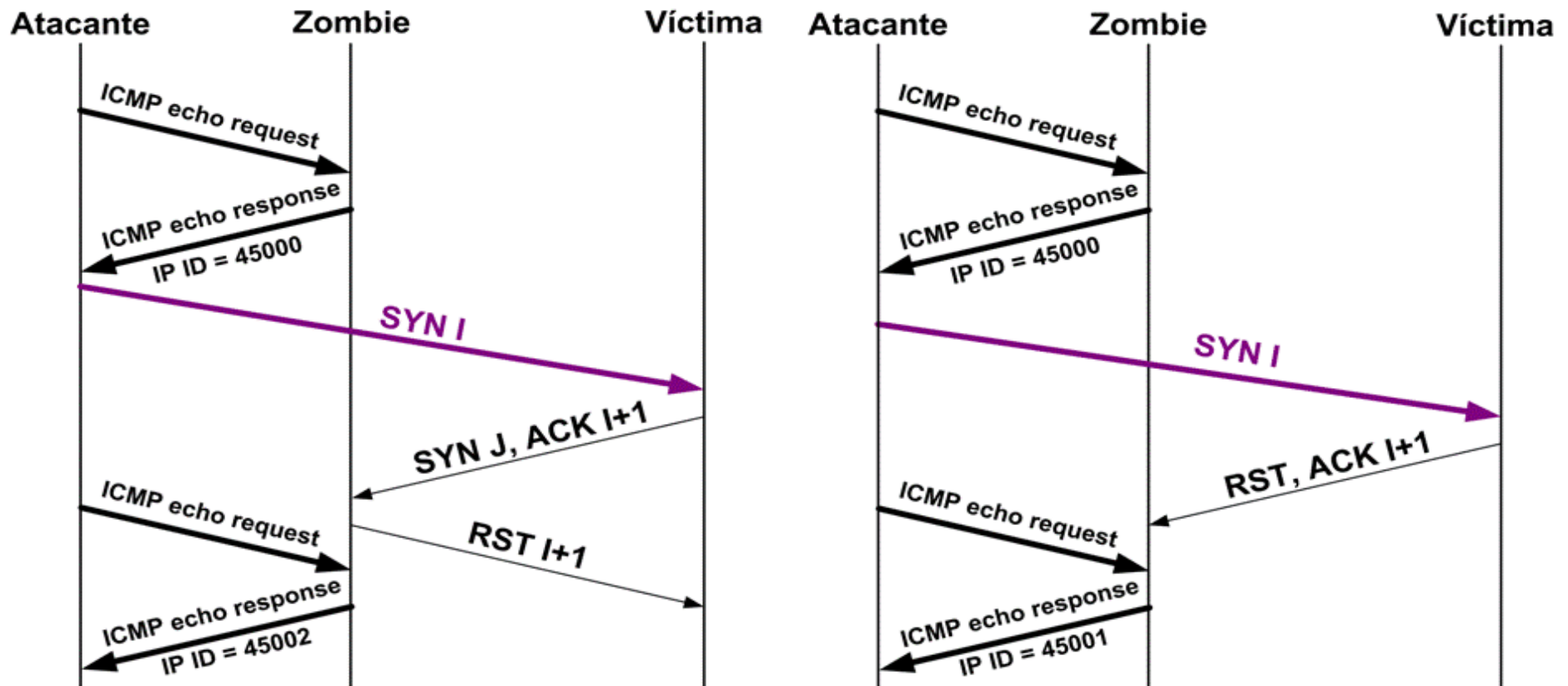
```
--- 128.0.0.1 hping statistic ---
```

```
10 packets tramitted, 10 packets received, 0% packet loss
```

```
round-trip min/avg/max = 21.1/21.3/21.7 ms
```

- Claramente, existen dos secuencias distintas de IP ID

Realizando un port-scanning de tipo "stealth"



- Enviando un paquete de prueba (ICMP echo request) al "zombie", el atacante puede identificar el estado de un puerto en el sistema víctima.

Aleatorizando el campo Identification

- Para mitigar las implicancias de seguridad de este campo, los valores de IP ID no deberían ser predecibles.
- Siempre se ha asumido que el uso de random() era inapropiado, ya que llevaría a colisiones de IP ID, y por ende traería problemas de interoperabilidad.
- Algunos sistemas tales como OpenBSD habían incorporado esquemas de PRNG para evitar la reutilización temprana de valores de IP ID. Sin embargo, se encontró que algunos de estos esquemas producían secuencias predecibles.
- Realizando un análisis de protocolos de transporte connection-oriented y connection-less, se pueden obtener indicios sobre el tipo de PRNG apropiados para la selección de IP ID.

Protocolos connection-oriented

- Las implicancias de la fragmentación IP en materia de performance se conocen de hace mas de 20 años.
- Por tal motivo, la mayoría de los protocolos conenction-oriented (por ej., TCP) implementan mecanismos para evitar la fragmentación IP (por ej., Path-MTU Discovery)
- De cualquier modo, considerando las tasas de transferencia actuales, y que el campo IP ID es de 16 bits, los valores de IP ID serían reutilizados demasiado rápido independientemente del esquema de selección de IP ID utilizado.
- Por lo tanto, recomendamos no utilizar fragmentación para protocolos connection-oriented, y aleatorizar (`random()`) los valores utilizados para el campo IP ID de los paquetes resultantes.

Protocolos connection-less

- Típicamente carecen de:
 - Mecanismos de control de flujo
 - Mecanismos de secuenciación de paquetes
 - Mecanismos de confiabilidad
- Por tal motivo, se los utiliza asumiendo que:
 - Las aplicaciones serán utilizadas en entornos en los que el reordenamiento de paquetes es poco probable y/o poco importante.
 - Las tasas de transferencia serán lo suficientemente bajas como para que el control de flujo no sea necesario
 - La pérdida de paquetes es poco probable y/o poco importante.
- Por lo tanto, recomendamos aleatorizar (`random()`) el IP ID de los paquetes correspondientes.
- Las aplicaciones preocupadas por esta política deberían considerar la utilización de un protocolo de transporte connection-oriented.

Siguientes pasos

- Esperamos trabajar en una revisión del documento publicado por UK CPNI próximamente. Son bienvenidas sugerencias y revisiones del documento en cuestión.
- El IETF I-D (draft-ietf-opsec-ip-security) se encuentra en proceso de revisión. Son bienvenidas sugerencias y revisiones del documento en cuestión.
- Asimismo, sería interesante que se involucren en el proceso de decisión en la IETF (lista de correo del opsec wg). Mas información en: <http://www.ietf.org/html.charters/opsec-charter.html>

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.



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>