Resultados de un análisis de seguridad de las especificaciones de la IETF de los protocolos TCP e IP

Fernando Gont
UTN/FRH, Argentina

proyecto realizado para

UK CPNI
United Kingdom's Centre for the Protection of National Infrastructure

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.
- Como resultado, la documentación de todas estas vulnerabilidades se encuentra desparramada en una gran cantidad de documentos que suelen ser difíciles de identificar.
- Asimismo, algunos de estos documentos proponen contramedidas a las mencionadas vulnerabilidades, sin realizar un análisis minucioso de las implicancia de las mismas sobre la interoperabilidad de los protocolos.
- Desafortunadamente, el trabajo de la comunidad en esta área no ha reflejado cambios en las especificaciones correspondientes de la IETF.

Situación actual

- Se hace notablemente dificultoso realizar una implementación segura de los protocolos TCP/IP a partir de las especificaciones de la IETF.
- Nuevas implementaciones de los protocolos re-implementan vulnerabilidades encontradas en el pasado.
- Nuevos protocolos re-implementan mecanismos o políticas cuyas implicancias de seguridad ya eran conocidas a partir de otros protocolos (por ejemplo, RH0 en IPv6).
- No existe ningún documento que apunte unificar criterios sobre las vulnerabilidades de los protocolos, y las mejores prácticas para mitigarlas.
- No existe ningún documento que sirva como complemento a las especificaciones oficiales, para permitir que la implementación segura de los protocolos TCP/IP sea una tarea viable.

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.
- Dichos documentos se irían actualizando en respuesta a los comentarios recibidos por parte de la comunidad y al descubrimiento de nuevas vulnerabilidades.
- Finalmente, se espera llevar al menos parte de este material al ámbito de la IETF, para promover cambios en los estándares correspondientes.

Algunas cuestiones a analizar en IP

- Rango de valores aceptables para cada campo del encabezamiento
  - En algunos casos, los rangos aceptables dependen del valor de otros campos. Ejemplo: IHL (Internet Header Length), Total Length, *link-layer payload size.*
- Análisis de las posibles implicancias de seguridad de cada mecanismo y política del protocolo.
  - Ejemplo: El campo TTL se puede utilizar (al menos en teoría) para OS fingerprinting, physical-device fingerprinting, TTL-triangulation, evasión de NIDS, GTSM, etc.
- Procesamiento deseable de las distintas opciones IP
  - Ejemplo: source-routing? IP Security options?
- Analizar posibles algoritmos para reensamblar fragmentos IP
  - ¿Qué chequeos de validación podrían realizarse para evitar la evasión de NIDS? ¿Qué políticas se podrían implementar para minimizar ataques de DoS?

Algunas cuestiones a analizar en TCP

- Establecer claramente el rango de valores aceptables para cada campo del encabezamiento y opciones
  - Ejemplo: Valores aceptables para la opción TCP MSS (Rose attack)
- Analizar posibles algoritmos para la aleatorización de puertos efímeros.
- Reducir las posibilidades de abusar de los algoritmos de control de congestión de TCP.
- Analizar posibles algoritmos para el manejo del buffer de reensamblado, y del buffer de retransmisión de datos.
- Analizar como reducir la precisión de técnicas de “remote OS finger-printing”.
  - ¿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?

Resultados preliminares

- Para el caso del protocolo IP, se generó un documento de 50 páginas, con mas de 70 referencias a reportes de vulnerabilidad y papers relevantes.
- Para el caso del protocolo TCP, se generó un documento de más de 100 páginas, con más de 100 referencias a reportes de vulnerabilidad y papers relevantes.
- Los documentos se beneficiaron de los comentarios de desarrolladores de implementaciones TCP/IP, tanto abiertas como cerradas.
- Sin embargo, en general los comentarios se obtuvieron por “vínculos personales” con los desarrolladores, mas que a través de los canales “formales” de los fabricantes. ☹

Algunos resultados interesantes

- El análisis de las especificaciones disparó discusiones sobre algunos mecanismos básicos de los protocolos.
  - Por ejemplo, está ampliamente asumido que el generador de ISNs de TCP debe producir una secuencia monotónicamente creciente, para garantizar un mínimo de confiabilidad. Sin embargo, esta confiabilidad es provista por otros mecanismos (“TIME-WAIT state” y “quiet-time concept”)
- Algunos mecanismos se encuentran “deprecated” por la IETF. Sin embargo, son utilizados actualmente en la industria (por ejemplo, IP security option)
- Incluso dentro de la propia comunidad de la seguridad informática, muchas de las implicancias de seguridad de los protocolos TCP e IP son ignoradas o comprendidas sólo parcialmente,

Modificando las especificaciones (IETF)

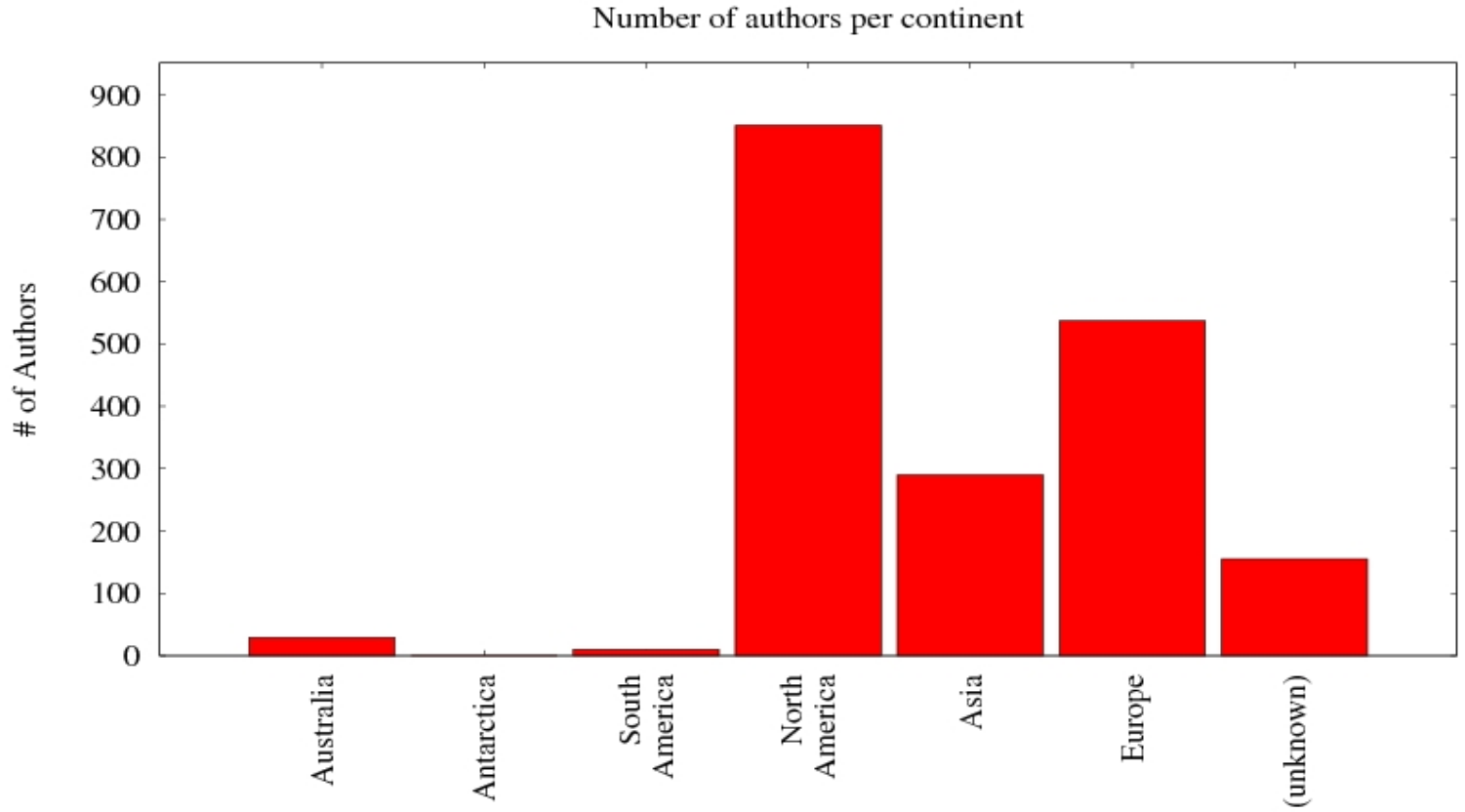
- Algunas porciones de este trabajo ya se llevaron a la IETF. Ejemplos:
  - Aleatorización de puertos: Se presentó un documento que fue adoptado por el TSVWG (BCP).
  - Ataques ICMP contra TCP: Se presentó un documento que fue adoptado por el TCPM WG (Informational) ☹. La versión inicial se publicó en **2004**. (!)
- Esta actividad suele requerir una gran cantidad de energía
  - Con el fin de lograr consenso, las propuestas presentadas en la IETF suelen tener que ser modificadas a niveles en los cuales el documento final termina difiriendo de la propuesta original.
  - Existe cierta resistencia a realizar modificaciones en IPv4 (ya que "*IPv6 reemplazará a IPv4*")
  - Los fabricantes suelen resistirse a implementar modificaciones vinculadas a seguridad

Contribuyendo con los documentos

- Estos documentos (así como todas las publicaciones de la IETF) precisan de los comentarios de la comunidad de operaciones. Algunos ejemplos (simples):
  - La IP security option no hubiera sido marcada como “deprecated” si hubieran habido comentarios por parte de sus usuarios.
  - La justificación del soporte de source-routing era el requerimiento de esta opción en acuerdos de peering. Sigue siendo esto actual?
- Se espera la publicación del documento correspondiente al protocolo IP para principios del mes de junio.
- Todavía no se tiene una fecha estimativa para la publicación del documento correspondiente a TCP.
- Ambos documentos estarán disponibles en el web site de CPNI (http://www.cpni.gov.uk)

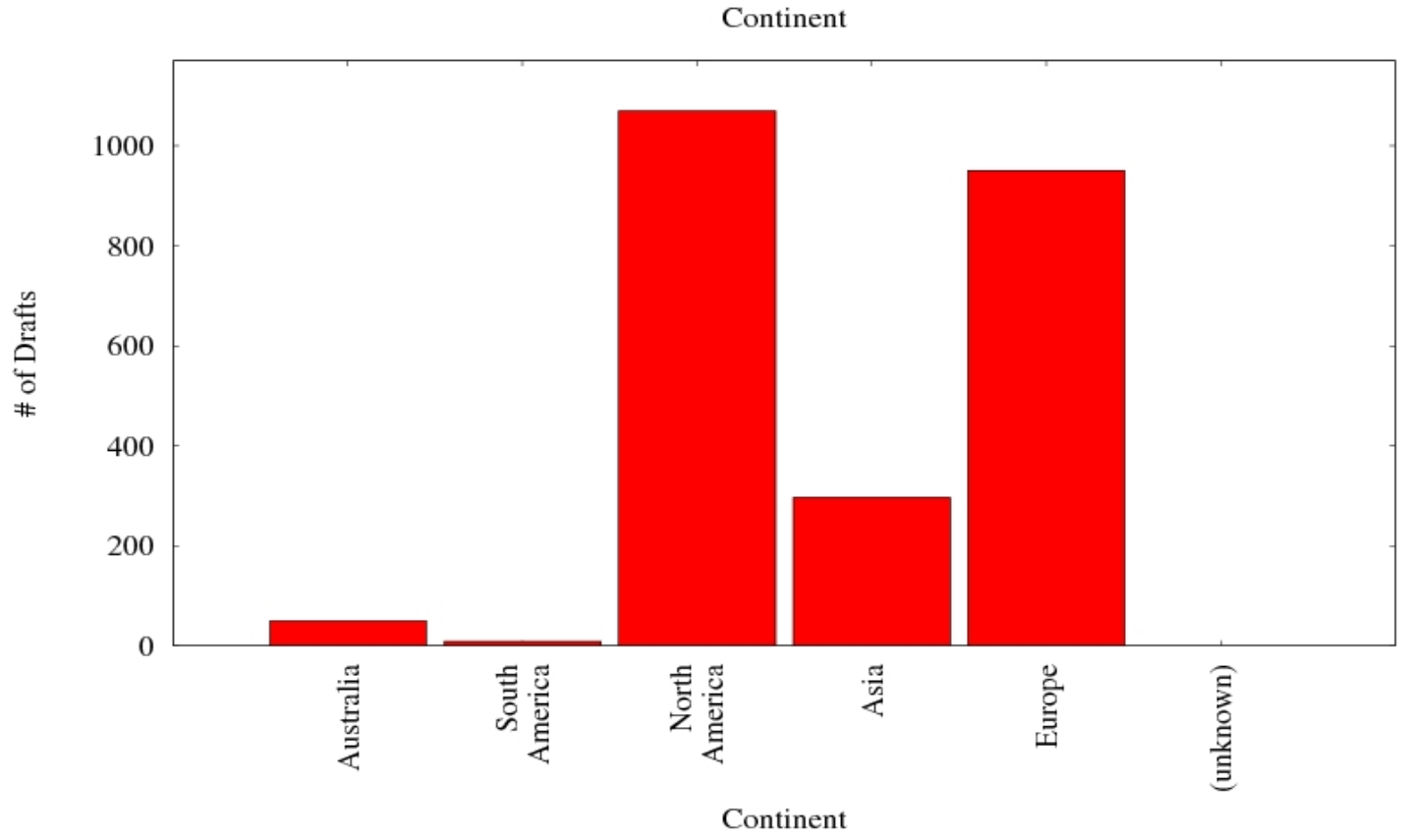
Shameless plug-in (versión 2.0)

- La primer versión de este plug-in (en LACNIC X) hablé sobre la participación latinoamericana en la IETF. En mayo de 2007, habían 3 latinoamericanos participando activamente en la IETF.
- Actualmente, somos más, pero seguimos siendo muy pocos (10):



Shameless plug-in (versión 2.0) (II)

- Latinoamérica tiene 9 drafts. Nuestro grupo de UTN/FRH es autor de 4 de ellos.
- No cuenta con soporte de ninguna empresa (ni económico, ni en equipamiento).



Preguntas?

Gracias!

- UK CPNI, por su apoyo para este proyecto
- Carlos M. Martínez, por todo su trabajo para este evento de seguridad, y en la lista de seguridad de LACNIC
- Todo el staff de LACNIC (sin su soporte no hubiera sido posible mi participación en este evento)

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar