Resultados de un análisis de seguridad de los protocolos TCP e IP

Fernando Gont

ekoparty 2008

Octubre 2, 2008
Somewhere only we know *(*)*, **Argentina**

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 esparcida 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 este material al ámbito de la Internet Engineering Task Force (IETF), para promover cambios en los estándares correspondientes.

Algunas áreas de trabajo 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 distintas políticas posibles para aplicar junto con distintos mecanismos. Por ej., en el caso del reensamble de 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 áreas de trabajo 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 selección 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. El mismo se encuentra disponible en: http://www.cpni.gov.uk/Products/technicalnotes/3677.aspx
- 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. Este documento todavía no ha sido publicado.
- Los documentos se beneficiaron de los comentarios de desarrolladores de implementaciones TCP/IP, tanto abiertas como cerradas.

Cooperación

- Hemos tenido el agrado de contar con una variedad de ingenieros e investigadores del área para la revisión de los documentos sobre seguridad en TCP e IP de este proyecto, lo cual ha contribuido muy positivamente con nuestro trabajo.
- Lamentablemente, la situación no ha sido la misma en lo que respecta a fabricantes
  - En muchos casos, no se recibió respuesta alguna.
  - En algun caso, respuestas del tipo “como este proyecto no fue patrocinado por nuestra compañía, no podemos hacer comentarios técnicos” (¿?¡!)

Actividades relacionadas en la IETF (I)

- Algunas porciones de este proyecto ya se llevaron a la IETF. Ejemplos:
  - “Security Assessment of the Internet Protocol”: El mismo documento publicado por CPNI en agosto de este año fue publicado recientemente como Internet-Draft. Todavía no ha sido adoptado como elemento de trabajo del OPSEC WG.
  - 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) ☹.
- Algunas otras publicaciones en el ámbito de la IETF, no vinculadas con este proyecto:
  - “Recommendations for filtering ICMP messages” (draft-ietf-opsec-icmp-filtering-00.txt): Este documento fue adoptado como WG item por el OPSEC WG. (es increíble que en el 2008 todavía muchos crean que “se puede filtrar todo ICMP”).

Actividades relacionadas en la IETF (II)

- 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 notablemente 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

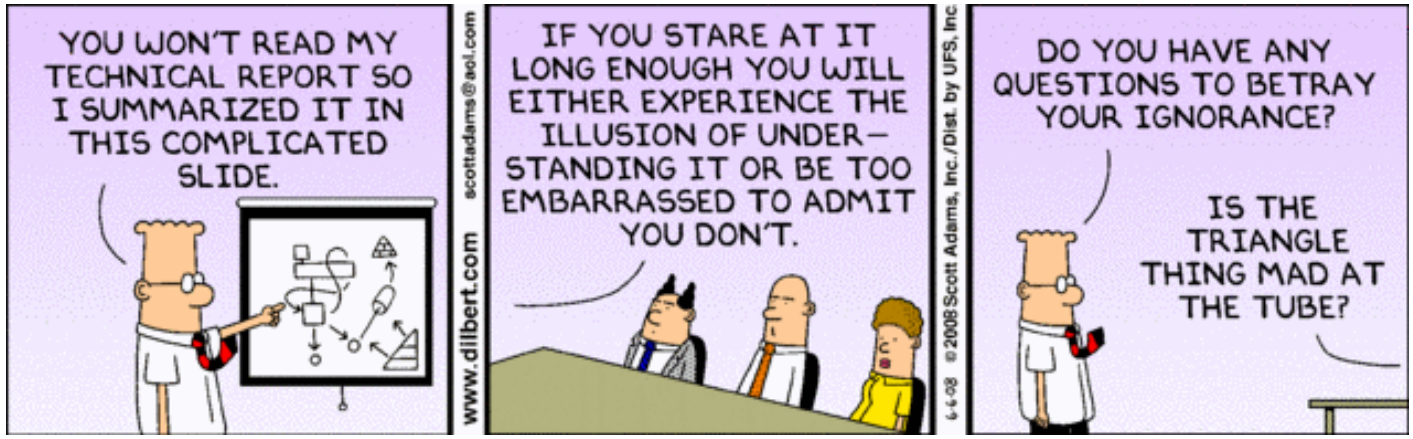
Algunos resultados

Algunos resultados definitivos

- En materia de aleatorización de algunos valores que desde siempre se han venido discutiendo, estas son algunas nuestras conclusiones:
  - IP IDs: random(). Y punto.
  - Ephemeral ports: *a la* RFC 1948
  - TCP timestamps: *a la* RFC 1948
  - TCP ISNs: *a la* RFC 1948
- En materia de nmap, establecimos lo que serían las respuestas adecuadas a determinados estímulos, para que la precision de OS-fingerprinting de nmap no sea lo ridiculamente **buena** que es hoy en día.
- … lean el documento publicado, y el que está por venir.

Conclusiones

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 muy positiva. Sin embargo, la colaboración por parte de fabricantes no fue la esperada.

Algunas conclusiones (II)

- Los mayores problemas de seguridad en TCP/IP tienen que ver con:
  - Adoración a protocolos que nunca se pensaron para ser utilizados como hoy en día.
    - Defensa del status-quo por parte de old-timers
    - Idiotez, desconocimiento o falta de actitud por parte de newcomers
  - Todo el mundo cree que conoce como funcionan los protocolos, sin haber leído ninguna especificación, sin haber revisado implementaciones, etc.
  - La IETF en general se resiste a documentar problemas de seguridad, y sus correspondientes contramedidas
  - Los principales fabricantes toman actitudes verdaderamente cuestionables antes cuestiones de seguridad.
  - Esa ridícula actitud o creencia de "*TCP/IP? Es viejo! Ya está todo dicho!*"

Shame-less plugin

Shameless plug-in: The new TCP bug

- Probablemente hayan escuchado del “nuevo bug de TCP” (Slashdot, The Register, y otros).
- En breve:
  - Son el conocido Naphta o Netkill, o variantes de lo mismo
  - Los autores no proveen soluciones.
- Nuestro doc incluye una discusión de dichos ataques, y contramedidas
  - Esperamos publicarlo pronto
  - Estamos trabajando con algunos fabricantes y colaboradores para pulir la versión actual del documento

Preguntas?

Información de contacto

Fernando Gont

fernando@gont.com.ar

Más información en:

http://www.gont.com.ar