UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

05/2008

Bruce Schneier, experto en seguridad informática

"El auténtico problema de la seguridad en las comunicaciones no es la criptografía sino el resto del proceso"

Bruce Schneier está considerado internacionalmente como un gurú de la seguridad informática. Fundó y actualmente dirige la división tecnológica de la compañía BT Counterpane, especializada en servicios de seguridad informática. Citado habitualmente en los medios de comunicación, Schneier ha escrito numerosos artículos en la prensa y ha testificado sobre seguridad ante el Congreso de los Estados Unidos. Bruce Schneier visitó la UAB con motivo de la celebración del Año de la Computación.

Bruce Schneier está considerado internacionalmente como un gurú de la seguridad informática. Fundó y actualmente dirige la división tecnológica de la compañía BT Counterpane, especializada en servicios de seguridad informática. Citado habitualmente en los medios de comunicación, Schneier ha escrito numerosos artículos en la prensa y ha testificado sobre seguridad ante el Congreso de los Estados Unidos. Bruce Schneier visitó la UAB con motivo de la celebración del Año de la Computación.

¿Algún consejo práctico para mantener el ordenador y los datos seguros?

Para la mayoría de los usuarios, lo mejor es hacer copias de seguridad, porque para la mayoría la seguridad es equivalente a la fiabilidad, y cuando algo falla en el ordenador entonces pierden los datos. Tener un programa antivirus, eso también es muy importante, y activar los *firewalls* de Windows … Son pequeñas cosas que se pueden hacer, pero lo más importante es hacer buenas copias de seguridad de manera regular.

¿El software libre es más seguro que el software privativo o es más inseguro?

El software seguro es aquél que ha sido analizado, y hay dos maneras de hacerlo. La primera es contratar gente que lo analize,y la segunda, en el caso del software de código abierto, es dejar que lo analize la comunidad. En ambos casos, hay una gran cantidad de software que nadie vigila, hay montones de software comercial que no ha sido analizado, por lo que ambos tipos pueden ser tanto seguros como inseguros. Por tanto, la seguridad no es una cuestión de si el software es libre o no lo es. Están sujetos a métodos distintos de análisis. El software que ha sido analizado por expertos es más seguro.

¿Y en cuanto al hardware, Mac o PC?

Hay dos preguntas diferentes a plantearse. Una es, ¿cuál de ellos es teóricamente más seguro al sacarlo de la caja?, es decir, si analizas Windows, Makintosh y Unix, ¿cuál es más seguro? Y la otra es, ¿cuál de ellos es más seguro al utilizarlo? No sabemos la respuesta a la primera pregunta, pero sí a la segunda: Windows es el menos seguro porque es el que utiliza más gente. Si eres un hacker, escribirás programas que afecten al mayor número de máquinas. Por ello, estas más seguro con Mac o utilizando Unix, pero no necesariamente porque se trate de sistemas operativos más seguros, sino porque son menos populares.

¿Considera la delincuencia en la red como un problema grave?

No creo que se trate todavía de un problema grave. Pero cada año se vuelve más y más importante. Los delincuentes han descubierto el ciberespacio como una fuente de dinero y de fraude. Y lo utilizan de manera creciente. Este tipo delitos se está haciendo cada vez más popular y, por lo tanto se está profesionalizando. Estamos observando un incremento del crimen organizado, más crimen con modelo de negocio. Creo que se está convirtiendo progresivamente en un gran problema, hasta que lo resolvamos.

Un ataque general a los sistemas de comunicaciones y de almacenamiento de datos de todo un país sería devastador. ¿Cree que podría ocurrir?

Creo que un colapso amplio de Internet sería mucho menos probable de lo que se suele atribuir en los medios. Internet tiene una sorprendente capacidad de supervivencia. Sobrevive ante los ataques tanto al hardware como al sofware. Vemos estos tipos de

ataques continuamente pero Internet no se colapsa, aunque es muy frágil. Por lo tanto, en realidad es más robusta que lo que la gente cree.

¿La criptografía cuántica es infalible para el intercambio de información?

Hay muchos métodos de encriptación que son absolutamente seguros. Nadie necesita la criptografía cuántica porque la que no es cuántica es suficientemente buena. El problema no es la criptografía, sino todo lo que la rodea: el ordenador, la red, el usuario. Esos son los auténticos problemas. No importa el algoritmo de encriptación que utilicemos, si es cuántico o no, ya que los problemas del entorno no cambian. Ya tenemos toda la criptografía que necesitamos y es todo lo segura que puede ser. Nadie la romperá. Pero todo lo demás es tan malo que nadie tiene necesidad de romper la criptografía.

Uno de los problemas cotidianos de los usuarios es el spam. ¿Existe alguna solución efectiva para evitarlo?

Efectivamente, el spam es uno de los casos de éxito en la seguridad informática. Hay muchas empresas que limpian el spam y lo hacen muy bien. Yo ya no tengo spam. Se trata de un problema inmenso en la columna vertebral de la red, pero los programas anti-spam son muy buenos parar eliminarlo después de recibirlo. Si tienes mucho spam es que no utilizas un buen filtro, así que ve a un ISP que utilice filtro anti-spam y dejarás de tenerlo.

¿Porqué todavía no ha llegado el spam al teléfono móvil?

Lo hay, pero no mucho, aunque cada vez veremos más. De vez en cuando recibo SMS spam, y también en la dirección de correo electrónico de mi móvil. No mucho. Pero a medida que se vuelve más y más popular, el SMS se convertirá también en un vehículo para el spam.

Entrevista: Octavi López Coronado

View low-bandwidth version