Bruce Schneier, expert en seguretat informàtica

05/2008 - **Telecomunicacions, Electrònica i Informàtica.**

"L'autèntic problema de la seguretat en les comunicacions no és a la criptografia, sinó en la resta del procés"

Bruce Schneier és considerat internacionalment com un gurú de la seguretat informàtica. Va fundar, i actualment dirigeix, la divisió tecnològica de la companyia BT Counterpane, especialitzada en serveis de seguretat informàtica. Citat habitualment als mitjans de comunicació, Schneier ha escrit nombrosos articles a la premsa i ha testificat diverses vegades sobre seguretat al Congrés dels Estats Units. Bruce Schneier va visitar la UAB amb motiu de l'Any de la Computació.

Bruce Schneier és considerat internacionalment com un gurú de la seguretat informàtica. Va fundar, i actualment dirigeix, la divisió tecnològica de la companyia BT Counterpane, especialitzada en serveis de seguretat informàtica. Citat habitualment als mitjans de comunicació, Schneier ha escrit nombrosos articles a la premsa i ha testificat diverses vegades sobre seguretat al Congrés dels Estats Units. Bruce Schneier va visitar la UAB amb motiu de l'Any de la Computació.

Bruce Schneier

Algun consell pràctic per mantenir l'ordinador i les dades segures?

Per a la major part dels usuaris, el millor és fer còpies de seguretat, perquè per a la major part de la gent la seguretat és equivalent a la fiabilitat, i quan alguna cosa falla a l'ordinador, aleshores es perden les dades. També és important tenir un programa antivirus, activar els firewalls de Windows… Són petites coses que es poden fer, però el més important és fer bones còpies de seguretat de manera regular.

El programari lliure és més segur que el privatiu, o és més insegur?

El programari segur és aquell que ha estat analitzat, i hi ha dues maneres de fer-ho. La primera és contractar a algú que l'analitzi, i la segona, en el cas del programari de codi obert, és deixar que l'analitzi la comunitat. En tots dos casos hi ha una gran quantitat de programari que ningú vigila, hi ha molt programari comercial que no ha estat analitzat, per la qual cosa, ambdós tipus de programari poden ser tant segurs com insegurs. Per tant, la seguretat no és una qüestió de si el programari és lliure o no. Són sotmesos a mètodes diferents d'anàlisi. El programari més segur és el que ha estat analitzat pels experts.

I pel que fa al hardware, Mac o PC?

Hi ha dues preguntes diferents a plantejar-se. Una és, quin d'ells és teòricament més segur en treure'l de la caixa?, és a dir, si analitzes Windows, Macintosh i Unix, ¿quin és més segur?. L'altra és, quin d'ells és més segur en utilitzar-lo? No sabem la resposta a la primera pregunta, però si a la segona: Windows és el menys segur perquè és el que utilitza més gent. Si ets un hacker, escriuràs programes que afectin el major nombre de màquines possible. Per això, ets més segur amb Mac o utilitzant Unix, però no necessàriament perquè es tracti de sistemes operatius més segurs, sinó perquè són menys populars.

Considera la delinqüència a la xarxa com un problema greu?

No penso que es tracti, encara, d'un problema greu. Però cada any es torna més i més important. Els delinqüents han descobert el ciberespai com a font de diners i de frau, i l'utilitzen de manera creixent. Aquest tipus de delictes s'està fent cada cop més popular i, per tant, s'està professionalitzant. Estem observant un increment del crim organitzat, crim amb model de negoci. Crec que, de manera progressiva, està esdevenint un gran problema, fins que el resolguem.

Un atac general als sistemes de comunicacions i d'emmagatzematge de dades de tot un país seria devastador. Pensa que podria succeir?

Crec que un col·lapse ampli d'Internet seria molt menys probable del que se sol atribuir als mitjans de comunicació. Internet té una capacitat de supervivència sorprenent. Sobreviu front els atacs tant de programari com de maquinari. Veiem sovint aquests tipus d'atacs, però Internet no es col·lapsa, tot i que és fràgil. Per tant, en realitat és més robusta del que molta gent pensa.

La criptografia quàntica és infal·lible per a l'intercanvi d'informació?

Hi ha molts mètodes d'encriptació que són absolutament segurs. Ningú necessita la criptografia quàntica perquè la que no és quàntica ja és prou bona. El problema no és la criptografia, sinó tot el que hi ha a l'entorn: l'ordinador, la xarxa, l'usuari. Aquests són els autèntics problemes. No importa l'algoritme d'encriptació que utilitzem, si és quàntic o no, ja que els problemes de l'entorn no canvien. Ja tenim tota la criptografia que necessitem i té tota la seguretat que pot tenir. Ningú la trencarà. Però la resta és tan dolenta que ningú té la necessitat de trencar la criptografia.

Un dels problemes quotidians dels usuaris és l'spam. Existeix alguna solució efectiva per a evitar-ho?

Efectivament, l'spam és un dels casos d'èxit en l'àmbit de la seguretat informàtica. Hi ha moltes empreses que netegen l'spam i ho fan molt bé. Jo ja no tinc spam. Es tracta d'un problema immens a la columna vertebral de la xarxa, però els programes anti-spam són molt bons en eliminar-ho després d'haver-ho rebut. Si tens molt spam vol dir que no utilitzes un bon filtre, així que vés a un ISP que utilitzi filtre anti-spam i deixaràs de tenir-ho.

Per què encara no ha arribat l'spam al telèfon mòbil?

Sí que n'hi ha, però no gaire, tot i què cada cop en veurem més. De tant en tant rebo SMS spam, i també a l'adreça de correu electrònic del meu mòbil. No gaire. Però a mesura que es torna més i més popular, l'SMS esdevindrà també un vehicle per a l'spam.

Entrevista: Octavi López Coronado