Cibercontrol Social

TXIPI :: 13/03/2008

Bajo este angustiante nombre se enmarcan las diferentes técnicas que se han venido desarrollando en el último cuarto de siglo para controlar al ciudadano de a pie tanto dentro de las redes de comunicación globales como fuera de ellas.

Olvidemos las películas de serie B de espías y contra-espías en el Telón de Acero, el objetivo ahora es cualquier ciudadano, en principio anónimo, que tenga potencialmente algo que esconder. El progreso tecnológico ha permitido esta labor que hace bien poco se antojaba imposible, aprovechándose además del amparo y la falsa sensación de anonimato que provoca el uso de Internet.

Sistemas de control en Internet

Desde los comienzos de Internet, cuando la antigua Arpanet tenía mucho más de aldea que de global, el proyecto Echelon ya funcionaba interceptando contenidos considerados como peligrosos en las comunicaciones electrónicas. En un principio nadie quiso creer paranoicas historias sobre sistemas de espionaje computerizado, satélites vigilando noche y día nuestras comunicaciones, filtros de correo electrónico, etc. Todo parecía sacado de una vieja película de espías. Sin embargo, 30 años después de su constitución en 1971, el Parlamento Europeo hizo pública su existencia en mayo de 2001:

"(...) No hay ninguna razón para seguir dudando de la existencia de un sistema de intercepción de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UK/USA; considerando, asimismo, que según las informaciones de que se dispone, es probable que su nombre sea "ECHELON", si bien no es éste un aspecto de importancia primordial (...) El sistema no se utiliza para interceptar comunicaciones militares, sino privadas y económicas (...) [1]"

Como vemos el sistema está orientado al espionaje del ciudadano de a pie en su vida cotidiana, atrás quedó el espionaje militar de la guerra fría, todo el mundo es un enemigo potencial. No sólo las comunicaciones personales por Internet son filtradas y espiadas, sino muchas conversaciones telefónicas, celulares, fax y GPS. Funciona con un sistema de "palabras clave" que activan el filtrado. Un ejemplo bastante escandaloso de este sistema es el que se relató en el programa "60 minutes" de la CBS. Una mujer hablaba por teléfono con una amiga explicándole que su hijo hizo un papel durante una obra de teatro en el colegio, usando la expresión "he bombed" (literalmente "puso una bomba", pero también en sentido figurado "fue muy deprisa"). El sistema detectó automaticamente la expresión, y su nombre y datos personales fueron a parar a la base de datos de posibles terroristas.

El "mejor" Gran Hermano jamas diseñado ha estado más de un cuarto de siglo espiando conversaciones por todo el mundo. La alianza entre las agencias de seguridad e inteligencia de todos sus participantes se han cubierto las espaldas en el terreno legal: es ilegal que un

gobierno espie a sus propios ciudadanos y mandatarios, pero siempre es posible pedir "favores" al resto de participantes en este sentido. Margaret Tatcher hizo uso de estos favores y espió a varios miembros de su gabinete solicitando informes a sus colegas canadienses. Organizaciones como Greenpeace o Amnistia Internacional han sido también espiadas, como se ha reconocido públicamente [2].

Obviamente esto sólo es la punta del iceberg, sin embargo cada vez la cantidad de información que hay que tratar se va haciendo más inmanejable y su eficacia está cayendo poco a poco. Por esto mismo, la NSA, Agencia de Seguridad Nacional de Estados Unidos, y el FBI están desarrollando nuevas herramientas para aumentar la capilaridad de sus sistemas de filtrado y espionaje. En este sentido destacan las colaboraciones de empresas que guían gran parte del futuro de Internet como Microsoft [3] o Cisco, líderes en el mercado del software y el hardware de equipamientos de red respectivamente. Ambas empresas han manifestado públicamente que supeditarán la privacidad de sus usuarios a los intereses de la NSA y FBI en cuestiones de seguridad. Este colaboracionismo se ha visto como algo muy negativo dentro de los grupos de usuarios concienciados con el tema, pero la gran mayoría de sus consumidores no se detienen a observar estos puntos de la licencia EULA (End User License Agreement) que aceptamos cada vez que instalamos uno de sus productos.

Además de los acuerdos de colaboración con Microsoft o Cisco entre otros, el FBI ha contado con la colaboración de hackers afamados como el grupo "Cult of the Dead Cow [4]", creador de la famosa herramienta de "administración remota" de sistemas (a veces considerada como software espía o troyanos) "Back Oriffice". Esto le ha hecho trabajar en la creación de programas espía (spyware) como "Magic Lantern [5]" o "Cyber Knight", programas capaces de editar el registro de Microsoft Windows, detectar claves secretas, manipular archivos o espiar conversaciones por chat, Messenger o ICQ.

Carnivore [6] es un proyecto en este mismo sentido. En palabras de los propios representantes del FBI "Carnivore es un sistema computacional diseñado para permitir al FBI; en colaboración con un proveedor de Internet (ISP) se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación". Como podemos ver, Carnivore solicita la colaboración de los proveedores de Internet, pidiendo los registros de correos electrónicos enviados o recibidos por y para una persona en concreto. Esto es bastante similar a lo que la nueva Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE), que obliga a guardar los registros de todo lo que sucede en proveedores de Internet y demás empresas que desarrollen actividades comerciales en Internet. A pesar de las protestas de asociaciones de internautas y grupos sociales relacionados con la telemática, el gobierno español ha seguido adelante con la ley, cuyo reglamento es a día de hoy una incógnita y podría afectar muy negativamente a las libertades digitales de mucha gente.

Por otro lado, sistemas como Microsoft Passport.Net pueden ser una amenaza grande contra la intimidad de los "netizens" o ciudadanos de la red. Mediante Passport.Net es posible introducir un usuario y contraseña en uno de los sitios en los que se utilice y no tener que volver a enseñar ese "pasaporte virtual" en el resto de sitios que funcionan con

este sistema [7]. Es muy habitual que entremos en Hotmail a revisar nuestro correo, vayamos a Amazon.com a comprar un libro o a Ebay a buscar algo en sus subastas y que esos sitios nos reconozcan al entrar y nos muestren nuestras preferencias, etc. Esto no supondría mayor riesgo si el sistema no pudiera utilizarse para hacer correlaciones complejas que dieran más información que la estrictamente necesaria para cada una de esas tiendas virtuales. Pongamos un ejemplo: si un hombre mediante Passport.Net compra unos pantys en una web de lencería, cualquiera podría pensar que son para su madre, hermana o novia. Si mediante este mismo sistema se hace con el mapa de calles de Leganés, es probable que vaya a pasar una temporada por allí, de vacaciones o por trabajo. Si además de esto, se compra una escopeta de caza, el sitio que se la vende pensará que tiene un coto privado, y si compra una sierra para cortar metales, es probable que quiera hacer obras en las cañerías de casa. El "problema" para este sujeto viene al ver todos estos datos a la vez, junto con la noticia de que un encapuchado ha asaltado una caja de ahorros en Leganés a punta de escopeta recortada.

Sistemas de control en Telefonía móvil

Desde el principio de la telefonía móvil ha sido posible localizar y rastrear geográficamente un teléfono conectado a la red. De hecho, esto es un principio básico en las redes telefónicas móviles, es necesario para poder seguir dando servicio cuando un teléfono se mueve de una posición a otra. Cualquier gobierno u organización con capacidad de controlar las redes de telefonía móvil tiene la posibilidad de averiguar la posición de un teléfono en cada momento, o lo que suele ser lo más habitual, de su propietario.

La parte técnica de este seguimiento contínuo del individuo es muy sencilla. Las antenas de telefonía móvil necesitan emitir en todas las direcciones, porque deben funcionar con independencia de en qué dirección se encuentre la persona que quiere usar su teléfono. Sin embargo, en lugar de utilizar antenas que emitan en 360 grados, usan 3 antenas que emiten en sectores de 120 grados, porque son más sencillas de construir. Cuando un teléfono móvil está encendido, intenta conectarse con el mayor número de antenas posible para tener mejor cobertura y no perder la conexión con la red telefónica en ningún momento. Entonces, sabiendo a qué antenas se ha conectado un teléfono móvil en concreto, podemos trazar un polígono en el que con total seguridad se encontrará el teléfono buscado. Es decir, si yo me encuentro en mitad de una plaza y hay torres de telefonía móvil en las cuatro esquinas de la plaza, mi teléfono se habrá conectado a las cuatro torres utilizando las antenas que apuntan hacia él, por lo tanto es muy sencillo deducir que el teléfono se encontrará en el área comprendida entre las cuatro antenas implicadas. La localización de un teléfono móvil empleando este procedimiento tiene una precisión bastante similar a la que podría proporcionar un servicio de GPS de uso civil sin corrección de errores, aunque como se puede intuir, cuanta mayor sea la densidad de antenas en una zona en concreta, mayor será la precisión obtenida.

Actualmente bastantes compañías telefónicas y otras empresas asociadas ofrecen este servicio a costes muy bajos [8], cobrando únicamente el coste del envío de un SMS o mensaje corto a la central de localización. Esto ha aumentado su uso en situaciones en las que el propietario del teléfono móvil ha dado su consentimiento -tácitamente o no- para ser localizado, como por ejemplo en empresas de transportes, o adolescentes con teléfono

móvil, por citar dos ejemplos típicos.

Burlar estos sistemas de localización es prácticamente imposible si quien lo intenta pretende seguir utilizando la red telefónica móvil, puesto que como hemos dicho al principio, es un pilar básico para que esta red funcione correctamente. Sin embargo hay esfuerzos por parte de hackers o phreakers (hackers expertos en telefonía) para introducir retardos aleatorios en su señal con vistas a despistar a sistemas rastreadores e incrementar sus márgenes de error. De todas maneras, estos intentos no son más que una pequeña molestia para el sistema de localización y no lo anulan.

Sistemas de control en la vida cotidiana

Ya no es necesario utilizar Internet o poseer un teléfono móvil para ser rastreado y controlado a diario, el simple hecho de hacer la compra en un supermercado puede convertir nuestra despensa en un localizador a distancia.

A finales de los noventa, un grupo de investigadores del M.I.T. se dio cuenta de que sus esfuerzos para que los sistemas automáticos de reconocimiento de objetos que estaban desarrollando detectaran la realidad en toda su complejidad eran poco provechosos y decidieron ayudar a estas máquinas ideando unas etiquetas de auto-identificación para cada objeto (Auto-ID) [9]. Así, un libro tendría una etiqueta que informara al sistema de reconocimiento de que era un libro, proporcionando además datos sobre su autor, fecha de publicación, editorial, etc., y una botella de agua podría hacer lo propio, indicando además su fecha de embotellado y su fecha de caducidad. Esta mejora en los sistemas de reconocimiento pronto se vió como una oportunidad para la gestión de stocks, sobre todo en el campo de la alimentación y las grandes superficies comerciales.

La cadena estadounidense Wal-Mart está decidida a obligar en 2006 a sus 100 mayores proveedores a sustituir la identificación de sus productos mediante código de barras por esta nueva tecnología, que tiene el nombre de RFID (Radio-Frequency IDentification). De esta manera se solucionarán sus problemas para tener consciencia del estado exacto de sus estanterías en cada momento. Bastará emitir una leve señal de radio para que los pequeños circuitos RFID adheridos a cada producto se carguen eléctricamente y emitan su posición exacta. El sueño de cualquier encargado de stocks ya está aquí.

El chip RFID tiene el aspecto de un chip empleado para evitar robos: consta de una espiral metálica más o menos amplia que sirve como antena y un pequeño chip que es el que contiene la información. En los RFID pasivos no es necesario alimentar el circuito con baterías, basta emitir una señal de radio adecuada para que el circuito se cargue al recibirla y sea capaz posteriormente de emitir una señal de vuelta. Funcionarían en ese caso como una clase de "reflectores", reflejando la señal recibida, parcialmente modificada. Esto hace que cualquier objeto sea susceptible de portar un chip RFID de forma bastante inocua para quien lo posee.

En este mismo sentido, bibliotecas estadounidenses como la Berkeley Public Library han optado a su vez por esta tecnología para llevar un registro del préstamo de libros [10]. Cada libro tiene adherido un chip RFID que lo identifica unívocamente y permite contabilizar cuántos libros están prestados y cuántos no, o detectar posibles robos.

Las posibilidades para quienes quieren controlar son ilimitadas, pero la sociedad civil ya se ha dado cuenta de las consecuencias. Lee Tien de Electronic Frontier Fundation ya ha puesto el grito en el cielo, afirmando que "las bibliotecas han sido tradicionalmente muy respetuosas con la intimidad". Jackie Griffin, director de la Berkeley Public Library responde enérgico diciendo que "cuando era un adolescente dudaba si era gay o no, y no podía ir a una biblioteca y pedir prestado un libro sobre ello, porque otras personas podrían ver lo que estaba haciendo", mientras que con este sistema, el préstamo es automático, sin necesidad de que un bibliotecario tome nota de los libros prestados. Sin embargo, lo que descuida Griffin y apuntuntilla certeramente Katherine Albrecht, presidenta de la asociación CASPIAN [11] (Consumers Against Supermarket Privacy Invasion and Numbering), es que cualquiera con un lector de RFID corriente será capaz de leer los valores de los chips que portan los objetos que poseemos incluso fuera de su ámbito original, esto es, el libro seguirá devolviendo la señal de un lector RFID aunque se encuentre a kilómetros de una biblioteca, si ese lector RFID se situa lo suficientemente cerca, o un test-antiembarazo podrá ser detectado una vez fuera del supermercado por una persona que tenga un lector RFID y muchas ganas de investigar sobre la vida privada de alguien.

Como casi siempre, las situaciones de miedo extremo hacen que la sociedad permita perder parte de su libertad en favor de más seguridad. Esto se ha visto reflejado en un hecho insólito que relata el experto en Seguridad de la Información Bruce Schneier en su página web: después de los atentados del 11 de septiembre, la administración Bush ha puesto en marcha una medida mediante la cual los ciudadanos de paises que actualmente no requieren de visado para entrar en los Estados Unidos de América deberán disponer de pasaportes que se ajusten a los nuevos controles de seguridad. Estos controles exigen que el pasaporte disponga de un chip RFID que informe en todo momento del nombre, apellidos, fecha de nacimiento y demás datos a la hora de accionar un lector RFID a menos de 10 metros de distancia del pasaporte [12]. Como comenta Schneier, los nuevos modelos de pasaportes sobre los que se estaba trabajando anteriormente también disponían de un chip con todos esos datos para agilizar su lectura, pero no era un chip de radio-frecuencia, era necesario pasar a través de un lector el pasaporte, como ocurre con las tarjetas de crédito. Es decir, el portador del pasaporte sabía cuándo se estaban leyendo sus datos y cuándo no. Con la nueva tecnología RFID esto no es así, en cualquier momento pueden estar leyendo los datos contenidos en el chip de su pasaporte sin que su portador lo sepa. Un agravante es que no solo los servicios de inmigración pueden hacer esto, sino que cualquier persona con la tecnología necesaria (un lector de RFID es algo barato hoy en día), puede leer esos mismos datos sin que nadie se entere aparentemente.

Las mejoras en la producción de estos chips espía han conseguido que se puedan fabricar en escalas inferiores al tamaño de una lente de contacto común, permitiendo su integración en casi cualquier producto. En 2003, Katherine Albrecht alarmó a la opinión pública al descubrir que en un supermercado de Cambridge de la cadena Tesco todas las cuchillas de afeitar Gillette poseían un chip RFID en su envoltorio y el stand donde estaban expuestas detectaba cualquier movimiento de su posición para hacer una foto de la persona que había cogido una cuchilla, como medida contra posibles robos de cuchillas. "No vamos a saber donde estarán esos productos etiquetados, y no sabremos tampoco cómo están siendo usados" manifestó por aquel entonces Albrecht. Horas después, las principales páginas web de noticias tecnológicas en Internet (slashdot.org o theregister.com, entre otras)

arremetieron contra esta nueva tecnología que viola la intimidad de los consumidores [13].

Referencias:

[1] El informe completo del Parlamento Europeo puede leerse aquí: http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

[2] De esta misma noticia se hizo eco el diario digital IBLNews en julio de 2001: http://www.iblnews.com/news/noticia.php3?id=18939

[3] El 3 de septiembre de 1999 la CNN hacía pública esta sospecha: http://www.cnn.com/TECH/computing/9909/03/windows.nsa/ y era ampliamente debatida en el foro de noticias tecnológicas Slashdot: http://slashdot.org/article.pl?sid=99/09/09/138209

[4] http://www.cultdeadcow.com

[5] Reconocido públicamente por el FBI: http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=25471

[6] http://www.fbi.gov/programs/carnivore/carnivore.htm

[7] # Tal y como se puede leer en la declaración de privacidad de Passport .Net:

"Utilización de Su Información Personal.

La información personal recolectada en este Sitio será utilizada para operar el Sitio y proveer el/los servicio(s) o llevar a cabo transacciones que hayan sido solicitadas o autorizadas por usted.

Para soportar estos usos, Microsoft puede utilizar información personal para proveerle un servicio al cliente mas eficiente, para mejorar el Sitio o cualquier producto o servicio relacionado con Microsoft, y para hacer el Sitio mas sencillo de utilizar al eliminar la necesidad de ingresar una y otra vez a la misma información o para personalizar el Sitio a sus intereses o preferencias particulares."

[8] http://www.el-mundo.es/navegante/2003/12/10/empresas/1071058091.html

[9] http://www.salon.com/tech/feature/2003/07/24/rfid/print.html

[10] http://www.salon.com/tech/feature/2004/07/26/rfid_library/print.html

[11] http://www.nocards.org/

[12] Aparecido el 4 de octubre de 2004 en el International Herald Tribune: http://www.iht.com/articles/541711.html

[13] http://www.boycottgillette.com/index.html , http://slashdot.org/articles/02/11/17/0327244.shtml?tid=126 , http://www.rfida.com/nb/gillette.htm

blog.txipinet.com

https://www.lahaine.org/est_espanol.php/cibercontrol_social