Criptología; Seguridad Informática y Derecho Leyes del Ciberespacio

MIGUEL A. GALLARDO ORTIZ

Ingeniero Superior de Minas, especialidad de Energía y Combustibles. Consultor Profesor de Unix & C.

(ESPAÑA)

La criptología es una elegante disciplina matemática con una fascinante historia y un prometedor futuro en el mundo de la informática y las comunicaciones digitales modernas.

Los algoritmos criptológicos representan, directa o indirectamente, el único procedimiento conocido para garantizar la confidencialidad y la autenticidad de la información, mediante la clave secreta y la firma electrónica.

Además de una breve, aunque sólida introducción técnica a la criptología moderna, y métodos de control de acceso, protección frente a actos vandálicos (virus y hackers), y monitorización del trabajo informático colectivo, el profesional del derecho informático debe tener conocimientos sobre cómo se contemplan en la legislación española, europea, y de países avanzados en este área como los EEUU y Japón.

La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y algunos artículos del proyecto de nuevo Código Penal, así como las normativas y leyes de menor rango que comienzan a tratar, con sus luces y sus sombras este nuevo fenómeno, darán lugar al desarrollo de una industria, y de unos contenciosos, entorno al delito informático.

Pero además, la ética del secreto, y su representación en el ordenador y transmisión por medio de enlaces telemáticos van a cambiar la conciencia

colectiva respecto al uso y al abuso de la información en una sociedad que cada vez está más cerca de ese modelo postindustrial que algunos autores han llamado infoesfera y otros ciberespacio, en los que se consigue la eliminación virtual de las distancias. Es aquí donde está, sin ningún género de dudas para nosotros, la más apasionante aventura intelectual de los tiempos en que nos ha tocado vivir.

FUNDAMENTOS DE CRIPTOLOGIA PARA PROFESIONALES DEL DERECHO

Como es bien sabido, la criptología es casi tan antigua como la escritura y, hasta el reciente desarrollo de la informática, ha estado al servicio exclusivo de los grandes poderes políticos y económicos. El cifrado de la información solía ocultar secretos de estado, o servir de cauce a comunicaciones militares.

Es previsible que, en España, la promulgación de la Ley Orgánica para la Regulación del Tratamiento Automatizado de los datos de Carácter Personal (LORTAD) provoque una rápida sensibilización de Administración y de empresas, especialmente en algunas actividades que hasta ahora se han ejercido con la mayor impunidad, y en ocasiones, fraudulentamente.

Actualmente, los más modestos sistemas informáticos son capaces de realizar complejas encriptaciones o cifrados de información, y lo único que queda en manos de los grandes poderes políticos y económicos es la remota posibilidad de intentar un acceso no autorizado, aunque para ello tengan que dedicar durante meses costosos ordenadores vectoriales tipo Convex, Fujitsu VP o Cray. Muchos más escasos aún son los especialistas capaces de ofrecer unas mínimas garantías de éxito en el ataque. Y desde luego, España no es una potencia en la Guerra Electrónica.

A continuación, describiremos brevemente el «state of the art» en esta estratégica tecnología, así como las instituciones que en España se dedican a tan fascinante disciplina y los acontecimientos que últimamente han estado estrechamente relacionados de una u otra forma con criptología.

TECNICAS MAS EMPLEADAS EN LA ACTUALIDAD

La microelectrónica ha hecho posible la rápida ejecución de programas con complejos algoritmos, pero todavía se siguen utilizando las series aleatorias, que básicamente consisten en una larga serie de números aleatorios (o pseudoaleatorios) a modo de libreta de uso único para el cifrado y descifrado de mensajes, y con una clave tan larga como el texto a cifrar. Aunque es bastante seguro, este método obliga a realizar complejos intercambios de claves y no aprovecha los recursos que ofrecen actualmente la microelectrónica.

Los métodos de cifrado más utilizados en la actualidad son los de clave privada, como el DES, pública, como el RSA, y se está experimentando con una nueva generación de algoritmos basados en curvas elípticas de la forma: $y^2 = x^3 + a\,x + b$

El gobierno de los Estados Unidos ha sido particularmente estricto a la hora de impedir la exportación de criptología, al igual que ha hecho con los ordenadores vectoriales y la fotónica.

En particular, el término Data Encryption Standard o DES no suele emplearse correctamente fuera de los EEUU, ya que el National Bureau of Standards no extiende el certificado de homologación a sistemas no americanos salvo en casos muy excepcionales. Parece ser que consideran que su divulgación puede afectar al modo de vida norteamericano, ya que ni ellos mismos serían capaces de descifrar las comunicaciones en las que se utiliza. Y hemos tenido ocasión de comprobar recientemente todo lo que los EEUU están dispuestos a hacer para protegerse.

El Data Encryption Algorithm o DEA, es el que una vez homologado proporciona el DES, y no es difícil conseguir alguna versión en C portable a MS-DOS, Unix, VMS, etc. Consiste en 16 pasos de sustitución y permutación de bits, y produce un mensaje cifrado tan aleatorizado que es prácticamente imposible obtener el texto legible si no se conoce la clave. Es mucho más eficiente si se ejecuta en un hardware orientado a la criptología, como el que suministra Intel, AMD o Motorola cuando disponen de información suficiente del usuario final.

Al igual que ocurre con el resto de los algoritmos considerados como seguros, también existen rumores de que se ha conseguido desarrollar un procedimiento de ataque al DES con grandes posibilidades de éxito. Sin embargo, nadie lo ha hecho público hasta ahora, y quien lo hiciera sin duda pasaría a la posteridad, ya que la inversión realizada mundialmente en tecnología DES es muy considerable, y cualquier técnica que cuestionase su seguridad provocaría medidas drásticas en el mundo financiero, político y diplomático de nuestros días.

La principal alternativa al DES es el RSA, que permite no sólo encriptar, sino también autentificar los mensajes. Los sistemas de clave pública como RSA se utilizan dando a conocer el método de cifrado y manteniendo en secreto el de descifrado, de forma que si A quiere mandar un mensaje cifrado y autentificado con su firma electrónica, lo que debe hacer es cifrarlo con el procedimiento que B publica, y descifrarlo con el suyo propio, de forma que cuando le llegue a B, éste pueda descifrarlo con su procedimiento y comprobar que proviene de A probando a cifrarlo con su procedimiento. Naturalmente, debe ser imposible deducir el método de descifrado aunque se conozca el de cifrado.

La seguridad del algoritmo RSA se basa en lo inabordable que resulta la descomposición factorial de grandes números formados por el producto de números primos también grandes. Incluso si se utilizase el más moderno Cray YMP, Convex C3, Fujitsu VP o Nec con varios procesadores vectoriales (tal vez los hipercubos o multiprocesadores con paralelismo masivo algún día los superen), es decir, con una potencia de cálculo de muchos MFLOPs, serían necesarios muchísimos años para descomponer en factores primos el producto de dos números primos de 150 dígitos cada uno. Aunque es previsible la aparición de sistemas órdenes de magnitud más potentes que los actuales, desde el punto de vista matemático resulta muy difícil mejorar la eficiencia de los algoritmos de ataque empleados actualmente.

Un desarrollo original para sistemas Unix y MS-DOS en el que actualmente estamos comprometidos es en el que se basa en lo que hemos denominado como «defensa activa». Se trata del Proyecto Pandora (X86), y consiste en comprimir y encriptar los datos fusionándolos con el programa desencriptador descompresor en un sólo ejecutable capaz de destruirse o de intoxicar en el caso de que se intente un acceso no autorizado.

CRIPTOLOGIA AQUI Y AHORA. EN EL ALMA DE UNA NUEVA EMPRESA

Probablemente, España sea uno de los países en los que las técnicas de seguridad empleadas guarden menos relación con el valor de la información que se protege. Podemos asegurar que hay mucho más morbo que economía, industria o inteligencia.

Mientras, Ejército y CESID dedican generosos presupuestos a proteger información prácticamente ociosa (a pesar de que hay agujeros que no serían difíciles de encontrar en sus sistemas), otras instituciones como la Policía o el Ministerio de Asuntos Exteriores ofrecen demasiada facilidad para acceder a información que, si no está clasificada, sin duda debería de estarlo.

Y lo que es peor, la capacidad de criptoanalizar información codificada de nuestros cuerpos y fuerzas de seguridad del Estado ha sido desafiada por la organización terrorista ETA. Parece ser que, rodeado de un cierto secretismo, los ordenadores requisados no han podido ser desprotegidos hasta el momento.

Desde el punto de vista académico, si bien se imparten unas nociones de criptología contempladas en los programas varias de escuelas de ingeniería y facultades, sólo en la Facultad de Informática de la Universidad de Granada existe actualmente una asignatura cuatrimestral con el nombre de «Criptología».

Desde Edgar A. Poe, y Alan Turing, ninguna persona o institución se autocalifica seriamente como experto en criptología inversa o criptoanálisis, aunque sí que se admiten algunas apuestas. En España se ha alquilado por

varios cientos de millones de pesetas anuales un potente ordenador vectorial que, según cabe deducir por las especificaciones técnicas que se formularon hace menos de dos años por parte de Defensa-INTA, parece destinado al menos a intentar el criptoanálisis, aunque no va a ser fácil realizar proyectos propios comparables a los de otros centros de la OTAN, mucho más por la falta de medios humanos, que materiales.

Como curiosidad, me permito dar a conocer que quien escribe esta comunicación ha tenido la gran satisfacción de colaborar con el autor de un elegante y eficaz criptoanálisis del programa de encriptación que WordPerfect ofrece a sus confiados usuarios en la opción Ctrl+F5 (Contraseña). Ahora podemos averiguar en segundos la palabra secreta con la que se ha protegido un documento WordPerfect independientemente de la versión, sistema operativo y hardware con el que se haya elaborado.

Tanto este curioso criptoanálisis, como los detalles del diseño del anteriormente mencionado proyecto Pandora, programa autodestruible–comprimible–encriptable–intoxicador, fueron expuestos en una ponencia que presentamos en la I Reunión Española sobre Criptología, celebrada en Palma de Mallorca del 2 al 4 de Octubre con el patrocinio del Gobierno Balear.

En dicha Reunión, organizada por el Laboratorio de Criptología del CSIC y la Universitat de les Illes Balears participaron responsables de la seguridad de la información de diversas instituciones públicas y privadas, así como varias empresas que ofrecen productos y servicios en un mercado del que se dice que todavía no ha visto la quiebra de ninguna empresa especializada en tan sensible y a la vez desconocida materia en España.

ZERO KNOWLEDGE PROOF. LA SOMBRA DE UN SECRETO

Muchas de las más brillantes ideas que pueden aplicarse en criptología son útiles también en las más variadas esferas profesionales. Pero pocas son tan elegantes como las pruebas con conocimiento cero.

El problema de la identificación segura es uno de los más apasionantes a los que se enfrenta tanto la informática como las comunicaciones digitales modernas. En esencia, cualquier sistema ha de asociar un identificativo (login) y un número secreto (password) a cada usuario autorizado.

Sin embargo, en los sistemas en los que se deposita información altamente confidencial, las suspicacias, y también la experiencia, aconsejan no revelar el número secreto ni siquiera al administrador o responsable del sistema.

¿Cómo puede verificarse entonces la autenticidad de la identidad que el usuario declara?

Pensemos en un matemático que descubre una nueva teoría con la que consigue explicar satisfactoriamente algunas observaciones o fenómenos.

Este matemático no desea dar a conocer la parte fundamental de su teoría, pero quiere convencer al resto de la comunidad científica de que la ha descubierto únicamente él, y de que es correcta.

La teoría del Zero Knowledge Proof consiste, básicamente, en elaborar un protocolo mediante el cual otros científicos hacen preguntas concretas al descubridor de la teoría secreta, y éste les responde con el conocimiento del secreto, pero sin dar detalles de él, hasta convencer a los demás de que sólo es posible la respuesta a las preguntas mediante el conocimiento de un secreto que los demás no poseen.

Para ilustrar gráficamente esta teoría, se recurre a la imagen de un secreto apantallada por una mampara que impide que el público lo vea directamente, pero de forma que dicho secreto pueda ser iluminado desde distintos ángulos. Los espectadores podrían llegar a tener la certeza de que, efectivamente, tras la mampara se esconde el secreto, y que éste es auténtico.

Matemáticamente, todo password o clave puede codificarse como un número entero de tantas cifras como sea necesario. La sombra de un password no sería más que el resto de dividir dicho entero secreto por un número menor que él.

Al igual que ocurre con el algoritmo RSA, los matemáticos especializados en teoría de números trabajan afanosamente tanto por proponer, como por comprobar y rebatir los detalles de los sistemas que se basan en este principio.

Ejemplos de complejas operaciones logísticas, tácticas y estratégicas basadas en el Zero Knowledge Proof son fáciles de encontrar en el terreno militar y diplomático y por supuesto, en las relaciones que mantienen servicios y sociedades secretas con la población ajena a sus intereses.

Pero también el mundo comercial y financiero conocen desde hace mucho tiempo que la información innecesaria que uno proporciona siempre acaba llegando, de la forma más perjudicial, al último interesado en ella, normalmente un adversario o competidor.

Y por supuesto, un buen abogado debe conocer los fundamentos del Zero Knowledge Proof, aunque sólo sea de una forma intuitiva, para realizar su trabajo cotidiano sin perjudicar a sus clientes.

CONTENCIOSOS INFORMATICOS ACTUALES, Y VICTIMIZACION SECUNDARIA

A lo largo de este último año se han visto en los tribunales tres casos en los que la información accesoria ha sido la clave de procesos de victimización secundarios.

El primero de ellos ha sido el escándalo de la red de tráfico de datos, en el que el interés, el lucro, la ignorancia y la pereza periodística han alejado la atención informativa de la verdad.

El segundo ha sido el del pirata informático que ha «robado» 12.000 millones a no se sabe quien. Sólo encubierta por una supuesta operación antidroga se pudo proceder al registro.

Y por último, un importante banco está siendo inspeccionado informáticamente en estos momentos, y al igual que en los casos anteriores, existen serias dudas sobre segundos o terceros usos que puedan hacerse de las órdenes de un juez.

De lo que no cabe ninguna duda es que si no escribimos nosotros las reglas de la justicia informática, alguien lo hará por nosotros, probablemente en inglés, y por bien que se traduzcan, será difícil salir beneficiados aquí con las de otros países.