APLICACIONES DE LOS MÉTODOS CRIPTOGRÁFICOS

Raúl Gonzalo

Durante mi reciente experiencia investigadora sobre los métodos de seguridad y el estudio de la criptografía como herramienta para proteger la información siempre que he conversado con alguien acerca del tema, al final ha surgido la misma pregunta: *«Bien, pero todo esto, ¿para qué sirve?, ¿dónde se utiliza?»*. En este artículo, además de pretender que el oído se vaya acostumbrando a esta nueva y rara palabra como es la criptografía, se intenta divulgar, manteniendo el espíritu de esta revista, las aplicaciones prácticas en sistemas reales.

La criptografía (del griego: *kryptós* y *graphos*) es, a grosso modo, la ciencia encargada de la seguridad de la información, y desde nuestro punto de vista como ingenieros, de la información en las comunicaciones. Es un tema de actualidad, o como diría una presentadora de un programa de TV de cuyo nombre no quiero acordarme, de rabiosa actualidad.

La necesidad de proteger información es tan antigua como la escritura misma y no extraña que la mayoría de los métodos antiguos (o clásicos) tuvieran una vinculación directa con la guerra. De hecho, en la II guerra mundial, se utilizaron muchos tipos de máquinas, las más famosas son la Enigma (alemana) y la Purple (japonesa) basadas en un principio de rotores. Hoy en día se conoce que la rotura de ambos códigos por parte de los aliados fue un factor importante para el desenlace de la guerra. Recomiendo la lectura de *The Codebreakers* [1] donde se da un repaso histórico y entretenido a la evolución de los sistemas criptográficos.

RAÚL GONZALO *es Ingeniero de Telecomunicación por la ETSETB, especialidad en Telemática. Realizó el Proyecto Final de Carrera sobre Criptografía.*

Tradicionalmente, las instituciones financieras y gubernamentales son las que más se han preocupado por la seguridad. Sin embargo, a pesar de la evidencia del problema, las redes actuales son generalmente inseguras, es decir, existen multitud de sistemas informáticos operando sin las protecciones adecuadas. El creciente uso presente y futuro de las redes de datos así como algunos ataques históricos concretos ha puesto en estado de alerta a los programadores de los sistemas informáticos, fundamentalmente los compartidos.

Existen multitud de anécdotas de fallos en la seguridad de sistemas. Los más conocidos son las acciones de escuchas telefónicas. Un típico caso muy utilizado son los ataques a bancos donde se redondean las fracciones de peseta de una cuenta para moverlas a la cuenta del atacante. Como son pequeños ataques, son inapreciables, pero repetidos pueden conseguir un efecto muy «deseado». Otro tipo de ataques intentan romper los accesos de los sistemas con password, como los entornos UNIX. Existe una gran variedad de ellos, desde los caballos de Troya (programas que emulan la pantalla del login para obtener la contraseña del usuario) hasta la búsqueda selectiva de la clave probando con nombres de pila, números de teléfono, fechas, nombres de entidades deportivas, etc..

La mayor de las violaciones de seguridad de las computadoras comenzó una tarde de noviembre de 1988, cuando R.T. Morris liberó un programa gusano en Internet. Su gusano representó en la seguridad de las redes de telecomunicaciones lo mismo que el hundimiento del Titanic para la industria del transporte. El gusano utilizaba tres métodos diferentes para intentar acceder a nuevas máquinas. El más elaborado de ellos utilizaba el programa *finger* de UNIX. El gusano llamaba a *finger* con una cadena especialmente diseñada de 536 bytes como parámetro. Esta cadena sobrepasaba la capacidad del búffer y escribía sobre su pila, aprovechando que no se verificaba el desbordamiento del búffer. Así, cuando el programa regresaba al procedimiento que realizó la solicitud, no volvía al main, sino a un procedimiento dentro de la cadena de 536 bytes de la pila, que intentaba ejecutar */bin/sh*. Si lo lograba, el gusano disponía entonces de un Shell que se ejecutaba en la máquina atacada.

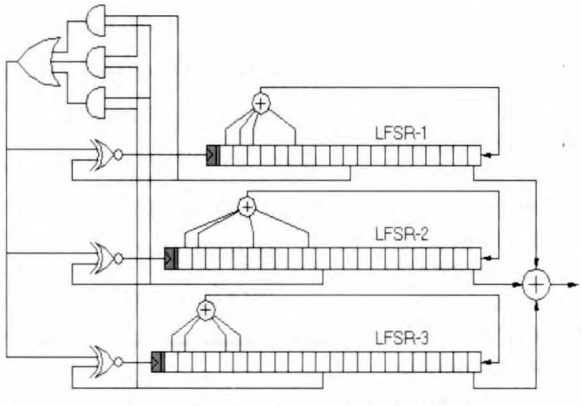

Figura 1.-Algoritmo A5 de GSM

Cada vez que el gusano lograba el acceso a una nueva máquina, verificaba si en ella existían copias activas del mismo. En tal caso, la nueva copia salía, excepto una vez de cada 7, tal vez para mantener al gusano en propagación, incluso en el caso en que el administrador del sistema tuviera su propio gusano para engañar al gusano real. El uso de 1 por cada 7 creó un número enorme de gusanos y fue la razón por la que poco tiempo después, las

máquinas infectadas fueron obligadas a parar: estaban totalmente infectadas por gusanos. Por suerte, el gusano de Morris no era dañino y sólo reproducía copias de sí mismo.

Desde entonces, se han incrementado las medidas de seguridad de las redes y se han creado nuevos estándares de seguridad en la transmisión de datos, gestión de claves, etc.. El uso de estos sistemas es más cercano a nuestras vidas de lo que pueda parecer a simple vista.

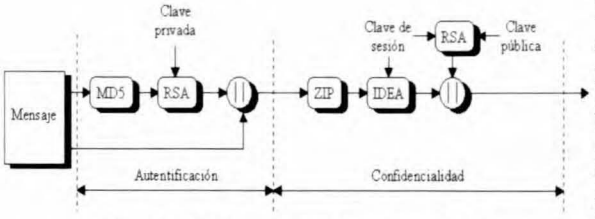

Figura 2.-Mecanismo de autenticidad y confidencialidad en PGP

Para amenizar la descripción de los sistemas más importantes actualmente (sería imposible comentarlos todos), en vez de enumerarlos en una lista, he pensado en narrar la siguiente historia.

Es posible que después de leer este interesante artículo, te acuerdes de que mañana es el cumpleaños de tu novio/a. Rápidamente, te diriges al cajero automático más cercano para sacar dinero y comprarle un regalo. Después de introducir la tarjeta de crédito, el cajero te pide un número (una especie de password): el PIN (Personal Identification Number). Lo que no saber es que ese número se cifra con un algoritmo llamado DES cuyo resultado está almacenado en la banda magnética, y es con el que se compara para validar tu identidad (la descripción de los métodos de cifrado DES, IDEA, RSA, ElGamal, las funciones hash MD5, SHA y los protocolos de comunicaciones se pueden encontrar en cualquier libro genérico de criptografía, como por ej. [2]).

Un poco más tarde, te diriges a una cabina telefónica desde donde piensas llamar a tu pareja para quedar mañana. Como no llevas suelto, utilizas la teletarjeta de Telefónica (usada como monedero electrónico). Dichas tarjetas inteligentes llevan un chip incorporado, y a diferencia de la banda magnética, puede realizar una autenticación mutua de los dos interlocutores, realizar cálculos y almacenar datos.

Si tu pareja es de las que se han comprado un teléfono móvil digital, la señal que recibirá en el terminal estará cifrada. En el sistema GSM, la seguridad se implementa mediante un protocolo de autentificación que utiliza dos algoritmos, el A3 y el A8. Durante la transmisión, la información se cifra bit a bit mediante el algoritmo A5. Según Schneier [3], el esquema del A5 (deducido de su código fuente), es tal como se indica en la figura 1.

El generador se compone de 3 LFSR de longitudes 19, 22 y 23. De cada registro, se toma el bit central y se realiza una votación por mayoría. Sólo cambian de estado los LFSR cuyo bit intermedio coincide con la votación. La salida es la suma de los últimos bits de los 3 registros.

Sin embargo, tu pareja tiene conectado el buzón de llamadas y simplemente le dejas el recado. Entonces decides mandarle también un mail para asegurarte de que va a recibir tu mensaje y te diriges a la sala de ordenadores.

Existen multitud de programas informáticos comerciales que implementan mecanismos criptográficos para proteger la información. Uno de estos mecanismos, por ejemplo, es el cifrador en flujo RC4, secreto hasta hace poco, utilizado en Lotus Notes, Apple's Computer AOCE, Oracle Secure SQL, ... y también en Netscape. El funcionamiento de este cifrador se describe en [3], donde también aparece el código C para que cualquiera lo pueda implementar, salvo en un programa comercial ya que está patentado. Existen muchos algoritmos que están patentados (algunos sólo en EEUU), como el RSA, el RC4, ... y para poder usarlos comercialmente es necesario pagar royalties. Para evitar esto, se han diseñado otros esquemas equivalentes no patentados, como por ejemplo, ElGamal frente al RSA.

Una vez delante del ordenador, utilizas el correo electrónico. Dependiendo de la máquina en la que te encuentres y el programa que ejecutes, utilizarás un sistema u otro. Uno de estos esquemas de correo es el llamado PGP (Pretty Good Privacy), desarrollado por Zimmermann. Su idea no fue desarrollar ningún nuevo tipo de cifrado, sino seleccionar los mejores sistemas disponibles e integrarlos en una aplicación de propósito general. En concreto, se escogió RSA para la gestión de las claves, IDEA para el cifrado simétrico de la información y MD5 como función hash para la autentificación del mensaje.

Las funciones hash, como el MD5, el SHA, ... son funciones que dada una tira de bits de cualquier longitud, devuelven un número fijo de bits (128 para el MD5 y 160 para el SHA), y además, dado el resultado, es muy difícil conocer un mensaje que produzca el mismo resultado.

Además del PGP, existen otros sistemas que se utilizan para correo electrónico. Muchos están estandarizados, como el MHS (Servicio de manejo de mensajes de Novell), y otros no, como el POP (Post Office Protococol, sólo para PC y Mac). Pero los más importantes son el PEM (Privacy Enhanced Mail) y el SMPT (Simple Mail Transfer Protocol) que son los algoritmos estándar en Internet. A diferencia del PGP, el PEM utiliza del DES en modo CBC para cifrar la información, y el RSA junto con el MD2 o MD5 para proporcionar la autentificación del mensaje.

Todos estos sistemas permiten que el envío de los mensajes esté lo suficientemente protegido como para evitar las posibles intercepciones y escuchas durante la transmisión.

Finalmente, como ya has enviado el mail que querías y ya no tienes nada que hacer, te pones a navegar por Netscape. Si te fijas, cuando le das al menú *About Netscape...* dentro de la ayuda, aparece una pantalla con información sobre la versión, si utiliza Java, y por último el sistema criptográfico que utiliza. En la versión 2.02, se utilizan los mecanismos RSA, MD2, MD5 y RC4. Por cierto, ya que estás en Internet, si quieres conocer algo más sobre el tema, busca esta dirección: http://www.quadralay.com/www/Crypt/Crypt.html.

Bibliografía

[1] D. KAHN, *The Codebreakers*. 1967

[2] W. STALLINGS, *Network and Internetword Security*. Prentice-Hall. 1995

[3] SCHNEIER. *Applied Cryptography*. John-Wiley & Sons. Segunda edición. 1996