Wikileaks y el manejo de información secreta

ene 20

Posteado a las 20 de Enero de 2011 - 10:38 | 0 comentario

Por Tomás Barros, director Ejecutivo de NIC Research Labs, profesor jornada parcial del Depto. de Ciencias de la Computación, FCFM, U. de Chile.

Una cosa que me he cuestionado sobre Wikileaks es cómo tuvo acceso a los Cables Diplomáticos de Estados Unidos. Supongo que alguien al interior del Gobierno fue quien proporcionó estos cables. Sin embargo, ¿cómo sólo una persona puede tener acceso a toda esa información?

Estados Unidos tiene procedimientos muy estrictos para el manejo de la información, la que es clasificada en distintos niveles de confidencialidad. Éstos son: desclasificada (el nivel por defecto, de libre acceso), confidencial, secreta y muy secreta. El nivel que corresponde a cada documento se determina de acuerdo al riesgo que significa para la seguridad nacional y sólo se puede clasificar en base a este criterio. La ley de acceso a la información de Estados Unidos (Freedom of Information Act) data de 1966 y su aplicación ha sido muy estricta.

Desconozco cómo se manipulan los documentos según su nivel de confidencialidad. Supongo que antes se manejaban en bodegas o cajas fuertes, donde para acceder a una documentación se requería pasar por distintas autorizaciones. Un caso muy usual son las cajas fuertes de los bancos que requieren dos llaves, una proporcionada por el cliente y otra por el banco. Esto implica que para poder violar esa seguridad, es necesario que al menos dos personas se coludan.

Para los documentos digitales, la criptografía moderna nos da soluciones sólidas y variadas para mantener la confidencialidad. Seguramente varios ya habrán escuchado sobre encriptar o cifrar datos. Cuando se cifra un documento, se aplica una transformación con una clave a los datos para que nadie pueda entenderlos (podemos decir que se desordenan los datos). Esta transformación es reversible (se puede volver a ordenar) sólo si se posee esa clave, la que es única y secreta cuando se habla de criptografía simétrica, o se trata de un par de claves, una pública y una privada, cuando se habla de criptografía asimétrica.

Es prácticamente imposible descifrar un mensaje si no se tiene la clave. El problema es que esta clave, más conocida como "llave" se transforma en el punto débil. Por una parte está el problema de dónde y cómo la almacenamos, cómo la distribuimos, cómo restringimos su acceso y, por otra, está el problema de que basta que una sola persona la tenga para que posea acceso completo a la información cifrada. Pero ¿qué pasa si la persona nos traiciona?, ¿si la persona muere y es la única con la llave? o ¿si a esta persona la amenazan para que haga uso de la llave? Sobre esto último, existen ya hace un tiempo técnicas conocidas como Threshold Cryptography (Criptografía con umbral, en una traducción libre).

En Threshold Cryptography, nadie tiene la llave completa, sino que hay un número N de personas que tienen un pedazo, algo similar a la caja fuerte del banco donde N = 2. Lo interesante es que tampoco necesito a las N personas para descifrar, sino que a un subconjunto de ellas. Por ejemplo, si distribuyo pedazos de la llave entre 10 personas, podría necesitar sólo 6 de ellas para descifrar, es decir, 6 es el "umbral" (threshold) de donde viene el nombre de la técnica. Esto es bueno porque evita la traición individual (necesito que al menos 6 se unan para traicionar), hay 4 que pueden morir y aún puedo acceder a la información y hasta 4 podrían estar bajo amenaza y seguir siendo seguro (con la técnica se pueden detectar esos 4).

Threshold Cryptography no es muy usada, pero existen implementaciones. En el caso de los cables diplomáticos, ¿no estaban protegidos? Si lo estaban, ¿alguien con acceso a la clave traicionó? ¿Existían técnicas que requerían de varios para acceder a la información? ¿Hubo una colusión? Supongo que nunca tendremos las respuestas, pero las preguntas me siguen dando vueltas.