La Seguridad en redes cuánticas, ¿La protección perfecta?

Los Peritos en Informática, nos vemos envueltos en numerosos casos, donde se ha roto la seguridad de redes, dispositivos, robo de información, etc. empleando técnicas de *hacking* o apropiándose de las credenciales del usuario mediante suplantación.

A lo largo de la historia, todo aquello que parecía seguro en criptografía, dejaba de serlo a los pocos años, motivado por la proliferación de nuevos algoritmos y por el aumento de la potencia computacional de los ordenadores.

Esta tendencia, se acortaba cada vez más en el tiempo, por el aumento de la eficiencia de los algoritmos y por el aumento colaborativo de varios usuarios, que empleando computación paralela, conseguían respuestas computacionales, superiores a grandes centros de procesos de datos.

Es por ese motivo que nació la encriptación cuántica como medio para un intento de solución definitivo en las comunicaciones, que aunque suene a ciencia ficción, no es más que la distribución de claves en envíos criptográficos, utilizando el comportamiento de la polarización de un fotón (estos sistemas se basan en la superposición y el entrelazado de micro partículas.), según el principio de incertidumbre de *Heisenberg*.

Aunque la primera tecnología de estas características surgió en 1980, el primer test se realizó nueve años más tarde y a finales del siglo XX ya se vendía un sistema capaz de transmitir claves cifradas a través de una fibra óptica de 30 millas de longitud. Las compañías como Quantique и MagiQ Technologies vendieron un sistema QKD que incluso un técnico corriente podría instalar.

Cerberis, el distribuidor de claves cuánticas a la venta

Esto, según las empresas distribuidoras del producto, sería el fin de los hacker, de los espías y la “Protección Perfecta”

Como afrontaría un Perito un caso basado en esta tecnología, presentando un informe claro, por parte de una empresa que ha adquirido un sistema “Cerberis” para garantizar sus comunicaciones y que estas han sido rotas por desconocidos, sustrayendo información relevante por parte del demandante.

Daremos por hecho, que los datos personales sustraídos, fueron publicados en un servidor ubicado fuera de la unión Europea y que la demanda se presenta en territorio Nacional.

La base científica por parte del demandado, sería demoledora, sus principios solidos que en un primer momento, arrojarían indicios de toda duda y por lo tanto, que los datos se habrían obtenido de cualquier otro modo, pero NO por romper la seguridad de las comunicaciones.

La empresa demandante, asegura, que los datos publicados, fueron transmitidos entre la sede A y la sede B ambas en el territorio Nacional, en una fecha y hora concreta.

- **Lo primero sería descartar que la fuga de información provenga de los servidores ubicados en las sedes A y B.**

Tras una inspección de ambos servidores, utilizando las credenciales de los responsables de cada centro y en su presencia, se observa:

> *El perito ha de expresar el método científico usado, las operaciones llevadas a cabo.*
> *A la vista de ello, el Juez puede evaluar la fiabilidad del perito, teniendo en cuenta las alegaciones de las partes y otras posibles pruebas*

1. Que se trata de controladores de dominio de solo lectura RODC y estos hospedan particiones de sólo lectura de la base de datos de Servicios de dominio de Active Directory® (AD DS). Por lo tanto de momento, queda garantizada la manipulación ya que un RODC proporciona un mecanismo más seguro para implementar un controlador de dominio. Puede conceder a un usuario del dominio no administrativo el derecho a iniciar sesión en un RODC, con un riesgo mínimo para la seguridad del bosque de Active Directory.
2. El servidor no tiene permitida la navegación por Internet.
3. No obstante, además se revisan los Registros de eventos, comprobamos las comunicaciones y puertos activos, No se localizan anomalías.
4. Comprobamos la seguridad física, que consta de una cerradura electrónica por “rfid” para el acceso al servidor, de la cual solo tiene permiso la persona responsable y cuyos registros de acceso coinciden con el acceso del mismo y no ha sido violentada.
5. Finalmente comprobamos las cámaras de seguridad, que enfocan tanto la puerta de acceso al servidor, como el interior del mismo, de las cuales tras su visionado y posterior copia para adjuntar como prueba, que ninguna otra persona ha accedido al servidor y que el/los responsable/s no ha/n utilizado ningún dispositivo externo para la extracción de la información.

Con esto descartaríamos la fuga de información desde las sedes y por lo tanto…

- **solo nos quedarían las comunicaciones.**

La parte demandada alegaría:

- El algoritmo cuántico se basa, en que emisor y receptor no pueden acordar de antemano qué bases utilizar para enviar cada fotón, ya que

nos encontraríamos con el problema de cómo hacerse llegar mutuamente de forma segura esa lista de bases, volviendo al inicio del problema.

- Por lo tanto, la base de polarización se envía por cualquier otro canal inseguro, indicando qué base de polarización utilizó para cada fotón, sin desvelar la polarización concreta. Esto produce que tras eliminar los bits con bases erróneas, queda una secuencia del 50% menor de la original, que constituye la clave de una cinta aleatoria 100% segura.
- Para detectar que la transmisión no ha sido interceptada (mediante filtros), se basa en que cuando la polarización de un fotón se mide con un detector equivocado, la altera, produciendo que el receptor reciba una secuencia menor al 50%, y por lo tanto sabrían que el canal es inseguro o ruidoso descartando la clave.

Lo anterior se basa en tres principios (Criptografía Cuántica):

1. Teorema de "no clonación" que nos asegura que un estado cuántico determinado no puede ser copiado. De forma coloquial, podemos decir que un texto cuántico no puede ser "fotocopiado", ya que no existe la "fotocopiadora" cuántica, al menos en teoría.

2. Cualquier intento de obtener toda la información cuántica de un *qbit* puede implicar una cierta modificación del mismo, o destrucción de la información que porta. Por lo que no se puede obtener información sin modificación de los datos transmitidos.

3. Las medidas cuánticas son irreversibles. Después de realizar una medida, el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido y ese proceso es irreversible, es decir, no se puede volver el sistema manipulado al estado que tenía antes de la medición. Es decir, en este caso, un hacker siempre dejaría rastro, no pudiendo ocultarse.

La robustez de las declaraciones de la parte demandada, son evidentes y solo con argumentos científicos pueden ponerse en entredicho.

- **Los argumentos científicos para desmontar a la parte demandada**

> *El perito ha de **fijar los hechos de los que parte**, describiendo la **fuente de conocimiento usada***
> *Estos hechos pueden ser objeto de comprobación por otros medios probatorios*

El Perito de la parte demandante, podría argumentar:

- La primera duda y la primera alerta de que las cosas podían cambiar, vino de la mano del Prof. Lucena que hacía referencia a la posibilidad de atacar el teorema de "*no clonación*" a partir de los avances en "teleclonación cuántica" logrados por científicos de la

Universidad de Tokio, la Agencia de Tecnología y Científica de Japón y la Universidad de York.

- Para lograr esta iniciativa, se usa el entrelazamiento múltiple, basado en "*estados gráficos*", algo en lo que se está avanzando mucho últimamente, y que ha servido para demostrar la paradoja del "Gato de Schrödinger". Todavía es pronto para decir que la teleclonación es un riesgo para la criptografía cuántica, ya que la precisión de la "copia" de los parámetros cuánticos, es de solamente un 58%.
- Se estima que el máximo teórico, por culpa del principio de incertidumbre de Heisenberg, será del 66%, algo a tener en cuenta. No obstante, tener el 66% de la clave, o del mensaje, puede ser muy significativo en algunos casos.

> *El Juez aplicará la **libre valoración**, que significa que aplicara las reglas de la **sana crítica** (criterios lógicos y máximas de la experiencia)*
> *En la pericial, el perito aporta al Juez **las máximas de la experiencia de un sector de la técnica** de las que carece el Juez*

➢ **Las conclusiones:**

- Todo lo que se ha comentado sobre la seguridad de los sistemas cuánticos es cierto, pero solo y exclusivamente, si el emisor envía por el canal cuántico un único fotón por cada *qbit* de información.
- Para lograrlo, el tamaño de la superficie de emisión de fotones del emisor, debe ser lo suficientemente pequeña, como para que solamente haya un electrón con el nivel energético adecuado.
- En teoría, esto se estaba logrando, pero se ha descubierto que eso no siempre es así, ya que en los sistemas existentes en la actualidad, la distancia máxima es de 100 millas aproximadamente. Así, que se necesitaría un repetidor para poder enviar la señal a grandes distancia, estando expuestos a los ataques man-in-the-middle.
- Cuando se aumenta la energía en el transmisor, para subir la velocidad de transmisión, o para aumentar la distancia del vano, científicos del *Toshiba Research Europe* han descubierto que los emisores cuánticos actuales emiten dos o más fotones idénticos por cada *qbit*.
- Esto es un **grave problema**, ya que en estas condiciones se puede recuperar el 100% de la clave usando uno de los fotones extra, **sin que seamos detectados por el sistema**. Esto se denomina "*Pulse Spliting*".

> *El perito establecerá las conclusiones sobre su pericia*
> *El Juez puede valorar estas conclusiones, atendiendo a razones objetivas que se lleven a la motivación de la sentencia (especialmente si existen varios dictámenes)*

*Las conclusiones, pueden tener un carácter **absoluto**, **probabilístico** o **posibilístico.***
*Hay que intentar en la medida de lo posible, que estas sean de carácter **absoluto**, facilitando al Juez la motivación de la sentencia*

- El **remate**

Es evidente que el problema no está en los principios cuánticos, está en la dificultad técnica para crear un emisor de fotones adecuado, algo circunstancial, pero que pone en tela de juicio la seguridad de esta novedosa tecnología de cifrado, al menos, temporalmente.

"Dicen que los pesimistas ven el vaso medio vacío; los optimistas, en cambio, lo ven medio lleno. Los ingenieros, por supuesto, ven que el vaso es el doble de grande de lo que sería necesario"
-- Bob Lewis

Algunos textos de este trabajo están basados en materiales previos, normalmente de los propios autores, en algunos casos de terceras personas (utilizados por la licencia de GNU Free Documentation License). Entre ellos podemos mencionar los siguientes (a riesgo de olvidar alguno importante):

Existen algunos fragmentos de Fundación Wikimedia, Inc., Lewis Page, Yaiza Martínez

El artículo "Demonstration of quantum telecloning of optical coherent states" ("Demostración de teleclonación de estados ópticos coherentes") se publicó en el número del 17 de Febrero de la publicación científica Physical Review Letters. La lista de autores completa es: S.Koike, H.Takahashi, H.Yonezawa, N.Takei, Prof. S.L.Braunstein, T.Aoki y Prof. A.Furusawa

El Autor D. Ricardo R. Jorge Rodríguez es Ingeniero Técnico en Informática de Sistemas, Máster Universitario en Software Libre, Perito en informática e Informática Forense, Autor de la publicación Desarrollo del proyecto de la red telemática ISBN 978-84-16207-58-9, Vice-Decano del Colegio Oficial de Ingenieros Técnicos en Informática de la Comunidad Valenciana. Es miembro de la Asociación de Titulados en Ingeniería en Informática (ALI), miembro de la Asamblea General del CONCITI.