NOTA DE PRENSA
PRESS RELEASE

TELEFÓNICA, HUAWEI Y LA UNIVERSIDAD POLITÉCNICA DE MADRID REALIZAN UNA EXPERIENCIA PIONERA A NIVEL MUNDIAL DE APLICACIÓN DE CRIPTOGRAFÍA CUÁNTICA EN REDES ÓPTICAS COMERCIALES PARA COMUNICACIONES SEGURAS

Madrid, 14 junio de 2018.- Telefónica, Huawei y la Universidad Politécnica de Madrid (UPM) han realizado una experiencia pionera a nivel mundial, demostrando la aplicación de criptografía cuántica en redes ópticas comerciales y su integración con la operación de la red por medio de tecnologías basadas en SDN (*Software Defined Networking*).

Es una prueba piloto de investigación avanzada de servicios de comunicación seguros basados en tecnología cuántica que Telefónica podrá proporcionar a sus clientes en el futuro. Tal y como afirma el **prestigioso físico, experto en computación cuántica y miembro del Consejo de Administración de Telefónica**, **Juan Ignacio Cirac**: "*Podemos hacer que la misma secuencia de números aleatorios aparezca simultáneamente en dos lugares separados, sin pasar por el medio. Es como si fuese magia, pero es algo que la física cuántica predice. Es una manera de intercambiar claves seguras de la que tenemos que sacar el máximo provecho, ya que no puede ser espiada.*"

Todas las comunicaciones seguras se basan en el uso de la criptografía, de manera que la información se cifra utilizando una clave que permite que sólo los participantes que la conocen sean capaces de descifrar los mensajes intercambiados entre ellos. Las técnicas actuales de criptografía están basadas en problemas matemáticos que son complejos de resolver. A medida que la capacidad de computación crece, el tiempo de resolución de estos problemas, y por tanto la seguridad de las claves, disminuye.

El tamaño de las claves y la complejidad de los algoritmos de encriptación han tenido que aumentar a medida que la capacidad de cálculo iba creciendo. Y estas técnicas pueden quedar completamente obsoletas con la aparición de los *ordenadores cuánticos*, capaces de aplicar los principios de la Mecánica Cuántica para la resolución de problemas actualmente insolubles, incluyendo el romper las claves generadas por los métodos actuales de criptografía, haciendo inútiles la mayoría de las infraestructuras de seguridad en las comunicaciones.

Como **Diego R. Lopez, gerente de Exploración Tecnológica y Estándares de Global CTIO,** explica: *"En Telefónica hemos estado trabajando para desarrollar una experiencia piloto que demuestra la provisión de servicios de comunicación segura basados en criptografía cuántica sobre redes ópticas comerciales gestionadas por tecnología SDN*".

Precisamente en las tecnologías cuánticas hay una solución a esta cuestión de la vulnerabilidad de los métodos actuales. Es posible aplicar principios cuánticos para intercambiar una clave entre los extremos de un canal de comunicaciones, de manera

que esa clave sea segura frente a cualquier ataque e incluso que cualquier intento de ataque sea inmediatamente detectado. Esta técnica, conocida como Distribución Cuántica de Claves (QKD, por el término *Quantum Key Distribution*) no es sólo una solución al problema de la amenaza que supone la computación cuántica para los algoritmos criptográficos en uso, sino que puede proporcionar un nivel de seguridad mucho más alto a cualquier intercambio de datos. QKD requiere de una infraestructura física de fibra óptica de alta calidad, y Telefónica está muy bien posicionada para poder prestar servicios basados en esta tecnología.

María Antonia Crespo, directora de Conectividad y Transporte IP de Telefónica de España señala: *"La red óptica de Telefónica de España, en combinación con nuestros sistemas de transmisiones ópticas de alta capacidad, ofrecen el rendimiento necesario para proveer comunicaciones seguras basadas en comunicaciones cuánticas. Este incremento en la seguridad es clave para la nueva generación de redes flexibles, virtualizadas y definidas por software".*

La viabilidad de QKD ha sido demostrada hasta ahora en laboratorios y en pruebas de campo controladas (como la que Telefónica y UPM realizaron en 2009, intercambiando claves a través de un anillo metropolitano de fibra), pero siempre ha habido problemas para poder desplegarla sobre infraestructuras comerciales y para su integración con los mecanismos de operación de estas infraestructuras. El despliegue sobre una infraestructura de comunicaciones en producción y usando sistemas de telecomunicaciones estándar es la primera de su clase, demostrando la capacidad de la tecnología para su uso en el mundo real.

"*La capacidad de usar nuevas tecnologías como SDN, diseñadas para incrementar la flexibilidad de la red, junto con nuevas tecnologías de QKD es lo que nos permite hacer converger las redes clásicas y cuánticas en la infraestructura de fibra óptica existente. Ahora tenemos, por primera vez, la capacidad de desplegar comunicaciones cuánticas de una manera incremental, sin grandes costes de inversión inicial y usando la misma infraestructura*", señala **Vicente Martín, director del Centro de Simulación Computacional, responsable del equipo de la UPM**.

La experiencia piloto utiliza una nueva tecnología para QKD basada en "variables continuas" (CV según el acrónimo del inglés *Continuous Variables*). Una característica especial de los dispositivos usados es que son muy flexibles, pudiéndose controlar completamente por software. Los sistemas están óptimamente adaptados para su integración en un entorno dinámico como el de las redes de nueva generación basados en SDN y virtualización de funciones red (NFV – *Network Function Virtualization*), donde la creación y los cambios en los caminos ópticos y el necesario cifrado dejan de ser estáticos y predefinidos, realizándose mediante interfaces de control basadas en software. Estas funcionalidades se aseguran integrando dispositivos CV-QKD con dispositivos estándar de transporte óptico. La integración de QKD y SDN-NFV abre un nuevo camino para dotar de un alto nivel de seguridad a estas nuevas redes, que son infraestructuras críticas para nuestra sociedad.

Momtchil Peev, coordinador del Proyecto de Comunicaciones Cuánticas en los Laboratorios de Huawei en Munich añade: *"Los dispositivos de CV-QKD que usamos aquí presentan claras ventajas: no necesitan complejos detectores funcionando a temperatura*

ultrabaja y pueden reusar componentes de los sistemas de comunicación coherentes clásicos. En lugar de enfocarnos en conseguir nuevos record de rendimiento, nos hemos centrado en desarrollar los interfaces de control y transferencia de claves, demostrando la capacidad de una integración más transparente en las redes modernas."

En el piloto usamos una infraestructura de fibra proporcionada por Telefónica de España, conectando tres centros diferentes en el área metropolitana de Madrid, junto con equipos CV-QKD desarrollados por los Laboratorios de Investigación de Huawei en Munich en los que también han colaborado la UPM, instalados en estos centros, módulos de gestión basados en SDN desarrollados por el equipo de Innovación en Tecnologías de Red del GCTIO de Telefónica, y los mecanismos de integración de la criptografía cuántica con tecnologías SDN y NFV desarrollados por la UPM. La integración de todos estos elementos nos permite demostrar el uso de técnicas QKD en un entorno de producción real, combinando la transmisión de datos y de claves cuánticas sobre la misma fibra, a la vez que demostramos cómo puede llevarse a cabo la gestión de estos servicios, y su uso por diferentes aplicaciones. La instalación sobre una infraestructura en producción y usando sistemas de comunicaciones estándar destaca la madurez de la tecnología.

Acerca de Telefónica

Telefónica es una de las mayores compañías de telecomunicaciones del mundo por capitalización bursátil y número de clientes, que se apoya en una oferta integral y en la calidad de la conectividad que le proporcionan las mejores redes fijas, móviles y de banda ancha. Es una empresa en crecimiento que ofrece una experiencia diferencial, basada tanto en los valores de la propia compañía como en un posicionamiento público que defiende los intereses del cliente.

Presente en 17 países y con 350 millones de accesos, Telefónica tiene una fuerte presencia en España, Europa y Latinoamérica, donde concentra la mayor parte de su estrategia de crecimiento.

Telefónica es una empresa totalmente privada que cuenta con más de 1,5 millones de accionistas directos. Sus acciones cotizan en el mercado continuo de las bolsas españolas y en las bolsas de Londres, Nueva York, Lima y Buenos Aires.

http://www.telefonica.com

Sobre Huawei

Huawei es proveedor líder global de soluciones de Tecnologías de la Información y Comunicación (TIC), infraestructuras y dispositivos inteligentes. Con soluciones integradas en cuatro entornos clave: redes de telecomunicaciones, TI, dispositivos inteligentes y servicios en la nube, nos comprometemos a llevar la digitalización a cada persona, hogar y organización para lograr un mundo totalmente conectado e inteligente.

El catálogo completo de productos, soluciones y servicios de Huawei es competitivo y seguro. A través de la colaboración con los socios del ecosistema, creamos un valor añadido para nuestros clientes y trabajamos para empoderar a las personas, enriquecer la vida en los hogares e inspirar la innovación en organizaciones de todo tipo.

En Huawei, la innovación se centra en las necesidades del cliente. Invertimos fuertemente en investigación, centrándonos en los avances tecnológicos que impulsan el avance del mundo. En la actualidad somos más de 180.000 empleados y operamos en más de 170 países y regiones. Fundada en 1987, Huawei es una empresa privada totalmente propiedad de sus empleados.

Para más información, visite Huawei online. Síganos en Twitter, Linkedin, Facebook, YouTube e Instagram.

Acerca de la UPM

El Grupo de Investigación en Información y Computación Cuántica (GCC) de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid pertenece al Center for Computational Simulation, que agrupa cerca de 100 investigadores en el área de la Ciencia Computacional pertenecientes a tres universidades de Madrid. El GCC está formado por investigadores, principalmente profesores de universidad, expertos en las áreas de matemática aplicada, física cuántica, redes y ciencias de la computación, entre otras. Tiene amplia experiencia en la distribución cuántica de claves y en la integración de comunicaciones cuánticas en redes de comunicaciones. La Escuela Técnica superior de Ingenieros Informáticos ha sido reconocida varias veces como la mejor en Estudios Informáticos del país en rankings nacionales e internacionales y atiende a más de 1700 estudiantes. La Universidad Politécnica de Madrid es la mayor Universidad Técnica de España, con dos Campus de Excelencia Internacional es una de las universidades españolas con mayor actividad investigadora y la primera en la obtención de recursos externos en proyectos competitivos. Con 35.000 estudiantes imparte cerca de 200 titulaciones entre grados, máster y programas de doctorado.

www.gcc.fi.upm.es
www.ccs.upm.es
www.etsiinf.upm.es
www.upm.es