www.premiosfronterasdelconocimiento.es

Discurso de aceptación

18 de junio de 2026

Vincent Rijmen, galardonado en la categoría de Tecnologías de la Información y la Comunicación (XVIII edición)

En primer lugar, me gustaría dar las gracias a la Fundación BBVA por haber creado este premio y concederlo cada año. En segundo lugar, agradezco al jurado que nos haya otorgado este premio a mi colega Joan Daemen y a mí. En una época en la que las corazonadas y las falsas apariencias muchas veces parecen tener más peso que las opiniones de los expertos, un reconocimiento como este cobra el doble de importancia.

La criptología es una rama de la ciencia que cuenta con una historia larga y gloriosa, aunque a menudo también trágica, vinculada principalmente a la diplomacia y al ámbito militar, por lo que siempre ha estado rodeada de secretismo, y en particular, en la órbita de los servicios secretos. Hasta los años ochenta, e incluso los noventa, cuando comencé mi trayectoria académica, no eran raros los proyectos de investigación abierta sobre criptología que se interrumpían o cuyo inicio se prohibía al considerarse que los ciudadanos observantes de la ley no tenían necesidad de ellos.

Esta situación cambió con la llegada de Internet, cuando los pagos en línea y servicios como la administración electrónica, pero también las redes sociales, aumentaron drásticamente la importancia de disponer de comunicaciones seguras con fines puramente civiles. Más tarde llegaron los teléfonos móviles y otras formas de comunicación inalámbrica, en las que las escuchas e interferencias son tan fáciles que incluso pueden producirse de forma accidental. De hecho, en la sociedad moderna, nos hemos vuelto muy dependientes de la transmisión segura de datos y de los comandos remotos. Pensemos en los sistemas inteligentes de distribución de energía, en los que ciertas partes de la red se reconfiguran continuamente en función del aumento o la disminución de la producción de energía verde y de las variaciones en la demanda. Sin ciberseguridad, sería posible colapsar la red eléctrica desde un

ordenador remoto. Hay muchos otros ejemplos de infraestructuras civiles críticas que deben protegerse contra los ciberataques.

En entornos abiertos en los que los productos de distintos proveedores deben poder integrarse y donde cualquiera tiene acceso a los productos y puede inspeccionar su funcionamiento interno, es imposible alcanzar una seguridad sólida basándola en los secretos comerciales. Por tanto, el principal instrumento de protección contra los ciberataques y las amenazas a la privacidad ha de ser la criptología. Esta constatación ha impulsado el uso y la necesidad de estándares abiertos en los métodos criptográficos, así como la investigación abierta sobre criptología y sistemas de ciberseguridad.

La criptología abarca tanto la creación de algoritmos como la evaluación de su seguridad. Puede que la gente se pregunte por qué resulta tan difícil diseñar sistemas seguros y por qué los criptógrafos no desarrollan de una vez por todas un estándar que pueda utilizarse para siempre. Esto se debe a que las evaluaciones de seguridad, o comprobaciones de seguridad, al igual que las demostraciones matemáticas, parten de unos supuestos básicos. En el caso de la criptología, entre ellos hay supuestos sobre las acciones que un ciberatacante podría llevar a cabo. Lamentablemente, resulta muy difícil predecir por completo el comportamiento, el ingenio y la motivación de los ciberatacantes. De ahí que el progreso en nuestro campo se caracterice por la intensa interacción entre un diseño muy resistente y una evaluación de seguridad rigurosa.

Otra cuestión igual de importante es la facilidad de uso de los sistemas de seguridad. Los usuarios tienen poca paciencia con los programas de cifrado lentos o complicados, o que obligan a memorizar contraseñas largas e impredecibles. Si bien no es tan difícil diseñar sistemas seguros o muy rápidos, sigue siendo muy difícil diseñar sistemas que sean seguros, rápidos y fáciles de usar.

Para conseguir un sistema de seguridad eficaz, tanto el diseño como el análisis deben basarse en el análisis asistido por ordenador, la estadística y las matemáticas avanzadas: se requiere paciencia y perseverancia por parte de los investigadores, pero también la confianza y el apoyo de organismos públicos de investigación o de organizaciones privadas, como por ejemplo las ayudas del Programa Fundamentos que concede la Fundación BBVA.

Desde mediados de la década de los setenta, la investigación abierta en este ámbito ha florecido y ha dado lugar a numerosos algoritmos criptográficos. Sin embargo, la mayoría son descifrados al poco de publicarse, porque los diseñadores suelen tener una visión demasiado optimista de su propia creación y tienden a no ver sus posibles puntos débiles. Por tanto, la confianza en un sistema criptográfico se basa necesariamente en la investigación abierta y el escrutinio público recíproco de los diseños de cada uno. Durante el desarrollo del Estándar de Cifrado Avanzado (AES), hemos estudiado muchos otros diseños, hemos inventado nuevos mecanismos y los hemos vuelto a descartar para sustituirlos por otras ideas.

Hoy en día, el AES se utiliza para proteger sitios web, pagos electrónicos, discos duros, teléfonos móviles, hogares inteligentes y muchos otros sistemas

de la vida cotidiana. Es más, en aplicaciones como los sistemas de navegación similares al GPS para coches, barcos y aviones, los sistemas civiles más modernos utilizan el AES, y su rendimiento es superior al de muchos sistemas de grado militar: lo considero un triunfo de la investigación abierta.

La investigación abierta, las pruebas minuciosas y el apoyo público mantienen a salvo nuestras vidas digitales; gracias por ayudar a hacerlo posible.