CSIC
Consejo Superior de Investigaciones Científicas

Nota de prensa

CSIC comunicación
Tel.: 91 568 14 77
g.prensa@csic.es
www.csic.es

Sevilla, jueves 25 de marzo de 2021

CSIC lidera un proyecto para aumentar la seguridad de los dispositivos digitales sin almacenar las claves

- **El proyecto Spirs, dotado con 5 millones de euros, propone un sistema que regenera las claves sin necesidad de guardarlas y contribuye a la seguridad integral del sistema**

- **Liderado desde el Instituto de Microelectrónica de Sevilla, también participa el Instituto de Tecnologías Físicas y de la Información 'Leonardo Torres Quevedo'**

El Consejo Superior de Investigaciones Científicas (CSIC) liderará, a través del Instituto de Microeletrónica de Sevilla (IMSE), centro mixto del CSIC y la Universidad de Sevilla, el proyecto europeo ***Security Platform for ICT System Rooted at the Silicon Manufacturing Process*** **(Spirs)**, dotado con cinco millones de euros y cuya duración será de tres años. Esta iniciativa, enmarcada dentro del programa marco Horizonte 2020 de la Unión Europea, permitirá el aumento de la seguridad en la conexión de dispositivos electrónicos a una red, de forma que el intercambio de información con la red se realice de modo seguro y preservando la privacidad de aquellos datos de contenido sensible. En el proyecto también participa el Instituto de Tecnologías Físicas y de la Información Leonardo Torres Quevedo del CSIC.

"La seguridad nace en el propio dispositivo a partir de lo que denominamos **raíz de confianza**. Este elemento es donde se basa la seguridad de todo el dispositivo electrónico. Normalmente los sistemas electrónicos han basado la confianza en claves criptográficas que suelen ser almacenadas en memorias no volátiles. Esto tiene una serie de problemas asociados porque un ataque a la memoria compromete la seguridad de todo el sistema", explica la investigadora del CSIC y directora del proyecto **Piedad Brox**, del **Instituto de Microelectrónica de Sevilla**.

Este enfoque cambia en Spirs porque se va a diseñar e implementar una raíz de confianza que se basa en una función física no clonable que prescinde de la memoria para el almacenamiento de claves. Esa función física no clonable permite extraer un identificador digital único asociado al dispositivo electrónico en el que se integra, su *huella dactilar*. Su respuesta es única, reproducible e impredecible de manera que dos

circuitos integrados diseñados exactamente de la misma manera y que han sido implementados en la misma tecnología generan respuestas totalmente distintas.

Este sistema puede usarse para la reconstrucción de claves criptográficas sin que sea necesario el almacenamiento de la clave. “Y esto es fundamental, ya que, si la clave no se almacena en memoria, sino que se regenera tantas veces como sea necesario, se añade un plus a la seguridad integral del sistema. De esta forma, si una información no está almacenada es más complicado que pueda ser adquirida a través de un ciberataque”, añade Piedad Brox.

“La pandemia ha precitado el uso de tecnología digital y Spirs nos ayudará a proteger la seguridad de nuestros dispositivos electrónicos ante amenazas cibernéticas”, concluye la investigadora del CSIC.

Erika López Palma / CSIC Comunicación Andalucía y Extremadura