CSIC
Consejo Superior de Investigaciones Científicas

Nota de prensa

CSIC comunicación
Tel.: +34 91 568 14 77 / 618 40 95 65
comunicacion@csic.es
www.csic.es

Madrid, jueves 11 de noviembre de 2021

Un proyecto del CSIC desarrollará tecnologías de identificadores seguros para dispositivos digitales

- **Recibe 5 millones de la UE para mejorar la ciberseguridad en las comunicaciones de la internet de las cosas, la industria 4.0, la telemedicina y la teleasistencia**

El proyecto Spirs mejorará la seguridad de los dispositivos digitales. / Adobe

Un equipo de investigadores del CSIC ha recibido 5 millones de la UE para desarrollar identificadores que mejoren la seguridad de los dispositivos digitales. El equipo, formado por investigadores del Instituto de Microelectrónica de Sevilla (IMSE) y el Instituto de Tecnologías Físicas y de la Información (ITEFI), desarrollará tecnología software y hardware para mejorar la ciberseguridad de los dispositivos integrados en la internet de las cosas (IoT), en la autenticación de dispositivos en la industria 4.0 (el proceso de automatización de la producción industrial mediante nuevas tecnologías de comunicación) y contribuirá e mejorar la telemedicina y la teleasistencia.

El proyecto, denominado Spirs (Secure platform for ICT systems rooted at the silicon manufacturing process), tiene el objetivo de generar tecnología robusta y segura para la creación, gestión, uso y eliminación de identificadores digitales. “Un identificador digital

es la información que nos permite mostrar a un sistema de información o a un servicio de internet que somos un cierto usuario, entidad u objeto", explica **David Arroyo**, investigador del CSIC en el ITEFI. "Ese identificador puede ser un nombre de usuario, de entidad o de objeto, o una cadena alfanumérica -por ejemplo, 02189aBDEFadf111-, que se muestra al sistema o servicio para poder iniciar el proceso de autenticación o validación necesario para empezar a usar dicho sistema o servicio", añade.

También es posible que el identificador sea una secuencia de bits generada mediante un dispositivo, de forma que dicho dispositivo se emplea por parte del usuario, entidad u objeto para presentarse al sistema de información o al servicio de internet. Una plantilla biométrica (representación digital de información relacionada con una muestra biométrica), como es el caso de plantillas vinculadas a huellas digitales, puede ser utilizado como identificador digital.

"El proyecto tiene un enfoque integral: abarca la generación de identificadores a nivel de hardware, su despliegue a través de computación segura de código abierto, y su utilización para que garantice la privacidad de los usuarios finales", añade **Arroyo**.

Cuatro niveles de seguridad

La finalidad de esta nueva tecnología es proteger el ciclo de vida de los identificadores digitales (su generación, uso, supervisión y eliminación) a tres niveles principales que reforzarán la seguridad de la arquitectura de un procesador denominado RISC-V. Este tipo de procesador es de código abierto, y se encuadra dentro de la iniciativa europea para desarrollar chips propios (EIP, European Processor Initiative).

Un primer nivel parte de la llamada *raíz de confianza del silicio*. "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", indica la investigadora del CSIC y directora del proyecto **Piedad Brox**, del Instituto de Microelectrónica de Sevilla. **"**Normalmente los sistemas electrónicos han basado la confianza en claves criptográficas que suelen ser almacenadas en memorias no volátiles (un tipo de memoria que retiene los datos almacenados después de apagar la alimentación). Esto tiene una serie de problemas asociados porque un ataque a la memoria compromete la seguridad de todo el sistema", añade.

Este enfoque cambia en el proyecto Spirs, explica **Brox**, 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", precisa la investigadora.

"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 la clave no se almacena en memoria, sino que se regenera tantas veces como sea necesario, de

manera que 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**.

"Para ello, el proyecto se centrará en el desarrollo de tales identificadores en el nivel físico (hardware), aprovechando propiedades físicas no reproducibles o PUF, del inglés Physical Unclonable Function", indica **Arroyo**. Los PUF pueden ser considerados como huellas digitales de un cierto objeto físico, y por ello pueden emplearse como mecanismos para evaluar la fiabilidad de un dispositivo final. Ese dispositivo final, a su vez, puede servir de validación o autenticación de la persona que lo porte.

En un segundo nivel, el proyecto generará procedimientos de verificación remota de dispositivos. Tales procedimientos estarán apoyados en una capa de cómputo seguro o TEE (del inglés, Trusted Executed Environment; la parte de los sistemas de computación encargada de garantizar que el código software se ejecuta de modo adecuado y fiable) construida sobre un procesador de tipo RISC-V. Sobre esa capa de cómputo TEE, se diseñarán e implementarán protocolos de verificación remota (procedimientos para verificar que el dispositivo o sistema de información al que nos estamos conectando es fiable y está realizando las operaciones que le solicitamos de modo adecuado) para garantizar que las operaciones de tratamiento e intercambio de información son fiables.

En un tercer nivel, y en consonancia con las exigencias y recomendaciones de la Comisión Europea en materia de derecho digital, el proyecto proporcionará una capa de protección de la privacidad para la generación de identidades funcionales (mecanismos criptográficos para mostrar propiedades concretas -por ejemplo, edad o franja de edad- de nuestra identidad digital sin necesidad de enseñar la descripción completa de dicha identidad) con el criterio de mínima explotación de datos personales.

Por último, en un cuarto nivel, el proyecto contempla el uso de tecnología *blockchain* para la supervisión y gestión de la seguridad de identidades digitales a lo largo de su ciclo de vida.

Tecnología para el reglamento europeo eIDAS

Los resultados de Spirs pueden contribuir a desplegar de forma robusta y fiable los procedimientos de autenticación de usuarios y entidades estipulados por el reglamento europeo de identidad digital, eIDAS (Electronic IDentification, Authentication and trust Services). "En estos momentos eIDAS está siendo modificado para dar cabida al nuevo paradigma SSI (Self Soverign Identity) de identidad digital. La raíz de confianza de silicio y su uso a lo largo de la pila de protocolos de los sistemas de información requiere mecanismos seguros y robustos. SPIRS proporcionará tales mecanismos", explica Arroyo.

La capa de protección de privacidad del proyecto Spirs también contribuirá a generar procedimientos criptográficos compatibles con el Reglamento General de Protección de Datos y con los requisitos del paradigma SSI adoptado por la Comisión Europea a través del marco ESSIF (European Self Sovereign Identity Framework).

El proyecto Spirs contribuirá a la generación de protocolos de blockchain para la identificación y tratamiento de amenazas en el ciclo de vida de identificadores digitales, poniendo especial atención en la atestación remota y los procedimientos de anclaje de confianza.

CSIC Comunicación

El proyecto Spirs contribuirá a la generación de protocolos de blockchain para la identificación y tratamiento de amenazas en el ciclo de vida de identificadores digitales, poniendo especial atención en la atestación remota y los procedimientos de anclaje de confianza.