TESTIGO DIGITAL: GESTIÓN SEGURA DE LA INFORMACIÓN EN DISPOSITIVOS ELECTRÓNICOS

En un mundo en el que los usuarios dependen cada vez más de sus dispositivos, éstos almacenan gran cantidad de información y son una fuente muy valiosa de conocimiento sobre su entorno. Sin embargo, la heterogeneidad y la densidad de los objetos conectados, características propias de la Internet de las Cosas (IoT), sirven de velo para ocultar conductas maliciosas que afectan a estos dispositivos, sin que quede rastro de tales acciones. El uso de arquitecturas de seguridad embebidas en los dispositivos móviles y otros objetos de uso personal está por debajo de su potencial. Actualmente el propósito de estas arquitecturas es o bien proteger los datos del usuario o facilitar el pago electrónico. Avances recientes permiten la firma a través del móvil empleando la última versión de DNIe que incorpora NFC. Sin embargo, estas arquitecturas pueden ofrecer mucho más. La tecnología objeto de patente desarrollada define el concepto y arquitectura del testigo digital, la cual permite que dispositivos personales y otros dispositivos con arquitecturas de seguridad embebidas puedan colaborar entre sí para alertar de conductas maliciosas y dejar constancia de éstas. Esta arquitectura hace posible la implementación de una cadena de custodia digital en la IoT.

Ventajas competitivas: Algunas ventajas que aporta un testigo digital frente a lo ya existente se enumeran a continuación: - Identidad vinculante entre dispositivos y usuarios, en objetos que utilicen la arquitectura de seguridad descrita en la patente. - Adaptación necesaria de la gestión de evidencias electrónicas a la IoT. - No-repudio en terminales móviles y otros objetos restringidos en recursos. - Delegación vinculante basada en roles. El envío de la evidencia electrónica aprovecha las ventajas de conectividad de la IoT. - El testigo digital ayudará a detectar los ataques desde su origen y a establecer responsabilidades. - Agrega una nueva funcionalidad al uso de dispositivos personales. - Clarifica los requisitos arquitecturales necesarios para mejorar las prestaciones de seguridad de un dispositivo personal u otros objetos de la IoT.

Usos y aplicaciones: Esta tecnología queda enmarcada en el sector de las TICs aplicada a la Seguridad de la Información. La aplicación más directa es la detección temprana de ataques que emplean objetos que cuenten con la tecnología descrita en la patente, y su uso más directo e implementación más simple podría recaer en objetos empleados por los cuerpos de seguridad del estado (desde terminales móviles hasta coches patrulla con ordenador de a bordo y TPM). Los usuarios con esta tecnología podrían denunciar actos cibernéticos ayudándose del testigo digital para reportar las evidencias electrónicas a las autoridades. Cabe destacar que, además, se puede aplicar en objetos de la IoT con pocos recursos computacionales. Este tipo de dispositivos pueden ser desde sensores industriales hasta wearables, siempre y cuando implementen los componentes de la arquitectura descrita en la patente.

Etiquetas: evidencias, IoT, anti-tampering, arquitectura de seguridad, seguridad de la información, elemento seguro

Sectores : TIC, Seguridad, Protección y Defensa

Áreas : Telecomunicaciones, Hardware / Dispositivos / Componentes, Internet y Redes, Seguridad y Protección

Número de publicación patente: ES2587584, WO2017068222

Titulares: Universidad de Málaga

Inventores: Ana Nieto Jiménez, Rodrigo Román Castro, Francisco Javier Lopez Muñoz

Fecha de prioridad: 22/octubre/2015

Nivel de protección: Mundial (países PCT)

Estado de tramitación: Solicitud de protección a nivel mundial (paises PCT)