A. Nieto, R. Roman, and J. Lopez, "Testificación Digital", *Revista SIC*, vol. 122, pp. 94-98, 2016.
NICS Lab. Publications: https://www.nics.uma.es/publications

Testificación digital

Ana Nieto, Rodrigo Román, y Javier López
Departamento de Lenguajes y Ciencias de la Computación (LCC), Universidad de Málaga
Edificio Ada Byron, Universidad de Málaga, 29071 Málaga (España)
{nieto, roman, jlm}@lcc.uma.es

Resumen. El creciente número de dispositivos interconectados trae consigo problemas de seguridad bien conocidos; por ejemplo, aquellos debidos a las vulnerabilidades en protocolos muy diversos – muchos de ellos propietarios - y al factor de error humano introducido por los usuarios. Sin embargo, cabe preguntarse cómo podemos usar el despliegue de tales dispositivos en beneficio de la ciberseguridad. En el proyecto IoTest se está desarrollando una solución, el *Testigo Digital*, que permitirá a los dispositivos personales con arquitectura de seguridad embebida reaccionar ante ataques virtuales, protegiéndonos de los ciberataques emergentes.

La explosión de lo impredecible

Diversos paradigmas como Internet of Things (IoT), Internet of Everything (IoE) o el Internet of You (IoY), representan lo mismo: interconexión masiva de objetos heterogéneos (en torno a los 6.5 billones en 2016[1]) bajo un marco común cooperativo, en el que el usuario se ve inevitablemente involucrado. En estos paradigmas, los dispositivos personales (p.ej. teléfonos móviles, *wearables*) alcanzan su mayor auge dado que se convierten en los interfaces entre el usuario y el mundo virtual. Son, además, un poderoso vehículo de mercado, mejorando la experiencia de clientes e incrementando la productividad de empleados.

Por otro lado, la inclusión de los dispositivos personales en entornos empresariales supone un claro riesgo para la seguridad de las organizaciones. Enfoques como BYOD (Bring Your Own Device), que abrazan esta inevitable simbiosis, aplican políticas de seguridad preventivas que continúan siendo insuficientes contra los ataques más sofisticados. Sin ir más lejos, en los últimos años, los *Advanced Persistent Threats* (APTs) han revelado lo expuestas que están las infraestructuras – incluyendo infraestructuras críticas- y sus usuarios, así como lo relativamente fácil que es obtener información sin coste alguno para el atacante, que elimina su rastro eficazmente.

Resulta muy paradójico que aunque las medidas de seguridad en estos dispositivos se vean reforzadas cada año (p.ej. arquitecturas de seguridad empotradas, mecanismos de privacidad y biométricos para la autenticación del usuario, pago electrónico), la explosión de dispositivos siga siendo un problema destacado, en lugar de jugar a favor de la seguridad.

[1] http://www.gartner.com/newsroom/id/3165317

Podría deducirse que, mientras que los atacantes han sabido adaptarse perfectamente al contexto del "*todo"*, no está ocurriendo lo mismo con la seguridad, y este es el verdadero problema. Aunque seguirán existiendo problemas de seguridad difícilmente resolubles en este contexto (p.ej. vulnerabilidades software, equipos desactualizados y desfasados), lo cierto es que no estamos aprovechando todo el potencial de los avances en seguridad. Por ejemplo, los dispositivos de usuario son meros contenedores de evidencias electrónicas, analizadas una vez que el ciberataque ha tenido lugar (ENISA, 2016 [3]). Sin embargo, ha llegado el momento de plantearse si la tecnología de seguridad en las plataformas móviles – y en otros objetos - tiene el grado de madurez suficiente como para ir un paso más allá [1].

Precisamente, el Proyecto IoTest[2] surge con el objetivo de fomentar el desarrollo de una solución de seguridad que permita a los dispositivos personales tener la capacidad de "testificar" contra conductas en la red que afectan a su usuario, empleando para ello arquitecturas de seguridad embebidas en los objetos. Nace así concepto de *testigo digital*.

¿Qué es un *testigo digital*?

Un *testigo digital* es un dispositivo confiable capaz de obtener y salvaguardar evidencias electrónicas que afectan a su usuario o a su entorno, en base a una serie de políticas definidas por expertos y aceptadas por el usuario. Sus capacidades dependen del perfil del usuario y de los recursos de su dispositivo, ya que este concepto abarca desde wearables hasta vehículos con arquitecturas de seguridad embebida que satisfagan los requisitos para ser considerado un testigo digital.

FIGURA 1 AQUÍ

El fin perseguido es que un dispositivo pueda almacenar evidencias electrónicas de conductas ilícitas que puedan causar un perjuicio a sus usuarios. Estas evidencias se almacenarán en el dispositivo, en un espacio protegido, hasta ser delegadas a los cuerpos de seguridad con potestad para su gestión oficial, sea bajo petición explícita del usuario o de forma automática si la configuración lo permite. Además, el testigo digital permitirá recabar evidencias electrónicas de su entorno de manera eficiente, ya que es una solución que se adapta a los recursos del objeto.

Se sientan así las bases para desplegar soluciones de respuesta temprana ante amenazas basadas en los propios criterios del usuario, bajo el asesoramiento de políticas de seguridad definidas por un equipo experto. Esta medida pretende, por un lado, desmotivar a los atacantes que usan la IoT como un paraíso donde ocultar su rastro, cobijándose en la amplia red de dispositivos y, por otro lado, entrenar al usuario sobre las medidas de seguridad a su alcance.

[2] https://www.nics.uma.es/projects/iotest

La tecnología, que ya cuenta con una patente, está destinada a las administraciones, cuerpos de seguridad del estado, ciudadanos de a pie, y al sector empresarial, ya que permite definir políticas adaptadas al contexto y los intereses de los diferentes participantes.

Casos de uso

Desde un ciudadano que requiera interponer una denuncia presentando evidencias electrónicas obtenidas con su Smartphone hasta una organización que necesite establecer políticas de grano fino para los dispositivos personales dentro del entorno empresarial (p.ej. en entornos BYOD), los escenarios de aplicación de los testigos digitales son muy diversos. A grosso modo podemos agrupar los casos de uso en tres bloques: ordenanza, privado e interno-administrativo.

FIGURA 2 AQUÍ

El primer caso de uso reside en facilitar la labor de las agencias de aplicación de la ley y el orden (LEA, por sus siglas en inglés*, Legal Enforcement Agency*). Bajo esta premisa, los testigos digitales más avanzados podrán recabar información de una escena sujetos a condiciones en la búsqueda de evidencias (p.ej. eventualmente determinados por una orden judicial). Este caso de uso, al ejecutarse sobre datos *de otros* con un marcado componente judicial, tiene restricciones sujetas al marco legal vigente. Los testigos digitales evitarían la pérdida de evidencias críticas en escenarios susceptibles de modificación al actuar sobre la escena automáticamente acorde a parámetros pre-configurados por los cuerpos de seguridad.

El segundo caso de uso afecta a los usuarios directos de un dispositivo de testificación digital que quieren usar su dispositivo de forma privada, controlando el flujo de los datos en primera persona. Este caso de uso se destina a permitir que el usuario indique qué es lo que considera una ofensa y permitir la configuración de su testigo digital para identificar indicios de los hechos. El usuario posteriormente decidirá qué hacer con las evidencias digitales. Es primordial tener en cuenta que este caso de uso también puede verse afectado por los datos de otros usuarios que estén en la escena (p.ej. afectar a la privacidad de localización de terceros).

El último caso de uso va dirigido a realizar análisis internos o de tipo administrativo. Este tipo de análisis se destinaría a aclarar la fuente de un ataque cuyo origen podrá ser aclarado por los testigos digitales. Involucra datos de otros, por lo que tiene restricciones que atañen a las empresas y sus trabajadores, y las condiciones acordadas para el uso de dispositivos de la empresa o personales dentro de la organización.

Así mismo, para cada escenario, la configuración de los testigos dependerá de las características disponibles en los objetos y de los usuarios o entidades que los gestionan.

Características de un testigo digital

Desde el punto de vista tecnológico, este novedoso concepto se apoya en cuatro pilares básicos: (i) vinculación de la identidad del usuario a su dispositivo personal, (ii) núcleo de confianza y ejecución confiable para preservar la integridad, (iii) control de acceso, (iv) trazabilidad y delegación vinculante con garantías de no-repudio, para desplegar *cadenas de custodia digital* adaptadas a la IoT (CCD-IoT).

Debido al carácter crítico de la información gestionada, los testigos digitales se asocian a sus usuarios por medio de *credenciales vinculantes*, relacionando las evidencias, los dispositivos involucrados y el usuario que da fe de los hechos. Se fija así el factor de responsabilidad sobre el uso del dispositivo que actuará como testigo digital, desalentando el uso mal intencionado del mismo, y permitiendo la trazabilidad de la evidencia. Los mecanismos biométricos ya disponibles en las plataformas móviles (p.ej., huella digital) serán fundamentales en aquellos casos en los que se requiera demostrar la presencia del usuario y su autorización explícita, aportando pruebas de no-repudio.

La identidad también permite determinar la jerarquía del testigo: testigo digital básico (p.ej. para los ciudadanos de a pie) y custodio digital (p.ej. para los cuerpos de seguridad del estado). Este último, realizará operaciones más sofisticadas dependiendo de las órdenes judiciales alojadas en el dispositivo, y servirá a su vez de tercera parte confiable.

FIGURA 3 AQUÍ

El proyecto IoTest define cadenas de custodia digital adaptadas a la IoT empleando los testigos digitales como eslabones. Este tipo de cadenas de custodia difiere de otras propuestas (p.ej. véase [3]) en que varios dispositivos limitados en recursos, pertenecientes a usuarios con muy diverso perfil, pueden formar parte de ellas. Además, la decisión sobre el siguiente testigo en la cadena también estará condicionada por la probabilidad de que dicho testigo alcance antes un punto oficial de recogida de evidencias (p.ej. un vehículo previsiblemente abarcará zonas más amplias que un dispositivo personal transportado por un humano).

Una característica fundamental es que los testigos digitales emplean mecanismos de seguridad acorde a las normas para la gestión de evidencias electrónicas (p.ej. UNE 71505, ISO/IEC 27037), y definen procesos que aseguran la integridad de las evidencias recabadas. Al emplear la arquitectura de seguridad embebida en el objeto – seguridad nativa – es posible aplicar políticas de seguridad más eficientes basadas en el contexto IoT.

Cabe destacar que son precisamente estas medidas de seguridad nativas las que permiten la definición del concepto de testigo digital, ya que elevan el grado de confianza en nuestros

dispositivos más que nunca. Sin embargo, esto es al mismo tiempo un arma de doble filo, ya que los dotamos de una funcionalidad que puede llegar a ser muy polémica.

La colaboración con el usuario

La traición nunca proviene de nuestros enemigos, dice el refrán. Es uno de los motivos por los cuales gran parte de las medidas de seguridad en los dispositivos móviles se centran en proteger la privacidad de los datos del usuario. Sin embargo, son justamente esos datos los que pueden ser determinantes a la hora de demostrar que un suceso tuvo lugar.

Al igual que una agresión contra un individuo en la vía pública (p.ej. robo) puede requerir de la colaboración ciudadana para frenar o denunciar el hecho, una agresión virtual necesita que aquellos que son capaces de identificarla – nuestros dispositivos – puedan dar testimonio de esto, sin afectar dos cuestiones básicas: (1) los datos que proporciona el dispositivo no deberán delatar a su usuario, y (2) el usuario debe controlar en todo momento los datos que serán accedidos, las posibles repercusiones de compartir dichos datos y las entidades involucradas en el proceso.

Las connotaciones legales de este y otros esquemas similares en los que el usuario se verá involucrado están aún por definir. Por ejemplo, el concepto de *cadena de custodia digital* se encuentra definido en base a los mecanismos de seguridad establecidos en las normas para la gestión de evidencias electrónicas, no en base a la legalidad. El proyecto IoTest representa un salto tecnológico en este sentido, ya que adapta estas definiciones al marco de la IoT.

El propósito de las evidencias digitales es, fundamentalmente, servir de base para aclarar un conjunto de hechos. En entornos IoT esto presenta un serio desafío (véase [4]). Pero, además, las medidas adaptables al IoT, como es el caso de los testigos digitales, tiene como contra partida que requieren que el usuario acepte estos mecanismos – los cuales pueden llegar a ser, según se mire, relativamente intrusivos en su forma de vida.

Por lo tanto, el grado en el que la testificación digital pueda ser aplicada vendrá dictada principalmente por factores como el contexto IoT donde se despliegue la solución, y por lo que un usuario (ya sea un individuo o una organización) esté dispuesto a ceder en aras de su protección y la de otros.

Referencias

[1] A. Nieto, R. Roman, and J. Lopez, "Digital Witness: Safeguarding Digital Evidence by using Secure Architectures in Personal Device", *In IEEE Network*, IEEE Communications Society, In Press.
[2] European Union Agency for Network and Information Security, “ENISA Threat Landscape 2015”, 2016.

[3] Y. Prayudi, S. Azhari. “Digital chain of custody: State of the art,” *International Journal of Computer Applications*, 114 (5), 1–9, 2015.
[4] A. Kasper, E. Laurits. "Challenges in Collecting Digital Evidence: A Legal Perspective," *The Future of Law and eTechnologies*, 195–233, 2016.

Figuras

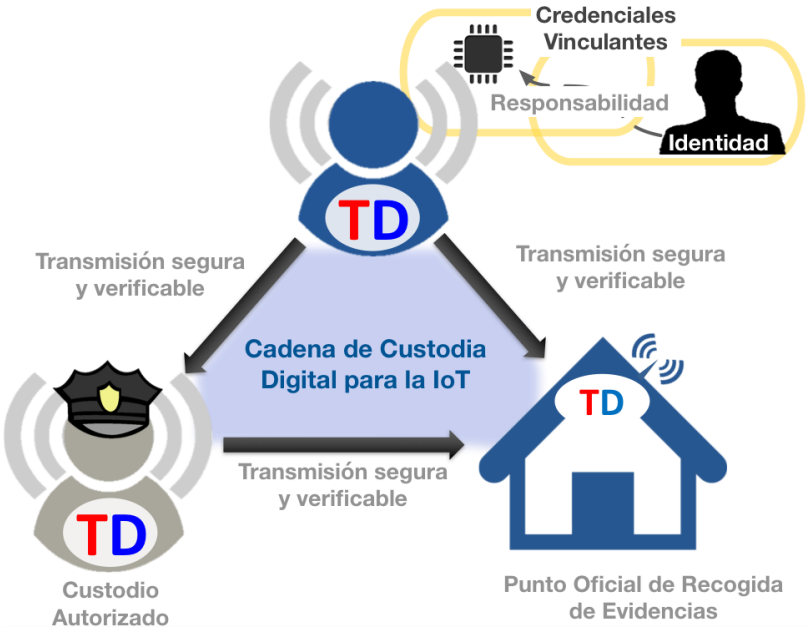

Figura 1. Cadena de custodia digital para dispositivos IoT (CCD-IoT)

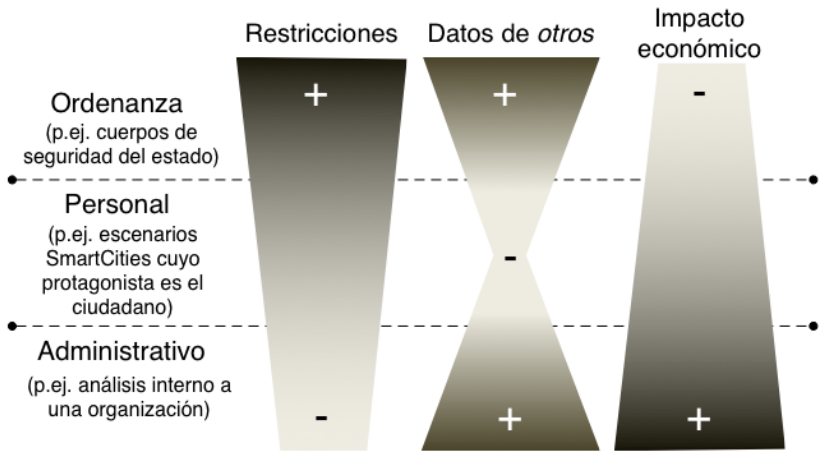

Figura 2. Casos de uso y factores

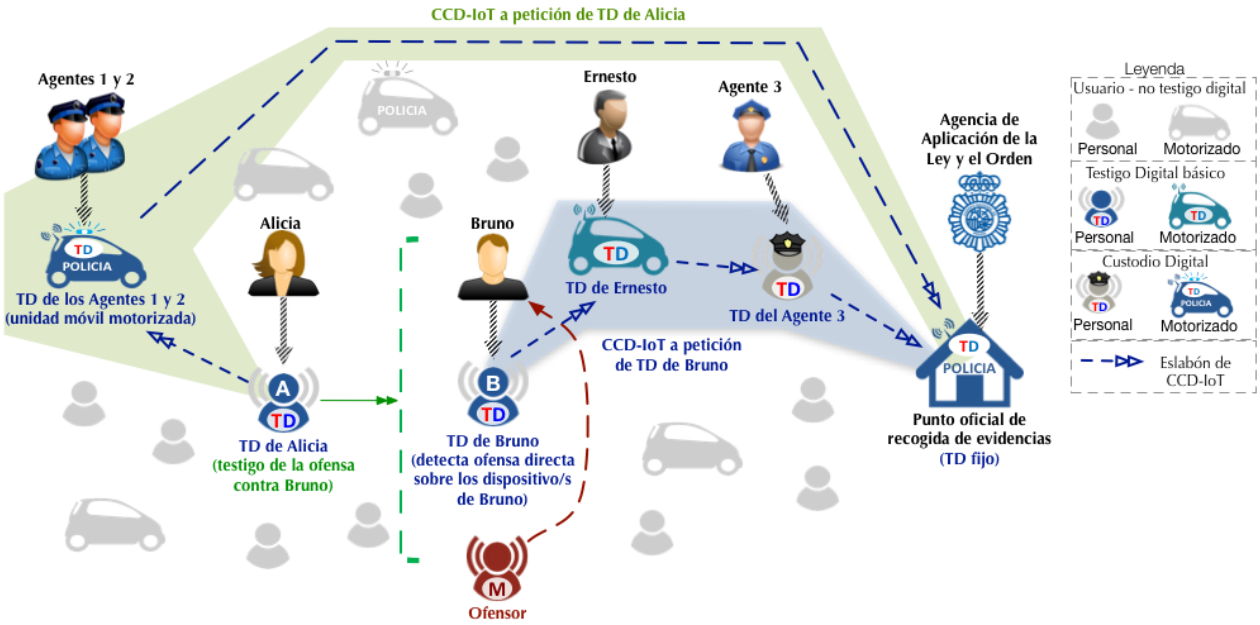

Figura 3. Ejemplo de caso de uso – Actores humanos y testigos