A. Nieto, and R. Rios, "Requisitos y soluciones de privacidad para la testificación digital", *III Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2017)* vol. Actas del JNIC 2017, pp. 51-58, 2017.
NICS Lab. Publications: https://www.nics.uma.es/publications

Requisitos y soluciones de privacidad para la testificación digital

Ana Nieto y Ruben Rios

Network, Information and Computer Security (NICS) Lab
Lenguajes y Ciencias de la Computación
Universidad de Málaga, España
Email:{nieto,ruben}@lcc.uma.es

***Resumen*—Los testigos digitales proponen un nuevo enfoque para que los dispositivos personales de la IoT - desde *wearables* hasta vehículos - entreguen evidencias electrónicas a una entidad autorizada para recibirlas y procesarlas. Como núcleo del testigo digital, las credenciales vinculantes identifican inequívocamente al usuario del testigo digital. El objetivo de este artículo es realizar un análisis crítico del enfoque de testigo digital desde el punto de vista de la privacidad, y proponer soluciones que ayuden a considerar algunas nociones de privacidad en el esquema (para aquellos casos en los que es posible). Además, se proponen medidas para permitir la testificación digital anónima, algo que no considera el enfoque actual, precisamente debido a la restricción de que se conoce la identidad de todos los eslabones de la cadena de custodia digital.**

***Index Terms*—Testigo Digital, Privacidad, IoT-Forense**

Tipo de contribución: *Investigación original*

I. Introducción

La *Internet of Things* (IoT) plantea desafíos en numerosos sectores, entre ellos se encuentra la informática forense [1]. Ésta es una disciplina que empieza a dar sus frutos tras años de esfuerzos de consolidación por parte de varias organizaciones (p.ej. el ENFSI-FITWG a nivel Europeo, o el SWGDE a nivel Estadounidense), en nuevos modelos y normas (p.ej. ISO/IEC 17025:2005, ISO/IEC 27037:2012, ISO/IEC 27042:2015, ISO/IEC 27050:2016+) y entidades encargadas de la acreditación de laboratorios digitales forenses (p.ej. ASCLD-LAB). Sin embargo, dicha consolidación no abarca, como es natural, los últimos cambios tecnológicos que se están produciendo gracias a la gran acogida de la IoT. Uno de los grandes desafíos abiertos es, precisamente, cómo desalentar a los ciberdelincuentes para que no empleen estas nuevas tecnologías en su propio beneficio; por ejemplo, aprovechando la alta densidad de dispositivos para ocultar sus acciones delictivas, o empleando los propios mecanismos de seguridad para coordinarse. Aunque existen algunos enfoques recientes que se hacen eco de la carencia de modelos y herramientas forenses para la IoT, así como algunas propuestas que plantean el despliegue de *Cadenas de Custodia Digitales* (DCoC) para flexibilizar el desempeño de los modelos digitales forenses, sigue habiendo un gran abismo abierto entre la informática forense tradicional y las expectativas de la IoT.

En este sentido, la testificación digital es un enfoque novedoso para el despliegue de *Cadenas de Custodia Digital en escenarios IoT* (DCoC-IoT, por sus siglas en inglés) [2]. El objetivo de este enfoque es tender un puente que permita acercar la informática forense a los ciudadanos, primando la cooperación de los dispositivos personales con *probadas características de seguridad*.

Sin embargo, cabe preguntarse más que nunca cómo este enfoque distribuido afecta a la privacidad del usuario, dado que se basa en el uso de *dispositivos personales*. Al ser el primer enfoque que se plantea de este tipo, un análisis de privacidad detallado sobre él sentará las bases para futuros trabajos relacionados.

En particular, en este artículo definimos las fases del testigo digital dentro de la norma ISO/IEC 27050:2016, para la gestión de evidencias digitales, estableciendo a su vez una correspondencia con el ciclo de vida de los datos personales. A su vez, analizamos el enfoque de *Testigo Digital* (TD) desde la perspectiva de la privacidad, destacando los pros y los contras de esta solución. Para ello, realizamos un análisis basado en casos de uso. Finalmente, proponemos soluciones para mitigar el efecto de las propiedades del TD en los requisitos de privacidad identificados durante el análisis. Pese a que considerar requisitos puramente éticos y legales es relevante de cara a estudiar la viabilidad de los testigos digitales como solución forense, en este artículo nos centramos en los aspectos técnicos relacionados con la privacidad.

Este trabajo se estructura como sigue. La Sección II analiza brevemente los trabajos relacionados. La Sección III describe los fundamentos del enfoque de testigo digital y analiza su relación con las fases de la norma ISO/IEC 27050:2016 y los datos personales. La Sección IV desglosa los casos de uso que servirán para el análisis desarrollado en la Sección V. La Sección VI propone algunos mecanismos que podrían ayudar a la testificación digital anónima, y a implementar otros requisitos de privacidad identificados en la Sección V. La última sección muestra las conclusiones y trabajos futuros.

II. Trabajo Relacionado

Existen claros conflictos entre la informática forense y la privacidad, como se describe en [3], donde se propone una utilidad de red basada en firmas de grupo para balancear privacidad y el análisis forense a nivel de red. En [4] se asume que este último viola la privacidad de los usuarios honestos, por lo que se propone un protocolo para proteger la privacidad de dichos usuarios mientras que se mantiene el análisis sobre el tráfico de los atacantes. De hecho, en [5] se emplean metodologías forenses para evaluar el grado de privacidad de las aplicaciones móviles centrado en los datos grabados en medios de almacenamiento (p.ej. tarjeta SD).

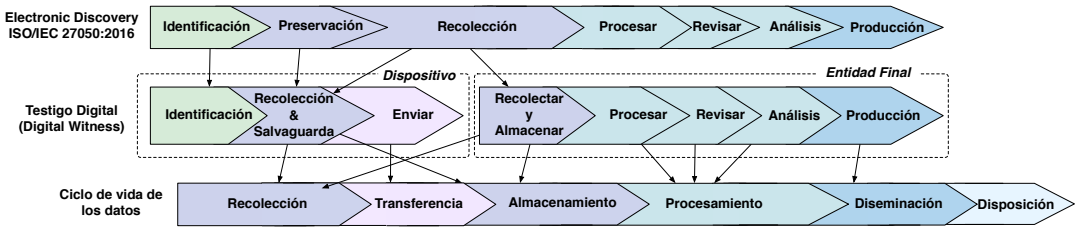

Figura 1: ISO/IEC 27050:2016, Testigo digital y Ciclo de vida de los datos

El testigo digital plantea un enfoque diferente para la recogida de evidencias electrónicas y su procesamiento. Fue inicialmente presentado en JNIC 2016 [6], donde se generó un interesante debate al respecto de los problemas que pudieran surgir de cara a la privacidad del usuario.

Ciertamente, ninguna de las soluciones propuestas hasta ahora dentro del ámbito del IoT-Forense [7] depende tanto del usuario y sus dispositivos personales como parte de la solución a un problema que de por sí es muy complejo. Otras soluciones relacionadas con la IoT-Forense se centran en proponer nuevos modelos para el análisis [8], [9], o bien en definir el concepto de *Cadena de Custodia Digital* (DCoC) [10]. Si bien estos trabajos no consideran el problema de la privacidad, es, sin lugar a dudas, uno de los principales problemas a los que se enfrentan las soluciones para la IoT y que por tanto debe ser considerado [11].

Por lo tanto, la principal contribución de este artículo es analizar los posibles conflictos entre un amplio conjunto de requisitos de privacidad y los testigos digitales y ofrecer soluciones para mitigar estas diferencias en la medida de lo posible.

III. Testigo Digital - Overview

El enfoque de los testigos digitales se definió en [6] y se amplió en [2] para identificar inequívocamente los requisitos de la solución. Un testigo digital es un dispositivo capaz de recolectar evidencias electrónicas de su entorno, almacenarlas en un espacio protegido (p.ej. elemento seguro), y enviarla a otros testigos digitales que estén autorizados para participar en la custodia de la evidencia electrónica. El fin perseguido es proporcionar un mecanismo por el cual es posible desplegar *Cadenas de Custodia Digitales* en la IoT (DCoC-IoT). Así, la evidencia electrónica se envía desde un testigo digital hasta una entidad final, el *Official Collection Point* (PRO), para su posterior análisis y procesamiento, siguiendo los procesos de la norma ISO/IEC 27050:2016 (Figura 1).

Cabe destacar, que a diferencia de otras soluciones para la gestión de evidencias electrónicas en entornos IoT [7] [9] [12], este enfoque se centra en la colaboración de dispositivos personales en la red capilar. Dado que la norma ISO/IEC 27050:2016 no contempla que los dispositivos personales puedan cooperar en los procesos que define, la correspondencia de estas fases a los testigos digitales no es directa, dividiéndose en dos partes: la primera, *realizada por el testigo digital*, agrupa las fases de identificación, preservación y collection (aunque local) de la norma. la segunda, realizada por el PRO, agrupa las fases de *collection* (de varias fuentes), *processing*, *review*, *analysis* y *production* de la norma.

A su vez, como se observa en la Figura 1, las fases del testigo se corresponden con las fases definidas para el ciclo de vida de los datos. A diferencia de la norma ISO/IEC 27050:2016, en el caso de los testigos digitales deben aplicarse los procedimientos de privacidad para la *transferencia* de datos. Esta fase no se define en la norma porque se asume que durante el proceso del análisis forense los datos no son transferidos, sino que forman parte de una investigación cerrada por el cual las evidencias electrónicas se obtienen de forma directa por personal autorizado a tal fin. Sin embargo, el enfoque de los testigos digitales, es más flexible a este respecto; permitirá la colaboración de la red capilar de dispositivos digitales, supeditada al despliegue de DCoC-IoT entre los cooperadores; otros dispositivos/entidades autorizadas capacitadas para actuar como testigos digitales. Para ello, deben darse dar las siguientes condiciones [2]:

- *Comportamiento anti-tampering*. La inicialización de un testigo digital se hace asegurando una cadena de confianza empleando seguridad embebida, capaz de realizar mediciones periódicas sobre la integridad del software en ejecución (p.ej. secure element, TPM). Si el dispositivo es en modo alguno corrompido no puede participar en la DCoC-IoT. Este control se hace desde el propio testigo.
- *Credenciales vinculantes* (BC, *Binding Credentials*). El testigo digital tiene una identidad de usuario ligada. Quiere decir que cuando recaba y envía las evidencias electrónicas van firmadas usando credenciales que identifican inequívocamente a la persona que da fe de las evidencias recabadas. Esto se hace así para desalentar el uso indebido del testigo digital - reportar una evidencia electrónica falsa adrede deberá ser amonestado.
- *Delegación vinculante* (BD, *Binding Delegation*). Procedimiento por el cual se despliega una **DCoC-IoT**. Esta capacidad permite transmitir la evidencia electrónica a otros testigos digitales autorizados, siguiendo unas pautas definidas por los roles de los dispositivos.
- *Procedimientos aceptados (p.ej. fases, mecanismos criptográficos) por las normas y estándares de gestión de evidencias electrónicas*. Un testigo digital actúa conforme a las recomendaciones para la gestión de evidencias electrónicas aceptadas por los expertos en la materia. En concreto, en este trabajo nos ceñimos a las fases publicadas en la norma ISO/IEC 27050:2016.

El testigo digital define diferentes perfiles de usuario y dispositivos. Por lo tanto, tiene sus propios requisitos de despliegue que pueden entrar en conflicto con los requisitos de privacidad (p.ej. anonimato). En particular, uno de los requisitos de esta solución es representativo de dicho coflicto: el usuario debe consentir vincular su identidad al dispositivo

personal que actuará como testigo digital.

A pesar de que el enfoque del testigo digital define políticas de privacidad para dejar constancia de que el usuario (i) puede escoger qué datos recaba su dispositivo y (ii) consiente en los términos del servicio, estas opciones están muy lejos de conseguir un enfoque que considere todos los casos de uso en los que pueden darse problemas de privacidad.

IV. Casos de uso

La solución de los testigos digitales se centra en desplegar DCoC-IoT en la *red capilar*, compuesta por otros testigos digitales que pueden tener dos perfiles o roles: ciudadano ó custodio. Pero, además, dentro de estos dos perfiles generales los dispositivos se clasifican en función de sus capacidades para ofrecer mecanismos de seguridad aceptados por las normas de gestión de evidencias electrónicas. El rol de los testigos digitales establece una jerarquía por la cual un custodio digital nunca delega sus evidencias electrónicas a un testigo digital básico. Además, un testigo digital podría tener varias identidades vinculadas (p.ej. un coche patrulla).

Un testigo digital establece una DCoC-IoT compuesta por otros testigos digitales como eslabones, cuyo objetivo es entregar evidencias electrónicas a un *Official Collection Point* (PRO), al que el testigo digital se encuentra adscrito (Sección IV-B). También puede transmitir las evidencias electrónicas al PRO empleando las DCoC *tradicionales*, ya definidas por otros enfoques. La adscripción a un PRO permite registrar los dispositivos que pueden actuar como testigos digitales; el PRO certifica que el dispositivo satisface los requisitos, esta vinculación permite que el testigo actúe conforme a un marco legal concreto.

IV-A. Colaboración en la red capilar

Las colaboraciones entre los testigos digitales se llevan a cabo en la red capilar. Como muestra la Figura 2 hay cuatro participantes básicos:

- Testigo digital víctima de la ofensa (B)
- Terceras partes testigos de una ofensa (A)
- Testigos digitales que actúan como enlaces DCoC-IoT
- Custodio digital - testigo digital con privilegios

La Figura 2 muestra dos tipos de ataques que podría detectar un testigo digital: ataques que se producen de forma local (p.ej. bluetooth) o bien ataques que proceden de otras redes, que no son fácilmente localizables, pero que son detectables por el rastro que dejan en el dispositivo. En estos últimos casos, las evidencias sólo las puede recabar el propio testigo digital. En los primeros casos otros testigos digitales podrían ser *testigos*, valga la redundancia, del suceso.

Una vez que las evidencias electrónicas se preservan en un espacio protegido el testigo digital puede (a) delegar la evidencia electrónica a cualquier otro testigo digital - sea custodio o no - lo antes posible o (b) guardar la evidencia electrónica hasta que él mismo encuentra un custodio digital - o bien directamente al PRO - y en ese momento la delega. También puede darse el caso de que otro testigo digital *A* - y no el propio afectado *B* - detecte el ataque (caso del ataque en la propia red) y lo reporta a una autoridad. Este es el motivo por el que en Figura 2 se muestran dos DCoC-IoT por el mismo suceso. Cabe destacar que *B* podría haber detectado el ataque pero no iniciar la DCoC-IoT en caso de que, por

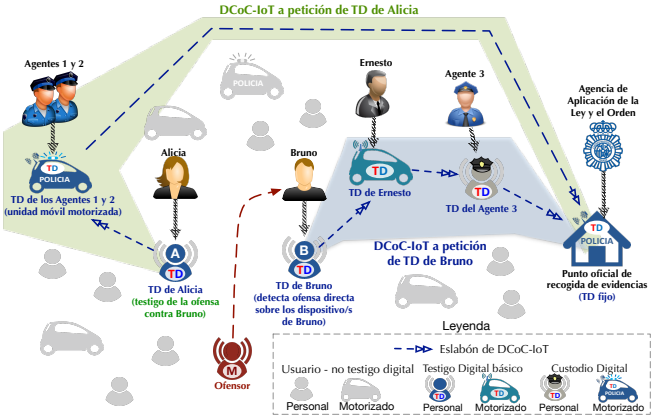

Figura 2: Actores de la red capilar [13]

ejemplo, no se encontrase en movimiento o bien no encontrase un testigo digital adecuado conforme a sus políticas para la transmisión. En dicho caso, *A* estaría reportando una ofensa sobre *otro* dispositivo antes de que se pronuncie al respecto el propio ofendido.

Cabe destacar que en Figura2 *A* podría decidir informar a *B* sobre su presencia en la escena, y esta información podría ser incluida en el informe reportado por *B*. Este hecho dependerá de las políticas configuradas en *A*, y de la disposición de *B* para generar un informe conjunto.

IV-B. Puntos de Recogida Oficial

Los *Puntos de Recogida Oficial* (PRO) reciben evidencias electrónicas que procesan y correlacionan para realizar análisis forenses que posteriormente tendrán que pasar una fase por la cual se decide si las evidencias electrónicas son *admisibles*. Un PRO puede ser una oficina de policía que ha sido autorizada para este propósito (p.ej. siguiendo el simil de que los laboratorios digitales forenses pueden ser certificados, deben crearse las pautas para definir cómo los PROs pueden ser certificados).

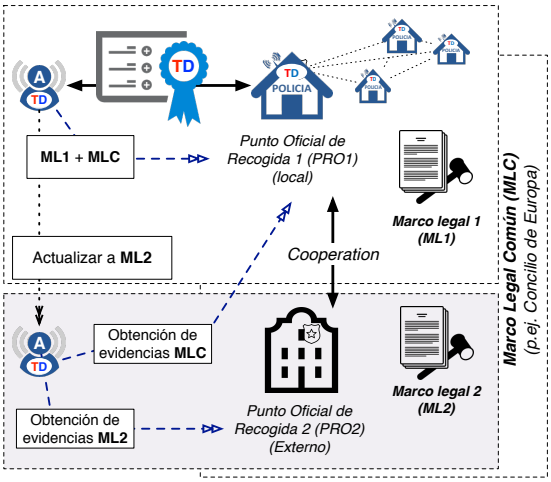

Figura 3: Testigo digital *A* (ML1) recabando conforme ML2

En la Figura 3 se muestra el testigo digital *A* adscrito al PRO1, denotado *local* por su relación con el testigo digital. En general, consideramos tres actores en este caso de uso:

- Testigo digital que cambia de jurisdicción (A), adscrito a su PRO local (PRO1).
- PRO (local, PRO1 en Figura 3).
- PRO (externo, PRO2 en Figura 3).

El PRO local recibe las evidencias de los testigos digitales bajo su jurisdicción. A su vez, pueden establecerse relaciones entre distintos PROs dentro de un mismo ámbito legal (p.ej. dentro del mismo país con el mismo marco legal). Sin embargo, debemos considerar también qué ocurre cuando el testigo digital cambia de jurisdicción. Los PRO foreign son PROs que pertenecen a otra jurisdicción distinta a aquella a la que el testigo digital está suscrito.

El testigo digital, de llegar a una localización donde no tiene jurisdicción su PRO, tiene dos opciones: (1) actuar conforme el mapa legal de la PRO receptora, (2) actuar conforme a el mapa legal común que ampare tanto a su PRO de origen como a la receptora (p.ej. marco legal europeo si las dos PROs forman parte de países de la Unión Europea). La opción (2) puede no darse si dicho marco legal común no existe.

Por otra parte, en caso de ser necesaria la cooperación entre PROs de diferentes jurisdicciones, deben respetarse los acuerdos iniciales que los testigos digitales tengan con cada PRO. En algunos casos el propio testigo digital puede estar interesado en esta cooperación (p.ej. se reporta una ofensa que exige una compensación por parte de un ciudadano o una entidad del país visitado). En otros casos la cooperación puede ser necesaria por quejas sobre un testigo digital externo. Por ejemplo, en Figura 3 el PRO2 recibe informes de sus testigos digitales sobre que el testigo digital *A* intenta recabar evidencias electrónicas sin actualizarse al LF2. En este caso, el PRO2 podría optar por reportar este suceso al PRO1. El usuario de *A* debería ser notificado de esta incidencia al igual que si de una multa se tratase.

V. Análisis

La Tabla I resume los requisitos de privacidad que pueden entrar en conflicto con el enfoque de testificación digital y que pasamos a describir en las siguientes subsecciones.

V-A. Anonimato

Una ofensa no es un crimen necesariamente (cuatro condiciones son necesarias para esto último: i) actus reus, ii) means rea, iii) concurrence, iv) causation); es algo bastante subjetivo y relativo a lo que personalmente consideramos injusto. Al reportar una evidencia electrónica, el testigo digital considera *qué es ofensivo para su usuario* en base a las políticas que el usuario define. Por ejemplo, puede ser ofensivo que algún software intente cambiar código de alguna aplicación (una ofensa interna al dispositivo), pero también el detectar cómo otro dispositivo en la red está siendo atacado. En este último caso, es una ofensa que potencialmente afecta a *otro*, pero que el usuario quiere que se reporte.

Dado que el usuario del testigo digital define las políticas acorde a criterios que consiente, nos centramos aquí en qué ocurre cuando se reportan *ofensas sobre otros*. Tal vez para el sujeto ofendido no se esté produciendo una ofensa o no quiera que otros dispositivos la reporten (p.ej. porque no quiera que se sepa dónde está). El esquema de testigo digital permite así que se den problemas de *anonimato*, ya que se puede averiguar la identidad del ofendido si es un testigo digital, porque está registrado con el PRO y además usa su identidad durante todo el proceso.

Además, entre los actores no sólo se encuentra el/los ofendidos potenciales y el/los ofensores, sino que seguramente habrá otros actores, sean testigos digitales o no. Ciñéndonos al caso de los testigos digitales, cuando uno de los TD - sea el directamente ofendido o no - reporta un suceso, puede estar dando información sobre el resto de testigos presentes. Esto significa, que el anonimato de otras fuentes que ni siquiera tienen porqué estar directamente implicadas en un suceso se ve afectado. Esto puede desalentar el uso del TD para aquellos usuarios que quieran usar esta tecnología tan sólo para enviar sus propias evidencias electrónicas y *permanecer invisibles* al resto de participantes. Para paliar esto la implementación de los testigos digitales debe considerar la posibilidad de que los testigos permanezcan *silenciados* o puedan *salirse*; dejar de usar el testigo digital en cualquier momento.

Por último pero no menos importante, el testigo digital tal y como está definido no permite la *testificación anónima*. La identidad del usuario se vincula a su testigo digital mediante las credenciales vinculantes para desalentar el uso indebido del DW. Sin embargo, esta restricción impide que usuarios bien intencionados usen sus testigos para testificar de forma anónima un suceso en el que no les gustaría verse involucrados pero que requiere ser reportado (p.ej. porque conozca al atacante y tema represalias). Aunque la testificación anónima podría afectar al requisito de garantizar la *procedencia* de la evidencia electrónica, también podría abrir la puerta a evidencias electróncias que ayuden de forma complementaria en un caso.

V-B. Privacidad en la atestación

Cabe preguntarse si un *testigo digital invalidado*, ya sea porque (a) presenta algún problema de funcionamiento, o (b) durante las comprobaciones de integridad se detectó que estaba comprometido, es visible en la red de testigos digitales. Conocer el *estado* del testigo puede afectar a la honorabilidad de su poseedor, pero además, puede ser un problema de cara a posibles atacantes en el entorno. Por ejemplo, atacantes que intentan aprovecharse de vulnerabilidades en el dispositivo podrían realizar búsquedas de dispositivos defectuosos y aprovecharse de la voluntad colaborativa y *transparencia* de los testigos digitales. Para evitar este tipo de problemas debe garantizarse la *privacidad en los mecanismos de atestación* que permitan verificar el estado de los testigos digitales con los que se desea colaborar sin revelar información que pueda comprometer al usuario o su dispositivo.

V-C. No-vinculación

El enfoque de testigo digital recalca que el camino seguido por las evidencias electrónicas debe conocerse, respetándose el principio de trazabilidad. Esto afecta a la propiedad de no-vinculación en tanto a que los eslabones - testigos digitales - de la cadena son conocidos para conocer quiénes tuvieron acceso, aunque sea de custodia (sin conocer el contenido) durante el proceso de delegación vinculante. A su vez, el análisis y correlación posteriores podrían afectar a esta propiedad.

V-D. Inobservable / Indetectable

Durante el proceso de presentación de evidencias digitales puede ser necesario identificar la presencia de otros testigos

Tabla I: Requisitos de Privacidad en base a las características del Testigo Digital

Propiedad TD	Red Capilar			Puntos de Recogida Oficial (PRO)		
	Propósito	Requisito Privacidad	Mitigación	Propósito	Requisito Privacidad	Mitigación
Comportamiento Anti-tampering	Enlaces confiables en la DCoC-IoT	Confidencialidad Priv. atestación	DAA Salida / Silencio	Dispositivo confiable	Datos de usuario en PRO	Consentimiento del usuario en el registro
Credenciales Vinculantes	Responsabilidad	Anonimato	TD Anónimo: Crowd-like Firma de grupo	Responsabilidad	Anonimato	Declaración multiparte
Delegación Vinculante	Trazabilidad	Anonimato, No-vinculación, Inobservable, Indetectable, Priv. localización, Priv. Transaccional	Descubrimiento de rutas con priv. Blockchain Smart Contracts	Trazabilidad y Correlación (varias fuentes)	Recopilación mínima (múltiples fuentes) Priv. localización	Clave de grupo compartida con PRO
ISO/IEC 27050:2016	Aceptación (procesos bien conocidos y aceptados)	Disposición (datos de los eslabones)	Consentimiento (otros) Prueba de borrado seguro	Aceptación (procesos bien conocidos y aceptados)	Disposición (datos almacenados)	Prueba de borrado seguro

digitales en el entorno local. Estos testigos digitales próximos, ya sean ciudadanos o custodios, pueden servir de enlace para transportar las pruebas hasta el PRO. Ante esta circunstancia, el enfoque del testigo digital no establece el modo de proceder para descubrir dispositivos del entorno. Sin embargo, esto puede afectar a las propiedades de Inobservable/indetectable, que establecen que la existencia de comunicaciones no debe ser observable por terceras partes y, en caso de serlo, no debe ser posible determinar quiénes se están comunicando. Así pues, si es un custodio el que anuncia su presencia esto puede, por ejemplo, afectar a su integridad física ya que podría ser víctima de ataques.

V-E. Privacidad de localización

Entre la información recabada por un testigo digital, la de su localización o la de los dispositivos del entorno podría ser relevante (de cara al dispositivo que recaba la información) produciéndose problemas de privacidad en la localización. Cabe destacar que incluso en aquellos casos en los que se detecte una ofensa que no sea necesariamente local (p.ej. el caso de uso en el que un ataque es externo a la red) el ofendido y los eslabones de la DCoC-IoT podrán tener problemas de privacidad. En estos casos tal vez la localización del ofendido no es relevante para el caso, y aún así se sabrá por la definición del TD. Al ser un mecanismo colaborativo el *cómo se anuncian los dispositivos* puede revelar información sobre la localización a terceros no autorizados.

La localización es relevante también para conocer el marco legal/jurisdicción en la que opera el testigo digital en un momento dado (Figura 3). A este respecto hay que destacar otro posible inconveniente, y es que pueda saberse dónde está un testigo - y por tanto su poseedor - en base a cómo se comporta. Dado que se ha comprobado que hay ataques dirigidos específicamente a dispositivos en base al país donde se encuentran [14], esto no sólo aporta información sobre el individuo, sino que lo expone a riesgos ante terceros si esta información llega a conocerse.

V-F. Privacidad transaccional

Cada testigo que aporta evidencias necesita una prueba / comprobante del resultado de esta transacción. La *privacidad transaccional* podría verse afectada debido a estas colaboraciones si los resultados pueden ser conocidos por otros dispositivos que no han participado en dicha colaboración. El grado en el que esta propiedad se verá afectada dependerá de cómo se implementen los mecanismos para la *delegación vinculante*.

Cabe destacar que el listado de testigos digitales que ha tenido potencial acceso a los datos debe ser *transparente* para el PRO, a fin de garantizar la *trazabilidad* y establecer *responsabilidades* ante posibles conductas indebidas, adicionales a las que pueda tomar el propio dispositivo. La DCoC-IoT debe mostrar todos los TD que participaron en la delegación vinculante, y todos los intentos fallidos de delegación vinculante (p.ej. intentó transmitirse una evidencia digital a un TD que de repente desapareció de la red o rechazó la conexión) deben conocerse, al menos, por el PRO. Estas relaciones entre participantes deben quedar reflejadas mediante contratos (p.ej. *smart contracts*) pero manteniendo principios de privacidad transaccional.

V-G. Recopilación de datos mínima

El principio de data minimisation corresponde con la necesidad de minimizar los datos que se recolectan. La definición de testigo digital considera la privacidad selectiva (Sección III) que ayuda a la minimización de datos vía los criterios de selección del usuario. Sin embargo, como se aprecia en los casos de uso de la red capilar (Sección IV-A), las evidencias digitales pueden llegar a los PROs desde varias fuentes, por lo que la información recolectada puede llegar a ser redundante, dependiendo del caso y del número de evidencias electrónicas recabadas sobre un mismo hecho. Mientras que podría ser un hecho que aporte mayor credibilidad a un suceso, existe no sólo el riesgo de afectar al principio de minimización de datos (ISO/IEC 29100:2011) sino también la posibilidad de que un mal uso de los testigos digitales provoque confusión o denegación de servicio en el sistema final.

V-H. Borrado seguro

Mientras que en las fases de los modelos forenses normalmente se considera la devolución de la evidencias físicas (p.ej. un PC), no se destacan cuáles son los procedimientos para la eliminación de las evidencias electrónicas. Si bien eso podría ser entendible en los enfoques tradicionales, no lo es en un enfoque como el del testigo digital que tiene como núcleo

la cooperación. Para fomentar esta cooperación voluntaria - de los testigos - es necesario establecer los mecanismos oportunos para garantizar la fase de *borrado seguro* dentro del enfoque.

El testigo digital define *políticas para eliminar las evidencias electrónicas almacenadas*, que son configuradas en base a las preferencias del usuario. Se trata de decisiones que afectan a las evidencias electrónicas gestionadas por su dispositivo, pero que por ejemplo no tienen en cuenta cómo *otros TD colaboradores* quieren que los datos que aportan sean eliminados. Esto también concierne a los datos del PRO. En definitiva, los testigos digitales que colaboran no tienen el control sobre los datos que aportan como prueba y no hay mecanismos definidos para la consulta de sus datos.

V-I. Síntesis

Del análisis anterior se desprende que el esquema actual del testigo digital permite que otros dispositivos del entorno - y no sólo el PRO o testigos digitales autorizados - puedan obtener información que permita identificar a usuarios que tal vez ni siquiera guardan relación con la ofensa.

Además, los propios testigos digitales actúan de forma *transparente* permitiendo que los usuarios, aún configurando las opciones de privacidad de sus dispositivos, se encuentren expuestos por la actividad de otros testigos digitales *que pueden reportar información sobre su entorno* (p.ej. por intentos de despliegue de DCoC-IoT fallidos). Por otra parte, la cooperación entre las PROs debe regirse en función de los acuerdos entre los *marcos legales* vigentes, y dependería del entorno específico. En cualquier caso, pueden implementarse soluciones de seguridad más robustas que no dependen de requisitos computacionales como ocurre en el caso de los testigos digitales. Los desafíos más significativos en cuanto a la privacidad se sitúan en la red capilar.

Mientras que la vinculación entre el dispositivo y su usuario son indispensables para el enfoque de testigo digital, deben proponerse mecanismos de mitigación que permitan balancear esta solución para proteger los datos personales que (i) o no son relativos a un caso o (ii) no son necesarios para que el objetivo primordial del testigo digital - esto es, delegar las evidencias electrónicas al PRO - se consiga.

Finalmente, en base a los casos de uso y el análisis realizado, los problemas que pueden darse en cuanto a la privacidad tienen dos vertientes: (a) que se obtengan datos personales *de otros* de los testigos digitales - recordemos que el testigo digital tiene consentimiento de su usario, pero no de otros - y (b) que los mecanismos del testigo digital den información a otros dispositivos de la red de forma involuntaria al desplegar la DCoC-IoT.

A continuación se proponen algunos mecanismos de mitigación que podrían ayudar a solventar ó implementar algunos requisitos de privacidad.

VI. Mecanismos de mitigación

En esta sección describimos posibles soluciones que podrían adoptarse para implementar algunas de las características de los testigos digitales considerando privacidad. Con este fin, definimos una solución para permitir el anonimato en la DCoC-IoT (testigos anónimos), no contemplada hasta ahora en el testigo digital (Sección VI-A). El resto de posibilidades para mitigar y/o solventar los problemas de privacidad encontrados podrían aplicarse a la definición actual de testigo digital (Sección VI-B), ya que dependen de la implementación.

VI-A. Anonimato en la DCoC-IoT

A fin de fomentar la cooperación es importante permitir que los ciudadanos se sientan que su identidad está protegida pero no es posible ofrecer un absoluto anonimato por los motivos expuestos anteriormente.

Una forma de permitir que *A* o *B* (Figura 2) reporten las evidencias electrónicas de forma anónima es usando técnicas de $k - Anonimity$ que aporten un balance adecuado entre anonimato e identificación. Estas técnicas permiten a un individuo ser indistinguible entre un grupo de k individuos con atributos muy similares. De manera que una acción sensible puede haber sido realizada por cualquiera de los k individuos con igual probabilidad.

En el caso del testigo digital, esta idea puede aprovecharse para garantizar la propiedad de *procedencia* dentro de un rango aproximado, lo que podemos denotar como $d-provenance$; distorsión en la *procedencia* de la evidencia electrónica introducida por los mecanismos de privacidad.

Aunque esta medida introduce cierto margen de error a la procedencia de la evidencia electrónica (he aquí un claro ejemplo de balanceo entre requisitos de privacidad y de informática forense), es cierto que otros mecanismos empleados en peritajes forenses también adolecen de ser exactos y aún así *junto con otras pruebas* pueden ser determinantes. Sirva de ejemplo que, aunque la información GPS no es concluyente debido a que hay en torno a 100m de imprecisión, el uso de estos mecanismos imprecisos - en cuanto a el origen - aporta pruebas contextuales que ayudan a delimitar la investigación.

Así pues, como se observa en la Figura 4, los usuarios podrían agruparse de manera que cuando uno de los testigos digitales *A* tenga algo que reportar iniciaría un protocolo estilo Crowds [15]. De cara al siguiente eslabón de la cadena de custodia (*C* en Figura 4), cualquiera de los miembros del conjunto podría haber originado el mensaje, aunque se haya recibido desde el testigo digital marcado como *B*.

Este tipo de mecanismos también podría ayudar para hacer anónimos los *eslabones de la DCoC-IoT*, pero con una restricción más fuerte. Mientras que la $d-provenance$ puede ser asumida, una vez iniciada la DCoC-IoT el PRO necesitará tener constancia de todo lo que ocurre y qué testigos digitales estuvieron involucrados. Por lo tanto, a diferencia de lo que ocurre en el diseño original de Crowds, el esquema de testificación digital requiere que las identidades de todos los miembros del Crowd puedan ser conocidas por la PRO. Una forma de solventar esto a la vez que proporcionar anonimato en los eslabones es ofuscar las identidades mediante algún mecanismo criptográfico tradicional (p.ej., con una clave de grupo que puede ir cifrada con la clave pública del PRO) o mediante un sistema de seudónimos, que el PRO pueda revertir con la colaboración de algunos miembros del grupo.

VI-B. Implementación de propiedades del testigo digital

Como se ha identificado en la Sección V, durante la cooperación para desplegar la DCoC-IoT pueden surgir varios problemas de privacidad que dependen de la implementación

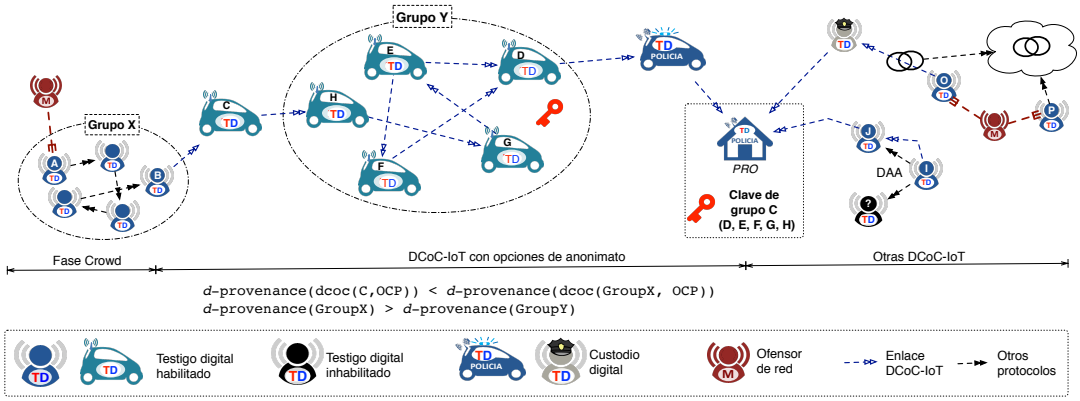

Figura 4: Ejemplos de mecanismos de mitigación

de algunas de las características definidas groso modo en el esquema original del testigo digital. A diferencia del punto anterior, las siguientes secciones no muestran re-definiciones del testigo digital sino opciones de implementación considerando los requisitos de privacidad identificados.

VI-B1. Atestación: Uno de los inconvenientes que puede darse es que el *estado* de los testigos digitales sea conocido. En particular, un riesgo del esquema original es que los testigos digitales del entorno sepan cuándo un testigo digital está inhabilitado, produciéndose problemas de *privacidad en la atestación*. Para llevar a cabo la atestación de un dispositivo sin revelar información sensible sobre el usuario, los testigos digitales pueden hacer uso del protocolo DAA (*Direct Anonymous Attestation*) [16]. DAA permite a un verificador comprobar que otro usuario utiliza una plataforma con un módulo hardware de seguridad certificado (p.ej. *I* en Figura 4 decide escoger *J* sin llegar a conocer la identidad del testigo digital invalidado). Además, este protocolo permite que esta verificación sea privada, de manera que el verificador no es capaz de comprobar con qué usuario se está comunicando o si ya se ha comunicado con este previamente. Este protocolo está disponible en la especificación TPM (*Trusted Platform Module*) [17], que es una de las tecnologías consideradas en la definición original de los testigos digitales para ofrecer un *nucleo de confianza* (CoT, por sus siglas en ingles) en la gestión de evidencias.

VI-B2. Descubrimiento de eslabones: El enfoque de testigo digital promueve el establecimiento de cadenas de custodia digitales (DCoC-IoT) lo más cortas posibles con el fin de minimizar la exposición de los eslabones a las posibles amenazas de red, a la vez que reducir el número de usuarios involucradosen la custodia. En estas situaciones donde es necesario recurrir a otros testigos, sería interesante incorporar protocolos capaces de detectar rutas bajo demanda hacia custodios (o el PRO) de longitud mínima. Para preservar la identidad del usuario en este descubrimiento de las rutas óptimas, se puede optar por usar protocolos heredados de redes MANET, por ejemplo AASR [18]. Una vez descubierta la ruta óptima hasta el destino, se procedería al envío de las evidencias.

VI-B3. Estampillado de tiempo: Los mecanismos de firma ciega, introducidos originalmente por Chaum [19], permiten a un individuo firmar digitalmente un documento sin conocer su contenido. Tras realizar la firma, el dueño del documento puede recuperar el documento original manteniendo la firma digital. Una de las aplicaciones para las que se puede usar este mecanismo en los testigos digitales es para *corroborar* la adquisición de evidencias electrónicas del entorno, sin que la tercera parte (p. ej. un testigo digital con mejores prestaciones que el que necesita el estampillado de tiempo) conozca el contenido de la evidencia. Si en lugar de utilizar la clave del testigo para cifrar los datos que posteriormente serán firmados, se utiliza la clave del PRO, este podrá recuperar los datos directamente sin necesidad de que los datos pasen nuevamente por el testigo para deshacer el cifrado. Esta idea, en combinación de esquemas de signature chaining [20], puede ser de gran utilidad para las DCoC-IoT.

VI-B4. Blockchain Smart Contracts: Blockchain es un mecanismo que permite realizar transacciones seguras entre individuos / entidades sin la involucración de una tercera parte confiable (p.ej. *Bitcoin*). Junto con la facilidad de los *smart contracts* (e.g., Ethereum), que permiten introducir programas definidos por el usuario en el blockchain, se obtiene un mecanismo muy robusto para realizar transacciones contractuales descentralizadas. En [21] se propone el framework *Hawk* para construir *blockchain smart contracts* teniendo en cuenta la privacidad. En el esquema del testigo digital este mecanismo puede ser una solución factible para el despliegue de cadenas de custodia digitales manteniendo la *privacidad transaccional*, dado que Hawk se basa en la existencia de una *tercera parte* que puede ser instanciado con un TCH (*Trusted Computing Hardware*). Precisamente, los testigos digitales se basan en la existencia de TCH (p.ej. secure element, TPM), por lo que esta característica que podría ser una limitación para otros sistemas, encaja muy bien en el testigo digital.

Otra ventaja añadida del uso de *blockchain* es la posibilidad de que otros testigos en la escena puedan consultar si un incidente ha sido ya reportado (p.ej. *P* en Figura 4).

VI-B5. Declaración multiparte: En determinadas ocasiones puede ocurrir que múltiples usuarios sean testigos de un suceso y estén de acuerdo reportarlo a las autoridades como si de una declaración/denuncia conjunta se tratase, pero manteniendo su propia versión de los hechos oculta al resto de participantes en el informe final. Uno de los beneficios de esta práctica es que permite aliviar la sobrecarga que supondría para el PRO la gestión de múltiples DCoC-IoT sobre un mismo hecho. Para implementar esta característica, se puede recurrir a protocolos basados en cifrado homomórfico [22] o

computación seugra [23], de manera que los testigos puedan compartir la información y operar sobre esta sin desvelar el contenido de sus declaraciones.

VI-B6. Garantías de eliminación: Por último, un usuario que aporta evidencias sobre un suceso, espera que los datos ofrecidos sean utilizados únicamente para resolver el caso en cuestión y que no sean utilizadas con otros fines. Por ello, es necesario facilitar mecanismos que permitan verificar que las evidencias han sido borradas una vez que los datos dejan de ser necesarios. Un ejemplo de este tipo de mecanismos es el de proporcionar a los usuarios que colaboraron una *prueba de borrado seguro*, permitiendo así comprobar a éstos si sus datos permanecen en el sistema en un momento dado [24]. Este tipo de verificaciones involucraría al PRO y a los testigos digitales que iniciaron las DCoC-IoT, ya que los testigos digitales intermedios ya definen mecanismos para eliminar los datos transmitidos por la DCoC-IoT.

VII. Conclusiones y trabajo futuro

En este trabajo realizamos un análisis del enfoque de *testigo digital* desde el punto de vista de la privacidad. Este mecanismo emplea formularios de consentimiento de usuario y políticas para la gestión de las evidencias (p.ej. tipo de evidencias recabadas, permisos, etc.). Sin embargo, no considera los problemas que pueden aparecer por los mecanismos cooperativos que permiten que los datos de *otros* individuos sean captados - intencionadamente o no. En base a los requisitos de privacidad identificados durante el análisis, proponemos soluciones que pueden adoptarse para mitigar la carencia de privacidad en aquellos casos en los que es posible. Como parte de estas soluciones, re-definimos el enfoque de testigo digital para permitir la testificación anónima. A este respecto, este trabajo sienta los primeros pasos en esta dirección, por lo que hay un largo camino por recorrer.

Por ejemplo, durante la realización de este trabajo identificamos que no existen modelos de referencia para este tipo de casos de uso en la informática forense. Esto dificultará, por ejemplo, consensuar un marco de trabajo común con otros enfoques similares que puedan surgir en el futuro. Cabe destacar que las mitigaciones propuestas son específicas del enfoque de testigo digital. Un aspecto que consideramos muy interesante es la $d - provenance$ y cómo podría afectar a la validez de las evidencias suministradas por los testigos digitales. Este estudio deberá considerar los diferentes tipos de DCoC-IoT que pueden desplegarse en base a los distintos participantes (p.ej. vehículos, móviles, etc.), quedando fuera del ámbito del presente artículo.

Agradecimientos

Este trabajo ha sido financiado por la Junta de Andalucía a través del proyecto FISICCO (TIC-07223), y por el Ministerio de Economía y Competitividad a través de los proyectos PERSIST (TIN2013-41739-R) e IoTest (TIN2015-72634-EXP).

Referencias

[1] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the internet of things promise," *Computer Fraud & Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[2] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal device," *IEEE Network*, In Press.

[3] M. Afanasyev, T. Kohno, J. Ma, N. Murphy, S. Savage, A. C. Snoeren, and G. M. Voelker, "Privacy-preserving network forensics," *Communications of the ACM*, vol. 54, no. 5, pp. 78–87, 2011.

[4] G. Antoniou, L. Sterling, S. Gritzalis, and P. Udaya, "Privacy and forensics investigation process: The erpina protocol," *Computer Standards & Interfaces*, vol. 30, no. 4, pp. 229–236, 2008.

[5] P. Stirparo and I. Kounelis, "The mobileak project: Forensics methodology for mobile application privacy assessment," in *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012, pp. 297–303.

[6] A. Nieto, R. Roman, and J. Lopez, "Testigo digital: delegación vinculante de evidencias electrónicas para escenarios iot," in *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)*, 06/2016 2016, pp. 109–116. [Online]. Available: http://ucys.ugr.es/jnic2016/docs/ActasJNIC2016.pdf

[7] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. IEEE, 2013, pp. 608–615.

[8] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*. IEEE, 2013, pp. 544–550.

[9] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of things (iot) digital forensic investigation model: Top-down forensic approach methodology," in *Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on*. IEEE, 2015, pp. 19–23.

[10] Y. Prayudi and A. Sn, "Digital chain of custody: State of the art," *International Journal of Computer Applications*, vol. 114, no. 5, 2015.

[11] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The internet of things (iot) and its impact on individual privacy: An australian perspective," *Computer Law & Security Review*, vol. 32, no. 1, pp. 4–15, 2016.

[12] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," in *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE, 2016, pp. 356–362.

[13] A. Nieto, R. Roman, and J. Lopez, "Testificación digital," *Revista SIC*, vol. 122, pp. 94–98, Nov 2016 2016. [Online]. Available: https://revistasic.es/index.php?option=com_content\&view=article\&id=1713\&Itemid=1498

[14] J. Guarnizo, A. Tambe, S. S. Bunia, M. Ochoa, N. Tippenhauer, A. Shabtai, and Y. Elovici, "Siphon: Towards scalable high-interaction physical honeypots," *arXiv preprint arXiv:1701.02446*, 2017.

[15] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions," *ACM transactions on information and system security*, vol. 1, no. 1, pp. 66–92, 1998.

[16] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 132–145.

[17] T. C. Group, "Tpm library specification," [Online], 2014. [Online]. Available: https://trustedcomputinggroup.org/tpm-library-specification/

[18] W. Liu and M. Yu, "Aasr: Authenticated anonymous secure routing for manets in adversarial environments," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585–4593, Nov 2014.

[19] D. Chaum, *Blind Signatures for Untraceable Payments*. Boston, MA: Springer US, 1983, pp. 199–203.

[20] A. Saxena and B. Soh, "One-way signature chaining: a new paradigm for group cryptosystems," *International Journal of Information and Computer Security*, vol. 2, no. 3, pp. 268–296, 2008.

[21] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 839–858.

[22] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doröz, and B. Sunar, "Practical homomorphic encryption: A survey," in *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, June 2014, pp. 2792–2795.

[23] N. P. Smart, *Secure Multi-party Computation*. Cham: Springer International Publishing, 2016, pp. 439–450.

[24] N. P. Karvelas and A. Kiayias, "Efficient Proofs of Secure Erasure," in *International Conference on Security and Cryptography for Networks (SCN 2014)*, ser. LNCS 8642, A. M. and D. P. R., Eds., 2014, pp. 520–537.