A. Nieto, R. Rios, and J. Lopez, "PRoFIT: modelo forense-IoT con integración de requisitos de privacidad", *XIII Jornadas de Ingeniería Telemática (JITEL 2017)* vol. Libro de actas, pp. 302-309, 2017.
http://doi.org/http://dx.doi.org/10.4995/JITEL2017.2017.7061
NICS Lab. Publications: https://www.nics.uma.es/publications

PRoFIT: modelo forense-IoT con integración de requisitos de privacidad

Ana Nieto, Ruben Rios, Javier Lopez
Network, Information and Computer Security (NICS) Lab,
Lenguajes y Ciencias de la Computación,
Universidad de Málaga
Campus Teatinos s/n, 29071 Málaga (España)
E-mail:{nieto,ruben,jlm}@lcc.uma.es

***Resumen*—La *Internet de las cosas* (IoT) complica sobremanera la extracción de evidencias electrónicas que pueden servir de base para una investigación forense. En entornos altamente cambiantes y con una densidad de dispositivos tan elevada, es muy difícil entender completamente el contexto de la ofensa. Es por ello que la cooperación de los individuos, aún no estando directamente implicados en la ofensa, puede ser muy relevante para el analista forense. En este artículo se propone un nuevo modelo para la IoT-Forensics, que pretende sentar las bases para la cooperación voluntaria de los individuos en las investigaciones de delitos telemáticos. Para ello, el modelo integra requisitos de privacidad de la norma ISO/IEC 29100:2011 durante todo el ciclo de vida de la investigación.**

***Palabras Clave*—forense, IoT, privacidad, seguridad, testigos digitales.**

I. INTRODUCCIÓN

La informática forense tradicional se basa en una serie de procesos bien establecidos que tienen como objetivo preservar la evidencia electrónica. Existen varios modelos muy similares entre sí, que describen conductas a seguir precisas y bien definidas, pero son exageradamente estáticos [1]. Las evidencias - discos o dispositivos de los que se extraerán evidencias electrónicas - se recaban por medio de una orden judicial al principio del proceso. Las evidencias electrónicas se obtienen conforme a su volatilidad, siendo posible que algunas de éstas se obtengan en la propia escena (p.ej. volcados de memoria). Se implementan cadenas de custodia por medio de documentos que firman los responsables autorizados a gestionar las evidencias. Esto es así con el fin de preservar la integridad de la prueba, pero no deja de ser un proceso poco flexible, concebido para escenarios muy estáticos.

Sin embargo, estamos viviendo un boom de dispositivos sin parangón. Actualmente los analistas forenses se encuentran con el problema de que hay un sinfín de dispositivos para los que aún no existen herramientas o procesos bien definidos para regular su tratamiento forense [2]. No sólo los dispositivos, sino también las infraestructuras/plataformas intermedias que se usan para la comunicación entre los objetos, plantean grandes desafíos forenses. Precisamente, en 2013 surge el concepto de IoT-Forensics [3] para destacar los problemas que el paradigma IoT introduce en el ámbito forense. Tanto a nivel de adquisición de información como a nivel de cómo se gestiona esa información [4], o la problemática de la avalancha de datos que deben procesarse y correlacionarse.

Pero en IoT-Forensics el problema va más allá; el usuario y sus dispositivos están demasiado conectados como para continuar obviando que el espinoso problema de la privacidad debe ser finalmente abordado. Precisamente, en este artículo definimos el modelo PRoFIT (*Privacy-aware IoT-Forensic*) que integra propiedades de privacidad conforme a la norma ISO/IEC 29100:2011 en las fases de un modelo forense adaptado para la IoT. Este modelo, más dinámico que sus predecesores facilitaría la cooperación voluntaria de los dispositivos del entorno, promoviendo enfoques como por ejemplo la *testificación digital* [5]. En dichos enfoques el dispositivo del usuario forma parte activa en la gestión de evidencias electrónicas, permitiendo adquirir información sobre *ofensas telemáticas* que de otra forma pasarían desapercibidas.

Este artículo se estructura como sigue. La sección II describe la base del modelo forense y los principios de privacidad bajo los que se definen el modelo PRoFIT, así como los trabajos relacionados con este área. La sección III describe el modelo PRoFIT. La sección IV propone un escenario de ejemplo para facilitar la comprensión del modelo, en la que un cliente solicita el inicio de una investigación empleando una herramienta PRoFIT-compliant y hay varios dispositivos que pueden actuar como testigos digitales del hecho. Finalmente se detallan las conclusiones.

II. ANTECEDENTES

Proponer un modelo forense con características de privacidad significa encontrar un balance entre dos posturas tradicionalmente enfrentadas pero que deben vivir en simbiosis dado que el usuario, y sus datos, juegan un papel central en la IoT. El objetivo de esta sección es sentar las bases para la comprensión del modelo propuesto, mostrando por una parte las fases de un modelo forense (Sección A) y, por otra, los requisitos de privacidad (Sección B).

A. Modelos Forenses

Los modelos forenses están destinados a preservar la evidencia electrónica durante todo su ciclo de vida. En esta sección presentamos algunos de estos modelos. En concreto nos centramos en modelos que describen detalladamente las fases a realizar por el analista. A pesar de que el modelo propuesto toma como partida las fases de un modelo tradicional, comentamos también modelos específicos para IoT con el fin de contar con una visión amplia de las soluciones relacionadas con el área de estudio.

1) Tradicionales: En 2001 se propone el modelo DFRW como un esfuerzo conjunto por parte de investigadores, empresas y entidades legales (conocidas como LEAs por sus siglas en inglés, *Legal Enforcement Agency*), que ha sido refinado posteriormente. En [1] se puede consultar una revisión del DFRW y otros modelos posteriores basados en éste (p.ej. ADFM, IDIP, etc.). A su vez, en dicho trabajo, se propone el *Enhanced Systematic Digital Forensic Investigation Model* (ESDFIM), que propone unas fases bastante intuitivas y generales. Estas fases, que detallamos a continuación, son fácilmente adaptables a entornos más restringidos y a la vez multidisciplinares como la IoT.

Durante la fase de (1) *preparación*, se realizan las acciones necesarias previas a la investigación (p.ej. análisis de la legalidad vigente, solicitud de órdenes de registro, preparación de las herramientas para recabar información). La fase de (2) *adquisición y preservación* marca el inicio del ciclo de vida de la evidencia (identificación, obtención de las evidencias volátiles y no volátiles, etiquetado y empaquetado, transporte, etc.). Cabe destacar que el modelo considera evidencias físicas tangibles en este punto. Durante la fase de (3) *examinación y análisis* el examinador forense y los expertos en la materia examinan y analizan *el contenido* de los dispositivos digitales que fueron obtenidos legalmente y convenientemente preservados. En los modelos forenses habitualmente las siguientes fases son para la generación de informes y admisibilidad [1], sin embargo, este modelo sugiere la fase de (4) *compartición de información*, que es la habilidad de intercambiar datos relativos a una investigación entre varios países, organizaciones, personas autorizadas y tecnologías. La siguiente fase es la de (5) *presentación*. Durante dicha fase se procede a presentar a las autoridades competentes los resultados de la investigación. La admisibilidad de la evidencia electrónica depende de cómo ésta se presente durante esta fase. Finalmente la fase de (6) *revisión* compete a la evaluación del proceso de investigación de cara a su mejora. Incluye los procesos para devolver la evidencia una vez procesada (p.ej. un PC) a su dueño.

Por otra parte, la multinorma ISO/IEC 27050:2016 define las fases: identificación, preservación, recolección, procesamiento, revisión, análisis y producción. Sin embargo, escogemos como base para este trabajo el modelo ESDFIM, dado que las fases anteriores pueden mapearse fácilmente a las definidas por la norma y, además, el modelo ESDFIM define la fase *compartición de información*, no contemplada en todos los modelos ni en la norma, que es de especial interés en escenarios de la IoT por permitir la colaboración entre diferentes entidades.

2) Especificos IoT: Los modelos IoT-Forensics que definen fases para la investigación son muy escasos. Como tales, definen fases [6] y [7], siendo este último el más exhaustivo. De hecho, [7] compara su framework con otras soluciones para IoT-Forensics no reflejadas aquí ([8] y [9]), ya que no definen exactamente fases. En concreto, [6] define las fases: planificación (autorización y obtención de órdenes judiciales), IoT, adquisición de datos (identificación de dispositivo, zona, triage, adquisición de datos de las plataformas de acumulación, datos estructurados y no estructurados), cadena de custodia, análisis en laboratorio, resultado, prueba y defensa, consecución y almacenamiento. Dentro del modelo [7], las fases son más generales: proceso proactivo (definición del escenario IoT, identificación de las fuentes de la evidencia, planificación de la detección de incidencias, recolección potencial de evidencias, preservación digital, almacenamiento de evidencias potenciales), IoT-forense (*Cloud forensics*, *network forensics*, *device level forensics*), proceso reactivo (inicialización, adquisitivo, investigativo), proceso concurrente (obtener autorización, documentación, cadena de custodia, investigación física).

Estos modelos aún no consideran la posibilidad de que la adquisición que están planificando afecte a la admisibilidad de la evidencia por no respetar derechos éticos fundamentales y de privacidad. Además, cuentan con el problema añadido de que dependen de órdenes de registro en la primera fase, no considerando entornos IoT con alta densidad de dispositivos que estén dispuestos a cooperar. Por ejemplo, los *testigos digitales* [5] proponen la cooperación entre dispositivos con capacidades de seguridad para desplegar *cadenas de custodia digital* en la IoT. Sin embargo, ningún modelo forense sienta las bases que permita dicha cooperación. A consecuencia de esto, los ataques contra los dispositivos del entorno se seguirán produciendo sin que queden evidencias sobre el suceso y, peor aún, sin que las víctimas lleguen a saberlo.

En resumen, tanto los modelos tradicionales como los modelos propuestos hasta ahora para entornos IoT no están concebidos para considerar la cooperación voluntaria de los actores del entorno, que puedan actuar por ejemplo como *testigos digitales*. Este es un enfoque que aquí pretendemos abordar, y para ello necesitamos precisamente considerar los requisitos de privacidad.

B. Principios de Privacidad

Existen diversas leyes que tienen como objetivo establecer límites a la recolección, procesamiento y difusión de información de carácter personal al que nos vemos sometidos cuando interactuamos con otras entidades o servicios. Estas leyes tiene el objetivo de proteger la privacidad de los usuarios mediante una serie de normas y buenas prácticas.

En 1974 una ley estadounidense establece lo que se conoce como prácticas justas de información (FIPs, *Fair Information Practices*). Esta ley establece una serie de principios que más tarde han sido recogidos y adaptados por diversas guías [10], directivas [11] y estándares, como la ISO/IEC 29100:2011 [12], que considera hasta 11 principios de privacidad, que se detallan a continuación.

Estos principios o prácticas tienen como objetivo devolver al usuario el control sobre sus datos personales. Para ello, el usuario debe dar su consentimiento expreso a la recolección y procesamiento de sus datos personales (P1: *consent and choice*). El sistema que quiere recoger y/o procesar datos del usuario debe informarle del propósito específico para tal recolección y éste debe ser legítimo (P2: *purpose legitimacy and specification*). Además, el sistema debe limitarse a solicitar aquellos datos estrictamente necesarios para el fin especificado (P3: *collection limitation*). Es necesario minimizar la cantidad de datos que son enviados y procesados por el sistema (P4: *data minimization*). El sistema no debe utilizar la información recabada para más fines que los especificados originalmente y no debe almacenarla una vez haya servido su propósito (P5: *use, retention and disclosure limitation*). La información aportada por el data subject debe ser precisa, veraz y actual. Esto es especialmente relevante si la información no procede directamente del usuario en cuestión (P6: *accuracy and quality*). El usuario debe ser consciente en todo momento de las políticas, procedimientos y prácticas de aplicación del sistema (P7: *openess, transparency and notice*). Además, debe tener la posibilidad de acceder a los datos recolectados sobre su persona así como proponer correcciones (P8: *individual participation and access*). Por otra parte, el sistema es responsable de seguir las prácticas o principios de privacidad establecidos y, en caso de no cumplirlos, el data subject puede solicitar compensaciones (P9: *accountability*). Por ello, el sistema debe poner en práctica los mecanismos necesarios para proteger la información personal de los usuarios de accesos no autorizados, pérdidas o manipulaciones (P10: *information security controls*) y medidas que permitan auditar o verificar que se cumple con las medidas de privacidad (P11: *compliance*).

Aunque la puesta en marcha de estas prácticas no garantiza completamente un uso indebido de la información personal de los usuarios, establece una base consistente sobre la que trabajar en pos de preservar la privacidad y ayuda a los usuarios a establecer cierto nivel de confianza con aquellas entidades que solicitan sus datos.

III. EL MODELO PROFIT

El modelo PRoFIT se basa en la cooperación de los dispositivos del entorno. Esto requiere redefinir las fases de los modelos de referencia usados hasta ahora. En particular, a continuación redefinimos las fases 1-3 del modelo ESDFIM (Sección A), definiendo las siguientes fases para PRoFIT (Fig. 1): (1) preparación, (2) recolección basada en el contexto, (3) análisis de datos y correlación, (4) compartición de la información, (5) presentación y (6) revisión.

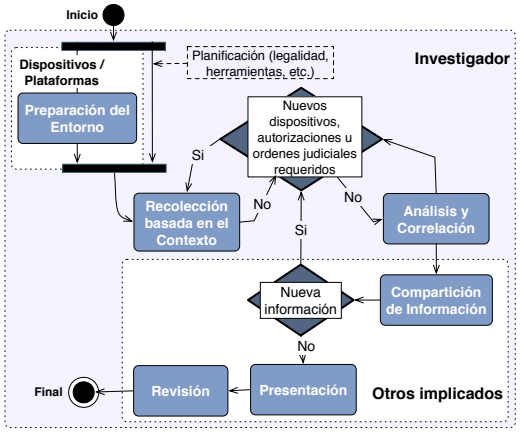


Fig. 1. Fases del modelo PRoFIT

En concreto, la fase 1 es híbrida en nuestro modelo. Esta fase se divide en dos flujos, uno para el investigador y otro para los dispositivos y/o plataformas IoT. Las fases 2-6 forman parte de la investigación forense, siendo el investigador su actor principal, aunque los dispositivos y los usuarios están involucrados para la implementación de los permisos de privacidad. Las fases 4-6 heredan los principios del modelo original (ESDFIM) mencionados en la Sección II.A. Estas fases se modifican para atender a los requisitos de privacidad que deben ser considerados. En concreto, la Tabla I resume los requisitos de privacidad considerados para cada una de las fases del modelo PRoFIT. Cabe destacar que, durante todo el proceso debe garantizarse que se cumple con los principios de privacidad. De ahí que P11 sea un principio trasversal a todas las fases.

Tabla I
REQUISITOS DE PRIVACIDAD EN LAS FASES PROFIT

Fases PRoFIT	**ISO/IEC 29100**					
Preparación del entorno	P1	P2	P4	P7		P11
Recopilación basada en el contexto	P1	P2	P3	P6	P8	
Análisis de datos y correlación	P9	P10				
Compartición de información	P1	P2	P10			
Presentación	P4	P6				
Revisión	P5	P7				

P1. Consentimiento y elección, P2. Legitimidad y especificación del propósito, P3. Recopilación limitada, P4. Minimización de datos, P5. Limitación de uso, retención y divulgación, P6. Calidad y precisión, P7. Transparencia y aviso, P8. Participación y acceso, P9. Responsabilidad, P10. Controles de seguridad de los datos, P11. Conformidad

A. Contexto de Investigación

IoT-Forensics [3] es un nuevo paradigma donde va a ser prácticamente imposible aplicar técnicas forenses eficazmente sin la información adicional de dispositivos que, a priori, tal vez no tengan nada que ver con un caso, pero que estaban en la escena de la ofensa. Para hablar de privacidad en IoT-Forensics necesitamos hacerlo en base al contexto (Fig. 2).

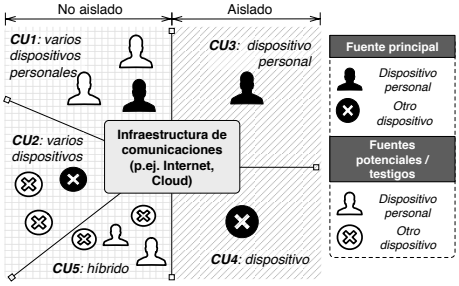


Fig. 2. Casos de uso

Simplificando el problema a un único dispositivo de entrada, que puede ser personal (p.ej. teléfono, implante) o no serlo (p.ej. dispositivos de carácter más general, como un PC del trabajo), la investigación puede consistir en obtener los datos de dicho dispositivo solamente, o requerir información de otros dispositivos - personales o no - que tengan relevancia. Distinguimos tres perfiles de dispositivo (con independencia de que sean personales) para la investigación:

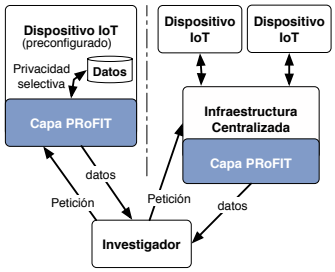
- Ofendido/víctima. Interesado directo en un caso que requiere aplicar mecanismos forenses (p.ej. demandante). Puede solicitar que se inicie una investigación sobre sus datos (c.f. caso de uso en Sección IV)
- Sospechoso. Dispositivo que puede contener evidencias electrónicas inculpatorias o bien exculpatorias y pertenece a un sospechoso.
- Testigo. Dispositivo implicado (directamente o indirectamente) en un caso por poder aportar evidencias electrónicas relevantes para la investigación, pero que a priori no es ni ofendido ni sospechoso.

B. Fase híbrida: preparación

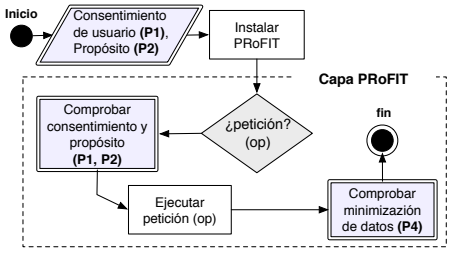
La fase de preparación define dos flujos: uno para el investigador que realiza la planificación tradicional (p.ej. preparación de herramientas forenses y otras operaciones que el investigador considere oportunas antes de la siguiente fase), y otro para la preparación del entorno IoT (dispositivos y/o plataformas).

Nos centramos en la *preparación del entorno IoT*; momento en el que los dispositivos pueden ser preconfigurados atendiendo a criterios de privacidad acordados con el usuario, p.ej. usando el software PRoFIT (Fig. 3(a)). Esto significa que cada dispositivo/plataforma recabará sólo la mínima información necesaria.

Cabe resaltar que este enfoque tiene diferentes interpretaciones y grados; puede ser tan restrictivo o laxo como se desee. Desde configurar un terminal para eliminar



(a) Preconfiguración del entorno IoT



(b) Ciclo de vida del software PRoFIT

Fig. 3. Preparación del entorno

toda la información concerniente a la privacidad de un usuario (p.ej. configurar que se borre el rastro de las aplicaciones de la memoria) - son técnicas anti-forenses, que pueden llevar a que la solución sea totalmente privada pero inservible para un análisis forense - hasta almacenar de toda la información pública a su alcance (p.ej. el usuario mantiene datos compartidos con otros usuarios que han pre-definido una relación abierta y consienten en ese nivel de privacidad abierta). Este último caso permite recabar toda la información posible, por lo que en ese caso la privacidad es obviada.

La Fig.3(b) simplifica la actividad esperada de un software compatible con PRoFIT instalado en un dispositivo IoT o en una plataforma intermedia. Conforme a los requisitos de privacidad, es necesario el consentimiento expreso del usuario (p.ej. el propietario del dispositivo o el administrador de la plataforma) sobre la instalación de este software (P1 y P2). Una vez instalado, el software controlará que las operaciones que se soliciten desde el propio sistema (p.ej. almacenar evidencia de forma local) o desde terceros (p.ej. solicitar evidencias) no interfieran con el consentimiento del usuario sobre los niveles de privacidad esperados. Una vez comprobada la petición y los derechos de ejecución, la petición se ejecuta y los resultados (p.ej. datos que deben ser enviados a un tercero o bien datos que deben ser almacenados en el dispositivo) se procesan de acuerdo al principio de minimización (P4).

C. Fases del investigador

La *recolección basada en el contexto* (fase 2) y el *análisis y correlación* (fase 3) corresponden al proceso de investigación. Ambas fases se muestran en la Fig.4(a).

Basándonos en los tres perfiles de dispositivo involucrados definidos (Sección A - ofendido, sospechoso y ofensor), durante la fase 3, el investigador recaba los datos

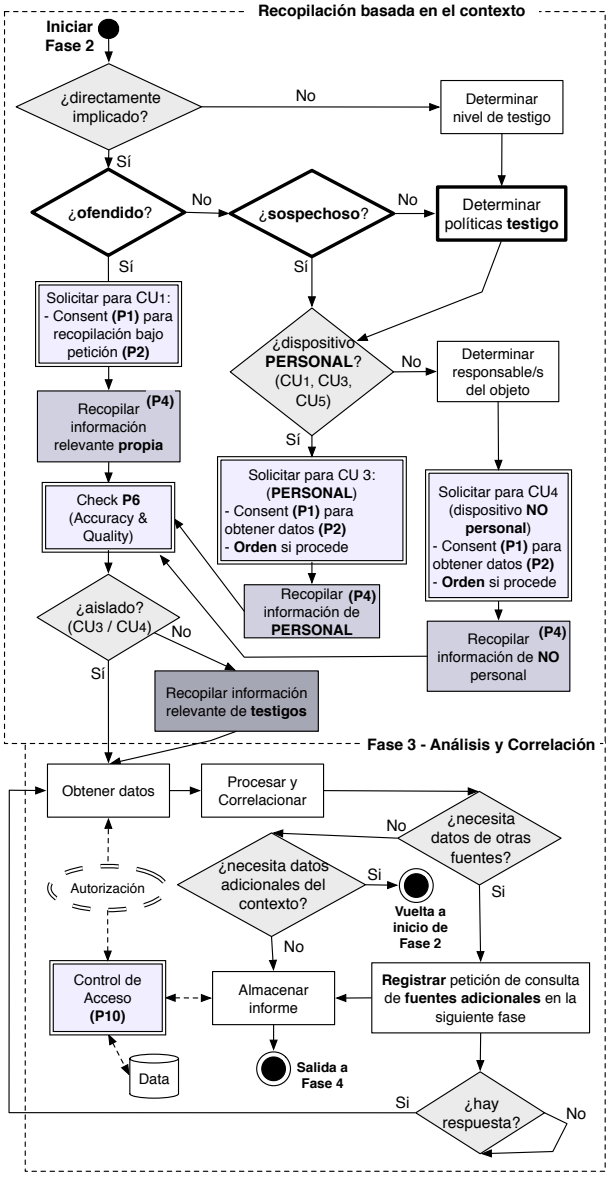
conforme al modelo PRoFIT considerando la privacidad de las fuentes. Destacamos que este enfoque se dirige a recabar las evidencias electrónicas de dispositivos que seguirán *bajo el control de sus propietarios o responsables durante todo el proceso*. De otra forma, se aplicarían los cauces tradicionales. En esta fase es donde se realiza la diferenciación entre los casos de uso (CU) a fin de establecer políticas de seguridad y privacidad de grano fino conforme al contexto.

Si el dispositivo a analizar es el *ofendido*, asumimos que se conoce la identidad del propietario del dispositivo personal, o la del responsable del dispositivo en caso de ser un objeto no personal (p.ej. porque hayan presentado una denuncia). En el consentimiento que el solicitante debe firmar (P1) tiene que constar el propósito para el que se usarán los datos (P2) - en este caso, constará que la investigación fue a petición del propietario/responsable. El investigador además debe comprobar que el dispositivo pertenece al usuario o que el responsable tiene autorización para solicitar la investigación. Entonces se realiza la recopilación de las evidencias electrónicas del dispositivo/plataforma que sean relevantes, empleando herramientas forenses, realizando pruebas para asegurar la integridad de la evidencia electrónica y documentando el proceso (P6).

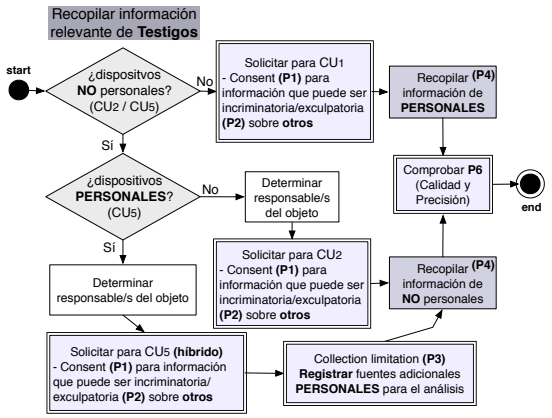
Si la investigación lo requiere, se comprueba entonces si el dispositivo estaba aislado, o si había otros dispositivos en su entorno. Por ejemplo, para determinar si hubo un posible contagio (p.ej. malware), o bien por si otro de los dispositivos tiene más datos que ayuden a la investigación del caso (p.ej. testigos digitales [5]). La Fig. 4(b) aporta información sobre los procesos a seguir para solicitar la colaboración de los posibles testigos, diferenciando también entre los diferentes contextos para determinar los responsables. Respecto a estos pasos, destacar que, considerando la propiedad P3, no se inician los procesos para el análisis de nuevos dispositivos personales si no es necesario (p.ej. si con la información recabada ya se puede resolver el caso).

Por otra parte, si el dispositivo a analizar pertenece a un *sospechoso*, los permisos solicitados serán diferentes. En este caso probablemente el investigador requiera poseer una orden judicial (*warrant*). A diferencia del ofendido o los posibles testigos, el sospechoso no tendrá un interés especial en la colaboración - a excepción de si su dispositivo contiene evidencias exculpatorias. Tanto en este caso como si el objeto es un *testigo*, deben determinarse los responsables del objeto, en caso de no ser un dispositivo personal (p.ej. porque se encuentre un dispositivo sospechoso y no se sepa quién tuvo acceso a este, o porque el testigo forme parte de una organización).

Por último, si el dispositivo va a ser analizado como *testigo*, incluimos una cláusula que indica que los datos recopilados no pueden ser usados para inculpar al testigo. Si un testigo puede ser un potencial ofensor, el investigador debe cuidarse de los datos que se recaban siguiendo este procedimiento, o no recabarlos. Cabe destacar, que si un sospechoso aporta sus evidencias electrónicas (i) se expone



(a) Preconfiguración del entorno IoT



(b) Recabar información relevante de testigos

Fig. 4. Fases - Investigador

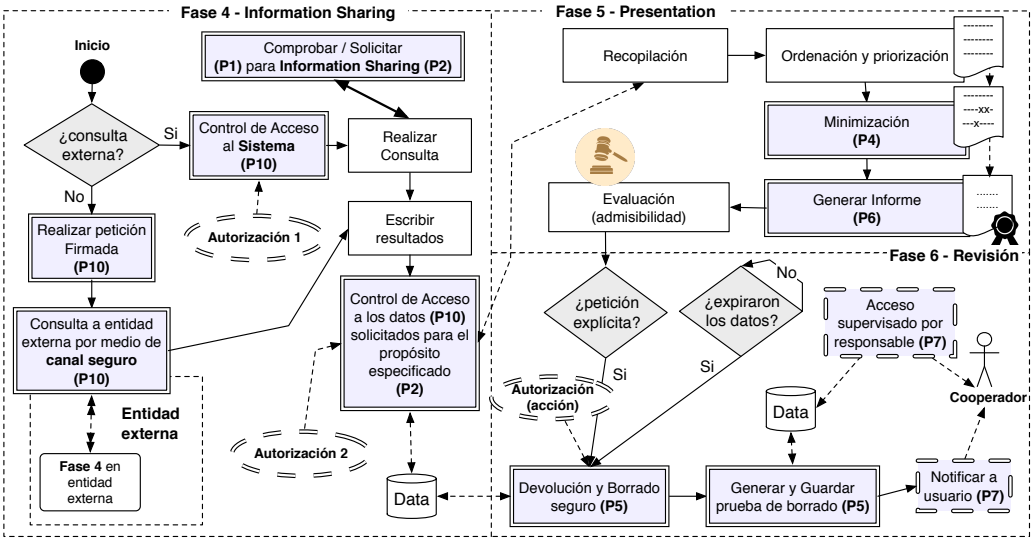


Fig. 5. Fases - Otros

a ser conocido y (ii) no invalida las evidencias electrónicas aportadas por otros, por lo que para el sospechoso resulta más sencillo eliminar sus evidencias electrónicas que ampararse en la cobertura de actuar como testigo.

Los datos recabados por este procedimiento pasan a la fase de *análisis de datos y correlación* (fase 3). Durante esta fase de la investigación se accede a las evidencias electrónicas almacenadas para su procesamiento y correlación. Como ya indicaba la Fig. 1, si durante esta fase se identifica que deben recabarse nuevas evidencias electrónicas se vuelve a la fase anterior. Así mismo, si el investigador considera que debe consultar otros datos - consultas externas - que pueden ser relevantes para el análisis, se pasa a la siguiente fase para obtener la información que sirva de retroalimentación. En ese caso, una vez que se tienen los resultados deben volver a consultarse los permisos de acceso a los datos por si durante el tiempo de la consulta - que podría tardar días o más tiempo - dichos permisos caducaron o fueron retirados.

Cabe destacar que los permisos P1 y P2 - que afectan al usuario - no se observan en esta fase, bajo la premisa de que los datos aquí tratados fueron proporcionados bajo los consentimientos proporcionados en la fase anterior.

D. Fases con participantes externos y de distinto perfil

Las tres últimas fases involucran distintos tipos de participantes. Estas tres últimas fases heredan los principios del modelo ESDFIM, aunque el modelo PRoFIT las redefine para su adaptación a la IoT y para integrar los requisitos de privacidad listados en la Tabla I. Comprende las fases de compartición de información (fase 4), presentación (fase 5) y revisión (fase 6).

La *compartición de información* involucra a usuarios externos (p.ej. otras entidades legales) con autorización para acceder a los datos. En este caso, consideramos que el propietario del objeto al que pertenecen las evidencias electrónicas tal vez no hubiese dado permisos para compartir esta información - o un resumen de ésta - con otras entidades externas, por lo que se comprueba el consentimiento dado y el propósito indicado (P1,P2). El flujo mostrado en la Fig. 5 sirve tanto para consultas sobre datos de diferentes investigaciones llevadas a cabo por la misma agencia, hasta consultas realizadas a entidades externas. Se consideran dos criterios de autorización; uno por el uso de los servicios de acceso a los datos y otra para poder realizar cambios sobre los datos.

La fase de *presentación* tiene como objeto generar el informe forense de forma que sea entendible por actores involucrados en el caso que no tienen que ser necesariamente expertos en la materia (p.ej. abogados, jueces) (Fig. 5). Considerando que durante las fases anteriores diversa información ha podido ser generada, durante esta fase se garantizará que la calidad y precisión de los datos son suficientes como para esclarecer el caso (P6). Se evitará dar más detalle del estrictamente necesario así como la aparición de datos sobre terceras partes no involucradas directamente en el caso (P4). Por lo tanto, se ordenan los resultados obtenidos y la minimización se aplica si hay datos redundantes, o bien datos que finalmente no son relevantes para el informe final. Dicho informe se genera teniendo en cuenta los requisitos de calidad (p.ej. legibilidad, entendimiento, información relevante al caso), y por último se procede a su evaluación, consistente en su admisibilidad para el caso.

Finalmente, el objetivo de la fase de *revisión* es eliminar de forma segura las evidencias electrónicas pasado un tiempo que no puede ser inferior a la duración de un caso. Entonces, se procede a eliminar el material de las bases de datos (P5) y a notificar al usuario de su eliminación. Este paso de notificación, así como el acceso supervisado para que el implicado compruebe que no constan sus datos (P7), son opcionales pero necesarios. Durante esta fase también se devuelven las posibles evidencias físicas (p.ej. PC) de haberse combinado el enfoque PRoFIT con los procedimientos tradicionales.

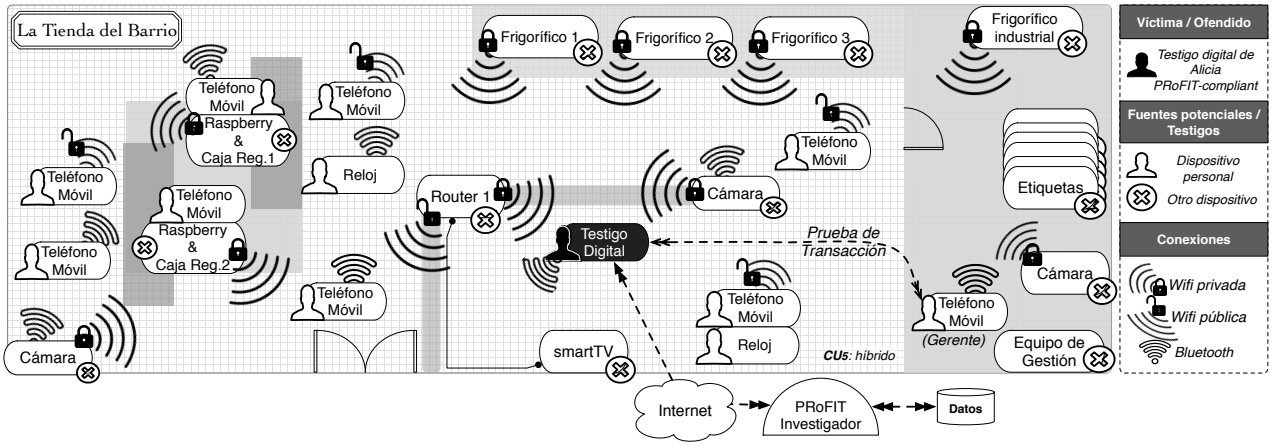


Fig. 6. Caso de uso 1: tienda de comestibles

IV. CASOS DE USO - TESTIFICACIÓN DIGITAL

En esta sección se propone dos casos de uso que se enfocan dentro del contexto de *testificación digital* [5]. Un testigo digital es un dispositivo IoT con características de seguridad probadas capaz de recolectar y salvaguardar evidencias digitales de su entorno. Suponemos que los testigos digitales que se muestran en estos casos de uso son *PRoFIT-compliant*. Esto significa que el software preinstalado en los testigos digitales, cuyos requisitos básicos se definen en [5], se encuentran adaptados para implementar las fases del modelo PRoFIT descritas en la sección III.

El primer caso de uso muestra un escenario de infección por malware en el que se pone de manifiesto la flexibilidad del modelo PRoFIT, mientras que el segundo caso de uso muestra un escenario en el que es necesaria una orden de registro. En este último caso, las opciones de privacidad son prácticamente nulas, no obstante también se siguen las fases del modelo PRoFIT. Mostramos así que el modelo propuesto permite balancear las características de privacidad según el contexto, y que los casos más tradicionales/restringidos basados en órdenes judiciales siguen respetándose.

A. Malware social - La tienda del barrio

Alicia tiene un teléfono móvil con software PRoFIT instalado (fase 1). Supongamos que Alicia entra en una tienda en la que hay varios dispositivos IoT, tanto personales como no personales (Fig. 6).

Durante su estancia en la tienda, el teléfono móvil de Alicia detecta un ataque que procede de un dispositivo del entorno. Tras detectar el ataque, el software PRoFIT decide almacenar la información relativa al mismo. Además, hace un hash a las evidencias recabadas y alerta a Alicia. Parece que algún dispositivo del entorno está infectado e intenta propagar un gusano aprovechando una vulnerabilidad en la aplicación *deals4U*, que utiliza la tecnología Bluetooth para escanear otros dispositivos del entorno y así conocer las ofertas del día y el número de unidades de alimentos disponibles (p.ej. en los frigoríficos).

Tras ser notificada de la ofensa, Alicia, que decide que este incidente debe ser reportado lo antes posible, envía las evidencias almacenadas al sistema PRoFIT, solicitando así el inicio de una investigación forense (fase 2). Entonces, el sistema asigna un investigador PRoFIT para el caso, que analiza los datos proporcionados (fase 3) y confirma que se trata de un ataque lanzado de forma local. Sin embargo, no tiene evidencias suficientes para poder llevar a cabo la investigación y sugiere al agente PRoFIT instalado en el dispositivo de Alicia recabar nuevas evidencias de otros dispositivos que quieran colaborar (vuelta a la fase 2).

Siguiendo la metodología (Sección III), el agente local PRoFIT pregunta primero a los dispositivos no personales, buscando a su responsable, en este caso el gerente de la tienda (derecha Fig. 6), para obtener la autorización. El responsable accede a colaborar y autoriza que sus dispositivos envíen información al investigador PRoFIT, usando el agente PRoFIT de Alicia como pasarela. Esta información se cifra y firma, y el agente tiene que emitir una prueba de que estos datos fueron enviados al agente PRoFIT remoto. El gerente de la tienda puede usar esta prueba para solicitar al investigador PRoFIT tanto (i) una comprobación de los datos que ha proporcionado, como (ii) retractarse y solicitar la eliminación de su declaración.

A la luz de las nuevas evidencias aportadas por el gerente de la tienda (fase 3), los resultados de la investigación apuntan a que el malware está latente en una de las Raspberry Pi de las cajas registradoras y que llegó a través del router, según los logs de este último. A partir de aquí la investigación continúa con el objetivo de llegar al origen del problema. Para ello, Alicia consiente que los datos proporcionados puedan ser compartidos con terceras partes (fase 4).

Tras unos días, una versión mejorada del malware causa daños en otros dispositivos IoT. Afortunadamente, el sistema PRoFIT guardó información sobre los inicios del ataque. La correlación con otras pruebas de un sistema externo permite determinar la procedencia del malware y se detiene a un sospechoso. Entonces, algunos de los datos aportados por Alicia y otros dispositivos se utilizan para elaborar el informe final (fase 5), que finalmente es admitido a juicio. Tras producirse la sentencia y transcurrido

un tiempo, los datos de los cooperadores son eliminados del sistema PRoFIT (fase 6).

Aunque este es un escenario hipotético y el malware, así como la aplicación *deals4U*, son ficticios, no es descabellado que ataques de este tipo pudieran producirse (o se estén produciendo) sin que el usuario lo perciba [13].

B. Registro en un almacén

El agente de policía Juan tiene un dispositivo que es testigo digital con capacidad de custodia, es decir, un *custodio digital*. Este tipo de testigo digital tiene privilegios en cuanto a que pertenece a un agente de la ley.

Juan tiene que realizar un registro en un almacén en el que hay varios dispositivos IoT (p.ej. cámaras, sensores y actuadores, etc.). Se sospecha que alguno de los dispositivos guarda evidencias electrónicas que pueden ser claves para resolver una investigación.

Para realizar el registro eficazmente, en el custodio se almacena una orden de registro firmada y es preconfigurado para recabar evidencias relevantes para el caso, conforme a los permisos y propósitos detallados en la orden judicial (fase 1). Nótese que, en este caso, la primera fase ejecuta ambos flujos de preparación: la tradicional - adaptada para automatizar la recogida de evidencias electrónicas - y del dispositivo IoT (Fig. 1).

Durante el registro, Juan es el especialista encargado de almacenar las evidencias digitales volátiles usando su custodio digital. Para ello, su dispositivo escanea la red del almacén y guarda el estado de las conexiones. También recibe los volcados de memoria y otros datos que Juan decide almacenar en el dispositivo. Todos estos pasos se hacen obviando las solicitudes y consentimientos de usuario porque se tiene una orden judicial para llevar a cabo los procedimientos que está realizando cabo Juan.

Una vez en el laboratorio, durante el análisis (fase 3) los datos recabados se procesan y se extraen las evidencias electrónicas relevantes para la investigación. En este caso particular, no se requieren consultas a bases de datos externas (fase 4). Los informes finales se redactan (fase 5), las evidencias son aceptadas para su vista y, transcurrido un tiempo, los objetos recabados durante el registro, de los que se extrajeron las evidencias, se devuelven a su dueño (fase 6).

V. CONCLUSIONES Y TRABAJO FUTURO

En este artículo definimos el modelo PRoFIT para la investigación forense en entornos IoT. A diferencia de otros enfoques, este modelo integra requisitos de privacidad (ISO/IEC 29100:2011) como parte de su metodología. El objetivo es promover la cooperación controlada de dispositivos IoT - personales o no - en investigaciones forenses. Para facilitar la comprensión del modelo se desarrollan dos casos de uso - análisis de la propagación de malware en una tienda de comestibles y recabación de evidencias electrónicas en base a una orden de registro.

Como trabajo futuro, queremos extender el trabajo actual para definir cómo usar este modelo en el contexto de la testificación digital, como un mecanismo de mitigación para los problemas de privacidad que pueden encontrarse en este tipo de contextos.

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 SMOG (TIN2016-79095-C2-1-R) e IoTest (TIN2015-72634-EXP).

REFERENCIAS

[1] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A review and comparative study of digital forensic investigation models," in *International Conference on Digital Forensics and Cyber Crime*. Springer, 2012, pp. 314–327.

[2] 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.

[3] 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.

[4] T. Geller, "In privacy law, it's the us vs. the world," *Communications of the ACM*, vol. 59, no. 2, pp. 21–23, 2016.

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

[6] 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.

[7] 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.

[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. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 279–284.

[10] Organisation for Economic Co-Operation and Development (OECD), "The OECD Privacy Framework," 2013, [Last Access: 02/2017]. [Online]. Available: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[11] The European Parliament and the Council of the European Union, "Regulation (eu) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," 2016, [Last Access: 02/2017]. [Online]. Available: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[12] *ISO/IEC 29100:2011 - Information technology - Security techniques - Privacy framework*, JTC 1/SC 27 Std., 2011. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

[13] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 925–941, 2014.