A. Nieto, R. Rios, and J. Lopez, "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach", *16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017)*, pp. 642-649, 2017.
http://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.295
NICS Lab. Publications: https://www.nics.uma.es/publications

Digital Witness and Privacy in IoT: Anonymous Witnessing Approach

Ana Nieto, Ruben Rios and Javier Lopez
Network, Information and Computer Security (NICS) Lab
Computer Science Department
University of Malaga, Spain
Email:{nieto,ruben,jlm}@lcc.uma.es

***Abstract*—The *digital witness* approach defines the collaboration between IoT devices - from wearables to vehicles - to provide digital evidence through a *Digital Chain of Custody* to an authorised entity. As one of the cores of the digital witness, *binding credentials* unequivocally identify the user behind the digital witness. The objective of this article is to perform a critical analysis of the digital witness approach from the perspective of privacy, and to propose solutions that help include some notions of privacy in the scheme (for those cases where it is possible). In addition, *digital anonymous witnessing* as a tradeoff mechanism between the original approach and privacy requirements is proposed. This is a clear challenge in this context given the restriction that the identities of the links in the digital chain of custody should be known.**

I. Introduction

The *Internet of Things* (IoT) poses challenges in many sectors, including forensic computing[23]. This is a discipline that is beginning to be consolidated, due to the efforts of several organisations, (e.g., the ENFSI-FITWG in Europe or the SWGDE in the United States) in new models and standards (e.g., ISO/IEC 17025:2005, ISO/IEC 27037:2012, ISO/IEC 27042:2015, ISO/IEC 27050:2016+) and entities responsible for the accreditation of digital forensic laboratories (e.g. ASCLD-LAB). Over the years several tools have been developed that greatly simplify the identification and extraction of digital evidence from a wide portfolio of devices.

Of course, this consolidation does not cover the latest technological changes that are occurring thanks to the widespread acceptance of the IoT paradigm. Therefore, there is no clear consensus on the protocols to follow or tools to use in highly dynamic, dense and heterogeneous scenarios where multiple devices could be victims of local offences or attacks propagated over the network. In this regard, the popular *Advanced Persistent Threats* take advantage of the lack of security controls in personal devices. The attacker introduce malware into infrastructures that are supposed to be protected or even isolated, using the personal devices or objects of their workers, clients or users as input vehicles. Moreover, cybercriminals are using the IoT for their own benefit; taking advantage of the high density of devices to hide their criminal activity, or using the security mechanisms to coordinate among themselves. This lack of control in IoT devices and platforms is generating several problems. Furthermore, these new paradigms require new, faster, and more efficient tools and procedures to collect digital evidence without compromising its admissibility in a court of law.

Specifically, *Digital Witnessing* is a novel approach to deploy *Digital Chains of Custody in IoT* (DCoC-IoT) scenarios, needed to carry digital evidence from a personal device to an authorised, *Official Collection Point* (OCP) [13]. Thus, this approach aims to bridge the gap between forensic computing and citizens, emphasising the cooperation of personal devices with *proven security features*. The existence of these new, more flexible solutions helps define new ways of collecting digital evidence and, they are therefore, changing the involvement of the user in these new paradigms.

However, how this distributed approach affects user privacy, may be questioned more than ever since it is based on the use of *personal devices*. As the first approach of this nature, a detailed privacy analysis of it will lay the foundation for future research work.

The contributions of this paper are:

- We define the phases of the *digital witness* within ISO/IEC 27050:2016 [1] (electronic discovery), and then map them to the lifecycle of personal data [16].
- We analyse the approach of *digital witnessing* from the perspective of privacy, highlighting the privacy requirements that should be considered.
- We propose solutions to balance the properties of the digital witness and the privacy requirements identified during the analysis.

This paper is organised as follows. Section II discusses the related work. Section III describes the fundamentals of the *Digital Witness* (DW) approach and analyses its relationship with the phases of ISO/IEC 27050:2016 and personal data. Section IV breaks down the use cases in the DW schema, which are discussed in Section V. Section VI proposes some mechanisms that could help define *anonymous witnessing* in the IoT and also implement other privacy requirements identified in Section V.

II. Related Work

There is a clear tradeoff between computer forensics and privacy, as stated in [2], where a network-layer capability called privacy-preserving forensic attribution is proposed to find a balance between privacy and network forensics. These authors discuss the use of group signatures as part of the schema. In [3] it is assumed that network forensics may violate the privacy of honest users and therefore proposes a protocol that offers privacy to honest users whilst holding attackers accountable. Indeed, mobile forensic methodologies have been used to assess the privacy of mobile applications in [21], focusing on *data at rest* (data recorded on storage media, e.g. SD card).

The digital witness approach poses a new and radical approach to the collection of digital evidence and its processing in the IoT [13]. Although this solution is within the scope of a recent topic denoted IoT-forensics [14], none of the solutions proposed so far depend on both the user and his/her personal devices as part of the solution to this highly complex problem. Other solutions related to IoT-forensics focus on proposing new models for the analysis [15], or in defining the concept of *Digital Chain of Custody* (DCoC) [17]. Although these approaches do not consider the problem of privacy, it is undoubtedly one of the main problems that need to be addressed in solutions for the IoT and should therefore be considered [5].

III. Digital Witness - Overview

The *digital witness* approach is defined in [13]. A digital witness is a *personal device* that is capable of identifying and collecting digital evidence, preserving it in a protected space, and sending it to other digital witnesses who are authorised to participate in the safeguarding of digital evidence. The aim is to provide a mechanism by which it is possible to deploy the *Digital Chain of Custody in the IoT* (DCoC-IoT). Thus, the digital evidence is sent from a digital witness to a final entity, the *Official Collection Point* (OCP), for further analysis and processing, following the processes of ISO/IEC 27050:2016 (Fig. 1).

It should be noted that, unlike other solutions for the management of digital evidence in the IoT (c.f. Section II), the DW-approach focuses on the collaboration of personal devices in the capillary network. In ISO/IEC 27050:2016 this kind of scenario is not considered. Therefore, the mapping between the phases of the standard and the DW approach is not direct, and is divided into two blocks as shown in Fig. 1. The first block is performed by the digital witness, and groups the phases of identification, preservation and collection (but local, at the device). The second block is performed by the OCP, and groups the phases of collection (from various sources), processing, review, analysis and production.

Fig. 1 also shows the mapping between the phases of a DW approach and the phases for the data lifecycle [16]. Unlike ISO/IEC 27050:2016, the digital witness must consider the *privacy requirements to transfer data*. This phase is not defined in the standard because it is assumed that during the forensic analysis process the data are not transferred. Rather they are part of a closed investigation whereby the digital evidence is obtained in person by authorised experts in the field. However, the DW approach is more flexible in this regard; it allows collaboration in the capillary network, subject to the deployment of DCoC-IoT between the cooperators - devices or entities authorised to act as digital witnesses. In order to be considered as a potential candidate to be a digital witness, a device must implement the following properties [13]:

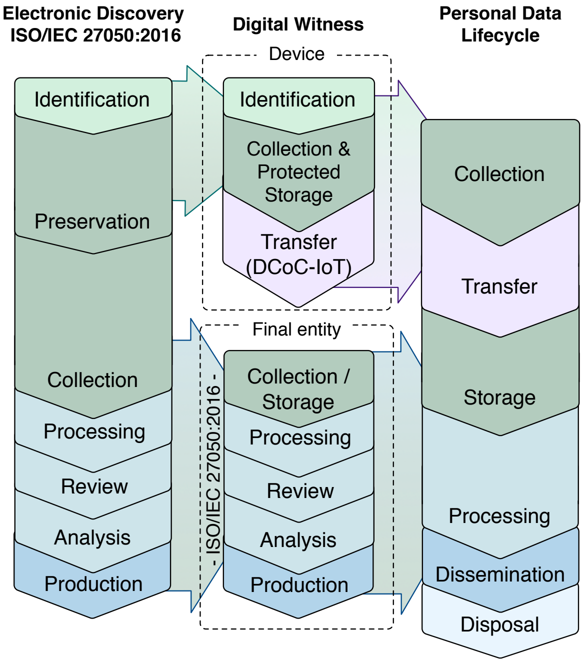


Fig. 1: ISO/IEC 27050:2016, Digital Witness and Data

- *Anti-tampering Behaviour*. A digital witness requires an anti-tampering *Trusted Computing Hardware* (TCH) embedded inside the device to check its integrity periodically (e.g. secure element, TPM). In the case an integrity check fails, or a malfunction is detected, the digital witness invalidates itself. If the device is corrupted in any way it cannot participate in the DCoC-IoT.
- *Binding credentials* (BC). The result of binding the user's identity to his/her device is a *binding credential*. This allows the digital witness to perform actions *on behalf of its user*. It means that when it collects and transmits the digital evidence, it signs the proof of integrity using these credentials that unequivocally identify the person who is responsible for the device. The objective is to discourage the misuse of the digital witness - to report false digital evidence should be a punishable offence.
- *Binding Delegation* (BD). The procedure by which a DCoC-IoT is deployed. This capability allows the transmission of digital evidence to other authorised digital witnesses, following a set of guidelines which depend on the capabilities and the roles of the devices (Section IV).
- *Accepted procedures (e.g. phases, cryptographic mechanisms) by the standards for digital evidence management*. A DW will act following a set of well-defined and established standards for the digital evidence management process. Specifically, in this paper we follow the phases published in ISO/IEC 27050:2016+ [1].

The digital witness approach defines different user and device profiles. Therefore, this solution has its own requirements for deployment that can be in conflict with known, desired privacy requirements (e.g. anonymity). One of the requirements of this solution is particularly challenging: the user must consent to link his/her identity to the personal device that will act as a digital witness.

Although some *privacy policies* are defined in [13] to ensure that (i) the user can choose what data is being collected by his/her device and (ii) understands and consents to the terms of the service, these options are insufficient to solve all the privacy requirements that could be demanded in a scheme like the one proposed.

IV. Use Cases

The analysis of privacy requirements for digital witnesses is based on the following use cases - and the main actors - shown in Fig. 2.

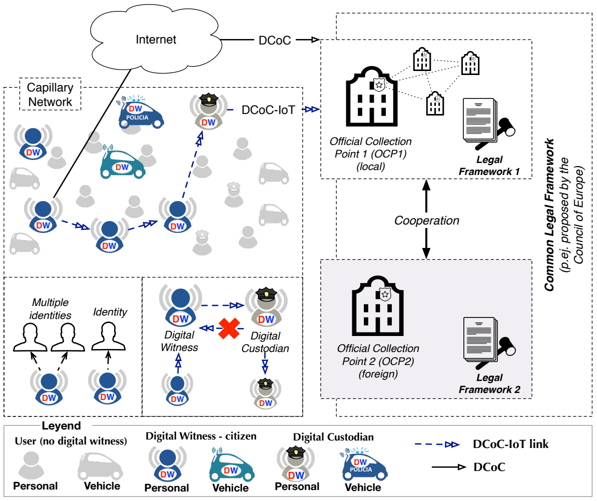


Fig. 2: Use cases

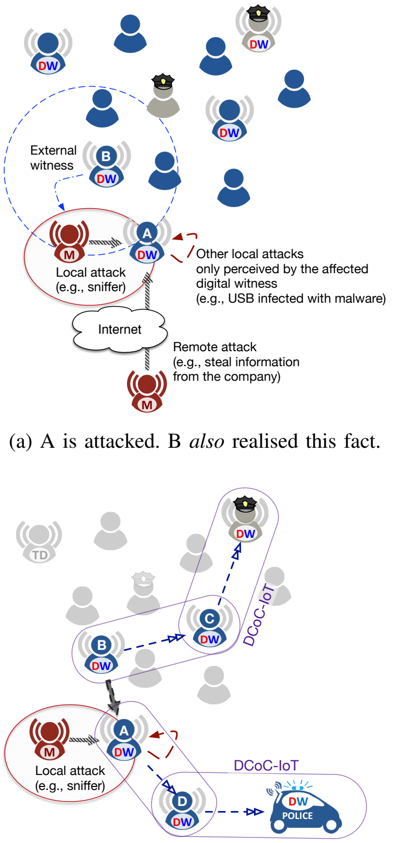
The solution of digital witnesses focuses on deploying DCoC-IoT in the capillary network, composed of other digital witnesses that can have two profiles or roles: *citizen* - denoted as a digital witness - or custodian - denoted as a *digital custodian* (DC), the latter being a digital witness with privileges. In addition, within these two general profiles the devices are classified according to their capacity to offer security mechanisms accepted by the standards of digital evidence management. Therefore, this approach establishes a hierarchy in which a digital custodian never delegates its electronic evidence to a basic digital witness. In addition, a digital witness could have several linked identities (e.g. a police car).

The origin of a DCoC-IoT is a digital witness registered in a *Official Collection Point* (OCP) where the digital evidence will be collected, as described in Section IV-B. A DCoC-IoT can be formed by several links, where each link is an intermediary digital witness. It is also possible to send the digital evidence to the OCP using traditional DCoC (Section II). The OCP is the entity that certifies that a device satisfies the requirements to act as a digital witness. Therefore, a digital witness will act in accordance with the specific *legal framework* of its OCP.

A. Collaboration in the Capillary Network

The collaboration between digital witnesses takes place in the capillary network. As Fig. 3 shows, there are four basic participants:

- Digital witness whose owner is offended party (A)
- Third-party witnesses to an offence (B)
- Digital witnesses, which are links in a DCoC-IoT (C, D)
- Digital custodian


DW
External witness
B
A
M
Local attack (e.g., sniffer)
Other local attacks only perceived by the affected digital witness (e.g., USB infected with malware)
Internet
Remote attack (e.g., steal information from the company)
TD
C
D
DCoC-IoT
DCoC-IoT
POLICE

(a) A is attacked. B *also* realised this fact.

(b) B can tell A that he was there (or not), and also send the digital evidence.

Fig. 3: Actors in the Capillary Network

Two types of attacks can be detected by a digital witness, as shown in Fig. 3a: local attacks (e.g. using Bluetooth) and remote attacks, which are difficult to trace back to the source (the attacker) but which could be detected by the trace left in the device. The digital evidence in the second case can only be collected by the digital witness itself. In the first case other digital witnesses could see the offence and report it.

When the digital evidence is stored in a protected space, the digital witness can (a) delegate the electronic evidence to any other digital witness as soon as possible (c.f. *D* in Fig. 3b) or (b) store the digital evidence until it finds a digital custodian - or the OCP - and then delegate it. It may also be possible that another digital witness B - and not the affected device A - detects the attack (e.g. the case of an attack on the local network) and reports it to the authorities. This is the reason why, in Fig. 3b, two DCoC-IoT are shown for the same offence.

It should be noted that A could have detected the attack but decided not to initiate the DCoC-IoT. For example, if A is not moving, or the digital witnesses around it do not meet its transmission policies. In this case, B will report the offence before the victim does.

Note that in Fig. 3b B could also decide to inform A as to its presence at the scene, and this information could be included in the report delivered by A to the digital custodian. This will depend on the policies configured in B, and the capability and willingness of A to generate a joint report/declaration about the offence committed.

B. *Official Collection Points*

The *Official Collection Points* (OCP) receive digital evidence that is processed and correlated. The results of these analyses contribute to the prosecution of the attackers but only if they are *admissible* in a court of law. An example of an OCP is a police officer who has been authorised for this purpose (e.g. just as digital forensic laboratories can be certified, guidelines should be created to define the requirements to certify OCPs).

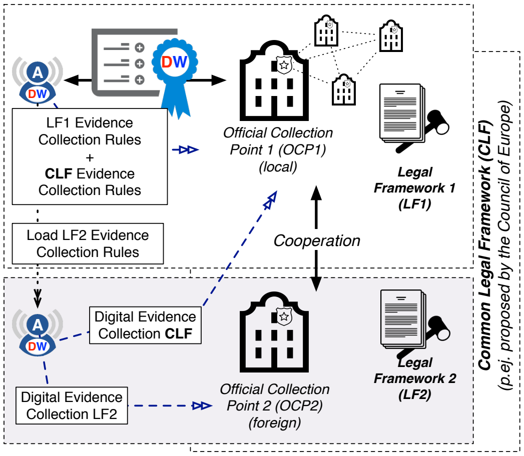

A
DW
DW
LF1 Evidence Collection Rules + CLF Evidence Collection Rules
Load LF2 Evidence Collection Rules
Official Collection Point 1 (OCP1) (local)
Legal Framework 1 (LF1)
Cooperation
A
DW
Digital Evidence Collection CLF
Digital Evidence Collection LF2
Official Collection Point 2 (OCP2) (foreign)
Legal Framework 2 (LF2)
Common Legal Framework (CLF)
(p.ej. proposed by the Council of Europe)

Fig. 4: Digital Witness A (LF1) in LF2

Fig. 4 shows the three actors considered in this use case:

- Digital witness that changes jurisdiction (A), registered in its local OCP (OCP1).
- Local OCP (OCP1 in Fig. 4).
- Foreign OCP (OCP2 in Fig. 4).

The local OCP receives the digital evidence from the digital witnesses under its jurisdiction. In turn, relationships can be established between different OCPs within the same legal framework (e.g. OCPs in the same country with the same legal framework). However, we must also consider what happens when the digital witness moves beyond the jurisdiction of its OCP.

When a digital witness arrives at a location where the OCP does not have jurisdiction, it has two options: (a) to act in accordance with the legal framework of the foreign OCP, or (b) to act in accordance with the common legal framework that covers both OCPs (e.g. European Legal Framework if both OPCs are countries of the European Union). Option (b) may not be possible if a common legal framework (or a similar legal agreement between the countries) does not exist.

V. Analysis

A *digital witness* (DW) is a solution for collecting digital evidence, defined considering computer forensic principles for its admissibility in a court of law (e.g. preservation, traceability). Therefore, the properties of a DW are defined based on these principles, which, in fact, can affect privacy as described in the following paragraphs and summarised in Table I.

The analysis considers a set of questions for the *investigative process* and the *admissibility* of the digital evidence. Privacy issues may arise if it is possible to deduce information from *other individuals* that are not strictly related to the investigation, or if this information can be inferred by unauthorised entities due to an incorrect implementation of the DW properties.

A. *Questions for the investigative process:*

1) Who is the victim/offended party?: An offence is not a crime (four conditions are necessary for the latter: i) *actus reus*, ii) *means rea*, iii) *concurrence* and iv) *causation*); it is quite subjective and it is related to what a person considers *unfair*. When a digital witness reports the digital evidence, it is considering *what is offensive to his/her user*, given the user's consent and policies. For example, it may be offensive that some software attempts to change the application code (internal device offence), but it could also be an attack on *another device in the network*. In the latter case, the offence mainly affects *another/s*, but the user of the digital witness wants to report it (B in Fig. 3b).

We focus on the latter case - a digital witness reporting an offence concerning *another* device. Perhaps the victim does not wish to report the offence (e.g. because what happened is not offensive to him/her, or has occurred in a place he/she prefers to keep secret). So, there are three privacy requirements that are not being considered: *anonymity*, *re-identification* and, potentially, *location privacy*. First, in the case the offended party has a digital witness, it is possible to know his/her identity because he/she is registered in an OCP. Second, even if the offended party does not have a digital witness, it is possible to deduce his/her identity using the contextual information provided to the OCP (e.g. by correlation). Third, the digital witness that reports the offence may consider that the location is relevant to the investigation - even if it is not.

2) Who was present?: Normally, when an offence is committed there will be several actors present, not just the potenially offended party and offenders, but also other devices will probably be around, whether they are digital witnesses or not.

If a digital witness is reporting an offence and giving information about the environment, it may be giving information about the other witnesses present. Unlike the previous question (*who is the offended party?*) in this case the digital witness is giving information about users who are simply at the scene, without necessarily being directly involved. Therefore, in this case the DW approach allows the violation of the following properties: *anonymity*, *unlinkability* and *location privacy*. This may discourage the use of the DW by those users who want to use this technology just to send their own digital evidence and *remain invisible* to the rest of the participants. To mitigate this, the implementation of the digital witness should consider the silent / opt-out option.

Finally, a digital witness is *disabled* if (a) it has some functional problem, or (b) the device's integrity check failed. Then the device can no longer act as a digital witness until these problems have been solved and it can prove that it is once more trustworthy. However, if the state of the digital witness once it has been disabled is known by other devices, then there are potential problems of *state confidentiality*, and *attestation privacy* if the state is known due to the attestation procedure before deploying the DCoC-IoT. In addition, this may attract attackers attempting to take advantage of the vulnerabilities in the device.

3) Where did the event occur? When? For how long?: The location privacy of all the digital witnesses directly or indirectly involved in a DCoC-IoT is affected. This has already been discussed above. However, there are cases in which an offence is not necessarily local (e.g. Fig. 3a- an attack can be external to the local network) and even in these cases the location of the offender and the links in the DCoC-IoT will be known. Other contextual information (*When? For how long, etc?*) may equally affect privacy depending on the implementation of the digital witness approach. For example, the *time stamping* procedures when a *Trusted Third Party* (TTP) is involved should guarantee that the TTP can sign the data (in this case the digital evidence) without knowing its content. Perhaps a solution would be to sign the hash of the digital evidence that is sent as proof of its integrity.

4) Were others affected?: Answering this question involves (i) identifying whether the same notification of the event was recived *in the OCP* but from another source (e.g. a DCoC-IoT from another victim) or (ii) *the DW* is able to ask others in its environment if they have suffered the same offence, and in that case, complete the digital evidence with data provided by others by mutual agreement. The first case reflects that digital evidence about the same event may be received from multiple sources. Therefore the number of identities involved as intermediaries in a DCoC-IoT grows as more digital witnesses report the offence. This may cause *data collection* problems, in turn causing *congestion* but it also allows the collected digital evidence to be contrasted when it is taken from different sources. The second case requires asking for other digital witnesses in the environment, affecting the *location privacy*. However, in addition, each digital witness will need a proof of the outcome of the transaction in the collaboration - either because it collaborated as a DCoC-IoT link or because it provided its digital evidence to help other digital witnesses. The *transactional privacy* could be affected by these collaborations if the results are revealed to other devices that have not participated in the collaboration.

B. Questions for admissibility:

1) Where is the data from?: The objective of this question is to know the *provenance* of the digital evidence. More specifically, the term provenance refers to the *chronology of the ownership, custody or location* of the digital evidence - and refers to *where*, *how* and *who* was involved during the lifecycle of the digital evidence. The *traceability* of the digital evidence is required to ensure its provenance.

So, answering this question affects the *anonymity*, since the digital witness approach as it is currently defined does not allow *anonymous witnessing*. The user's identity is linked to his/her digital witness by using the binding credentials to discourage misuse of the DW. However, this restriction prevents well-meaning users from using their digital witnesses to anonymously report an offence which needs to be reported but in which they would rather not be involved (e.g. because they know the attacker and could be subject to retaliation).

2) Who has had access to the data during the DCoC-IoT? Which participant and what type of access?: The list of digital witnesses that have had potential access to the data must be transparent to the OCP in order to ensure the *traceability* property and establish accountability for possible misconduct, in addition to those that the device itself can have (anti-tampering behaviour, Section III). The DCoC-IoT must include information about all the DWs that participated in the binding delegation, including all failed binding delegation attempts (e.g. attempted to transmit digital evidence to a DW that suddenly disappeared from the network or refused the connection). All this information should be transparent, at least, to the OCP.

It should be noted that this transparency in the DCoC-IoT does not maintain the principles of *unobservability* and *undetectability*, which establish that the existence of communications should not be observable by third parties and, if so, it should not be possible to determine who is communicating. How the digital witnesses advertise their presence to other digital witnesses is critical in evaluating the degree to which these properties are not being met.

In addition, the digital witness follows a set of *local policies* to eliminate stored digital evidence which are configured by the user [13]. These options concern the user's data in his/her digital witness but do not take into account the preferences of *other DW contributors* in how to delete their data. This also concerns the digital evidence finally stored in the OCP. In short, the cooperating digital witnesses do not have control over the data they provide as digital evidence and there are no defined mechanisms for consulting their data.

3) Did the digital witness act in accordance with the legal framework and respecting ethical principles?: A digital witness must act in accordance with a *legal framework*. However,

TABLE I: Relationship between DW Properties, Privacy Requirements and Mitigation Methods proposed

Property DW	Capillary Network			Official Collection Point		
	Purpose	Privacy Required	Mitigation	Purpose	Privacy Required	Mitigation
Anti-tampering Behaviour	Trustworthy links in the DCoC-IoT Preservation	Status Confidentiality Privacy Attestation	Direct anonymous attestation Opt-out / Silent	Trustworthy device	Users data in OCP	Users in OCP users consent
Binding Credentials	Responsability Access Control	Anonymity	Anonymous DW: Crowd-like Group signature	Responsability	Anonymity	Multi-Party Declaration
Binding Delegation (DCoC-IoT)	Traceability Preservation Provenance	Anonymity, Unlinkability, Unobservability, Undetectability, Location,Transaction	Privacy-based route discovery Blockchain Smart Contracts	Traceability Correlation (different sources) Provenance	Data collection (multiple sources) Location privacy re-identification	Key group OCP
ISO/IEC 27050:2016	Final acceptance (well known and accepted procedures)	Disposal (link data)	Consents (others) Proof of secure erasure	Final acceptance (well known and accepted procedures)	Disposal (stored data)	Proof of secure erasure

this can change depending on the location of the DW (Fig. 4). So, the *location privacy* is affected if he/she has to reveal where he/she is in order to comply with the legal framework. Furthermore, if the behaviour of the digital witness depends on the legal framework, unauthorised third parties could deduce the location of the user by monitoring how his/her device behaves. Since it has been proved that there are attacks directed specifically to devices based on the country where they are located [8], this exposes the user to these attacks if this information becomes known.

Finally, in the case of cooperation between OCPs of different jurisdictions, the initial *agreements* that the user's digital witness has with each OCP must be respected. In some cases the owner of a DW may be interested in this cooperation (e.g. an offence requiring that a citizen or entity should be compensated, in the country being visited, is reported). In other cases cooperation may be necessary in the case of complaints against a foreign digital witness. For example, if, in Fig. 4 A attempts to collect digital evidence without updating to LF2 (and this is reported by digital witnesses to OCP2), then OCP2 may choose to report this event to OCP1. The user of A should be notified of this procedure as it would be if it were a traffic ticket.

C. Synthesis: Approachable Privacy Requirements

A summary of the privacy-related properties that are affected in the use cases (Section IV) based on the results of the previous analysis is shown in TABLE I.

It is clear from the aforementioned questions that the current definition of the digital witness approach allows *other devices* in the environment - and not only the OCP and authorised digital witnesses - to obtain information about users who were not even directly related to the offence, or deduce information which is not relevant to the investigation. One of the main reasons for this, is that digital witnesses act transparently to allow the *traceability* of digital evidence in the DCoC-IoT. Thus, even if the user has configured the privacy options for his/her digital witness, he/she is exposed by the activity of other digital witnesses who can report information about their environment (e.g. failed DCoC-IoT deployment attempts).

In addition, the cooperation between OCPs should be governed by the agreements between the existing legal frameworks and will depend on the specific deployment environment. In any case, we assume that the OCPs are not resource-constrained entities and, therefore, more robust security solutions can be deployed to ensure collaboration between legal entities. Therefore, the most significant privacy challenges lie in the capillary network.

While the link between the user's identity and his/her device is a key piece in the definition of the digital witness approach [13], mitigation mechanisms should be proposed that allow balancing this solution to protect personal data that (i) are not relevant to an investigation or (ii) are not necessary for the primary purpose of the digital witness - that is, to delegate the digital evidence to the OCP without risking its admissibility.

VI. Mitigation Methods

This section describes potential solutions that could be adopted to implement some privacy countermeasures in the digital witness approach. We define a set of solutions, not considered to date, to enable anonymity in the DCoC-IoT (Section VI-A). The rest of the solutions presented are intended to mitigate some of the privacy problems that may appear in the digital witness approach depending on how some features are implemented. These solutions are presented in Section VI-B

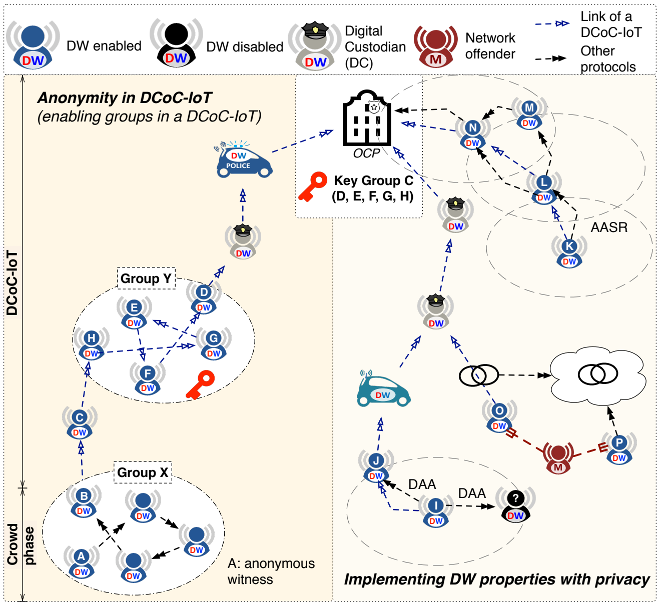
A. Anonymity in DCoC-IoT

In order to encourage the user to cooperate, it is important that citizens feel their identity is protected. However, providing total anonymity is not possible in these scenarios, to prevent this technology from being misused.

A possible way of allowing A or B (Fig. 3) to report digital evidence anonymously is by using k-anonymity techniques [22]. These provide an adequate balance between anonymity and identification since they allow an individual to remain indistinguishable within a group of k individuals with similar attributes. Thus, an observer cannot ascertain who in the group has taken potentially sensitive action.

In the digital witness approach, this idea can be exploited to guarantee the property of *provenance* within an approximate geographical area. We refer to this as d-provenance, meaning the distortion in the digital evidence provenance due to the inclusion of privacy mechanisms. Even though this mechanism introduces some error in the provenance of data this is not new and some existing mechanisms currently employed in forensic examinations have the same limitation but can still be, together with other evidence, decisive in the investigation. For example, GPS data can be as imprecise as 100 meters out but they will provide contextual evidence that helps delimit the investigation. Therefore, as shown in Fig. 5, the users may group together in such a way that whenever one of the digital witnesses, say A, has evidence to report, it will initiate a Crowds-like protocol [18]. With such a protocol in use, the next link in the chain of custody (C) is unable to tell which of the members in the crowd is the actual source of the message, even though the message was received from the digital witness marked as B.

This sort of mechanism may also help *anonymise the links of the DCoC-IoT* but in this case anonymity restrictions are stronger. While providing d-provenance is acceptable, once the DCoC-IoT has started, the OCP needs to know which digital witnesses have been involved in it. The anonymous witnessing approach can solve this by obfuscating the link identities of the members of the group by using some sort of group signature or pseudonym system that can be reverted by the OCP, possibly with the collaboration of some of the members of the group.



d-provenance(dcoc(C,OCP)) < *d*-provenance(dcoc(GroupX, OCP))
d-provenance(GroupX) > *d*-provenance(GroupY)

Fig. 5: Mitigation Methods

B. Digital Witness Implementation

The original design of the digital witness approach provided a high-level description of the characteristics that IoT devices must have so that the evidence collected by them remains intact and can therefore be accepted for processing in a forensic investigation (Section V). These features are subject to implementation decisions which may have privacy implications. Next we provide a list of mechanisms that take into account the previously identified privacy requirements.

1) Attestation: The process of attesting the state of a digital witness may have privacy implications. A potential risk of the original scheme is that devices nearby may know when a digital witness has been disabled from its duties thereby leading to *attestation privacy* problems (Section V-A2). To prevent these problems, digital witnesses may resort to *Direct Anonymous Attestation* (DAA) [4] protocols. DAA allows a verifier to check whether a user, the prover, is using a platform with a certified hardware security module. Moreover, when using DAA the verifier does not learn who the prover is or whether they have previously interacted with each other. Thanks to DAA, the digital witness I in Fig. 5 can choose J without knowing the identity of the disabled witness. Interestingly, this protocol is available in the TPM (*Trusted Platform Module*) specification [7], which are one of the technologies considered in the original definition of digital witnesses to offer a *Core of Trust* (CoT) for evidence management.

2) Links Discovery: The digital witness approach advocates that chains of custody (DCoC-IoT) should be as short as possible so as to reduce the exposure of links to threats and attacks. In those situations, when turning to other digital witnesses to reach a custodian (or the OCP) is a must, it would be useful to incorporate routing protocols capable of preserving the identity of those involved in the discovery process. This can be achieved by using or adapting anonymous routing protocols reminiscent of mobile ad-hoc networks, such as AASR [11]. Once an optimal route to a destination has been discovered, evidence can be transmitted anonymously.

3) Timestamping: Blind signature mechanisms [6] allow an entity to digitally sign a document without knowing its content. After signing, the owner of the document can retrieve the original document while maintaining the digital signature. One of the applications of this mechanism in the digital witness approach is to corroborate the acquisition of electronic evidence of the environment, without the signer (e.g. a more powerful digital witness) knowing the contents of the evidence. In the case that the public key of the OCP is used to encrypt the data, instead of the key of the digital witness, the data can be signed and retrieved by the OCP directly. This idea, in combination with signature chaining schemes [19], could be very useful for DCoC-IoT.

4) Blockchain Smart Contracts: Blockchain is a mechanism that enables the realisation of secure transactions among entities without the need for a trusted third party. The most notable example of this mechanism is in the *Bitcoin* cryptocurrency. Blockchain can be used in conjunction with *smart contracts* (e.g. Ethereum) as a robust mechanism for defining contractual transactions (i.e. programs) in a decentralised way. These transactions are usually public but recently in [10] a mechanism to preserve their privacy named Hawk is proposed. This could be a solution to the deployment of digital chains of custody capable of protecting *transactional privacy*, since Hawk is based on the presence of a third party, which may be instantiated using *Trusted Computing Hardware* (TCH). This apparent limitation is not really one, because digital witnesses are based on the presence of a TCH, such as TPM.

Blockchain could be used for additional purposes. One potential use of this technology is to provide digital witnesses with a mechanism to check whether an incident has already been reported (e.g. P in Fig. 5). This may not only be beneficial in terms of overhead but may also allow witnesses to decide whether it is necessary to expose their own evidence (and their privacy) if an incident has already been reported.

5) Multi-party Declaration: Some incidents may affect or be witnessed by several individuals simultaneously. In these situations, it may be advisable (e.g, to alleviate the OCP's overhead in managing multiple DCoC-IoT) to allow the witnesses to elaborate a joint declaration/complaint. However, some of the witnesses may be reluctant to share their own version of the incident with other participants. To implement this interesting feature it is possible to use protocols based on homomorphic encryption [12] or secure computation [20] in such a way that the witnesses can collaboratively share and operate over the statements of each of the participants without discovering the contents of the declarations.

6) Disposal Guarantees: A user who provides evidence of an incident usually expects that the data offered will only be used to resolve the case in question and will not be used for other purposes. Therefore, it is necessary to provide mechanisms that allow users to verify that the evidence has been deleted once the data are no longer necessary. An example of this type of mechanism is a *proof of secure erasure*, by which means a verifier can check whether or not a prover has erased its memory [9]. This type of verification would only involve the OCP and digital witnesses who store information about other digital witnesses not considered in the DCoC-IoT. Digital witnesses in a DCoC-IoT already define mechanisms to eliminate the data transmitted in the deployment of the DCoC.

VII. Conclusions and Future work

This paper has provided a critical analysis of the *digital witness* approach from the point of view of privacy. This approach defines some basic privacy mechanisms for the management of evidence and user agreement consent forms. However, it does not consider the problems that arise from the cooperation of devices, which may result in data being revealed to other entities, which are not entitled to access this information. Based on the privacy requirements identified during the analysis, we propose solutions that can be adopted to mitigate the lack of privacy in some situations. As part of these solutions, we have redefined the digital witness approach to allow anonymous witnessing. This paper paves the way towards an anonymous digital witnessing approach but much research is still needed until this vision becomes a reality.

Acknowledgment

This work has been funded by Junta de Andalucia through the project FISICCO (TIC-07223), and by the Spanish Ministry of Economy and Competitiveness through the project IoTest (TIN2015-72634-EXP /AEI).

References

[1] Iso/iec 27050:2016+ - information technology - security techniques - electronic discovery, 2016.

[2] Mikhail Afanasyev, Tadayoshi Kohno, Justin Ma, Nick Murphy, Stefan Savage, Alex C Snoeren, and Geoffrey M Voelker. Privacy-preserving network forensics. *Communications of the ACM*, 54(5):78–87, 2011.

[3] Giannakis Antoniou, Leon Sterling, Stefanos Gritzalis, and Parampalli Udaya. Privacy and forensics investigation process: The erpina protocol. *Computer Standards & Interfaces*, 30(4):229–236, 2008.

[4] Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 132–145, New York, NY, USA, 2004. ACM.

[5] Xavier Caron, Rachelle Bosua, Sean B Maynard, and Atif Ahmad. The internet of things (iot) and its impact on individual privacy: An australian perspective. *Computer Law & Security Review*, 32(1):4–15, 2016.

[6] David Chaum. *Blind Signatures for Untraceable Payments*, pages 199–203. Springer US, Boston, MA, 1983.

[7] Trusted Computing Group. Tpm library specification. [Online], 2014.

[8] Juan Guarnizo, Amit Tambe, Suman Sankar Bunia, Martín Ochoa, Nils Tippenhauer, Asaf Shabtai, and Yuval Elovici. Siphon: Towards scalable high-interaction physical honeypots. *arXiv preprint arXiv:1701.02446*, 2017.

[9] Nikolaos P. Karvelas and Aggelos Kiayias. Efficient Proofs of Secure Erasure. In Abdalla M. and De Prisco R., editors, *International Conference on Security and Cryptography for Networks (SCN 2014)*, LNCS 8642, pages 520–537, 2014.

[10] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 839–858. IEEE, 2016.

[11] W. Liu and M. Yu. Aasr: Authenticated anonymous secure routing for manets in adversarial environments. *IEEE Transactions on Vehicular Technology*, 63(9):4585–4593, Nov 2014.

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

[13] Ana Nieto, Rodrigo Roman, and Javier Lopez. Digital witness: Safeguarding digital evidence by using secure architectures in personal device. *IEEE Network*, In Press.

[14] Edewede Oriwoh and Paul 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)*, pages 544–550. IEEE, 2013.

[15] Sundresan Perumal, Norita Md Norwawi, and Valliappan 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*, pages 19–23. IEEE, 2015.

[16] Tom Petrocelli. *Data Protection and Information Lifecycle Management*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2005.

[17] Yudi Prayudi and Azhari Sn. Digital chain of custody: State of the art. *International Journal of Computer Applications*, 114(5), 2015.

[18] M.K. Reiter and A.D. Rubin. Crowds: Anonymity for Web Transactions. *ACM transactions on information and system security*, 1(1):66–92, 1998.

[19] Amitabh Saxena and Ben Soh. One-way signature chaining: a new paradigm for group cryptosystems. *International Journal of Information and Computer Security*, 2(3):268–296, 2008.

[20] Nigel P. Smart. *Secure Multi-party Computation*, pages 439–450. Springer International Publishing, Cham, 2016.

[21] Pasquale Stirparo and Ioannis Kounelis. The mobileak project: Forensics methodology for mobile application privacy assessment. In *Internet Technology And Secured Transactions, 2012 International Conference for*, pages 297–303. IEEE, 2012.

[22] Latanya Sweeney. k-anonymity: A model for protecting privacy. *Int. Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[23] Steve Watson and Ali Dehghantanha. Digital forensics: the missing piece of the internet of things promise. *Computer Fraud & Security*, 2016(6):5–8, 2016.