A. Nieto, R. Rios, and J. Lopez, “A Methodology for Privacy-Aware IoT-Forensics”, *16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017)*, pp. 626-633, 2017.
http://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.293
NICS Lab. Publications: https://www.nics.uma.es/publications

A Methodology for Privacy-Aware IoT-Forensics

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 Internet of Things (IoT) brings new challenges to digital forensics. Given the number and heterogeneity of devices in such scenarios, it bring extremely difficult to carry out investigations without the cooperation of individuals. Even if they are not directly involved in the offense, their devices can yield digital evidence that might provide useful clarification in an investigation. However, when providing such evidence they may leak sensitive personal information. This paper proposes *PRoFIT*; a new model for IoT-forensics that takes privacy into consideration by incorporating the requirements of ISO/IEC 29100:2011 throughout the investigation life cycle. PRoFIT is intended to lay the groundwork for the voluntary cooperation of individuals in cyber crime investigations.**

I. Introduction

Traditional computer forensics is based on a series of well-established processes whose primary goal is to preserve the integrity of digital evidence. To that end, there are several similar models that describe precise actions to be followed but they are are not prepared for dynamic and heterogeneous environments [1]. These traditional models are defined to manage physical evidence from its seizure until it is returned, and the collection of digital evidence is part of this process. Throughout the process, chains of custody are implemented by means of documents manually signed by the people in charge of managing the evidence. This cumbersome process is to ensure the integrity of the evidence but it is rather inflexible and conceived for static scenarios.

These rigid methodologies are unsuitable for current scenarios with a growing number of devices of a heterogeneous nature, as is the case in IoT environments [3]. Nowadays, forensic analysts face the problem of a lack of *tools and methodologies* for the treatment of IoT devices [2]. Not only devices but also intermediate platforms and infrastructures pose great challenges. For example, the exponential increase of data that needs to be processed [4], and the need to deploy collaborative approaches where IoT devices are able to install forensic software to help to include them as collaborators (a.k.a. witnesses) in a crime scene [13]. In this respect, the approach in [13] provides a technical solution to preserve the digital evidence and share it with remote entities, but without considering privacy requirements over the lifecycle of the investigative process. Not only in this approach, but in general, steps have to be taken to integrate privacy issues in *IoT-forensics* [3] to deal with new scenes of cybercrime due to the IoT.

The problems that have been considered so far in IoT-forensics are just the tip of the iceberg. The IoT is not only about billions of heterogenous devices connected to the Internet. The user also plays a fundamental role in this paradigm and obviating it is a terrible mistake. Collecting evidence from IoT devices may have implications for individual privacy and thus tackling this problem is critical in IoT-forensics. This is precisely the goal of this article. We define the PRoFIT (*Privacy-aware IoT-Forensic Model*) methodology to integrate privacy properties in accordance with ISO/IEC 29100:2011 throughout the phases of a forensics model adapted to the IoT. Moreover, unlike previous approaches, the PRoFIT model highlights the importance of collaborating with surrounding (and potential *sporadic*) devices to gather electronic evidence that helps to fully clarify the context of the crime scene.

This paper is organized as follows. Section II describes the forensic models and privacy principles on which the PRoFIT methodology is built. Section III explains the phases of the PRoFIT model and Section IV the methodology. Then, a use case scenario is presented in Section V to illustrate the model more clearly. Finally, Section VI concludes the paper.

II. Background

This section provides some background information about existing digital forensic models and their phases. It also introduces some privacy principles that need to be considered when dealing with personal information.

A. Forensic Models

Forensic models are intended to preserve evidence throughout its life cycle, from acquisition until it is processed and possibly returned. A review of several of these models is presented in [1], where the *Enhanced Systematic Digital Forensic Investigation Model* (ESDFIM) is proposed. This model contemplates the following phases:

- *Preparation*: refers to all actions performed prior to the investigation, including analysis of the legal framework, application for search warrants, setup of information processing tools, etc.
- *Acquisition & Preservation*: includes the identification, collection of evidence, labelling, packaging, etc.
- *Examination & Analysis*: at this stage, the investigators examine and analyze *the contents* of the devices that were collected and appropriately preserved.

- *Information Sharing*: refers to the ability of different authorized organizations to share and exchange data relating to an investigation.
- *Presentation*: the authorities are presented with the results of the investigation. This phase is critical for the admissibility of the evidence.
- *Review*: this stage is intended to evaluate and improve the investigation process. It also considers the process for returning the collected evidence (e.g., a PC).

ISO/IEC 27050:2016 [5] defines different phases for the management of electronically stored information: identification, preservation, collection, processing, review, analysis and production. These can be easily mapped to the ones defined by the ESDFIM model with the exception of the *information sharing* phase, which is not considered. This phase is of particular interest in IoT scenarios and thus we adopt the ESDFIM model.

There are very few models specific to IoT-forensics. To the best of our knowledge, the only models that define phases in their methodological approach for IoT-forensics are those proposed in [6] and [7] (TABLE I). Other IoT-forensic solutions (e.g., [8], [9]) are not considered here because they do not strictly define phases.

TABLE I: IoT-forensics Models with phases

Model	Phases
[6]	Planning (authorization and warrant obtained), IoT data acquisition (base device identification, zone, triage examination, acquisition of data from data accumulation platforms, structured data / unstructured data), chain of custody, lab analysis, result, proof & defense, achieve & storage
[7]	Proactive process (IoT scenario definition, evidence source identification, planning incident detection, potential evidence collection, digital preservation, storage of potential evidence), IoT-forensics (cloud forensics, network forensics, device level forensics), Reactive Process (initialization, acquisitive, investigative), Concurrent Process (obtain authorization, documentation, chain of custody, physical investigation)

Even though [7] considers the possibility of setting up the IoT environment, these models do not yet consider ethics and privacy rights as part of their methodology. In addition, these models use search warrants from the beginning of the process thereby delaying the investigation in high-density scenarios. Usually search warrants are needed to collect digital evidence from a suspect or potentially involved devices in an investigation. However, in some scenarios the user might be disposed to cooperate (e.g., as a witness).

In summary, neither traditional nor IoT models currently consider the potential benefits of voluntary cooperation. In this paper we wish to exploit the social side of the IoT to boost the successful resolution of forensic investigations but to that end we need to carefully consider user privacy throughout the investigative process.

B. Privacy Principles

Several laws and directives are intended to set limits on the collection, processing and dissemination of personal information when interacting with other entities and services. Among them, one of the first to consider privacy was the US Privacy Act of 1974, where the *Fair Information Practices* (FIPs) were established. These practices or principles were later embraced and adapted in several guidelines [10], directives [11] and standards, such as the ISO/IEC 29100:2011 [12], which considers the following privacy principles:

- *Consent and choice* (**P1**): the user must give explicit consent to the collection and processing of his/her data.
- *Purpose legitimacy and specification* (**P1**): the system must clearly present the purpose for data collection to the user.
- *Collection limitation* (**P3**): the system must collect the data that is strictly necessary to fulfil the original purpose.
- *Data minimization* (**P4**): the data sent to and processed by the system must be reduced to its minimum.
- *Use, retention and disclosure limitation* (**P5**): the system must not use the collected data for a purpose other than the one originally specified. Also, it must be disposed of once the purpose has been accomplished.
- *Accuracy and quality* (**P6**): the data provided by the user must be precise, truthful and current.
- *Openess, transparency and notice* (**P7**): the user must be aware of the policies, procedures and practices of the system with regard to personal data.
- *Individual participation and access* (**P8**): the user must be able to access his/her own data as well as ask for corrections.
- *Accountability* (**P9**): the system is responsible for following the privacy policies and, in the case of non-compliance, the user can ask for compensation.
- *Information security controls* (**P10**): the system must protect personal data from unauthorized access, loss and manipulation.
- *Compliance* (**P11**): the system must implement auditing mechanisms to verify that it is compliant with privacy principles.

In general, these privacy principles try to return control over their own data to the users. More precisely, they establish that the user must be aware of the data collection and consent to it. The purpose for data collection must be clearly specified and under no circumstances may the data collected be used for other purposes. Moreover, the data collector must only request the minimum amount of data necessary to provide the service and once provided it should be deleted. In the meantime, the data must be safe from intrusion or harm.

III. Privacy-aware IoT-Forensic Model (PRoFIT)

This section describes the PRoFIT model. The proposed model defines six phases detailed in Section III-A, which take into consideration the privacy requirements established by ISO/IEC 29100:2011, as described in Section III-B, and the use cases in Section III-C.

A. PRoFIT Phases

The cooperation of devices nearby calls for the re-definition of the phases of the reference models used so far. In particular, we maintain the definition of the last three phases of the ESDFIM model (Section II-A), but we re-define the first three phases and the methodology to adapt the model to an IoT-forensic environment. Thus, PRoFIT defines the following phases: (1) *Preparation* (planning and environment set up), (2) *Context-based collection*, (3) *Data analysis and correlation*, (4) *Information Sharing*, (5) *Presentation* and (6) *Review*. A summary of the PRoFIT model workflow is shown in Fig. 1.

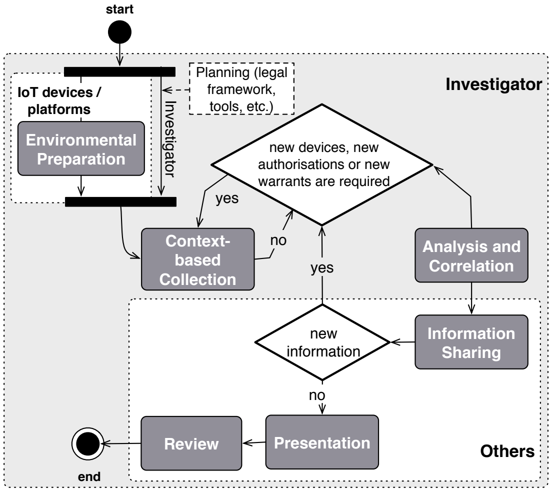


Fig. 1: PRoFIT workflow

More precisely, phase (1) in our model is divided into two flows. One is related to the investigator and the other is associated with IoT devices and/or platforms. Phases (2) to (6) are concerned with the forensic investigation therefore the investigator is the main actor even though devices and users are also involved because of the implementation of privacy principles. Phases (4) to (6) are inherited from the ESDFIM model but are modified so as to take into account the privacy principles defined in Section III-B. It is worth noting that phases (2) to (4) can be accessed several times if new information is provided to the investigator.

The following sections describe the main objectives of the PRoFIT phases, while the workflow of each phase will be detailed in Section IV.

1) Preparation: Unlike the ESDFIM model, the *Preparation* phase separates the tasks involving the investigator and the task to prepare the devices and platforms of the IoT environment. At this stage, the investigator elaborates the traditional plan before any investigation (c.f. Section II-A), but there is an optional - although recommended - task related to the *preparation of the environment*. This optional phase involves configuring the devices and the IoT platform to consider the requirements of the PRoFIT model. Thus, the PRoFIT model is intended to simplify the subsequent phases of the investigation.

This preparation may consist in installing a piece of software (e.g., a middleware, Fig. 2) to assist and advise the user about the information contained in the device according to privacy policies and forensic restrictions, as well as to manage the data offered to requestors depending on the data provided, such as a signed warrant. We have called this software the PRoFIT software. Note that there is a dependency on the ability of IoT devices and platforms to install any piece of software. This is subject to the owner of the device. Therefore, we assume that not all the devices will have PRoFIT software installed and so the investigator will be responsible for complying with the privacy requirements of those willing to collaborate in the investigation.

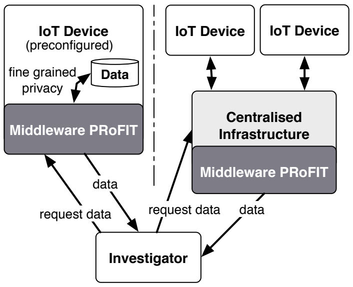


Fig. 2: Preconfiguration of IoT Devices and Platforms

It is important to highlight that the PRoFIT model tries to solve the case with the information voluntarily provided by the users. In this way, PRoFIT promotes the collaboration of devices while promoting user privacy. By doing so, we expect to reduce the cumbersome and time-consuming process of requesting authorization for collecting digital evidence. Nonetheless, some investigations may require that court orders are requested in the first phase and not only after a person is already collaborating. PRoFIT allows both approaches and is more dynamic that its predecessors so as to better adapt to the IoT context.

2) Context-based Collection: This phase concerns the collection of data from the devices involved in the case and the deployment of chains of custody. Depending on the investigation it may be necessary to request court orders, as in the traditional approach, but the PRoFIT model is specifically intended to promote the user's cooperation while preventing the requisitioning of personal devices.

The process shown in Fig. 5a is performed by the investigator. This process ends when there is no new information or permissions to request (Fig. 1). The devices may or may not be pre-configured with the PRoFIT software. We distinguish three types of device profiles for the investigation:

- Victim / Offended: belongs to the person who suffered an offense. The owner of the device will therefore want an investigation into his/her device's data to be opened (c.f. use case in Section V).
- Suspect: is a device that may contain digital inculpatory or exculpatory evidence.
- Witness: provides relevant digital evidence for the investigation but it is neither the victim nor the suspect.

3) Data Analysis and Correlation: This step is devoted to the analysis and correlation of the data obtained in the previous phase. This phase may also receive information from new sources via phase 3, as shown in Fig. 1. Unlike the ESDFIM model, in our definition we consider that all the inputs are digital evidence and probably raw data collected from the cooperative devices. Due the heterogeneity of IoT environments, working with heterogeneous formats may be a requirement. All the data must be processed to filter useful, relevant information to the case. As this is a phase that may require feedback and therefore the knowledge is incremental, some of the data to be correlated could be pre-processed from a previous step. So the tools in this phase should be designed to work both with well-structured digital evidence and with raw data.

4) Information Sharing: This phase maintains the main objective of the ESDFIM model (Section II-A). However, our methodology modifies the behavior to consider the privacy requirements (Section II-B).

5) Presentation: The focus in this phase is to present the results of the investigation to the authorities for its admissibility (c.f. ESDFIM model in Section II-A). However, the methodology defined in the PRoFIT model is different so as to consider the privacy requirements (Section II-B).

6) Review: This last phase pursues the main objective of the ESDFIM model (Section II-A). However, in order to consider the privacy requirements (Section II-B) the methodology in the PRoFIT model is very different from its predecessor.

B. Privacy Requirements

TABLE II aligns the privacy requirements described in ISO/IEC 29100 with each of the phases of the PRoFIT model.

TABLE II: Privacy Requirements in PRoFIT phases

PRoFIT phase	ISO/IEC 29100					
Preparation	P1	P2	P4	P7		P11
Context-based collection	P1	P2	P3	P6	P8	
Data analysis and correlation	P9	P10				
Information sharing	P1	P2	P10			
Presentation	P4	P6				
Review	P5	P7				

P1. Consent and choice, P2. Purpose legitimacy and specification, P3. Collection limitation, P4. Data minimization, P5. Use, retention and disclosure limitation, P6. Accuracy and quality, P7. Openness, transparency and notice, P8. Individual participation and access, P9. Accountability, P10. Information security controls, P11. Compliance

During the *environment preparation* phase it is necessary to comply with several data protection principles, especially those focused on the user being well informed and aware of the practices to be carried out. On the one hand, the purpose of the PRoFIT software must be clearly and concisely specified (P2, P7). After that, the user can choose whether or not to accept the conditions of the software installation (P1). During the normal execution of the device, PRoFIT will be able to collect information according to the policies and the consent offered by the user (P2). For example, the software can help the user avoid having to store data about third parties thereby promoting the principle of data minimization (P4). Finally, the user must be able to check what data is being collected by PRoFIT (P7). In the case of being ask to collaborate, the user will decide whether or not these data are offered to the investigator without a warrant.

The *data collection* phase begins when the forensic investigator requests data from the device. The investigator will request only those data that are relevant to the investigation (P3). To ensure that the data have not been falsified (P6), remote attestation mechanisms based on reliable platforms will be used, allowing both the user and the investigator to check the integrity of the system. Likewise, the requests of the investigator can be limited if they are considered abusive by the user's policies (P4). In this respect, the software may decide to offer the information requested but in less detail or simply not offer it. Once offered, the user can verify that the data collected by the investigator are correct. In the case that it is necessary, the user can later offer a finer level of granularity and even provide new evidence (P8).

Once the data have been collected, during the *analysis and correlation* phase, it is critical to ensure that the data are adequately protected from tampering, manipulation or loss (P10). Otherwise, the user may demand accountability and even compensation (P9).

In some investigations, it may also be necessary to share information with other agencies or entities to solve the case. If this possibility has not been contemplated from the start, the system will ask the user to give consent (P1, P2). Once consent is given, the transfer or access to the information will be carried out under strong security measures to protect the confidentiality and integrity of the data (P10). The same data protection principles and security guarantees must be offered at the destination as the origin.

In the *presentation* phase, it will be ensured that the quality and accuracy of the data are sufficient to clarify the case (P6). It is important to avoid giving more detail than strictly necessary as well as preventing the appearance of data on third parties which are not relevant for the clarification of the case (P4). The *revision* phase will help investigators to improve the data collection, analysis, protection and dissemination processes. In this phase, the investigators must proceed to the secure erasure of data and to return any material confiscated (P5). In addition, the user must be able to verify that the data has actually been deleted (P7).

Throughout the process, internal audits and mechanisms must be performed to ensure that the process complies with the privacy principles (P11).

C. Use cases for the Methodology

The efficient application of digital forensic techniques will be virtually impossible in IoT scenarios without the cooperation of devices nearby. For example, imagine that the crime scene is in a hospital, where the delincuent uses local access technologies to affect pacemakers and other body area network devices. Therefore, the devices at the scene of the crime may or may not be involved in the case but having access to their information can help the investigation, especially when the attack uses wireless technologies for propagation. Obviously, in order to promote the cooperation of the different users at the crime scene we need to consider privacy and this is dependent on the context surrounding the devices (Fig. 3).

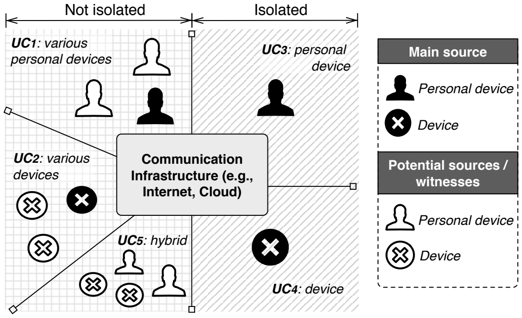


Fig. 3: Use Case Contexts

The policies to be applied to an investigation vary depending on whether the personal device or object is alone (UC$_3$ and UC$_4$), or it is surrounded by more *things*: other personal devices (UC$_1$), objects (UC$_2$), or both (UC$_5$). The reason for this is that personal devices store information that may be subject to privacy restrictions. In addition, they may store information due to their relationships with other entities. On the other hand, non-personal devices may belong not only to one user, but also to a group of users, a public or private organization, etc. They can store non-personal information or sensitive information that concerns a set of users, such as patient data in a hospital.

It is worth noting that the dynamism of the IoT may also involve changes in the context of the investigation. At the beginning of the investigation the investigator may think that a personal device was isolated (UC$_3$) and consequently use a set of policies considering this use case. Later, the investigator may realize that there were more devices in the area (UC$_1$, UC$_2$, UC$_5$). In this case, the investigator may request the collaboration of the devices nearby as potential witnesses in the investigation.

IV. PRoFIT Methodology

For the sake of simplicity we reduce the problem to investigating a case starting with a single victim device. This device may be personal (e.g., a cellphone) or non-personal (e.g., a workstation) and the investigation can consist of obtaining data from that device alone or require information from other devices nearby. The process should be replicated in the case there are several victims. The exposition of methodology is guided by the phases defined by the PRoFIT model.

A. Environment preparation

We focus on devices that may be set up with the PRoFIT software (Fig. 2) according to the privacy criteria agreed upon with the user. Therefore, devices are configured to collect information according to the data minimization principle.

Note that this process can be as restrictive as desired but it is advisable to find the right balance between privacy and usability. The device can be configured to remove any information that may expose user privacy (e.g., by using anti-forensic techniques) but this would result in a useless device from the point of view of an investigation. To the contrary, the device can be configured to collect as much public information as possible (e.g., data shared by others) but sharing all this information may result in privacy violations.

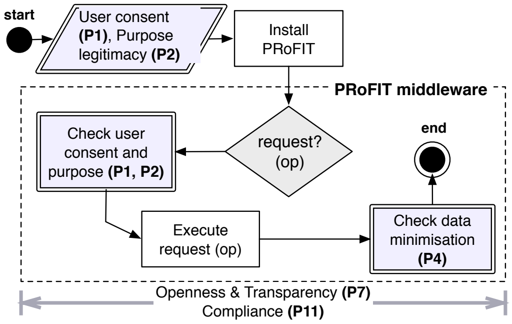

start
User consent (P1), Purpose legitimacy (P2)
Install PRoFIT
PRoFIT middleware
request? (op)
Check user consent and purpose (P1, P2)
end
Execute request (op)
Check data minimisation (P4)
Openness & Transparency (P7)
Compliance (P11)

Fig. 4: PRoFIT software lifecycle

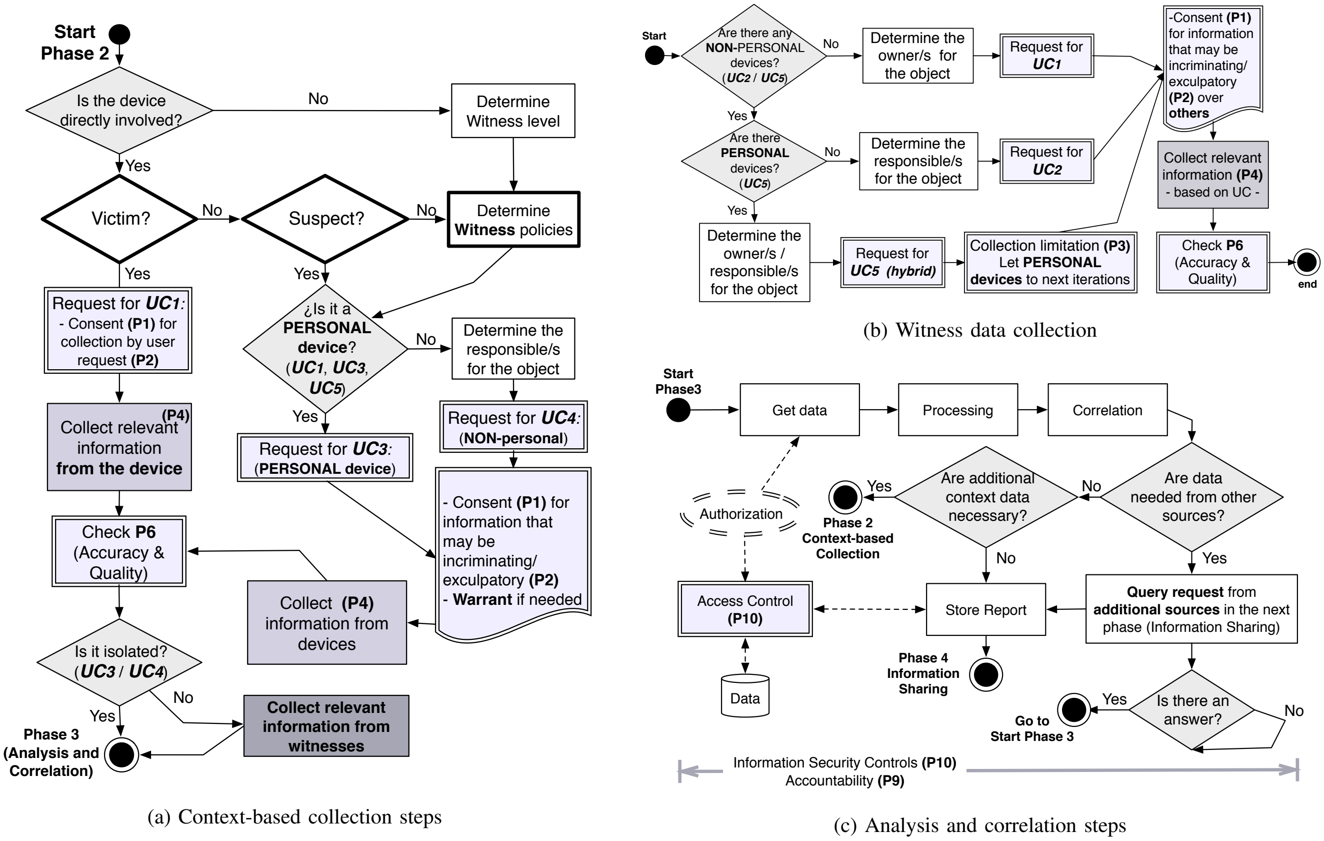
Fig. 4 shows the process of installing a PRoFIT-compliant software and its activities within an IoT device or platform. According to the privacy requirements it is necessary to ask for the user's consent to proceed with the installation of the software (P1, P2). Once installed, the software controls the operations requested by the system (e.g., store evidence) or by third parties (e.g., request evidence) ensuring they are not in conflict with the privacy policies of the user. Once the operation has been granted and executed, this is done according to the principle of data minimization (P4). For example, a device will send information to an investigator up to a particular level of granularity.

B. Context-based collection

The process of data collection is guided by the types of devices involved in the investigation: victim, suspect and witness, as shown in Section III-A. These particular steps are depicted in Fig. 5a, where it is worth noting that throughout the process of gathering digital evidence the devices will *remain under their owners' control*. Otherwise, if the owner is not willing to cooperate, the investigator will proceed as usual, requesting warrants and confiscating the devices.

When the device to be analyzed is the *victim*, we assume that the identity of the owner (or manager) of the device is known. In this case, the victim is presented with the purpose and practices to be performed on the data (P2), which needs to be confirmed by the victim (P1) in order to start the investigation. The investigator must also check that the device belongs to the user or that the manager is authorized to request the investigation. If so, evidence is collected from the device using forensic tools while ensuring the integrity of the evidence and documenting the process (P6).

If required by the investigation, it is checked whether the device was isolated or not. This is useful in the case other devices can provide new evidence to clarify the case (e.g., digital witness [13]) or to identify new cases of infection due to



Start Phase 2
Is the device directly involved?
No
Determine Witness level
Yes
Victim?
No
Suspect?
No
Determine Witness policies
Yes
Yes
Request for UC1: - Consent (P1) for collection by user request (P2)
¿Is it a PERSONAL device? (UC1, UC3, UC5)
No
Determine the responsible/s for the object
Collect relevant information from the device (P4)
Yes
Request for UC3: (PERSONAL device)
Request for UC4: (NON-personal)
- Consent (P1) for information that may be incriminating/ exculpatory (P2) - Warrant if needed
Check P6 (Accuracy & Quality)
Collect (P4) information from devices
Is it isolated? (UC3 / UC4)
No
Yes
Collect relevant information from witnesses
Phase 3 (Analysis and Correlation)

(a) Context-based collection steps

Start
Are there any NON-PERSONAL devices? (UC2 / UC5)
No
Determine the owner/s for the object
Request for UC1
Yes
Are there PERSONAL devices? (UC5)
No
Determine the responsible/s for the object
Request for UC2
-Consent (P1) for information that may be incriminating/ exculpatory (P2) over others
Yes
Determine the owner/s / responsible/s for the object
Request for UC5 (hybrid)
Collection limitation (P3) Let PERSONAL devices to next iterations
Collect relevant information (P4) - based on UC -
Check P6 (Accuracy & Quality)
end

(b) Witness data collection

Start Phase3
Get data
Processing
Correlation
Authorization
Yes
Are additional context data necessary?
No
Are data needed from other sources?
Phase 2 Context-based Collection
No
Yes
Access Control (P10)
Store Report
Query request from additional sources in the next phase (Information Sharing)
Data
Phase 4 Information Sharing
Yes
Is there an answer?
No
Go to Start Phase 3
Information Security Controls (P10)
Accountability (P9)

(c) Analysis and correlation steps

Fig. 5: Forensic Investigation

the spread of a malware. In that case, we propose following the steps depicted in Fig. 5b to collect information from witnesses. Here we also take into consideration different contexts. We wish to emphasize that, the analysis of new devices is not undertaken unless it is strictly needed to solve the case. Thus satisfying the principle of collection limitation (P3).

When the device to be analyzed belongs to a *suspect*, the requested permissions will differ from the previous case. In this case, the investigator will probably need a warrant to obtain the data since a suspect is highly unlikely to cooperate, unless his/her device contains exculpatory evidence. In either case, it is necessary to find out who is responsible for the device when the device is not a personal device directly linked to a person.

Finally, in the case that the device is considered to be a *witness* and to encourage cooperation, we include a clause stating that the data collected from the device cannot be used against the witness him/herself. The investigator must carefully look at the data collected following this procedure or simply discard them. Note that, if the attacker is a *false witness* and he/she signs a collaboration contract then the inculpatory evidences found on his/her device cannot be used against him/her. However, it would be easier for him/her to simply delete the data from the terminal rather than revealing the truth about him/herself.

C. Analysis and correlation

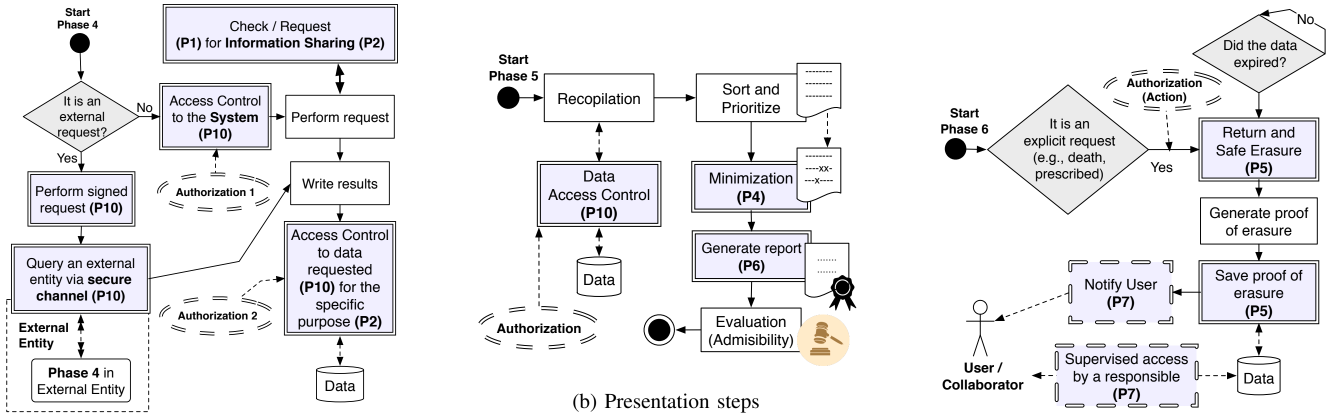
This phase includes the access to, processing and correlation of data from different sources (see Fig. 5c). In the case that during this phase the need for new evidence is identified, the workflow leads the investigator back to phase 2. Likewise, if the investigator considers that it is necessary to query external sources for data, it jumps to phase 4 to obtain the information (recall the PRoFIT workflow in Fig. 1). Once the results have been obtained, access control permission must be checked again because the permission on the data may have been revoked or expired.

Note that principles P1 and P2 affecting the user are not present in this phase because we assume that the data provided here were obtained using fair information practices.

D. Information Sharing

This phase involves remote entities, such as foreign authorities, requesting access to the evidence collected from a device (Fig. 6a). We consider that the owner of the device who offered the data may have only authorized the use of these data for a particular entity or to a particular investigation. This is the reason why we enforce the principles of purpose specification and consent (P1, P2) once again.

The workflow shown in Fig. 6a is valid both for queries for data from different investigations carried out within the same agency and for queries issued by external entities. We


Start
Phase 4
It is an external request?
No
Yes
Check / Request
(P1) for Information Sharing (P2)
Access Control to the System (P10)
Perform request
Authorization 1
Write results
Perform signed request (P10)
Query an external entity via secure channel (P10)
Authorization 2
Access Control to data requested (P10) for the specific purpose (P2)
External Entity
Phase 4 in External Entity
Data
Start
Phase 5
Recopilation
Sort and Prioritize
Data Access Control (P10)
Minimization (P4)
---xx-
---x----
Data
Generate report (P6)
Authorization
Evaluation (Admisibility)
Start
Phase 6
It is an explicit request (e.g., death, prescribed)
Yes
Authorization (Action)
Did the data expired?
No
Return and Safe Erasure (P5)
Generate proof of erasure
Save proof of erasure (P5)
Notify User (P7)
User / Collaborator
Supervised access by a responsible (P7)
Data

(a) Information sharing steps

(b) Presentation steps

(c) Review steps

Fig. 6: Cooperation, admissibility and erasure

consider two authorization criteria; one to receive access to the data and the other to enable the modification of data (e.g., to include new information).

E. Presentation

The goal of this phase is to generate a forensic report. This report should be clear to all the actors involved in the case, including those without expertise in the area, such as lawyers and judges. The steps involved in this phase are depicted in Fig. 6b. During this phase, the investigator sorts all the evidence and information generated in the previous phases. Data minimization is applied in the case of redundant data or in the case that the data are considered irrelevant for the generation of the final report. While elaborating this report, the investigator must pay particular attention to a number of quality parameters (e.g., legibility) in order to ease the evaluation of the case.

F. Review

Finally, digital evidence must be erased after a period of time that must be no less than the timespan of the case. After that time, it is necessary to delete all the material from data bases and notify the users involved in the investigation of this fact. The generation of proof of erasure and its transmission to the user are optional but revelant for the principles of transparency (see Fig. 6c). At this point, it is also necessary to return physical evidence (e.g., a workstation) to the user in the case it was confiscated due to the combination of PRoFIT with traditional procedures.

V. Use case - Social Malware

Here we describe a realistic scenario to illustrate how to apply the PRoFIT methodology in practice. Let us suppose Bob has a smartphone with a PRoFIT-compliant software installed (phase 1). He walks into a coffee shop, where there are several IoT devices, both personal and non-personal (see Fig. 7). While Bob is in the coffee shop, his device detects an attempted attack from some of the devices in its vicinity. After detecting the attack, the PRoFIT software decides to **store information** related to the attack. Moreover, it alerts Bob to the presence of a device nearby trying to propagate a worm, exploiting a vulnerability in the *meetMe* application, which uses Bluetooth to detect other users in the vicinity with similar interests. After being notified of the offense, Bob decides that this incident needs to be reported to the authorities as soon as possible. To that end, Bob decides to request the start of an investigation by sending the evidence stored in his device to the PRoFIT system (phase 2). A PRoFIT investigator is assigned to the case, who, after *analyzing the data* confirms that the attack was launched from the local network. However, the investigator needs more evidence to properly carry out the investigation and commands the PRoFIT agent installed in Bob's device to collect new evidence from any devices nearby willing to collaborate (back to phase 2).

Following the methodology described in Section IV, the local PRoFIT agent first asks non-personal devices for any information they can offer. The person responsible for some of these devices is the owner of the coffee shop, who agrees to collaborate and allows the devices (e.g., the cash register) to send information to the investigator using the PRoFIT agent installed in Bob's device as the gateway. This information is encrypted and signed. After reception by the investigator, the device receives a proof of correct reception that can be checked by its owner. This proof can be used by the owner of the coffee shop to ask the investigator to (i) check the correctness of the data provided, and (ii) to recant and request the erasure of the statement. Based on the new evidence provided by the coffee shop owner (phase 3), the results of the investigation indicate that the malware is latent in a non-personal device, the Raspberry Pi, and the infection was received from outside the network, as indicated by the logs of the router. Since it has not been possible to identify the source of the problem with the information collected, Bob gives his consent to the investigator to **share his information** with other agencies but only for the purpose of the investigation (phase 4).

After some time has passed, an improved version of the

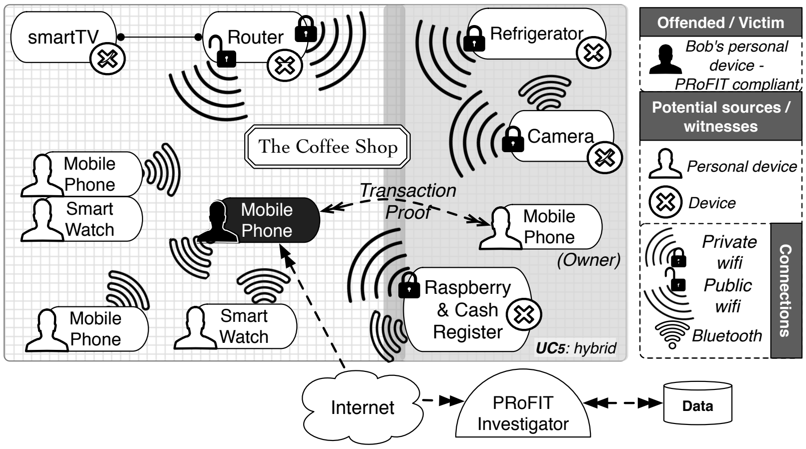


Fig. 7: Scenario

same malware affects new IoT devices. Since the PRoFIT system has kept information regarding the initial attack, it is possible to correlate these data with new evidence taken from various sources and discover the source of the attack and a potential suspect. The data provided by Bob and other devices are finally used to elaborate a final report (phase 5), which is admitted at the trial. Some time after the court ruling, Bob is notified that the **data he provided has been removed** from the system. A proof of deletion is provided to him (phase 6).

Although this is a hypothetical scenario and the malware as well as the *meetMe* application are fictitious, it is reasonable to think that this type of attack is occurring (or will occur) without the user even noticing it [14].

VI. Conclusion

This paper has presented the PRoFIT model for conducting digital forensic investigations in IoT environments. Unlike previous approaches, the PRoFIT model integrates privacy requirements (ISO/IEC 29100:2011) as part of the methodology. The goal of considering privacy is to promote the voluntary collaboration of personal and non-personal IoT devices in digital forensic investigations. The proposed methodology has been applied to a realistic use case scenario of malware propagation in an IoT-enabled coffee shop.

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] 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] *ISO/IEC 27050:2016+ - Information technology - Security Techniques - Electronic discovery*, ISO/IEC JTC 1/SC 27 Std., 2016. [Online]. Available: http://www.iso27001security.com/html/27050.html

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

[14] 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.