REVIEW

Open Access

Cybersecurity profiles based on human-centric IoT devices

Ana Nieto* and Ruben Rios

*Correspondence:
nieto@lcc.uma.es
Department of Computer Science, University of Malaga, Campus de Teatinos s/n, 29071 Málaga, Spain

Abstract

This paper proposes a methodology based on the concept of *Human Factors* to obtain Cybersecurity profiles. The profiles are determined by a set of parameters that help model the skills of individuals (potential offenders, victims, etc.) during a digital investigation. The definition is flexible enough to allow the cybersecurity profiles to grow when more data is available. A critical part of the solution is the inclusion of personal devices as important elements of the profiles. This is highly relevant as paradigms such as the *Internet of Things* (IoT) are transforming society, bringing humans closer to their devices than ever before. IoT devices also produce a lot of data, which can be useful to complete cybersecurity profiles and therefore understand the whole context of a digital investigation. Thus, IoT devices are included in the proposed methodology to capitalise on the strong dependence between users and devices during the analysis.

Keywords: Security, Human factors, Cybersecurity profiles, Digital investigation, IoT

Introduction

Cybersecurity tools usually depend on huge amounts of data that must be processed in real time. Once these data have been processed, the information deduced from them must be presented to different experts, who may or may not be technicians. To facilitate understanding of how different actors are involved in a cybercrime, data related to individuals can be presented in the form of cybersecurity profiles.

However, as the number of devices continues to grow with the development of the *Internet of Things* (IoT) [1] more data is available for interpretation. Note that in 2019 there are 7 billion internet-connected devices worldwide, according to IoT Analytics [2]. Clearly, this poses new challenges but also offers new opportunities. With data available from myriads of IoT devices, the complexity of the solutions increases but having so much data can be exploited to generate much more complete cybersecurity profiles, which in turn leads to a better understanding of the whole context of a digital investigation. Unfortunately, even though these data are readily available there is still no way to automate the process of gathering these data and linking them to users. Consequently, more research is necessary to unleash the full potential of cybersecurity profiles.

This paper works precisely in this direction by proposing a new methodology for defining advanced cybersecurity profiles. This methodology considers, for the first time, the importance of IoT devices in the analysis of a cybercrime scene. In particular, we exploit the strong relationship between users and their devices. Moreover, the approach presented here is flexible enough to build dynamic profiles which evolve as more information about suspects becomes available.

Leveraging IoT devices

The strong dependence of users on technology makes IoT devices a critical factor from a cybersecurity point of view. Users are amidst IoT devices, carry them and even have them attached to their bodies. These devices collect much information about their owners (location, habits, relationships, etc.), which can be exploited to conduct different types of cyberattacks. IoT devices also expose the user to privacy breaches as the data collected by them can be used when accessing online services on the Internet.

However, this not only affects potential victims but also attackers. As such, we can take advantage of the same tools used by attackers to build better cybersecurity profiles of the various actors involved in a cybercrime. By doing so we can gain insight into the security deficiencies of potential victims as well as the abilities of the attacker, thereby clarifying the context of the digital investigation.

Motivation and structure

This paper proposes a methodology for defining cybersecurity profiles that takes advantage of the strong interdependence between users and devices. This motivates the definition of the concept *Human Factors for Cybersecurity* (HFC), which represents the set of parameters that should be considered to define the complete profiles. The methodology is built upon this concept, and therefore receives the same name. Instead of building a restricted methodology only considering IoT devices, we design a solution capable of defining general parameters that will be fed with the data acquired from IoT devices. As a result, this paper provides a mapping between human factors and cybersecurity, but including IoT devices as an important element of the context. Unlike related approaches in this area, HFC also considers enablers (e.g., sensors and public information) and disablers (e.g., data privacy) as an intrinsic part of the solution.

The structure of the paper is as follows. First, we analyse related work and highlight the novel contributions of this paper in the area. Then, we introduce the concept Human Factor and identify a set of general parameters that help to clarify what is missing in current related work and that should be included in new solutions to define cybersecurity profiles. The Human Factors for Cybersecurity (HFC) methodology is proposed next, based on the requirements identified and the new definition of human factor. The methodology is validated in the context of a digital investigation with three main suspects and diverse sources of data to be analysed. Finally, we conclude the paper with a discussion on how privacy is inevitably related to these approaches and some potential lines of future work.

Related work

There are diverse contributions related to the definition of cybersecurity profiles. These work either directly or indirectly towards the design of mechanisms or tools that can aid in defining these profiles.

In [3] the results of a survey to identify features of the participants in a cybersecurity competition are provided. The survey considers the following characteristics:

personality, interests, culture, decision-making and attachment styles. The final goal of this research is to determine the motivation (e.g., professional aspirations or to address challenges) of those participants. The results of this survey can help in understanding the profile of actors with technical skills in cybersecurity. The focus in [4] is to analyse investigative tools denoted as criminal profiling and the availability of these tools to assess police investigations towards the provisioning of expert witness evidence. The analysis is carried out from a psychological point of view, considering law experts in the field but not their technical skills. In [5] the change of context introduced by cybercriminal activity is analysed. While it is stated that "cyber crime victims are typically organisations whose systems are penetrated, and the customers of that organisation", the reality is that what is considered cybercrime is migrating to a wider scope, sometimes being intrinsically personal and not always dependent on technical skills to be committed (e.g., cyberbullying). In [6] the resources of the offender are analysed and classified. For example, the author differentiates between *crimeware* tools (software specifically designed for the sole purpose to enable cybercrime, e.g. exploit kits, botnet kits, keyloggers) and *dual-use* tools (designed for the public interest, but adapted for use in illegal activities, e.g. penetration testing tools).

General user profiles for cybersecurity are considered in [7], where previous papers in this field are classified. Most of the contributions are based on logs (e.g., windows logs or web searches) or social content (e.g., Twitter, Facebook). The profiling criteria is very diverse: user's interests, knowledge, skills, demographic information, intention, behaviour (online and offline), social media activity and network traffic. The analysis is organised, considering *User Features* (UF) for: (i) information: interests, knowledge/skills, demographic information and intention/motivation; (ii) behaviour and social network activity; (iii) network traffic. The proposed model considers (i) four data sources (network traffic, web, human resource, logs), (ii) the steps for processing the data and (iii) a classification based on a feature vector. The classification by the authors is very interesting and can help clarify the cybersecurity context. However, the IoT perspective is ignored.

A different approach is followed in [8], where the profiling of human attackers is used to identify bots. The idea is to classify the adversary as a type of human. In the case the profile generated for the human is not realistic, then the attacker is considered a bot instead of a human being. The features expected from a (human) attacker are: skill, education, risk, gender, goal, speed (commands per second), mistakes, and anti-forensics. As a result, a tool is provided to show the information of the attacker classified by these characteristics.

In addition, there have been several tools developed to gather data about individuals and extract relevant information within the context of digital investigations. For example, the Open Source Intelligence (OSINT) Framework [9] provides a list of tools and methods to obtain public information about targets, classified with very different characteristics such as: username, e-mail address, terrorism, dating, etc. Unlike OSINT, *Social Media Intelligence* (SMI or SOCMINT) is focused on social channels and conversations. SOCMINT together with sentiment analysis can, for example, identify potential threats against a society (e.g., terrorism). One of the problems is that all the information generated must be processed. In [10] the objective is to reduce the amount of information present in the graphs generated to represent the attacks and their properties (attack profiles). The solution is based on the simplification of graphs based on the similarities between characteristics (e.g., IP similarity). This technique can be useful for those technical characteristics that can be aggregated, but some subjective parameters could be more complicated for aggregation, especially if the information about the attack/er is incomplete.

Despite the aforementioned contributions, the relationship between IoT devices, humans and cybersecurity is not usually found in the definition of cybersecurity profiles. Although several tools can help define such relationships (e.g., Maltego includes "persons", "cameras" and "vehicles" as entities to be related to each other), this is not trivial because both worlds—social (human) and technical (devices)—are still treated separately by professionals from different areas. As stated in [11], useful information about IoT devices can be acquired from different sources. This information can help complete cybersecurity profiles.

Human Factors

The term *Human Factors* in cybersecurity is not clearly defined. Until now, this concept has been closely linked to insiders (e.g. employees with access to an organisation that decides to act against it) and closely related to ergonomics [12]. However, that is insufficient to cover cybersecurity, which is a very general concept as ENISA stated [13]. Therefore, this concept needs to be redefined in order to adapt it to our context.

We define the concept of Human Factors for Cybersecurity (HFC) as *any piece of information that can be related to a Cybersecurity profile; be it virtual and/or physical*. In Fig. 1 we show the nature of human factors expressed in terms of conceptual bubbles which define features to be expressed. This classification arises from the need to define a set of general characteristics that will turn into specific aspects as a digital

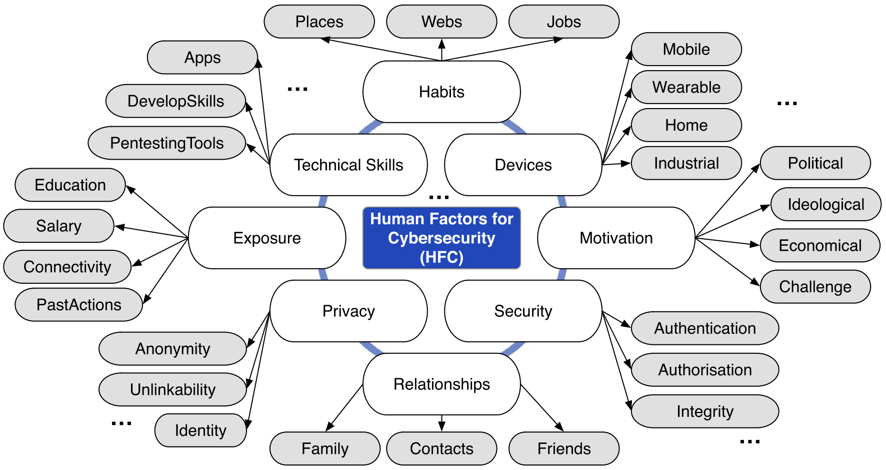

Fig. 1 HFC approach for the definition of cybersecurity profiles. Bubbles representing relevant concepts for a cybersecurity profile in a first level of abstraction

investigation progresses. Most of the human factors described below (first level) need the acquisition of digital evidence from different sources and the analysis of the data in order to be useful during an investigation.

The following sections will provide more details about the implications of this definition.

Habits

The habits of a person are very representative of the personality and routines of that person. In this paper, habits are considered at any level (in order to serve different disciplines); daily routine of the suspect, favourite programming language (if any), etc. The habits or manias of a person can help in the identification and even the tracking. For example, habits can help determine the location of an individual (e.g., working hours). Some habits will be chosen by the individual, while others will be imposed by society or necessity. The habits of an individual cannot be expressed by a unique parameter, because the information at this point can be very different. Instead, this requires a division into multiple domains, depending on the activity of the individual. For example, it is possible to determine the time and days a user is online by monitoring his/her activity in social networks. This can be done manually or automatically using the Application Programming Interface (API) to connect to social networks and track the behaviour of the users. If the account of the user in question is private then additional steps may be necessary, for example trying to connect with the target. The tool Tinfoleak [14] enables the collection of information about a Twitter user, the devices used by him/her to connect and any other valuable information that can be stored in a cybersecurity profile.

Devices

The devices closest to an individual can contain relevant information for a digital investigation. In this respect, IoT devices play a fundamental role as they provide a network's sensing capacity. These sensory capabilities are what provide vital information for an individual's decisions. IoT devices should be considered not only as tools against an individual (e.g., in case they are controlled remotely by an attacker) but also as potential tools to stop cyberattacks or to store relevant data about unusual activities (e.g., used as IoT-forensics tools [15]). As for the tools to gather information from devices, it is worth mentioning Shodan [16] which can be used as in Listing 1 but with devices instead of users. That is, Shodan can be used as a browser for devices, including IoT devices. Once we know the characteristics of a user's device it is possible to determine additional information about it using Shodan. Furthermore, it is possible to know the degree of exposure of a victim because Shodan can be used to search for vulnerable devices based on various criteria. In addition, some papers such as [17] analyse the need for labelling IoT devices, and others such as [18, 19] identify new scenarios where IoT devices must be integrated.

Motivation

The motivation behind an attack is highly relevant. Some authors have classified cyberattacks based on the motivations to commit the crime [20]. By using the motivation as a characteristic in a cybersecurity profile it can be possible, for example, to extract relationships between individuals which can derive from common motivations to commit cyberattacks (e.g., relationships motivated by hacktivism). However, this feature is not necessarily associated with the relationships between individuals because some cyberattacks can be motivated by other factors, such as revenge or hate. As such, this characteristic will be strongly related to a cyberattacker profile rather than a cybervictim. Moreover, it will be highly dependent on the rest of the parameters in a cybersecurity profile.

Security

Security mechanisms can help protect individuals from cyberattacks. As suggested by the routine activity theory, this will affect the suitability of a victim to be attacked given that security tools are in place protecting the victim. It is expected that security tools will be able to limit the scope of a cyberattack. However, this will depend on the security mechanisms used and the context of the cyberattack. Unfortunately, the attacker can also use security tools to commit cyberattacks (e.g., *ransomware* uses encryption to cipher the disk). This feature is necessary to understand how security tools can be used to minimise the scope of the cyberattack, even when the cyberattackers are using their own security tools. In addition, packers and obfuscators are considered as security solutions by many developers who want to protect their source code, preventing it from being copied or replicated by third parties for dishonest purposes. Cyberattackers also use these tools to protect their malware code.

Relationships

The relationships of an individual with others help determine group habits. The theory of social learning indicates that criminal behaviour (also named *deviant behaviour*) is learned from the social circumstances surrounding an individual [21]. For example, in [22] software piracy and hacking activities are analysed in the context of friendship relationships of students. The analysis determines that if the student's friends participate in these activities, the student will be more likely to do so as well. Therefore, the relationships of an individual can determine the motivations for a cyberattack. Tinfoleak also helps identify relationships between users in Twitter. However, this is not enough. It is necessary to correlate this information with other networks to determine the strength of the relationship in question. Users with relationships in different social media could have a relationship on the physical plane. Listing 1, written in Phyton, checks a set of user profiles using Pipl [23]. Pipl is a browser that helps to verify the identities and investigate people. This can be used to get a basic profile of a set of *human* targets and then, using additional sources, to correlate them. Like many other tools, this one provides an API for developers that can be used in any source code. This tool requires an API key to collect the data. In this case, the use of the API is not entirely free. The responses of this tool can give us the following information: gender, phone, address, country, education, ethnicity, image, job, language, etc. This information, together with additional information from other sources (e.g. Tinfoleak) can enrich a context formed by cybersecurity profiles. For example, some artefacts such as files (e.g. images) can be processed to extract and analyse the metadata and then use this new data to contrast the information in the profile (e.g. using Foca [24]).

Listing 1 Get information about users

```
def searchUsersPublicInfo(self):
    # 1.- Get users in a context
    users = self.context.getall(Context.USER)
    # 2.- Perform the requests:
    for u in users:
        request = SearchAPIRequest(u.email(), u.name(),
                                   u.last_name(), self.APIkPipl)
        response = request.send()
        self.context.correlate(response)
```

Privacy

Although it may seem obvious that cyberattackers want to remain completely anonymous and their actions undetected, this is not always the case. Some cyber-attackers, like terrorists, tend to claim responsibility for their actions in order to show the world what they are capable of. In such cases, they typically want to reveal their identity but wish to keep their location undisclosed because this could lead to their arrest and imprisonment. Therefore, the use or lack of privacy mechanisms can be a relevant piece of information when building a cybersecurity profile. Not only that, but also the type of privacy tools used (e.g., encrypted communications, proxy servers, anonymity overlays, steganography, and so on) can help infer the motivations or technical skills of an attacker.

Exposure

Users have different degrees of exposure depending on the technologies they use and their technical skills. Moreover, the degree of exposure is related to the habits of the individual (e.g. participation in forums or presence on social networks). In general this affects the footprint of a person on the Internet. The level of exposure of an individual is closely related to the *suitability* of a victim *to be attacked* (c.f. routine activity theory [6]). This must be adapted to the cybersecurity context and also consider the scenarios where this is possible (e.g., proximity-based attacks [25]). Some factors that can influence this feature are, for example, the past actions (e.g., probability of re-offending) and the level of education to identify the specific threat to which the victim is exposed. Note that the degree of exposure not only affects a potential victim but can also measure the probability that an actor will become criminal. The completeness of these data will depend on cooperation with law enforcement agencies (LAW) to determine documented past actions and convictions.

Technical skills

Technical skills are relevant to cybersecurity profiles in different ways. For example, this feature can be useful to determine the feasibility or even the likelihood of committing a certain type of cyberattack. Some attacks do not require sophisticated technical skills, as is the case of cyberbullying. Therefore, the absence of technical skills is also a characteristic in itself. Interestingly, this human factor should not only be seen from the point of view of the attacker, but also as the ability of the victims to protect themselves or identify a possible threat. As shown next, this may also be related to security and privacy features, but not necessarily. Technical skills can be measured in different ways, but many of them are subjective or depend on the analysis of artefacts. For example, if the user in question participates in technical forums or advanced groups whose members are chosen only by invitation, it can be deduced that this individual has technical skills. Moreover, if the suspect is using a repository such as GitHub, then this can help us determine his/her skills by analysing this code. Things to take into consideration range from the type of tools used, the presence of typos in the code or preferred obfuscators (if any).

Building dynamic cybersecurity profiles

In this section we focus on high-level requirements that must be considered when defining cybersecurity profiles. These requirements are detailed below.

Addressing *Uncertainty* during a digital investigation

The information that is considered relevant changes during the various phases of a digital investigation: identification, acquisition and analysis/investigation (c.f. ISO/IEC 27043:2015). Therefore, the nature of the problem to be solved requires a *dynamic model* capable of integrating new information; starting with a basic set of characteristics that might change as soon as new and fresh information is available.

This notion fits nicely with the *Context-based Parametric Relationship Model* (CPRM) proposed in [26]. This model helps define a dependencies-based system and there is a extensible tool which can be configured with an initial set of parameters, will be used in a later section to implement a proof-of-concept for HFC.

A CPRM is not static; instead, the definition grows as more information becomes available about the final context. This can be useful to define those cybersecurity profiles for which not all the information is available from the beginning.

In order to provide a dynamic and extendable solution, HFC can be expressed, following the rules for a CPRM-based context, using the parameters that are critical to define the cybersecurity profiles. Initially two types of parameters must be defined:

- General parameters (GP). The most abstract, high-level definition of a parameter which is understandable by any expert (e.g., “Devices”). These parameters can be detailed as types or layers; can even be detailed as part of a *general context* (GC) structure. This will depend on the level of granularity desired to express the parameters and the relationships.
- Specific parameters (SP). More specific parameters that instantiate the previous parameters (e.g., Raspberry Pi can instantiate the general parameter Device). These parameters will be detailed as part of a *particular context* (PC) structure.

Following this notation, the first group of parameters (GP) must be defined considering the (general) requirements to define cybersecurity profiles, while the second group (SP) are more specific and will depend on the specific proof of concept.

The rules governing the dependencies between the parameters are further detailed in [26]. The objective in this paper is not to test CPRM, but rather to show how analysing the dependencies between the parameters in cybersecurity profiles can help during a digital investigation, by helping to select either the best methodology for organising the acquisition of evidence or the best tools to conduct the analysis.

Inclusion of virtual and physical descriptions

Cybersecurity profiles are destined to combine the *virtual* and *physical* profiles of an individual. These are the digital representations of the individual and the administrative information (e.g. European identity card), respectively. These values can be pure (only exists in the virtual or the physical plane) or hybrid (may have a presence in both planes). This is detailed below. In addition, it is also important to distinguish between *interpretation* of facts and facts. This is a requirement in ISO 27043 [27], in order to highlight the information that is subjective (e.g. the degree of intimacy in a relationship based only on a set of comments in a forum) from what is not (e.g. the name of a person).

In Fig. 2 a simplified example of a cybercriminal profile is shown. The aim of this example is to show why a criminal profile needs to be expressed using various types of parameters (virtual, real and hybrid). In this classification it is important to know that real parameters define facts that can lead to the prosecution of the cybercriminal or his identification. In the case of a remote cyberattacker perhaps we can only know his technical skills and additional info that can be highly subjective (e.g. a picture of a cat in his profile can lead us to think that he likes cats).

As stated, virtual parameters define a characteristic which is only present or valuable in cyberspace. For example, the reputation of a person in a forum only makes sense in the forum itself. This could have an effect on that person's physical life. In fact, the effect will be greater when the digital identity of the individual can be linked to the real identity.

Unlike virtual parameters, physical or real parameters express the physical context of a person, directly associated with the identity. For example, the social security

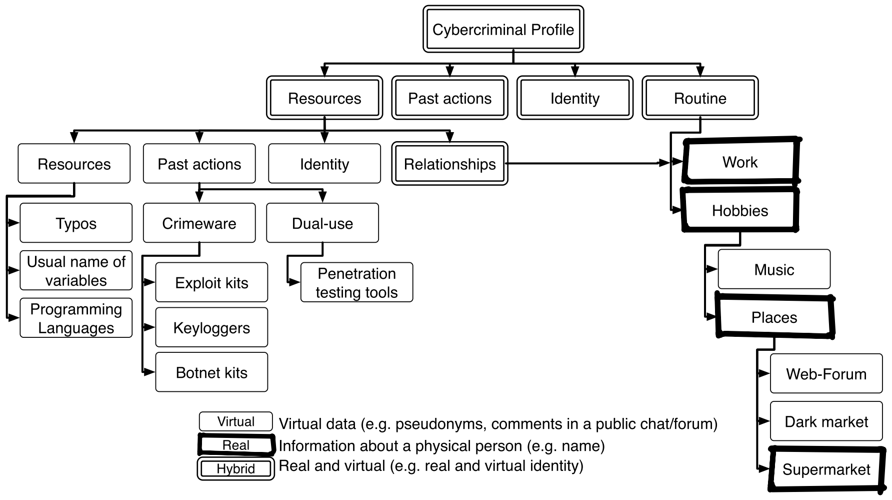

Fig. 2 Example of cybercriminal profile. Example of parameters that can be used to describe a cybercriminal profile. The parameters are classified as virtual, real and hybrid data

number or the identity card of a person is a physical parameter in itself. Also the physical places that an individual visits regularly are parameters that may provide relevant information.

The link between both types of parameters, virtual and physical, is very close. Indeed, there are some parameters that will be present in both worlds. In these cases the parameters will be denoted as hybrid (virtual and physical).

Ability to express tendencies

Ideally, cybersecurity profiles should be able to alert experts to possible threats (e.g., hate speeches). Powerful tools extract relevant information from social media (SOCMINT, c.f. "Related work") in order to identify patterns of threats that could be materialised in the physical plane (e.g., terrorism). For example, Tinfoleak [14] is a tool that is capable of gathering information about people from Twitter. It is possible, for example, to extract relationships between profiles. In addition, the tools Gephi [28] and Gource [29] can be used to show the relationships organised in visual graphs. Even so, the information deduced from these analyses is focused on determining trends in a specific topic (e.g., cyberterrorism), and also on identifying those individuals with the biggest diffusion capacity to be able to determine control points of the information. This is necessary because otherwise the analysis of the data could be unattainable. However, in order to define the expressiveness that a cybersecurity profile allows, it should be possible to relate parameters at different abstraction layers.

IoT devices as sources of data

IoT devices are close or even attached to their owners and other entities. However, when the *resources* used by the attacker are analysed (c.f., "Introduction"), how the presence of IoT devices changes the whole context is not further analysed. New definitions of cybercriminal profiles must consider IoT devices as particular cases, strongly linked to the users. Indeed, being aware of these devices can help determine the technical skills of an individual (e.g., based on the type of IoT device and the difficulty of configuring it), the capabilities of self-protection (e.g., based on the native security of the device) or the degree of exposure of a victim (e.g., given the vulnerabilities of the device).

As a matter of fact, there are several tools that can be used to search vulnerable devices connected to the Internet. For example, in [11] a methodology to define honeypots for the IoT is proposed, based on a preliminary search of vulnerable and accessible devices using search engines like Shodan [16]. The methodology also includes steps for classifying the adequacy of IoT devices to be emulated based on their position in the sales rankings and the suitability for attack. These premises are critical to understand the suitability of a victim to attack. New models must consider the ability to get information from these sources and use this information to complete the cybersecurity profiles about the individual.

Consider the following scenario. A potential victim wants to determine the degree of risk he is exposed to. So, this person decides to create a cybersecurity profile and indicates which IoT devices he is using. Without the appropriate technical skills, the tool should be able to complete the information about the IoT devices used by the victim, automating the searches in known websites for IoT devices, and advising the victim and the experts on how to improve the security of the victim, given the resources available. The criteria followed must be to minimise the chances of a cybercriminal being successful.

Human Factors for Cybersecurity profiles (HFC) methodology

The methodology proposed to define cybersecurity profiles based on human-centric IoT devices is denoted HFC. Instead of being a methodology restricted to IoT devices, the objective is to define a general methodology that can be fed with additional data from IoT devices when available. HFC is based on three general phases (Fig. 3):

- Preparation: decisions about the parameters and the representation/language are made in this phase, considering the requirements to build cybersecurity profiles.
- Feeding: the profiles are completed with online and offline data, manually or automatically depending on the tools chosen and/or the authorisation required to access the data.
- Analysis: defines the scope of the digital investigation and performs the analysis using the Human Factors for Cybersecurity (HFC) profiles defined as sources.

The requirements described thus far are addressed in the implementation of these phases. In particular, the language and tools used to model the HF profiles must be flexible enough to change dynamically as more information becomes available. The profiles must contain both virtual and physical information about the actor. During the analysis it must be possible to extract relevant information about the objectives considered given the scope of the digital investigation. Furthermore, in this methodology not only are *humans* important, but also the devices play a relevant role; in order to do that, specific searches must be carried out on the devices to complete the cybersecurity profiles. This will help, for example, to determine the degree of exposure.

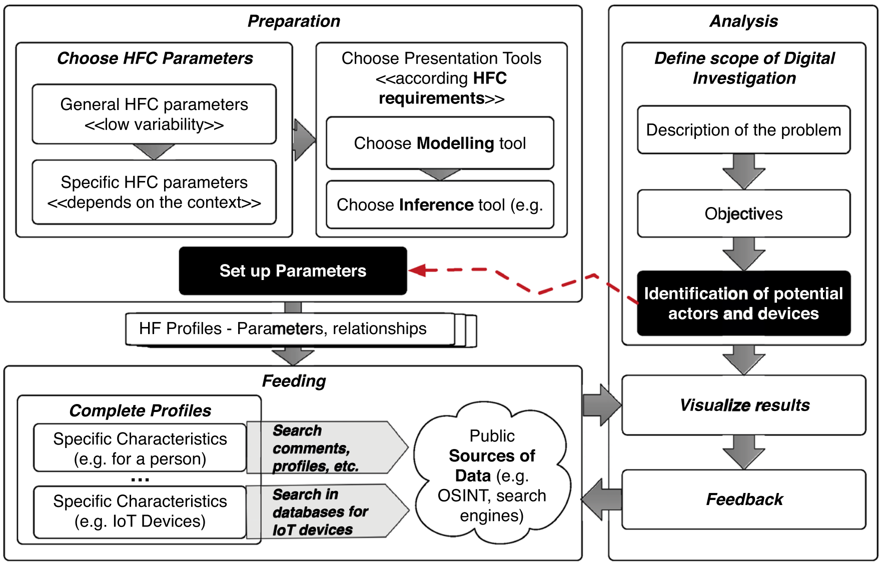
Preparation
Choose HFC Parameters
General HFC parameters <<low variability>>
Specific HFC parameters <<depends on the context>>
Choose Presentation Tools <<according HFC requirements>>
Choose Modelling tool
Choose Inference tool (e.g.
Set up Parameters
HF Profiles - Parameters, relationships
Feeding
Complete Profiles
Specific Characteristics (e.g. for a person)
...
Specific Characteristics (e.g. IoT Devices)
Search comments, profiles, etc.
Search in databases for IoT devices
Public Sources of Data (e.g. OSINT, search engines)
Analysis
Define scope of Digital Investigation
Description of the problem
Objectives
Identification of potential actors and devices
Visualize results
Feedback

Fig. 3 HFC methodology. Phases to define cybersecurity profiles based on parameters

The following subsections describe how to model the actors and devices considering the context of a digital investigation, as well as how to use the profiles to identify possible attackers after an incident.

Actors in a digital investigation

One of the purposes of building cybersecurity profiles is to help in the context of a digital investigation, as will be further described during the Proof-of-Concept. Therefore, it is critical to define the components used by HFC to express the context of a cybercrime scene.

As mentioned, in the routine activity theory, which is one of the theories used in criminology to understand a crime [6], the crime is delimited by the presence of (i) a suitable victim, (ii) a motivated offender and (iii) the absence of a guardian. This approach has its limitations in the context of cybersecurity, where victim and offender are not necessarily related by the same physical location. However, the division of the problem into these three actors is a good starting point to analyse the context. Following this approach, the three actors (criminal, victim and guardian) are modelled in the HFC methodology as Fig. 4 shows. In addition, a fourth actor is added in the role of *witness*.

This is closely related to the concept of digital witness defined in [15], where IoT devices are allowed to identify and report malicious actions suffered by their owners or help other devices in a crime scene to report an incident. The use of digital witnesses has several privacy implications which have already been analysed in [30]. While the concept of guardian is intended for entities with authorisation or privileges to perform actions on other entities (e.g. a police officer), a witness is an entity destined to include citizen collaboration in new methodologies such as HFC. Both, guardian and witness, can use security mechanisms, but the first one can have authorisation to apply reactive actions on other individuals/devices.

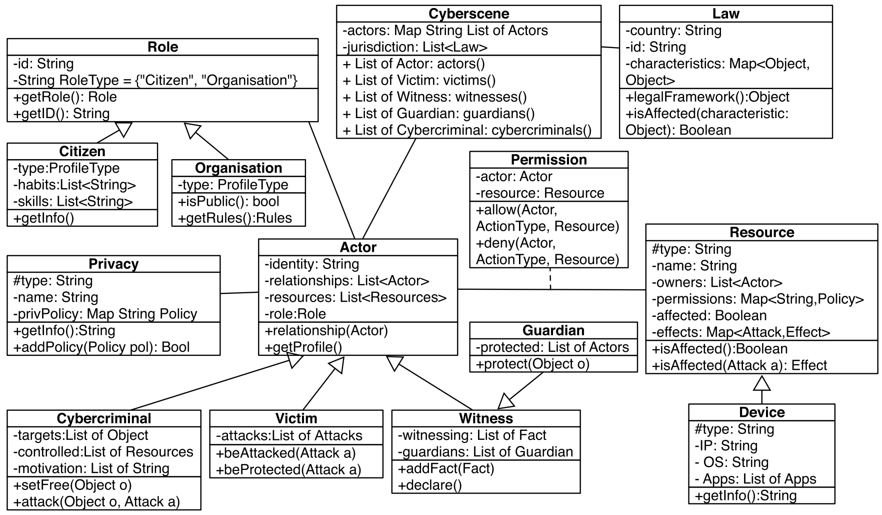

Fig. 4 Components in a cybercrime scene. This is a technical description of the components (and their relationships) to model a cybersecurity profile

In addition, each actor will have a certain role in the crime scene. In Fig. 4 we consider only two basic roles, namely citizen and organisation. The actors, regardless of their role, belong to the crime scene conditioned by the law(s) determined by the country and state. Privacy laws will be contemplated in this part. However, regardless of privacy laws, any person may have their own privacy requirements, and for this reason, Privacy is an entity on its own.

Finally, all the actors have a list of resources (e.g., tools) with which they interact based on a number of permissions (e.g., ownership or shared use). This last part can be critical to deduce relevant information that will affect the classification of the actors as one of the four types under consideration (criminal, victim, witness and guardian).

While a *resource* must be interpreted as a generic abstraction (e.g., it can be a software tool, a forum, a hardware component or a physical device), in this paper the analysis is focused on the role of the IoT devices as resources by their proximity to the actors in the crime scene.

Tools and methods for acquiring public information

The previous classification provides a basic set of empty parameters. Some of them should be completed with physical information about the individual (e.g., identity), while others can be completed using tools for acquiring information from public sources, using for example APIs when available in order to automate the searches and complete the profiles.

Some of these tools have been mentioned before (e.g. Tinfoleak, Pipl, Shodan), although the list is very long [9, 31]. Just as happened with penetration testing tools, there are emerging specific-purpose platforms devised for OSINT, such as Buscador [32], which integrates tools focused on this type of search. Some of these tools are indeed included in very famous penetration testing distributions such as Kali Linux. This is due to the enormous relevance of these searches during any recognisance phase. So, tools such as Maltego use API tools to collect data about users and devices and show relationships between users (performing similar requests to those shown in Listing 1. However, we still need more flexible solutions than currently existing ones. Dynamic parameters that can change depending on the context (or can be interpreted in a different way) must be considered, as well as establishing a much more intimate link between a user and the devices surrounding him so as to take full advantage of this relationship for the process of data correlation.

In addition, the use of these tools must be accompanied by the intuition of the digital investigator to discern which data is most relevant and be able to identify new clues.

Matching cybersecurity profiles in private environments

Last but not least, it is important to remark that cybersecurity profiles may have different requirements for their generation and maintenance. This can depend on the role of the user (victim, attacker, guardian). Also, the use of this methodology can change depending on the context of the digital investigation. For example, considering a database with information about cybercriminals (that is not public), the profiles can be compared and updated after a cyberattack as Fig. 5.

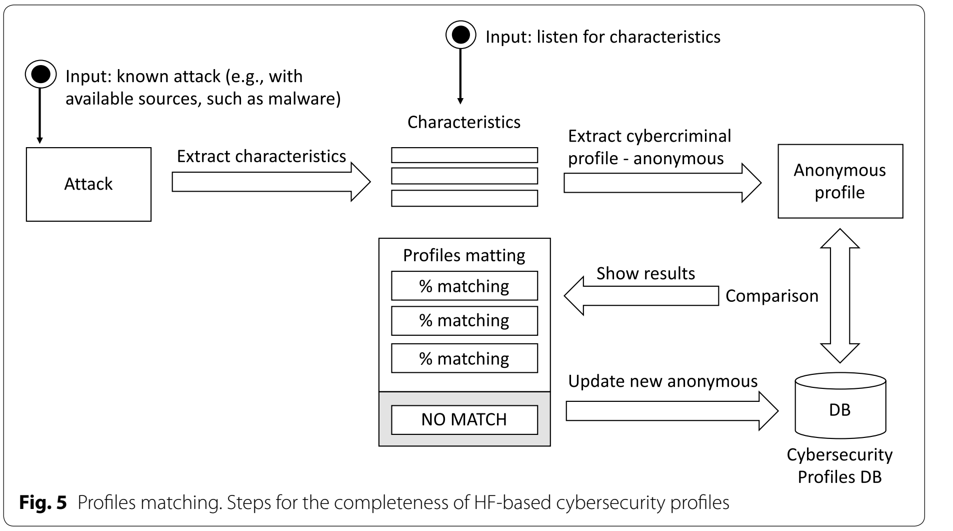
Input: listen for characteristics
Input: known attack (e.g., with available sources, such as malware)
Characteristics
Attack
Extract characteristics
Extract cybercriminal profile - anonymous
Anonymous profile
Profiles matting
% matching
% matching
% matching
NO MATCH
Show results
Comparison
Update new anonymous
DB
Cybersecurity Profiles DB

Fig. 5 Profiles matching. Steps for the completeness of HF-based cybersecurity profiles

The profiles can be created on demand or after an attack. In the second case, some characteristics might be extracted from the incident (e.g., using logs or malicious code gathered by a honeypot). These characteristics must be processed and completed using external sources (e.g., OSINT tools). Then, some parameters can be identified (those that are considered by the experts in the cybercriminal profile defined). In the case there is no information available about who the attacker is, the first profile is anonymous. This can change if new inputs are received or new information is inferred during the lifecycle of the digital investigation. The profiles must be compared with other databases containing profiles to determine if there is a profile, similar or equal to the anonymous profile. If the tool finds a match, then the profile is no longer anonymous and the existent profile is completed with the new information about the attack. Otherwise, a new entry must be added to the database.

Note that only one database is shown in Fig. 5. Ideally, the database should be shared by multiple experts and organisations participating in a digital investigation or under certain cooperative conditions. These scenarios must be analysed with utmost care, taking into consideration any privacy laws and regulations applicable [30].

Proof of concept

This section presents a proof-of-concept for the HFC methodology considering the manual representation of cybersecurity profiles. The history behind and the actors in it are not real. The incident (data leak) has been prepared in a controlled environment and is used in practice to teach digital forensics to our students. We apply the methodology to this use case in order to check whether or not the results correspond with the logical interpretation after the analysis of the digital evidence.

In what follows the methodology is used to describe the characteristics of a set of potential suspects during a digital investigation. To do so, we define a initial set of dependencies between the parameters in Table 1 that will be modified based on the specific information in the profiles of the users, which are simplified for the sake of clarity.

Table 1 Example: Three actors defined based on HFC characteristics

Characteristic	Denise Cantora	Bob Protocolo	Clark Firewall
Habits	9:30–14:30: working	9:30–14:30: working	15:30–18:30: working
	Hobbies: marketing, management, office	Hobbies: Recipes, desserts	Hobbies: Hacking, security
Technical Skills	Apps: OpenOffice, Thunderbird	Apps: OpenOffice, Tunderbird	Apps: fcrackzip, Thunderbird
	Role: user	Role: user	Role: admin
Devices	PC={IP:192.168.1.3, OS:Win10(user)}	PC={IP:192.168.1.4, OS:Win7(user)}	PC={IP:192.168.1.2, OS:Ubu10(admin)}
	Smartphone(own), USB (shr)	Smartphone(own), USB(shr)	Smartphone(own), USB(shr)
		USB Printer	Router(admin)= {IP:192.168.1.1}
			Allow(admin)={Denise's PC; Bob's PC}
			Rubber Ducky
Exposure	WebActivity: high	WebActivity: high	WebActivity: high
	Character: distrustful	Character: friendly	Character: trusted
	Salary: very good	Salary: low	Salary: very low
	Job: AC Directive	Job: Creative	Job: Technician
	Past: None	Past: betrayed the company	Past: None
Motivation	Personal	Economical, revenge	Economical, challenge
Privacy	vid: dcantora	vid: bprotocolo	vid: cfirewall
	Domain: acantora.com	Domain: acantora.com	Domain: acantora.com
	pol:null	pol:null	pol:null
Security	AC: user mode	AC: User mode	AC: Admin
	pol: Default	pol: Default	pol: Default
	dem: null	dem: null	dem: null
	idps: Win.Defender	dem: Win7 Firewall	dem: Ubu18 Firewall
			Tools: Secure Erasure
Relationships	Contacts: Bob Protocolo, Clark Firewall	Contacts: Abuela Cantora, Denise Cantora	Contacts: Denise Cantora
	Family: Abuela Cantora	Family: Alice Protocolo	
	Friends	Friends: Clark Firewall	Friends: Bob Protocolo, Sue Picious

own owner, *shr* shared, *vid* virtual id, *id* identificator, *pol* policy, *AC* access control, *dem* digital evidence management, *idps* intrusion detection and prevention system

As detailed in the previous sections, this information can be completed using API tools to acquire public information about the suspects. However, in this case we prefer to focus on the dynamic adaptation of the context for the interpretation of the digital investigation based on the profiles, since it is an aspect that cannot be implemented using the APIs. The integration of new information from the APIs is for future work because it requires the design of new correlation models that are beyond the scope of this paper.

Set-up of basic profiles based on HFC characteristics

Table 1 defines characteristics for three users of a system that has suffered a data leak. The (fictious) incident is as follows.

The incident has occurred in a family business called *La Abuela Cantora*. None of the users seem to be guilty; Clark is the administrator of the network but his technical skills (and security expertise) are quite limited. A USB Rubber Ducky [33] has been found camouflaged as a normal USB device in a set of USBs shared between the three suspects. This is assigned to Clark, who has acknowledged that he received it through a contact but did not know what it was.

The three participants have mixed feelings: Denise thinks that Bob is responsible because in the past he betrayed the company by leaking secrets to the reporter Alice Protocolo. On the other hand, Bob distrusts Clark because he considers him a hacker. Clark believes the attacker is an outsider.

A Rubber Ducky is a special USB. Once connected to the victim's machine it will install keyboard drivers and will not be announced as a storage device. Instead, it will use its emulated keyboard and its mini processor to execute commands on the victim's computer. In this example, the Rubber Ducky has been prepared to open a backdoor in the victim's computer, which was Denise's computer. Then, the attacker, using Meterpreter copied documents (some traces are also observed in the memory). This is something that can be observed once the digital investigator starts to analyse the devices of the three suspects.

It is important to try to deduce information using the characteristics showed in Table 1 and understand if these should be completed and how. This can help improve the timeline of the digital investigation.

In order to test our approach the CPRM model [26] is used to represent the information shown in Table 1. To that end, the characteristics have been expressed in layers (e.g, habits, devices) and the specific, common descriptors inside the characteristics (e.g., hobbies, apps, role) have been defined as general parameters inside the layers. The relationships between the parameters have been defined to express the dependencies between them. The tool [26], implemented in Matlab [34], uses Graphviz [35] to generate graphs as Fig. 6 shows. The graphs can be quite complex, and this is one of the reasons why the analysis is based on the results after operating with these graphs.

Analysis-preliminary results

The specific values for the different actors are expressed as particular contexts. Based on the initial information, Clark's profile has the higher probability of being considered the *offender*. This is because of his role in the system but also given that he has specific tools that could have been used to commit the attack (e.g., Rubber Ducky) and the fact that he has also shown interest in hacking pages. Similarly, Bob is more likely than the rest of participants to be the *victim*. The reason for this is that his computer does not have security tools enabled beyond the Windows 7 firewall. Furthermore, the code programmed for the Rubber Ducky is intended for Windows systems; Denise also uses Windows, but Windows Defender will stop this specific threat.

To make the analysis feasible, the model is trained using a basic set of parameters and relationships. When the parameters or the relationships change then the expected behaviour also changes. The objective in this case is to evaluate whether or not the model can determine if the suspects (Denise, Bob or Clark) are potential victims, offenders, guardians or witnesses. Therefore, the *target* in our requests to the tool are the parameters targeted as "Actors": Victim, Offender, Guardian, Witness. The model, without being instantiated shows the expected behaviour in Fig. 7. This means that, as it is, there are many more parameters that finally influence the parameter "Offence". This is

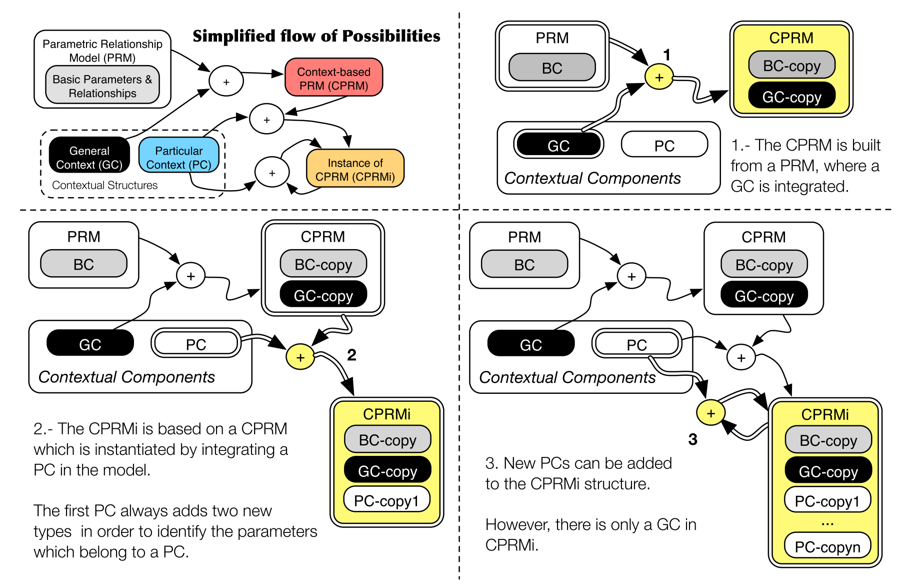
Simplified flow of Possibilities
Parametric Relationship Model (PRM)
Basic Parameters & Relationships
Context-based PRM (CPRM)
General Context (GC)
Particular Context (PC)
Contextual Structures
Instance of CPRM (CPRMi)
+
PRM
BC
CPRM
BC-copy
GC-copy
1
GC
PC
Contextual Components
1.- The CPRM is built from a PRM, where a GC is integrated.
2
CPRMi
PC-copy1
2.- The CPRMi is based on a CPRM which is instantiated by integrating a PC in the model.
The first PC always adds two new types in order to identify the parameters which belong to a PC.
3
PC-copyn
3. New PCs can be added to the CPRMi structure.
However, there is only a GC in CPRMi.

Fig. 6 CPRM-based tool. Schema used to model the solution. In this figure a portion of the relationships defined to model the use case is shown

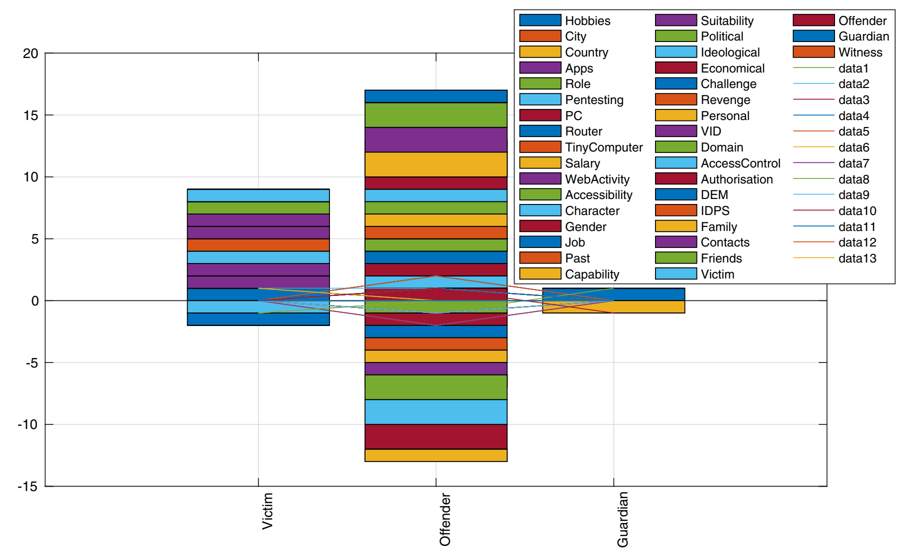

Fig. 7 Impact on target parameters. Default behaviour before providing the parameters with specific values for their profiles (instantiation). The values denoted as *data* only represent the lines without aggregation

not good or bad, it is merely the way in which the parameters and relationships have been defined for this use case.

What really changes the results is the *particular context* (PC) defined for each participant in the experiment. In this case, there are three PCs, one per physical actor: Denise, Bob and Clark. The PCs have been defined based on the columns in Table 1. In this

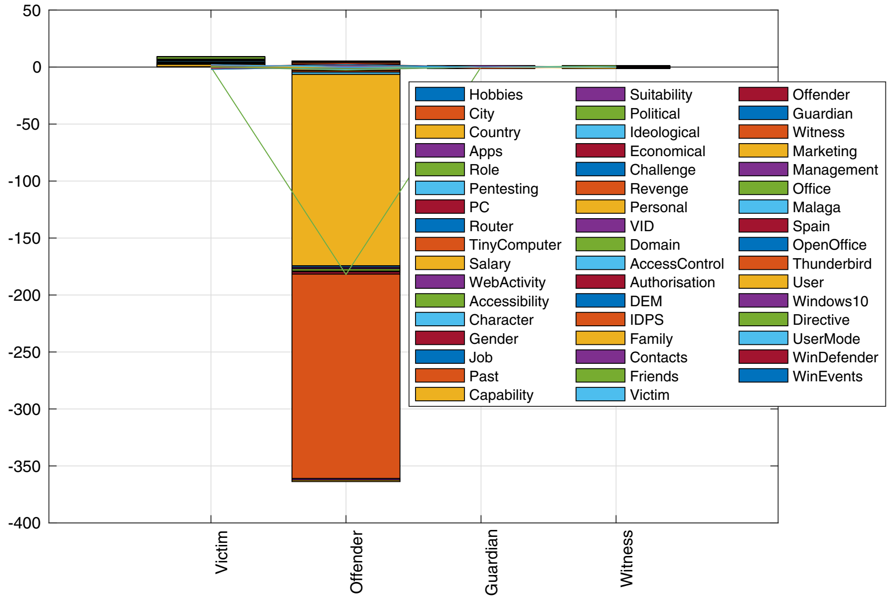

Fig. 8 Impact on target parameters. Results for Denise

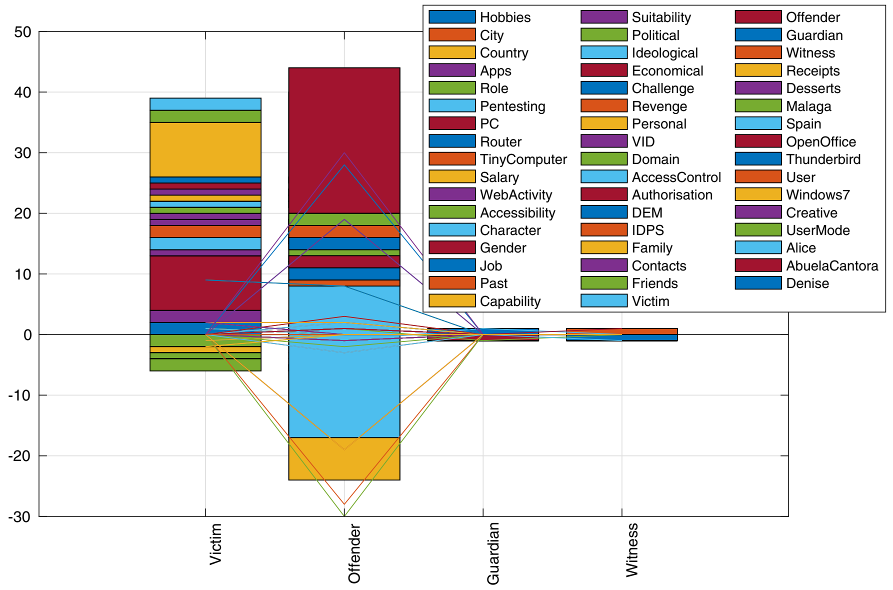

Fig. 9 Impact on target parameters. Results for Bob

experiment, each PC will be combined, separately, with the previous context (Fig. 7). More specifically, Figs. 8, 9 and 10 show the results after combining each profile (Denise, Bob and Clark) with the basic behaviour defined previously. This is done using the rules defined in the CPRM model. Using these rules the dependencies between the parameters can be expressed and those considered as *general* can be broken down into more specific parameters in a process defined as *instantiation*, which is a process that in turns

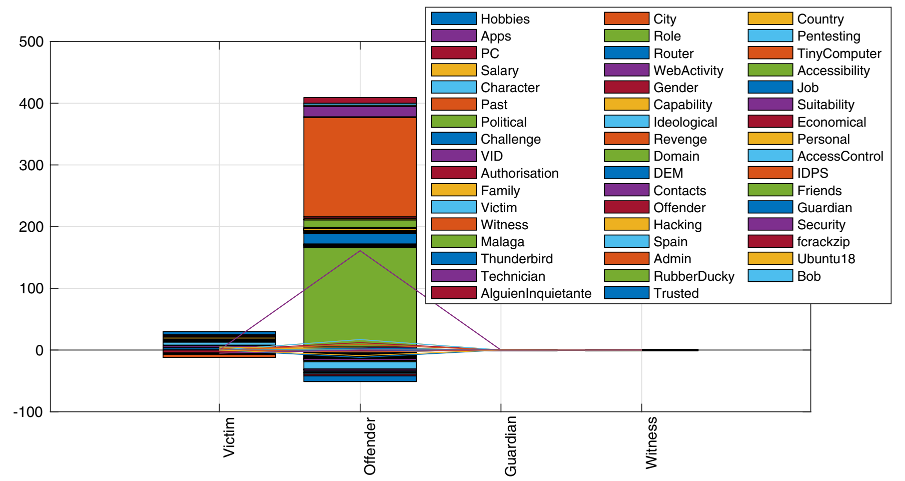

Fig. 10 Impact on target parameters. Results for Clark

has its own definition of conditions (c.f. mathematical formulation and description of rules of a CPRM model [26]).

For example, during this example the model is used to interpret the type of profile of Denise, Bob and Clark by defining the parameter Actor and instantiating this value with the parameters "Victim", "Guardian", "Witness" and "Offender". Therefore, the results for the users depend on the specific values of the parameters in Table 1 (e.g. Technical skills for Denise, Bob and Clark). This language is highly dependent on and sensitive to context, which can be a limitation in a productive environment with a large number of parameters, but is useful to show a proof of concept of the methodology with a problem limited to three actors. In addition, note that when the number of parameters increases, the visualisation of results becomes very complex. For clarity we focus on those parameters that directly affect the interpretation implemented in the model.

The results in Fig. 8 show that, according to the model, Denise is probably not the Offender. Moreover, these results show that even combining an increasing and decreasing of parameters the values to be "Offensive" are negative. Denise could be a victim or a guardian/witness. The reason for these results is that during the modelling, Denise's operating system was considered to be more secure given the threat. Also, the relationship of Denise with the organisation (i.e., being a member of the family) decreases her motivational values. Moreover, Denise has a good salary and this decreases her Economic motivations to commit an attack. All these features affect the "Offender" parameter, which is minimised in the case of Denise.

In the case of Bob (Fig. 9), the results are more interesting. His Windows 7 operating system makes him vulnerable to the specific threat considered in this use case, which is motivated by a particular USB device belonging to Clark (apparently). His relationship with Alice Protocolo, who is known for being an activist at *"La Gaceta del RAT"*, makes his possible motivation to be "ideological". Then, there are various features that make Bob's system vulnerable and therefore can make him a potentially desirable victim. However, in this case the results are not completely conclusive. The capacity of Bob to commit this attack is not clear as he does not have proven technical skills. Nevertheless, this indecision could be an indication that this system is being used as a victim and attacker. This is the case indeed since the leak occurred in Bob's device after connecting the Rubber Ducky. Therefore the results are in line with reality.

At this point one would think that Clark is entirely guilty. The results for Clark are shown in Fig. 10. Clearly Clark has been targeted as Offender, with also a certain probability of being a victim. This is motivated by several factors. For example, Clark has access to the entire system because he is administrator. Also his salary is very low, so that is a motivation. His hobbies will not help his case either (hacking and security), although these could be understandable given his role in the system (e.g., if he is interested in improving security). Clark has the motivation, the opportunity and the weapon (Rubber Ducky).

Moreover, Clark has two people that he considers to be his friends. One is Bob Protocolo and the other one is Sue Picious. Initially Sue is not considered a relevant actor until the investigators' team reveal that he has exchanged several hacking emails with Clark and also sent him the Rubber Ducky. After this new information, the relationship between the parameters "Friends" and "Challenge" grows for Clark. This means that the values for "Offender" also grow. These results show that in this chain of facts the culpability of Clark could be higher than the rest of the actors.

Discussion

As has already been established, human factors are highly relevant to the definition of cybersecurity profiles. However, this is doubtlessly at odds with personal privacy.

On the one hand, the tools and mechanisms used to collect the information required for creating cybersecurity profiles may be sensitive. Therefore, data collection should not affect citizens unless there is plausible cause. Note that even privacy laws include provisions to allow for personal data collection without consent when it is deemed necessary to prevent and prosecute criminal activities, as well as to protect national or public security, among other reasons.

On the other hand, criminals are likely to use tools to prevent information about them being leaked. The most common tool for protecting information privacy is data encryption, as it prevents the content of communications from being spied on. Tools like PGP are common to enable this, although some applications, such as Silent Phone [36], are integrating built-in encryption capabilities. However, this is insufficient in most cases since the simple fact of knowing that two people are communicating may be sensitive information. More advanced tools for protecting online privacy are anonymous proxy servers and more concretely anonymity overlays, which consist of networks of proxy servers that hide the relationship between the communicating parties. Probably, the most well-known anonymity overlay is the Tor network [37]. While Tor allows anonymous access to Internet services, Freenet [38] creates a private network where users can create websites, share files and send/receive emails with other members of the network. Users cannot select what content they host, and it is stored encrypted.

When using protection tools it is worth noting that the privacy expectations of an individual may be jeopardised by others. When two users are known to be related to one another and the former is using a lower level of protection, the privacy of the latter is immediately reduced to the same level. For example, if one person is using location privacy obfuscation tools but a family member is posting geo-located pictures of both of them on a social network, the privacy protection of the former is clearly affected.

As a matter of fact, these and other tools are not only used by cybercriminals but also by military personnel, journalists, whistle-blowers and even ordinary citizens who want to protect their privacy or simply live in countries where Internet access is filtered by the government. Therefore, the use of a particular anonymity network or tool does not necessarily imply an illegal activity or behaviour but this together with other evidence helps complete the cybersecurity profile and make relevant inferences.

Conclusions and future work

The Internet of Things (IoT) is changing the cybersecurity context. *Humans* now depend on their devices more than ever before, and this dependence will continue to grow as IoT devices (e.g., wearables, sensors, cameras, etc.) not only simplify common tasks but also facilitate human interaction via social applications. As such, it is important to consider the relationships between humans and their devices as essential elements of the cybersecurity profiles.

The results of this paper will serve as guidelines to define cybersecurity profiles based on human factors and IoT devices. To this end, we have defined the concept of Human Factors for Cybersecurity (HFC) and used it as the core element of a new methodology. The HFC methodology can be extended with new features and can be used in various contexts. To validate our approach three profiles have been defined and tested using a Context-based Parametric Relationship Model (CPRM). Although the results demonstrate that the definition of cybersecurity profiles according to HFC can be useful during a digital investigation, it is important to note that the CPRM model, as it is, is not a sufficiently efficient approach when the number of parameters is large.

A final solution should be adapted to the actual platform/tools used to build the cybersecurity profiles. In this paper we simply wished to show how the profiles can be constructed progressively based on the requirements of a digital investigation. Moreover, although we have commented on tools that allow completing these profiles with publicly available data, this part of the methodology has not been implemented during the proof of concept. We are already working in this direction but as this may require the definition of new models for the correlation of data, this has been left for future work.

Authors' contributions

Both authors have equally contributed to the development of this paper. Both authors read and approved the final manuscript.

Funding

This work has been financed by the Spanish Ministry of Economy and Competitiveness through the project IoTest (TIN2015-72634-EXP/AEI), and by the European Unions Horizon 2020 research and innovation programme through the project NECS (H2020-MSCA-ITN-2015-675320). The first author has been financed by INCIBE (INCIBEI-2015-27326) through the program of aids for the excellence in advanced cybersecurity research teams. The second authors is supported by the 'Captación del Talento Investigador' fellowship from the University of Málaga. In addition, the scenario in the proof of concept has been motivated by the Educational Innovation Project PIE19-183 funded by the University of Málaga.

Availability of data and materials

The material used to conduct the experiments in this manuscript will be published by the authors.

Competing interests

The authors declare that they have no competing interests.

Received: 1 February 2019 Accepted: 16 October 2019
Published online: 01 November 2019

References

1. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376. https://doi.org/10.1109/COMST.2015.2444095
2. IoT Analytics. market insights for the internet of things: State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. Accessed 2019
3. Bashir M, Wee C, Memon N, Guo B (2017) Profiling cybersecurity competition participants: self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Comput Secur 65:153–165
4. Kocsis RN, Palermo GB (2016) Criminal profiling as expert witness evidence: the implications of the profiler validity research. Int J Law Psychiatry 49:55–65
5. Nykodym N, Taylor R, Vilela J (2005) Criminal profiling and insider cyber crime. Comput Law & Secur Rev 21(5):408–414
6. Chon KHS et al (2016) Cybercrime precursors: towards a model of offender resources
7. Chen M, Ghorbani AA et al (2019) A survey on user profiling model for anomaly detection in cyberspace. J Cyber Secur Mobil 8(1):75–112
8. Loukas G, Kapetanakis S (2014) Towards real-time profiling of human attackers and bot detection. In: In Proceedings of CFET 2014: cybercrime Forensics Education & Training. Citeseer
9. Nordine J. OSINT Framework. https://osintframework.com. Accessed 2019
10. Pillai M, Karabatis G (2016) Using multiplex networks to model cybersecurity attack profiles. In: OTM confederated international conferences "On the Move to Meaningful Internet Systems". Springer, pp 918–933
11. Acien A, Nieto A, Fernandez G, Lopez J (2018) A comprehensive methodology for deploying IoT honeypots. In: International conference on trust and privacy in digital business. Springer, pp 229–243
12. Salvendy G (2012) Handbook of human factors and ergonomics. Wiley, Hoboken
13. Brookson C, Cadzow S, Eckmaier R, Eschweiler J, Gerber B, Guarino A, Rannenberg K et al (2015) Definition of cybersecurity-gaps and overlaps in standardisation. Heraklion, ENISA
14. Tinfoleak: Search for Twitter users leaks. https://tinfoleak.com. Accessed 2019
15. Nieto A, Roman R, Lopez J (2016) Digital witness: safeguarding digital evidence by using secure architectures in personal devices. IEEE Netw 30(6):34–41
16. Shodan: The world's first search engine for Internet-connected devices. https://www.shodan.io. Accessed 2019
17. Matheu-García SN, Hernández-Ramos JL, Skarmeta AF, Baldini G (2019) Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Comput Stand Interfaces 62:64–83
18. Ravishankar Rao A, Clarke D (2019) Perspectives on emerging directions in using IoT devices in blockchain applications. Internet Things. https://doi.org/10.1016/j.iot.2019.100079
19. Ficco M, Palmieri F (2019) Leaf: an open-source cybersecurity training platform for realistic edge-IoT scenarios
20. Uma M, Padmavathi G (2013) A survey on various cyber attacks and their classification. IJ Netw Secur 15(5):390–396
21. Udris R (2017) Psychological and social factors as predictors of online and offline deviant behavior among Japanese adolescents. Deviant Behav 38(7):792–809
22. Hollinger RC (1993) Crime by computer: correlates of software piracy and unauthorized account access. Secur J 4(1):2–12
23. Pipl: The World's Leader in true identity solutions. https://pipl.com. Accessed 2019
24. Eleven Paths: FOCA: Fingerprinting Organizations with Collected Archives. https://www.elevenpaths.com/es/labstools/foca-2/index.html. Accessed 2019
25. Nieto A, Acien A, Lopez J (2018) Capture the rat: proximity-based attacks in 5g using the routine activity theory. In: 2018 IEEE 16th Intl Conf on dependable, autonomic and secure computing, 16th Intl Conf on pervasive intelligence and computing, 4th Intl Conf on Big Data intelligence and computing and cyber science and technology congress (DASC/PiCom/DataCom/CyberSciTech), IEEE, pp 520–527
26. Nieto A, Lopez J (2014) A context-based parametric relationship model (CPRM) to measure the security and QoS trade-off in configurable environments. In: ICC, pp 755–760
27. International Organization for Standarization: ISO/IEC 27043:2015–Security Techniques–Incident investigation principles and processes. https://www.iso.org/standard/44407.html
28. Gephi: The Open Graph Viz Platform. https://gephi.org. Accessed 2019
29. Gource: A software version control virtualization tool. https://gource.io. Accessed 2019
30. Nieto A, Rios R, Lopez J (2018) IoT-forensics meets privacy: towards cooperative digital investigations. Sensors 18(2):492
31. Bazzell M (2018) Open source intelligence techniques: resources for searching and analyzing online information. CreateSpace Independent Publishing Platform, Santa Cruz
32. Intel Techniques: Buscador 2.0 OSINT Virtual Machine Released. https://inteltechniques.com/blog/2019/01/25/buscador-2-0-osint-virtual-machine-released/. Accessed 2019
33. Hak5: USB Rubber Ducky. t. https://shop.hak5.org/products/usb-rubber-ducky-deluxe. Accessed 2019
34. The MathWorks, Inc.: Matlab. https://www.mathworks.com/products/matlab.html. Accessed 2019.
35. Graphviz: Graph Visualization Software. https://www.graphviz.org. Accessed 2019.
36. Silent Circle: Secure Enterprise Communication Solutions. https://www.silentcircle.com. Accessed 2019
37. The Tor Project: Tor-Anonymity Online. https://www.torproject.org. Accessed 2019

38. FREENET: Browse websites, post on forums, and publish files within Freenet with strong privacy protections. https://freenetproject.org. Accessed 2019

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.