Security and Privacy Requirements Engineering for Human Centric IoT Systems using eFRIEND and Isabelle

Florian Kammüller and Juan C. Augusto and Simon Jones
Department of Computer Science
Middlesex University London
Email: {f.kammueller|j.augusto|s.jones}@mdx.ac.uk

Abstract—**In this paper, we combine a framework for ethical requirement elicitation eFRIEND with automated reasoning. To provide trustworthy and secure IoT for vulnerable users in healthcare scenarios, we need to apply ethics to arrive at suitable system requirements. In order to map those to technical system requirements, we employ high level logical modeling using dedicated Isabelle frameworks for (1) infrastructures with human actors and security policies, (2) attack tree analysis, and (3) security protocol analysis. Following this outline, we apply these frameworks to a case study for supporting Security and Privacy when diagnosing Alzheimer's patients with smartphone and sensor technology.**

I. Introduction

The Internet of Things (IoT) denotes the combination of physical objects with their virtual representation in the Internet. It consists not only of human participants but "Things" as well. The IoT has a great potential to provide novel services to humans in all parts of our society. Amongst the biggest problems for this technology to catch on in critical applications are security flaws, due to technical restrictions, immaturity of software applications, and mainly a lack of transparency. The main trigger for security problems is human behaviour, either unintentional or malicious. In this paper, we give an overview of how we apply formal techniques to enhance security and privacy of human centric IoT systems. We focus on healthcare aiming to support low-cost Alzheimer's diagnosis. We outline the process used in the CHIST-ERA project SUCCESS. In detail, we report on using a combination of the ethical framework eFRIEND with interactive theorem proving with Isabelle. The eFRIEND framework provides a set of rules to derive requirements based on ethical considerations which can be transformed into technical system requirements. We use the proof assistant for the modeling and attack analysis of infrastructures with humans and for the formal definition cryptographic. We apply the Isabelle Insider framework for human centric infrastructure analysis and the inductive approach for security protocol verification to support the secure IoT system development in the early security requirement phase as well as the technical network security level.

II. Background

This section provides a short summary of the techniques used in the process of formal development that is used in SUCCESS before highlighting the contributions of the current paper.

A. Overview of SUCCESS project

The core idea of our approach is to use formal methods and verification tools to provide more transparency of security risks for people in given IoT scenarios. SUCCESS will validate the scientific and technological innovation through pilots, one of which will be in collaboration with a hospital and will allow all stakeholders (e.g. physicians, hospital technicians, patients and relatives) to enjoy a safer system capable to appropriately handle highly sensitive information on vulnerable people while making security and privacy risks understandable and secure solutions accessible.

This international collaboration is funded by the European programme CHIST-ERA [1]. It applies techniques from hardware and software, user behaviour and human-computer interaction to a research pilot from the healthcare sector on supporting IoT monitoring techniques that are human understandable and can be certified by automated techniques.

- specification and verification techniques for secure IoT components and their composition [2],
- verification methods and risk assessment techniques [3] for IoT scenarios with models of human behavior [4], social interactions and human-system interactions,
- implementation and modeling languages with algorithms for the certification of safety, availability, secrecy, and trustworthiness across from the model to the platform [5].

B. Contribution of this Paper and Overview

This paper summarizes how the requirements for the IoT healthcare system can be derived using the eFRIEND framework leading to a high level formal specification in the Isabelle insider framework [4] which also allows attack tree analysis [6].

This first phase of the process, the eFRIEND framework, is introduced in Section III. Its use in the context of the SUCCESS project is illustrated in Section IV. We map a few of the requirements onto a simplified architecture and use cases for the pilot case study. As a result of this first phase, the input to the BIP-based analysis and component architecture design and certified code generation is provided. We omit details on this phase since it is not within the scope of the paper. The output of this process however is a Java Script smartphone app capable of synchronous communication within the phone and via Bluetooth with sensors in the environment of the phone in the patient's home. The communication of the smartphone app with data servers in hospitals and other institutions (like research centers) is asynchronous and channeled via the Internet. It cannot be part of the certified code generation in BIP (which is restricted to synchronous communication). Therefore, we show up in Section V what is the state of the art of technically realizing secure communication for privacy sensitive data using web services and data interchange formats using our own protocol that we have developed for this end-to-end secure connection [7],

III. eFRIEND Framework

One important aim of our research is to reinforce the link between the improved technology and problem solving capabilities and the human beneficiaries. The research we report in this article is consistent with other user-centric activities developed by the authors (see for example [8], [9]). Part of these user-centred activities involve the use of processes to develop systems which are better aligned with people's expectations. One such initiatives, is the use of the *eFRIENDS* ethical framework [10]. By *ethical framework* here we mean a set of principles which have to be considered when creating a system, in our case we developed it thinking specifically of Intelligent Environments (IEs) [11].

The shorter explanation of eFRIEND is that the following nine principles have to be observed in the construction of an IE:

1) Beneficence / Non-maleficence
2) Accessibility, Dignity, and Inclusiveness
3) User-centricity
4) Privacy
5) Data Protection
6) Safety, Security, and Reliability
7) Transparency
8) Autonomy
9) Multiple users (stakeholders) consideration

However eFRIEND aims to go beyond the usual (and of course, useful) philosophical debate about ethics in ICT. Our ethical framework is an engineering tool. Applying it really means teams have to embed its principles into the construction of the system itself, that is, stakeholders have to identify ways within the system to represent those nine principles above, developers have to translate them onto requirements and materialize them in the real system and stakeholders have to agree at the end these have been achieved in the behaviour of the system.

For example in our SUCCESS project possible ways to address these principles are as follows:

Beneficence: enhancing the well-being and quality of life of SUCCESSs primary users and intended beneficiaries

Non-maleficence: avoid causing harm to SUCCESS users and intended beneficiaries.

Accessibility: Where smartphones provide the point of access to SUCCESS, interface design heuristics, navigability and usability should be considered

Dignity: IoT networks should not replace or substitute for human care

Inclusiveness: Ensure equal access to potential benefits, regardless of socio-economic/cultural factors

User-centricity: A broad range of other stakeholders should be consulted, including health and social care professionals, and representatives of relevant professional and voluntary associations.

Privacy: SUCCESS should specify the terms of access to, and use of, diagnostic and therapeutic medical data, by 3rd party commercial entities such as insurance and pharmaceutical companies.

Data Protection: Informed consent procedures to include certification of authorised proxies or delegated users where primary users have diminished consent competence.

Security: Robust security and integrity of data transmission and transfer when live, between home and hospital systems, between patient records and other datastores, and between devices and IoT components.

Safety: using the system outside safe environments can endanger the user by attracting undesirable attention towards the mobile phone or its data.

Reliability: data loss or unavailability at optimal times will discourage adoption

Transparency: The functionality of SUCCESS, and its potential weaknesses and effects, should be explained to its primary users in understandable terms.

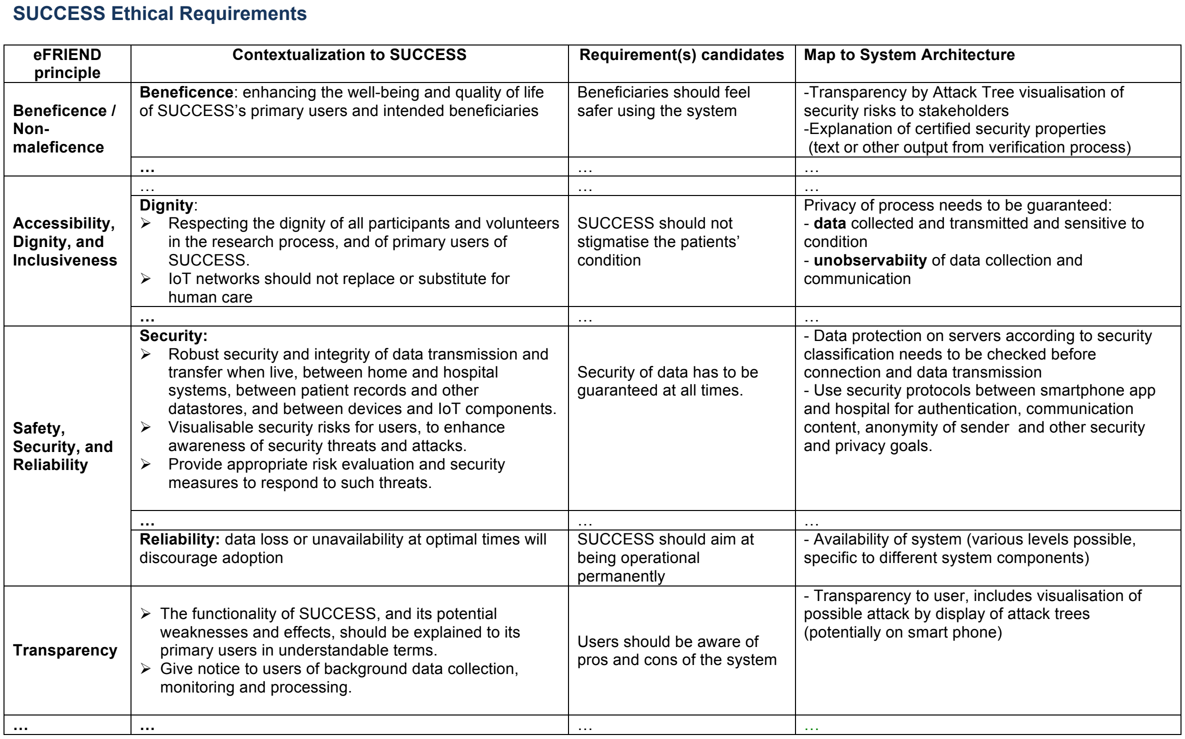
Autonomy: Provide users with control over the IoT sensor environment (systems where users feels trapped, coerced or unable to opt-out have lower adherence ratios).

Multiple users (stakeholders) consideration: SUCCESS will be accessed by several users and stakeholders with different, and sometimes conflicting, expectations.

The application of the eFRIEND framework is shown for some points in Table 1. For the analysis of the techical requirements, we use formal methods as is illustrated in the remainder of the paper.

IV. Healthcare Case Study in Isabelle Insider Framework

The case study we use as a running example in this paper is a simplified scenario from the context of the SUCCESS project for Security and Privacy of the IoT [1]. A central topic of this project for the pilot case study is to support security and privacy when using cost effective methods based on the IoT for monitoring patients for the diagnosis of Alzheimer's disease. As a starting point for the design, analysis, and construction, we currently develop a case study of a small device for the analysis of blood samples that can be directly connected to a mobile phone. The analysis of this device can then be



SUCCESS Ethical Requirements

eFRIEND principle	Contextualization to SUCCESS	Requirement(s) candidates	Map to System Architecture
Beneficence / Non-maleficence	**Beneficence**: enhancing the well-being and quality of life of SUCCESS's primary users and intended beneficiaries	Beneficiaries should feel safer using the system	-Transparency by Attack Tree visualisation of security risks to stakeholders -Explanation of certified security properties (text or other output from verification process)
	…	…	…
Accessibility, Dignity, and Inclusiveness	…	…	…
	Dignity: ➢ Respecting the dignity of all participants and volunteers in the research process, and of primary users of SUCCESS. ➢ IoT networks should not replace or substitute for human care	SUCCESS should not stigmatise the patients' condition	Privacy of process needs to be guaranteed: - **data** collected and transmitted and sensitive to condition - **unobservabiity** of data collection and communication
	…	…	…
Safety, Security, and Reliability	**Security:** ➢ Robust security and integrity of data transmission and transfer when live, between home and hospital systems, between patient records and other datastores, and between devices and IoT components. ➢ Visualisable security risks for users, to enhance awareness of security threats and attacks. ➢ Provide appropriate risk evaluation and security measures to respond to such threats.	Security of data has to be guaranteed at all times.	- Data protection on servers according to security classification needs to be checked before connection and data transmission - Use security protocols between smartphone app and hospital for authentication, communication content, anonymity of sender and other security and privacy goals.
	…	…	…
	Reliability: data loss or unavailability at optimal times will discourage adoption	SUCCESS should aim at being operational permanently	- Availability of system (various levels possible, specific to different system components)
Transparency	➢ The functionality of SUCCESS, and its potential weaknesses and effects, should be explained to its primary users in understandable terms. ➢ Give notice to users of background data collection, monitoring and processing.	Users should be aware of pros and cons of the system	- Transparency to user, includes visualisation of possible attack by display of attack trees (potentially on smart phone)
…	**…**	…	…

Fig. 1. Relevant eFRIEND framework's rules (left column) yield ethical requirement (middle column) that can be mapped to techncial system requirements (right column).

communicated by a dedicated app on the smart phone that sends the data to a server in the hospital.

A. Healthcare Scenario

In this simplified scenario, there are the patient and the carer within a room together with the smart phone (see Figure 2). The carer has access to the phone to support the patient in handling the special diagnosis device, the smart phone, and the app. The insider threat scenario has a second banking app on the smart phone that needs the additional authentication of a "secret key": a small electronic device providing authentication codes for one time use common for private online banking. Assuming that the carer finds this device in the room of the patient, he can steal this necessary credential and use it to get onto the banking app. Thereby he can get money from the patient's account without consent.

B. Isabelle Insider framework Analysis

The Isabelle Insider framework enables formalization of the infrastructure as a graph of locations, like room or smartphone, in which human actors reside in locations and local policies are attached to them as well. The details of this modeling and analysis of the case study is given in [6]. As a brief illustration we give some excerpts here. The local policies are given by the following Isabelle definition and explained below.

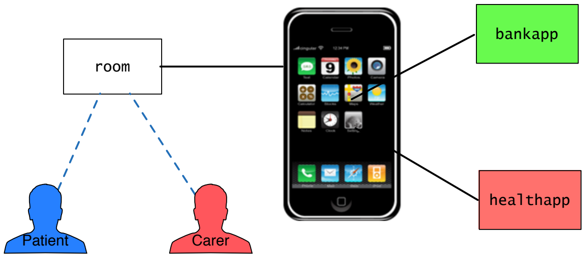


Fig. 2. Health care scenario: carer and patient in the room may use smartphone apps.

```
local_policies G  ≡
 (λ x. if x = room then {(λ y. True,{get, put, move})}
   else (if x = sphone then
    {((λ y. has (y, ''PIN'')), {put,get,eval,move}),
      (λ y. True, {})}
        else (if x = healthapp then
         {((λ y. (∃ n. (n @_G sphone) ∧ Actor n = y)),
          {get,put,eval,move})}
              else (if x = bankapp then
               {((λ y. (∃ n. (n @_G sphone)
                 ∧ Actor n = y ∧ has (y, ''skey''))),
                 {get,put,eval,move})}
                 else {}))))
```

In this policy, any actor can move to the room and when in possession of the PIN can move onto the sphone and do all actions there. The following restrictions are placed on the two other locations.

> healthapp: to move onto the healthapp and perform any action at this location, an actor must be at the position sphone already;
>
> bankapp: to move onto the bankapp and perform any action at this location, an actor must be at the position sphone already and in possession of the skey.

C. Attack Tree Analysis

Attack Trees [12] are a graphical tree-based design language for the stepwise investigation and quantification of attacks. They have been integrated as an extension to the Isabelle Insider framework [6]. This integration extends the Insider model described in the previous section with a proof calculus and modelchecking semantics for attack trees. The extension allows stepwise refinement of attacks exhibiting possible attack paths. The refinement of attack trees is illustrated in Figure 3 with the refined attack path highlighted. The following refinement shows the logical expression of this attack refinement. It expresses that the carer can evaluate the money transfer on the bankapp by first stealing the skey, getting on the phone, on the bankapp and then evaluating.

$$\texttt{[Goto bankapp, Perform eval]} \oplus_{\wedge}^{move-grab}$$
$$\sqsubseteq_{hc\_scenario}$$
$$\texttt{[Perform get, Goto sphone, Goto bankapp, Perform eval]}$$
$$\oplus_{\wedge}^{move-grab}$$

The proof calculus uses the refinement to prove that the sequence of actions [Perform get, Goto sphone, Goto bankapp, Perform eval] represents an attack in the given infrastructure. The underlying semantics providing the notion of validity of an attack is based on the state transition relation defined in the modelchecking foundation (Kripke-structure over infrastructure states) constructed in the Isabelle Insider framework.

The attack tree analysis enables formalizing the requirements and high level architecture of the pilot case study. The found attacks can be used to improve the security policies on the model to provide a security enhanced formal specification for the next phase of applying the BIP methodology to develop a component architecture for the target IoT infrastructure in which the security properties of the initial model are preserved and certified code for the components (sensors and smart phone) can be generated. We omit any details of this phase since they will be reported elsewhere. In addition, the attack trees and paths are naturally suited to visualize the security risks to users showing up potential attacks.

V. Security of Web-Services for Mobile Devices

We now move to the level of the overall system architecture of SUCCESS in order to show up security and privacy risks of IoT devices connected to data servers via Internet and smart phone technology. In order to be compatible with existing standard technologies, the target code for the smartphone healthapp will be implemented in Java Script. This app represents the client side interface to the database servers in hospitals and other institutions, like research centers. Fortunately, the BIP methodology [3] is flexible enough to produce a Java Script app as certified target code for this component. However, BIP is designed for the formal development of synchronous systems. For the local scenario of sensors connected to a central hub like the smartphone either by physical link – like a blood sample sensor that can be connected via the micro usb or lightning port of the smartphone – or through close range networking protocols – like motion sensors communicating with the phone via Bluetooth [13], this is sufficient. Bluetooth is a packet-based protocol with a master-slave structure where all slaves share the master's clock, i.e., it is synchronous and thus amenable to the BIP code generation and certification process. But the main data upload of the diagnosis data is to databases on external servers connected via Internet. This is asynchronous communication using web-services. The overall architecture is shown in Figure 4 showing yet another Insider attack by the carer (discussed further below).

Current standards of best practice for web services for mobile applications have settled on two combinations of technology (1) Java Script Object Notation (JSON) [14] over RESTful web services using http(s) or (2) eXtensible Markup Language XML over SOAP using Web Service Security (WSS) [15]. Solution (1) is more lightweight since the JSON data transfer standard is much less complex than XML. REST prescribes a standard format for web services that is also less complex than SOAP. So from that perspective, it is a clear choice that in the context of mobile application the former is preferable to guarantee less resource consumption caused by an overhead of the SOAP/XML solution. The critical point is the consideration of security. While the combination of JSON over an https based RESTful web service is slick and appears sufficient it relies on the "s" in https, i.e. Transport Layer Security (TLS) (or Secure Socket Layer (SSL) how it was originally called and is still more widely known as). TLS is a good standard solution providing point-to-point security between the http port or http proxy of the smart phone and its counterpart on the database servers. However, it does not provide end-to-end security. The difference is that in an end-to-end security connection the security protection would be between the healthapp and the database application on the server instead of in between the http socket of the smartphone usually on port 80 and the connected socket on the same port on the server as it is provided by a TLS connection. Do we need end-to-end security for SUCCESS? Consider again Figure 3: since the carer needs to have access to the smart phone to support the patient, he can still endanger privacy by the following attack. Suppose, we only use point-to-point security as given by TLS available on smart phones and servers by default. The carer can use his access to the smartphone to download a sniffer app from the app store, like Wireshark and thereby he can trace and intercept all message communication on the smartphone. This is again an insider attack since again the carer is the attacker. The CMU Insider Threat Guide

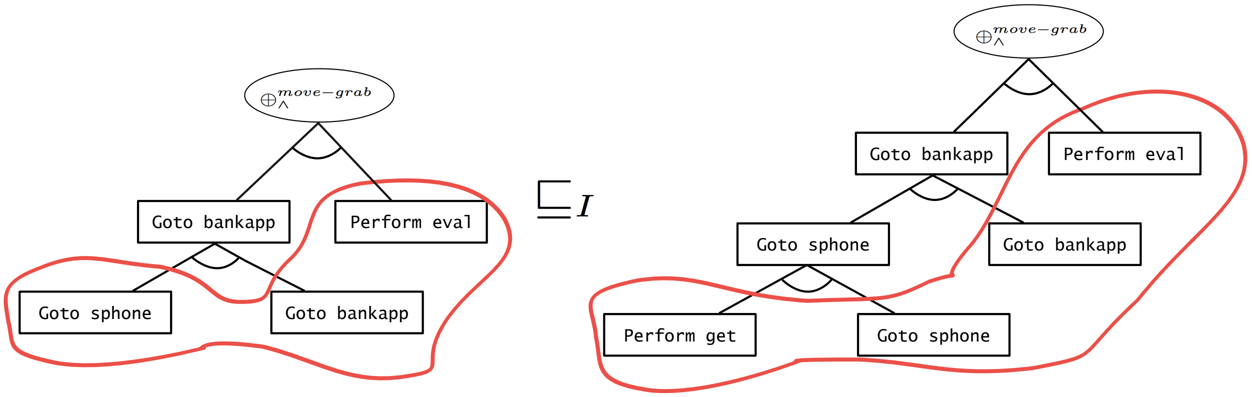


Fig. 3. Attack tree refinement enables stepwise attack path discovery.

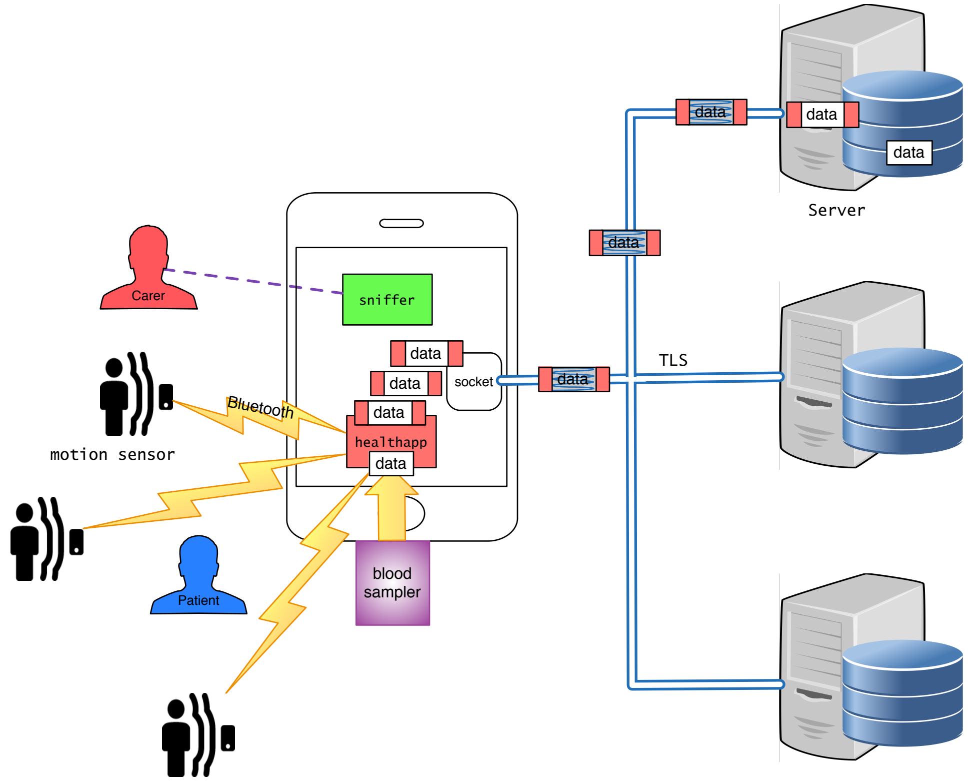


Fig. 4. Carer puts sniffer on smart phone eavesdropping on cleartext TCP packets.

provides the Insider Attack pattern of ambitious leader: if the carer would collaborate with an ambitious leader outside the home, he could install a specialized app on the phone that would forward intercepted packages from the healthapp to the server of the ambitious leader who could sell the data to interested parties or use it directly for blackmail. Using the Isabelle Insider framework with its extension to attack trees [6] this attack can be discovered and proved in the attack tree calculus.

```
[Goto sphone, Perform put,
 Goto sniffer, Perform eval]
```

$\oplus_{\wedge}^{put-sniffer}$

It exposes an interesting challenge for the Isabelle Insider framework since an actor extends the infrastructure (and thus implicitly the local policies) by adding the new location sniffer.

Technically, this Insider attack shows the necessity to have an end-to-end encrypted connection between the smartphone app process and the database application on the server. We solved this in [7] by defining a dedicated end-to-end cryptographic protocol between the app and the server database application. Both stages, the attack analysis and the protocol definition, are supported by Isabelle frameworks: (a) the Isabelle Insider framework for human centric infrastructure analysis and (b) the inductive approach for security protocol verification. The combination of both within the Isabelle framework is straightforward.

VI. Discussion and Conclusions

In this paper, we have given an overview of applying a range of formal techniques to the security and privacy sensitive scenario of healthcare focused on mobile Alzheimer's diagnosis. We only sketched the overall process but detailed on the use of the eFRIENDS framework in combination with interactive theorem proving in Isabelle in two stages: (1) for the elicitation of ethically motivated requirements (2) for a formal machine-supported analysis of attacks at early development stages. Whilst we have applied eFRIEND to other projects, this is the first time we are attempting to verify (or formally check somehow) the application of the requirements derived from its principles. A more technical consideration of the architecture for the healthcare scenario revealed another Insider attack possibility which could be remedied by a dedicated end-to-end cryptographic protocol between a smart phone app and server database applications. This protocol has been developed using the inductive approach to security protocol verification in [7].

Related work on the formal treatment of component architectures is manyfold. For example, Hu et al [16] use stream functions to specify component systems to define regular behaviour and analyse for fault tolerance. However, they do not address ethical issues nor security and do not use verification tools. In the analysis of IoT architectures, mostly simpler logical techniques are used for simulation and validation, for example, Chmai et al. [17] use linear programming to evaluate their efficiency.

It seems promising and a future challenge for SUCCESS to explore this integration on privacy of IoT solutions for vulnerable agents. Initial challenges like dynamic extension of the infrastructure graph and local policies (example of the sniffer app download) have already been identified in this paper. The suggested use of the Bluetooth protocol [13] for the short distance communication in the patients home offers an additional security vulnerability due to symmetric key agreement protocols. However, there is a stronger implementation that uses asymmetric key establishment and that is feasible for certain devices including smart phones [15]. Starting from Bluetooth version 2.1 it is required to use Secure Simple Pairing (SSP) for pairing which is the public key based pairing method. If the attack analysis will show that a Bluetooth based attack is a risk SUCCESS needs to address, then we have to verify whether this asymmetric solution is feasible between the motion sensors and smartphone. This part is addressed in the central part of the formal development of a component based architecture using the BIP methodology and is not covered in this paper.

References

[1] CHIST-ERA, "Success: Secure accessibility for the internet of things," 2016, http://www.chistera.eu/projects/success.

[2] A. Basu, S. Bensalem, M. Bozga, J. Combaz, M. Jaber, T.-H. Nguyen, and J. Sifakis, "Rigorous component-based system design using the bip framework," *IEEE Software*, vol. 28, no. 3, 2011.

[3] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks," in *Principles of Security and Trust, POST'14*, ser. LNCS. Springer, 2014, pp. 285–305.

[4] F. Kammüller and C. W. Probst, "Modeling and verification of insider threats using logical analysis," *IEEE Systems Journal, Special issue on Insider Threats to Information Security, Digital Espionage, and Counter Intelligence*, 2016, accepted for publication. [Online]. Available: http://dx.doi.org/10.1109/JSYST.2015.2453215

[5] N. B. Said, T. Abdellatif, S. Bensalem, and M. Bozga, "Model-driven information flow security for component-based systems," 2014, pp. 1–20.

[6] F. Kammüller, "Formal modeling and analysis with humans in infrastructures for iot health care systems," in *4th Int. Conf. on Human Aspects of Security, Privacy and Trust*, ser. LNAI. Springer, 2017.

[7] ——, "Human centric security and privacy for the iot using formal techniques," in *3d Int. Conf. on Human Factors in Cybersecurity*. Springer, 2017.

[8] J. C. Augusto, "User-centric software development process," in *2014 International Conference on Intelligent Environments, Shanghai, China, June 30 - July 4, 2014*, 2014, pp. 252–255.

[9] J. Augusto, D. Kramer, U. Alegre, A. Covaci, and A. Santokhee, "The user-centred intelligent environments development process as a guide to co-create smart technology for people with special needs," *Universal Access in the Information Society*, 2017.

[10] S. Jones, S. Hara, and J. C. Augusto, "efriend: an ethical framework for intelligent environments development," *Ethics and Information Technology*, vol. 17, no. 1, pp. 11–25, 2015.

[11] J. C. Augusto, V. Callaghan, D. Cook, A. Kameas, and I. Satoh, """intelligent environments: a manifesto"," *Human-centric Computing and Information Sciences*, vol. 3, no. 1, p. 12, 2013.

[12] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2004.

[13] Wikipedia, "Bluetooth," Accessed 4.3.2017, https://en.wikipedia.org/wiki/Bluetooth.

[14] JSON, "Ecma-404 the json data interchange standard," 2017, http://www.json.org.

[15] OASIS, "Web services security: Soap message security. working draft 13, document identifier: Wss: Soap message security-13," 2002, location: http://www.oasis- open.org/committees/documents.php.

[16] J. Z. G. Hu and R. Lee, "Formal specification and implementation of priority queue using stream functions," *International Journal of Software Innovation (IJSI)*, vol. 1, no. 3, 2013.

[17] G. Chmai and H. Selvaraj, "Energy-efficient computing solutions for internet of things with zigbee reconfigurable devices," *International Journal of Software Innovation (IJSI)*, vol. 4, no. 1, 2016.