chist-era SUCCESS

M2.1: Conceptual Framework First Draft

Grant Agreement:	N/A
Project Acronym:	SUCCESS
Project Name:	SecUre aCCESSibility for the internet of things
Instrument:	CHIST-ERA Call 2015
Thematic Priority:	SPTIoT
Start Date:	1 December 2016
Duration:	36 months
Document Type[1]:	T (Technical Report)
Document Distribution[2]:	CO (Confidential)
Document Code[3]:	SUCCESS-MU-PR-001
Version:	v1.1
Editor (Partner):	F. Kammüller (MU)
Contributors:	J.-C. Augusto (MU), Richard Bayford (MU), Simon Jones (MU)
Workpackage(s):	WP1,WP2,WP3,WP4,WP5
Reviewer(s):	Axel Legay (Inria)
Due Date:	Month 6
Submission Date:	September 2017
Number of Pages:	14

Funded by EPSRC Engineering and Physical Sciences Research Council, ANR Agence Nationale de la Recherche, NWO Netherlands Organisation for Scientific Research

[1]MD = management document; TR = technical report; D = deliverable; P = published paper; CD = communication/dissemination.
[2]PU = Public; PP = Restricted to other programme participants (including the Commission Services); RE = Restricted to a group specified by the consortium (including the Commission Services); CO = Confidential, only for members of the consortium (including the Commission Services).
[3]This code is constructed as described in the H2020 Project Handbook.

M2.1: Conceptual Framework First Draft

Florian Kammüller[1]

[1]MU

REVISION HISTORY

Date	Version	Author	Modification
25.8.2017	1.0	F. Kammüller	Started the document
20.9.2017	1.1	F. Kammüller	Finalised after feedback

APPROVALS

Role	Name	Partner	Date
Approver	A. Legay	INRIA	12.4.2018

Contents

1 Executive Summary **4**

2 Some Requirements, Application Scenarios, and Architectural sketches **5**
2.1 Requirements 5
2.2 Scenarios 6
2.3 Architecture 9

3 Conceptual Framework — Draft **11**

4 Conclusion **12**

1 Executive Summary

SUCCESS 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 [4],
- verification methods and risk assessment techniques [2] for IoT scenarios with models of human behavior [11], 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 [14].

Initial architectural drafts have been created. Security and other requirements have been collected. This document assembles these items and gives a first sketch of the framework we plan to create for SUCCESS. The initial results presented here are published in scientific conferences [7, 8, 9, 10]. This report uses parts from these papers.

2 Some Requirements, Application Scenarios, and Architectural sketches

2.1 Requirements

The main scope of SUCCESS is the development of a formal framework for the development of security and privacy enhancing IoT health care solutions. Our conceptual framework starts from a pilot case study in this area. We need to assemble requirements to arrive at a meaningful architecure for the pilot.

Security and privacy for healthcare of vulnerable groups of people brings special attention to ethical requirements. We use the *eFRIENDS* ethical framework [5]. 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) [3].

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 SUCCESS's 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 2.1. For the analysis of the techical requirements, we use formal methods as is illustrated in the remainder of this report.

2.2 Scenarios

Human centric scenarios for Alzheimer's need to take into account that patients might not be able to use the healthcare monitoring system necessitating the involvement of care personnel. We show here a typical scenario as used in related publications [7, 8] there to illustrate the use of Isabelle modeling and verification.

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.

We gradually 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. These consideration have been published in [8, 10].

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.

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)
…	**…**	…	…

Figure 2.1: Relevant eFRIEND framework's rules (left column) yield ethical requirement (middle column) that can be mapped to techncial system requirements (right column).

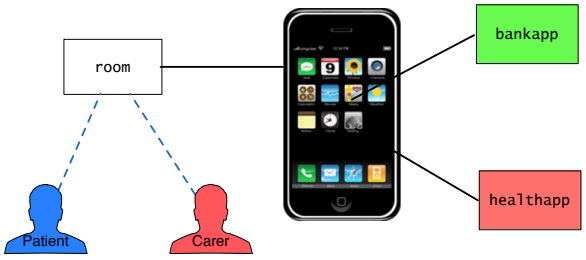

Figure 2.2: Health care scenario: carer and patient in the room may use smartphone apps.

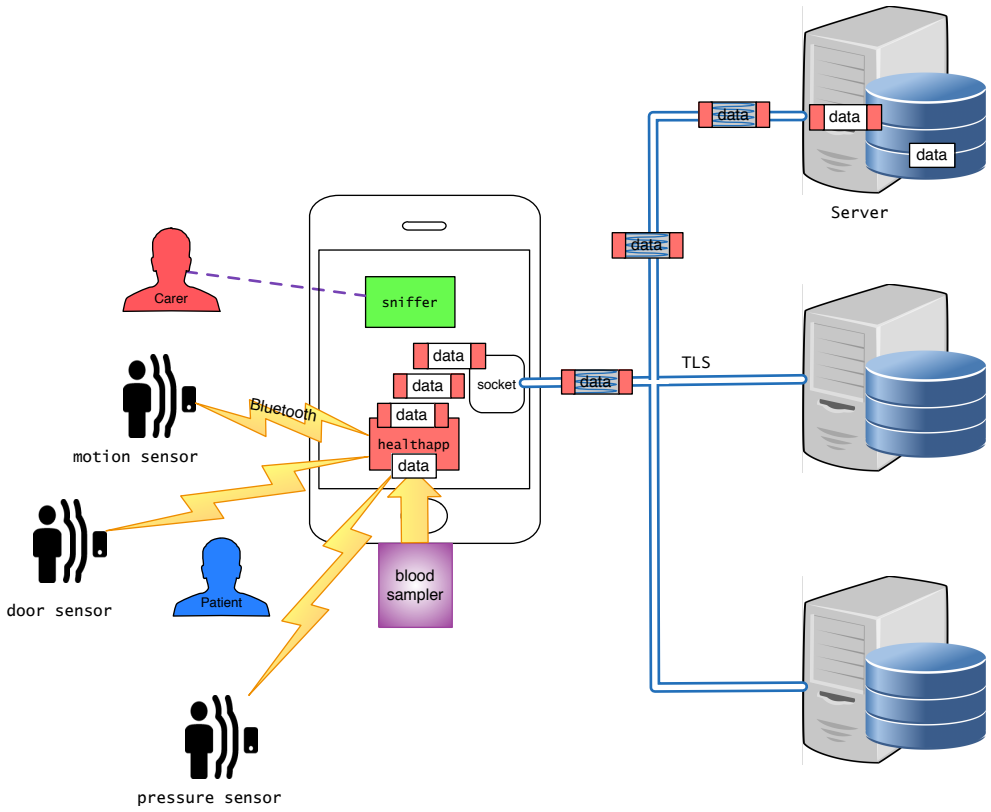

Figure 2.3: Carer puts sniffer on smart phone eavesdropping on cleartext TCP packets.

Fortunately, the BIP methodology [2] 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 [16], 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 2.3 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) [6] over RESTful web services using http(s) or (2) eXtensible Markup Language XML over SOAP using Web Service Security (WSS) [13]. 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 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 [11] and the Isabelle attack tree formalisation [9] this attack can be discovered and proved in the attack tree calculus [9].

```
[Goto sphone, Perform put,
 Goto sniffer, Perform eval] ⊕_∧^{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 [8] 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.

2.3 Architecture

A definite architecture for the SUCCESS case study needs to take into account security requirements as presented in Section 2.1.

An initial draft for a system architecture is depicted in Figure 2.4. We consider devices connected physically to smartphones as well as senors connected to the smartphone. With respect to the used sensor technology, we might employ off the shelf-sensors with proprietory software, i.e., non-open source operating systems. This is a restriction that challenges our certified code generation methodology.

To accommodate this case, we add a sensor-hub with additional (motion)-sensors to the tentative architecture in Figure 2.4. This sensor-hub may be connected via the WLAN protocol to the smartphone. The smartphone is the hub for physical devices and other sensors or measuring devices directly connected via close range communication protocols like bluethooth. Altogether,

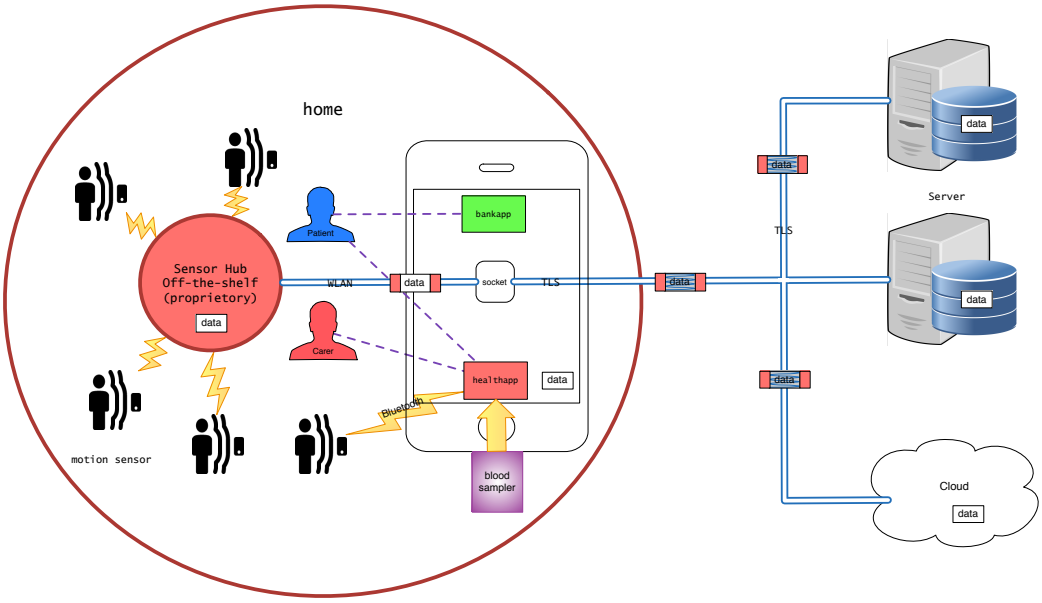

Figure 2.4: Initial system architecture for SUCCESS pilot.

we consider in the tentative architecture the node “home” to be the unity of these various connected devices.

A critical question is where the user data is collected and stored within the system. We have introduced data base symbols to the initial architecture sketch to show all potential locations where user data might be kept. Data collection, storage, and retention is a central and critical issue. Additional difficulties are added to those because of differing EU reglations. The new European General Data Protection Regulation (GDPR) [15] is beneficial since we can orient our framework towards this upcoming standard.

3 Conceptual Framework — Draft

Steps of a tentative Framework:

- Use eFRIEND for requirements elicitation of ethical requirements.
- Map the non-functional requirements to functional (technical) requirements:
  - Use Isabelle framework as illustrated in previous sections to
    - Derive a formal specification of high level system infrastructure with actors and Security and Privacy policy from requirements specification
    - Perform analysis of this formal specification by formal proof of security properties using attack tree calculus [9].
- Open question for SUCCESS requirements elicitation process:
  - How do we extend by other requirements (not just ethical ones)?
  - (Proposition) Use Unified Requirements Notation (URN) [1] and requirements engineering methodologies *i** [12] for a systematic development from requirements to functional specification in Use Case Maps. (Consider other methodologies, e.g. scrum going from epics to user stories – less heavy weight seems good since we already are very loaded with formal notations)[1].
- Risk analysis and transparency with attack trees based on work by UT partners. Questions:
  - Can the attack trees introduced at high level specification also be used for more technical system models?
  - Attack tree extension by time and probabilities to add detail and allow deeper security analysis.
  - How can attack trees be presented to the user to improve transparency of security and privacy risks?
- Component architecture with certified code generation (BIP) by French partners. Questions:
  - Is probabilistic model checking of attack trees possible?
  - How can the attack trees be integrated into BIP process?

[1] Requirements tracing is based on names not on a deep integration between our models – no close integration planned (decision taken at kick-off workshop Jan 2017).

4 Conclusion

This report summarised some initial work on ethical requirements elicitation, attack scenarios and first formal steps towards analysis as well as initial sketches of a system architecture for the SUCCESS pilot. It also presented a draft of a conceptual framework that we envisage based on our initial experiments.

It is important to keep in mind that the goal of the project is Security and Privacy of IoT with an special emphasis on user transparency taking into account vulnerable people. Therefore, the pilot case study that we construct is not an end to itself but just a case study that shall reveal whether the established software engineering and formal techniques can be lined up to provide a methodology that enables the construction of privacy preserving IoT systems. As a practical exploitable product the methodology may serve in particular if it guarantees ethical requirements as well as privacy protection legislation. Since we are using formal methods, if our conceptual frameworks succeeds in practice, we may claim much better guarantees than traditional methods because of formal specification and certified code generation.

The attack tree formalism supports user transparency. Challenges are here how to display the attacks to the user to make security and privacy risks understandable taking into account special needs.

Bibliography

[1] D. Amyot. Introduction to the user requirements notation: learning by example. *Computer Networks*, 42(3):285–301, 2003.

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

[3] J. C. Augusto, V. Callaghan, D. Cook, A. Kameas, and I. Satoh. "intelligent environments: a manifesto". *Human-centric Computing and Information Sciences*, 3(1):12, 2013.

[4] 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*, 28(3), 2011.

[5] S. Jones, S. Hara, and J. C. Augusto. efriend: an ethical framework for intelligent environments development. *Ethics and Information Technology*, 17(1):11–25, 2015.

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

[7] F. Kammüller. Formal modeling and analysis with humans in infrastructures for iot health care systems. In *5th Int. Conf. on Human Aspects of Security, Privacy and Trust, HCII-HAS 2017*, volume 10292 of *LNCS*, pages 339–352. Springer, 2017.

[8] F. Kammüller. Human centric security and privacy for the iot using formal techniques. In *3d International Conference on Human Factors in Cybersecurity, affiliated with AHFE'2017*, volume 593 of *AISC*, pages 106–116. Springer, 2017.

[9] F. Kammüller. A proof calculus for attack trees in isabelle. In *Data Privacy Management, DPM'17, 12th Int. Workshop, co-located with ESORICS'17*, volume 10436 of *LNCS*. Springer, 2017.

[10] F. Kammüller, J. C. Augusto, and S. Jones. Security and privacy requirements engineering for human centric iot systems using efriend and isabelle. In *IEEE/ACIS 15th International Conference on Software Engineering Research, Management and Application, SERA2017*, CPS. IEEE, 2017.

[11] 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*, 11:534–545, June 2017 2017.

[12] L. Liu, E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. In *Proceedings of the 11th IEEE International Conference on Requirements Engineering*, RE '03, pages 151–, Washington, DC, USA, 2003. IEEE Computer Society.

[13] 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.

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

[15] E. Union. The eu general data protection regulation (gdpr), Accessed 20.9. 2017.

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