DRAFT

Full paper published in:

Proceedings of 25th Healthcare Computing conference
21-23 April 2008, Harrogate, UK

Arguing trustworthiness of e-health services with the Trust-IT framework

J Górski[1], A Jarzębowicz[1], J Miler[1]

[1]Department of Software Engineering, Gdansk University of Technology,
Narutowicza 11/12, 80-952 Gdansk, Poland

Keywords: trustworthiness, trust case, e-health, risk

Abstract

Open e-health services involve numerous risks to patient's safety and privacy which gives rise to concerns about their trustworthiness. We present how the concept of the trust case and the associated Trust-IT framework were used to analyse and argue about the trustworthiness of health related services delivered by PIPS, a personalised information platform for health and life services.

Introduction

Trustworthiness of e-health services is becoming an issue of growing importance, in particular with respect to privacy, safety and security. Trustworthiness means that there are 'good' reasons for trust and in some cases we expect that those reasons are given in an objective and verifiable way. The level of assurance should be proportional to the criticality of the properties we are supposed to trust in. Even in non-life-critical situations the concerns of safety (understood as possible future negative effect on health) remain. Safety is one of properties for which we expect a very high assurance and this expectation is reflected in the related standards, regulations and recommendations. In particular, it is common to require that safety is justified by giving an explicit safety case[1,2] and the methodological and tool support for safety cases has been established[3,4].

In our work we extended the idea of safety case into *trust case*[5] which is different in several respects. First, we extend the scope of the properties addressed by the case. Secondly, we do not assume that a trust case must convince someone about the trustworthiness of the considered object. Instead, we assume that trust case collects the available evidence supporting the claim about trustworthiness and the assessment if it is sufficiently convincing is left to the user (or his/her representative). Consequently, the compellingness of a trust case becomes a subjective issue.

In this paper we report on our experiences with developing a trust case for the PIPS system - an open platform for e-health services developed in PIPS (Personalized Information Platform for life & health Services) project. PIPS is an EU 6th Framework Programme Integrated Project focusing on delivering services related to health and lifestyle[6]. This is a 4-years project (2004-2008) which groups 17 partners from 8 countries.

PIPS: project objectives and scope

PIPS focuses on long term medical assistance in conditions which are not directly life-threatening but still important to health and well-being of EU citizens and having large impact on healthcare budgets, e.g. diabetes, hypertension, overweight. The system allows monitoring the patient in open environment (home, workplace, travelling) with the use of IT solutions. The monitoring is based on the information delivered by patient and on vital signs (e.g. blood pressure, glucose level) and other measurements taken by electronic devices integrated with PIPS (e.g. pedometer). Medical data of a patient together with the information related to his/her lifestyle (e.g. physical activity, eaten food) are kept in so called Virtual Ego to provide personalised services tailored to patient's needs and preferences. The system automatically sends recommendations and motivating messages based on the user's Virtual Ego and the knowledge sources integrated in PIPS. The whole process is under supervision of healthcare professionals who are continuously kept in the decision loop. Although the system is not intended to be deployed and used in life-critical situations, there are still serious concerns about patient's safety and privacy and the users would expect that these concerns were addressed with adequate assurance.

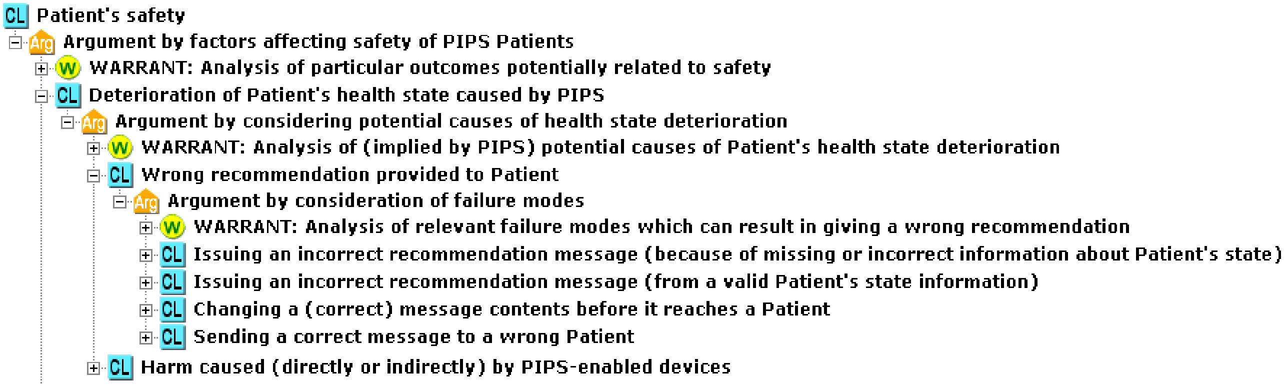
Example scenarios considered in PIPS are:

- Strolling and Motivation – this scenario aims at promoting a healthy lifestyle by encouraging users to follow some physical activity programs. The system collects the data (e.g. from a pedometer assigned to a user) and undertakes some motivating action (e.g. by sending reminders, reward messages etc.).

- Home Care Management – this scenario is related to the patient who has to follow a specified care plan. The scenario integrates all the actors to be involved in the plan (e.g. home care nurse, doctors, family members, informal care givers).
- Cooking – enables a user to plan and manage menu for the whole family taking into consideration chronic conditions, nutritional restrictions and food preferences of all family members. Includes also management of food ingredients in stock and planning of shopping.

Trust case – a tool to demonstrate trustworthiness

Patient monitoring and advisory system (such as PIPS) is used on the voluntary base and its success depends not only on the (expected) added value delivered to the users but to large extent on the users' trust that the system does not pose any significant risk to them. Although such trust can be influenced by many different factors, our particular focus is on building trust by providing an explicit argument about trustworthiness referring to the available evidence. Such argument is represented in the form of the *trust case* and is developed with the help of our *Trust-IT* framework. The *Trust-IT* framework defines the language for trust cases, the patterns of business processes related to trust case development and maintenance, an inventory of application scenarios and the TCT tool platform which supports distributed development and usage of trust cases[7]. Trust case has a tree-like structure and is composed of nodes of different types. Each node contains a piece of information and its type represents the role of this information in the argument structure. The structure of argument follows the approach from Toulmin[8] where a claim (represented as CL) is supported by an argument (represented as Arg) which refers to (more specific) claims or facts (represented as F). The claims can be recursively supported by further arguments which results in a tree like structure as presented in Figure 1 (please note that this tree develops from left to the right). An argument is associated with its warrant (represented as W) which contains explanation why the conclusion (the higher level claim) results from the premises (the lower level claims and facts referred to by the argument). The warrant itself can also be supported by explicit arguments.
Figure 1 presents a fragment of the PIPS system trust case built according to the above rules.



- CL Patient's safety
  - Arg Argument by factors affecting safety of PIPS Patients
    - W WARRANT: Analysis of particular outcomes potentially related to safety
    - CL Deterioration of Patient's health state caused by PIPS
      - Arg Argument by considering potential causes of health state deterioration
        - W WARRANT: Analysis of (implied by PIPS) potential causes of Patient's health state deterioration
        - CL Wrong recommendation provided to Patient
          - Arg Argument by consideration of failure modes
            - W WARRANT: Analysis of relevant failure modes which can result in giving a wrong recommendation
            - CL Issuing an incorrect recommendation message (because of missing or incorrect information about Patient's state)
            - CL Issuing an incorrect recommendation message (from a valid Patient's state information)
            - CL Changing a (correct) message contents before it reaches a Patient
            - CL Sending a correct message to a wrong Patient
        - CL Harm caused (directly or indirectly) by PIPS-enabled devices

Figure 1. A fragment of PIPS system trust case

To develop arguments as presented in Figure 1 we first have to identify the claims to be argued about. While developing the PIPS trust case the claims were primarily related to two categories: patient's safety risks and patient's privacy related requirements addressing generic privacy risks covered by the privacy related standards and recommendations.

Addressing safety risks and privacy requirements

From the safety viewpoint the analysis focused on the risks related to PIPS scenarios and the risk analysis process followed the recommendations of ISO 14971 standard[9]. We used our RiskGuide Internet-based tool[10] to support the risk identification and analysis and to encourage active involvement of project partners. Safety risks were identified with the help of dedicated checklists derived from ISO 14971 standard and by systematic review of system services against generic failure modes. Some examples of identified risks are given below:

R1: Patient receives wrong recommendations from PIPS – the recommendations given by PIPS are inadequate with regards to Patient's health state and, when followed, can result in harm.

R2: PIPS-supplied devices do harm to a patient – devices used in PIPS are unsafe due to flawed design, incorrect usage or wrong configuration.

The identified risks were subjected to further analysis. For instance, investigating the causes of R1 we have identified more specific risks:

R1.1: PIPS information on patient's health state is missing or incorrect – PIPS provides wrong recommendations because of incorrect or incomplete source information.

R1.2: PIPS generates incorrect recommendations based on correct data – PIPS provides wrong recommendations despite correct source data because of faulty logic.

R1.3: PIPS incorrectly communicates recommendations to patient – PIPS builds correct recommendations but they are made incorrect in the communication channel.

R1.4: PIPS sends recommendations to incorrect patient – PIPS build correct recommendations for one patient, but sends them to another patient, for whom they are incorrect.

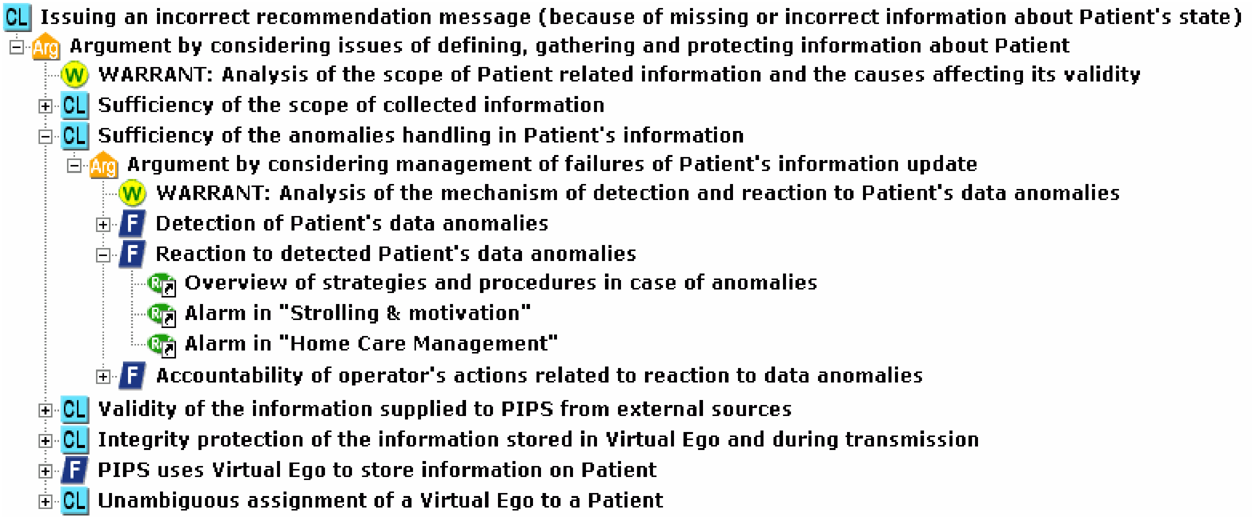
Further on, the results of those analyses drove the trust case structure as illustrated in Figure 1. The analysis of user's privacy was based on the requirements of EU directives 95/46/EC, 2002/58/EC and 2006/24/EC, OECD guidelines, Data Protection (Amendment) Act 2003 and US standard HIPAA. We have identified some 17 generic privacy requirements, examples are:

PR1: Purposes of the processing - Data may be processed only for specific, explicit and legitimate purposes. This means that the data subject must be made aware of the processing carried out on his data and, in details, must be informed on the purposes for which his data are processed.

PR2: Data accuracy - System should maintain the personal and health data accurate and up to date. If a user identifies errors in data they must be able to request corrections and erasures. The data controller must be able to insert a supplemental statement stating corrections, disputes or other matters relating to allegations that the data may be inaccurate.

PR3: Data protection - System should take appropriate technical and organization measures to protect personal data against accidental or unlawful loss, alteration, unauthorized disclosure.

The requirements were then analysed to identify more specific system properties and develop an argument to support the claim that a given requirement is adequately supported.



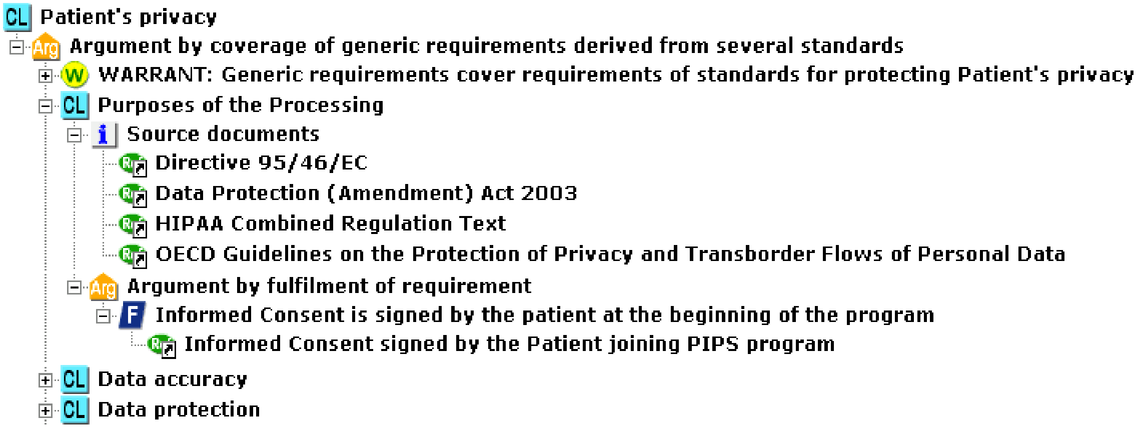
- CL Issuing an incorrect recommendation message (because of missing or incorrect information about Patient's state)
  - ⊟ Arg Argument by considering issues of defining, gathering and protecting information about Patient
    - W WARRANT: Analysis of the scope of Patient related information and the causes affecting its validity
    - ⊞ CL Sufficiency of the scope of collected information
    - ⊟ CL Sufficiency of the anomalies handling in Patient's information
      - ⊟ Arg Argument by considering management of failures of Patient's information update
        - W WARRANT: Analysis of the mechanism of detection and reaction to Patient's data anomalies
        - ⊞ F Detection of Patient's data anomalies
        - ⊟ F Reaction to detected Patient's data anomalies
          - Overview of strategies and procedures in case of anomalies
          - Alarm in "Strolling & motivation"
          - Alarm in "Home Care Management"
        - ⊞ F Accountability of operator's actions related to reaction to data anomalies
    - ⊞ CL Validity of the information supplied to PIPS from external sources
    - ⊞ CL Integrity protection of the information stored in Virtual Ego and during transmission
    - ⊞ F PIPS uses Virtual Ego to store information on Patient
    - ⊞ CL Unambiguous assignment of a Virtual Ego to a Patient

Figure. 2. Details of a trust case with evidence on safety risk mitigation

Developing arguments

For each claim concerning a given safety risk or representing a privacy requirement we were seeking how it can be supported by an argument and the available evidence. Examples of the evidence are: documented design decisions, scenario descriptions, results from system validation and verification, specifications of system components and so on. The evidence sources were not restricted to internal project documents - in many cases it was necessary to refer to external sources, e.g. in case of medical devices or adopted communication protocols. Figure 2 presents an example of more detailed argumentation related to risk R1.1. The trust case fragment includes references to the external sources of evidence (denoted ↗). By use of those references these evidence is fully integrated in the trust case and is made accessible to the trust case users.

The privacy part of the trust case is structured according to the generic privacy requirements. For each requirement, the source documents (e.g. standards, directives) are clearly identified and made accessible as so called information nodes (denoted i). Figure 3 represents the PIPS trust case fragment related to patient's privacy.



- CL Patient's privacy
  - Arg Argument by coverage of generic requirements derived from several standards
    - W WARRANT: Generic requirements cover requirements of standards for protecting Patient's privacy
    - CL Purposes of the Processing
      - i Source documents
        - Directive 95/46/EC
        - Data Protection (Amendment) Act 2003
        - HIPAA Combined Regulation Text
        - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
      - Arg Argument by fulfilment of requirement
        - F Informed Consent is signed by the patient at the beginning of the program
          - Informed Consent signed by the Patient joining PIPS program
    - CL Data accuracy
    - CL Data protection

Figure 3. High level decomposition of PIPS privacy analysis

Conclusions

In this paper we reported our experiences with developing an argumentation about trustworthiness of e-health services. The argumentation was developed with the help of our Trust-IT framework and is represented as a trust case. Trust case builds on risk analysis by allowing to clearly present evidence about current state of risk and mitigation activities and augments it with explicit argumentation how the risk is mitigated. The trust case can be assessed by the relevant stakeholders (for instance patients associations or medical bodies) to assess if the proposed services are sufficiently trustworthy. It can be also presented to the patients although it is rather unlikely that the patients will thoroughly study the trust case contents. We are currently working on a mechanism supporting the communication of the trust case to the patients by means of recommendations.

The PIPS trust case additionally addresses the issue of security of the key information assets of the PIPS system which was not discussed because of the space limits. In PIPS we are also developing more specialised trust cases, for instance related to the Health on the Net (HON) portal providing its users with access to trustworthy medical sources in the Internet and a LAP (Life Assistance Protocol), a dedicated procedure aiming at supporting patients during their everyday activities.

References

1. Ministry of Defence Directorate of Standardisation. Defence Standard 00-55 Issue 2: The procurement of safety critical software in defence systems.
2. Railways (Safety Case) Regulations 2000, Health and Safety Executive.
3. Kelly TP. A systematic approach to safety case management, Proc. of SAE 2004 World Congress, Detroit, 2004.
4. Adelard Safety Case Editor (ASCE), (http://www.adelard.com), Adelard, UK, 2006.
5. Górski J, Jarzębowicz A, Leszczyna R, Miler J, Olszewski M. Trust Case: justifying trust in an IT solution, *Reliability Engineering and System Safety* - Vol. 89 (2005), pp. 33-47.
6. PIPS project website - http://www.pips.eu.org
7. Górski J. Trust-IT – a framework for trust cases, *Workshop on Assurance Cases for Security - The Metrics Challenge*, Proc. of DSN 2007, June 25 - 28, Edinburgh, UK, 2007.
8. Toulmin S. *The Uses of Argument*, Cambridge University Press, 1958.
9. International Standard ISO/FDIS 14971: Medical devices — Application of risk management to medical devices.
10. Risk Guide homepage - http://iag.pg.gda.pl/RiskGuide/