Trustworthiness: safety, security and privacy issues

J. Górski, G. Gołaszewski, J. Miler, M. Piechówka
Gdańsk University of Technology
Gdańsk, Poland
E-mail: {jango,grzo,jakubm,macpi}@pg.gda.pl

H. Baldus
Philips Research Europe
Aachen, Germany
E-mail: heribert.baldus@philips.com

***Abstract*—The paper presents the Angel[1] approach to analyzing and demonstrating trustworthiness in the context determined by the selected set of application scenarios. The focus is on safety, security and privacy issues. The analysis is based on two 'pillars': the analysis of risks in the context of Angel scenarios and the analysis of the requirements derived from the relevant standards. The way Angel addresses the risks and requirements is represented in the Angel trust case – a structured argument which integrates all the trustworthiness supporting evidence. The article gives more detail on the approach taken during the safety, security and privacy related analysis and explains the idea of Angel trust case.**

I. INTRODUCTION

An object is trustworthy if it deserves trust and confidence. We consider two aspects of this definition. First, the trust and confidence are usually in some selected properties of the object, for instance privacy, safety, security and so on, whereas some others are less important. Secondly, to decide weather the object deserves trust and confidence, we need to refer to an (explicit or implicit) argument supported by some evidence.

The Angel approach to trustworthiness explicitly addresses the following issues: (a) which object is to be trusted, (b) which properties are to be trusted, and (c) what argument supports the trustworthiness.

Concerning (a) we distinguish between *Angel system* which delivers some business value to its users and *Angel platform* which can be specialized to different systems by its customization and by providing a dedicated application layer (more on this issue can be found in [1]).

Concerning (b), we concentrate on three different (although not necessarily independent) properties: safety, security and privacy. Safety relates to protection of users' health and life. Security relates to protection of valuable information assets against intentional and unintentional threats. And privacy relates to user's right to have her/his personal information protected against unaccepted disclosure.

Concerning (c) we assume that trustworthiness is justified by providing an explicit argumentation and that the arguments are supported by evidence or otherwise are 'grounded' in explicitly made assumptions.

The approach to achieving and assessing trustworthiness involves a mixture of the following two strategies: (1) risk driven approach, and (2) standards and guidelines driven approach. The first strategy focuses on identifying and analyzing relevant risks and then on their adequate management. It provides for concentrating the effort on the risks that are most significant and helps in avoiding over-investment in terms of time and effort. The second strategy brings into the project the wisdom contained in the relevant standards and guidelines which protects against 're-inventing the wheel' and helps in choosing adequate scope and employing the best practices. We are following the Trust-IT methodology [2,3,4,5,6] and the related tool framework [7] in developing and maintaining the argumentation about the trustworthiness of Angel.

The paper is organized as follows. In the next section we briefly describe the scope of Angel application scenarios and the concepts of Angel system and platform. Then we introduce the Trust-IT approach to trustworthiness justification and analysis. The next three sections describe the approach taken with respect to the three main trust objectives considered in Angel: safety, privacy and security. We conclude by summarizing the contents of the paper.

II. ANGEL: SYSTEM AND PLATFORM

The scope of Angel functionalities covers the following three generic scenarios: ***Scenario 1*** – *Personalized indoor environmental monitoring and control for wellbeing.* It focuses on monitoring and adjusting habitat conditions to better suit user needs. ***Scenario 2*** – *Post-acute and chronic disease management.* It is dedicated to monitoring person's health status to reduce specific medical risks as well as support home convalescence. ***Scenario 3*** – *Personal wellness and related enabling services.* It describes functions

[1] ANGEL - 'Advanced Networked embedded platform as a Gateway to Enhance quality of Life' is a research project partially supported by the European Commission within the 6th Framework Programme (IST project 2005-IST-5-033506-STP). More information on ANGEL can be found at http://www.ist-angel-project.eu.

envisioned to support people in staying healthy, particularly addressing physical activities.

To enable development of different systems within the scope determined by the above three scenarios Angel distinguishes the concept of *platform*. The platform consists of three main components: (1) WSN – wireless sensor network providing the means to monitor and control environmental conditions and to monitor personal parameters. (2) Gateway – the focal point of the project – which encompasses more computationally intensive algorithms, enables both local user interaction and remote access and integrates different WSNs and remote services. (3) Operator terminal – a remote entity that can communicate with the gateway by means of traditional networks (both wired and wireless). It provides user access to the monitored parameters and supports management of both, WSN and the gateway. It can be deployed in a gateway or in a remote service centre.

To develop an Angel system one needs to select and configure the platform components and then to provide application software for each component, as shown in Figure 1.

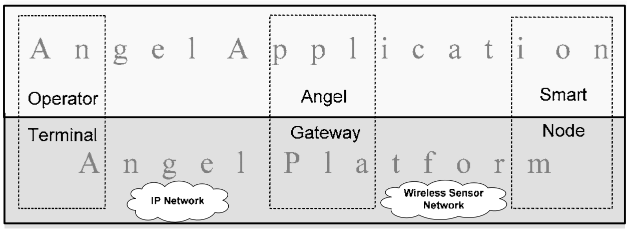


Figure 1. Angel System. The horizontal line separates Angel platform and Angel application (together they constitute an Angel system).

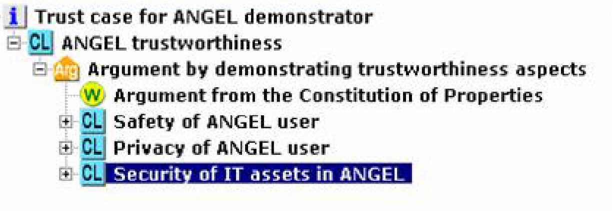
III. The Trust-IT approach

Trust-IT is a framework supporting development and application of trust cases. The framework consists of the application, methodological and tool support components. The application component explains possible scenarios of trust case application. The methodological component explains how to develop and maintain trust cases. The tool component provides support for the full scale exploitation of the two other components. The definition says that [2]: *trust case is a documented base that provides a satisfactory, from a given viewpoint, justification for a specified set of claims to make a judgement about their trustworthiness*. The viewpoint can represent an individual user who decides about using system's services, an expert giving her/his opinion about the expected quality of service, a certifying institution deciding about issuing a specific certificate, and so on. The criteria weather the justification is satisfactory can vary, from highly formalized and quantitative (as for safety critical systems) to more informal and rather qualitative. The 'documented base' mentioned in the definition can include any material like: design evidence, assumptions, expert opinions, simulation and test results and so on.

Trust-IT approach is used in Angel with two complementary objectives: (1) to justify the trustworthiness with respect of chosen quality attributes (safety, privacy and security), and (2) to influence the development process with the objective to produce and collect enough evidence supporting the trustworthiness of Angel.

The process of trust case consists of two main functions: *selection of trust objectives* and *justification of trust objectives*. Selection of trust objectives is based on the requirements of the relevant standards and the analysis and assessment of relevant risks. The choice of what is 'relevant' for Angel depends on the application scenarios described in the previous section. A trust objective can be for instance a particular requirement from a standard or a claim postulating that a particular risk is adequately mitigated. Justification of trust objectives involves selection of valid argumentation strategies and collection and integration of adequate evidence. The process of development of a trust case needs support and active participation of relevant stakeholders (to represent the variety of viewpoints at the issue of trustworthiness).

Angel trust cases (one for the Angel platform and another for an example Angel system, called 'Angel demonstrator') are maintained in the TCT tool [7] and are accessible in the Internet. The topmost decomposition of the Angel demonstrator trust case is shown in Fig.2.



i Trust case for ANGEL demonstrator
⊟ CL ANGEL trustworthiness
⊟ Arg Argument by demonstrating trustworthiness aspects
W Argument from the Constitution of Properties
⊞ CL Safety of ANGEL user
⊞ CL Privacy of ANGEL user
⊞ CL Security of IT assets in ANGEL

Figure 2. Structure of the trust case for Angel demonstrator

The picture shows the claim about Angel trustworthiness which is supported by the argument referring to the claims about three Angel trustworthiness aspects: safety, privacy and security.

IV. Safety

Safety risk management follows the process defined in the ISO 14971 standard [8] and applies the standard-recommended HAZOP method to hazard identification. It is organized in the following steps: (1) Identification of system-level hazards which can directly lead to accidents affecting Angel users. Hazards are identified from ISO 14971 Annex A questionnaire and by systematic review of failure modes of Angel services with the help of HAZOP-implied checklists, following the approach from [9]. (2) Evaluation of the hazards severity with the help of a team of experts selected from the Angel consortium. (3) Identification of platform-level failure modes leading to the system-level hazards. Multiple system-level hazards may originate from the same platform-level failure as the causal chain of events can split beyond the platform boundary, in the application related part of the system. In such cases it is assumed that the severity rank of the platform-level failure is the maximum from the severity ranks assigned to the related system-level hazards. This FTA like approach is then complemented by the FMEA like analysis looking at the possible consequences of systematically reviewed platform failure modes. (4) Identification of mitigation mechanisms for unacceptable platform-level failure modes.

Examples of platform-level failure modes and related system-level hazards are given below:

TABLE I. EXAMPLE PLATFORM FAILURE MODES

Platform failure mode	System hazard
Inability of ANGEL platform to send notifications and alarms	Alert is incorrectly sent in case of unexpected event e.g. fire
Inability of ANGEL platform to control correctly the environment	Temperature is incorrectly adjusted to suit user's needs
Inability of ANGEL platform to present reliable data	Harmful advice on lifestyle improvement is presented to user

Safety risk analysis is supported with Internet tool RiskGuide [10], which offers a knowledge-base of standard-derived checklists, collects the identified accidents, hazards and failure modes, supports risk evaluation, provides access to risk assessment reports and records decisions concerning risk mitigation measures.

V. PRIVACY

The need for privacy protection has been widely recognized which is reflected in different regulations and recommendations. The process of derivation the privacy protection requirements in Angel comprises the following steps: (1) Identifying the relevant source documents. The following regulatory and recommendation documents have been taken into consideration: Directive 95/46/EC [11], Directive 2002/58/EC [12], OECD Privacy Guidelines [13], HIPPA Privacy Rule [14]. The result was the list of *generic privacy requirements*. (2) Interpreting the generic requirements in the context of Angel scenarios to derive *system level privacy requirements*. (3) Mapping the system level privacy requirements to Angel platform to identify the *platform level privacy requirements.*

Example platform level privacy requirements are as follows. (PR1) Platform should enable identification of Patient's Health Information, (PR2) In addition to real user names the user should be identified by aliases. Platform should allow for private data purge, (PR3) Platform should ensure confidentiality of privacy-related data over all communication routes, (PR4) Platform should ensure integrity of privacy-related data over all communication routes.

Full traceability is maintained from platform level requirements through system level requirements to generic requirements and the related source documents.

Further analysis will involve decisions about the ways of requirements implementation and their assignment to system and platform components. The evidence about handling of the privacy requirements will be referred to from the Angel trust cases to justify Angel trustworthiness concerning the privacy aspect.

VI. SECURITY

The Angel security management process, inspired by [15,16,17], is illustrated in Fig. 3.

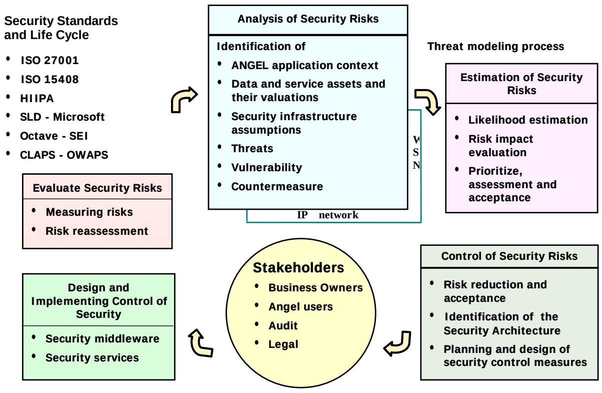
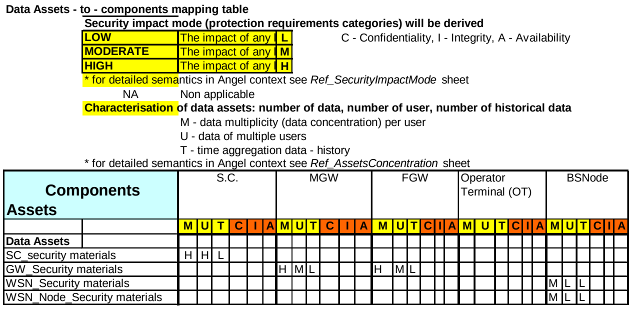

Security Standards and Life Cycle
ISO 27001
ISO 15408
HIIPA
SLD - Microsoft
Octave - SEI
CLAPS - OWAPS
Analysis of Security Risks
Identification of
ANGEL application context
Data and service assets and their valuations
Security infrastructure assumptions
Threats
Vulnerability
Countermeasure
Threat modeling process
Estimation of Security Risks
Likelihood estimation
Risk impact evaluation
Prioritize, assessment and acceptance
W
S
N
IP network
Evaluate Security Risks
Measuring risks
Risk reassessment
Stakeholders
Business Owners
Angel users
Audit
Legal
Control of Security Risks
Risk reduction and acceptance
Identification of the Security Architecture
Planning and design of security control measures
Design and Implementing Control of Security
Security middleware
Security services

Figure 3. Angel security management process

Security assets identification has been performed referring to Angel scenarios and use cases and the assets model has been developed and is represented in UML.

The (data and service) assets are subjected to the analysis targeting at their valuation with the help of the security impact criteria (characterizing the consequences of possible loss of confidentiality, integrity and/or availability). The mapping of the assets into components is also considered (taking into account the aspects like: the number of allocated/transferred data, the number of users assigned to these data and the amount of historical data maintained on a component) which results in the components security valuation. The data structure which supports this analysis is shown in Fig.4.



Data Assets - to - components mapping table

Security impact mode (protection requirements categories) will be derived

LOW	The impact of any	L
MODERATE	The impact of any	M
HIGH	The impact of any	H

C - Confidentiality, I - Integrity, A - Availability

* for detailed semantics in Angel context see *Ref_SecurityImpactMode* sheet

NA Non applicable

Characterisation of data assets: number of data, number of user, number of historical data

M - data multiplicity (data concentration) per user
U - data of multiple users
T - time aggregation data - history

* for detailed semantics in Angel context see *Ref_AssetsConcentration* sheet

Components Assets	S.C.						MGW						FGW						Operator Terminal (OT)						BSNode					
	M	U	T	C	I	A	M	U	T	C	I	A	M	U	T	C	I	A	M	U	T	C	I	A	M	U	T	C	I	A
Data Assets																														
SC_security materials	H	H	L																											
GW_Security materials							H	M	L				H	M	L															
WSN_Security materials																									M	L	L			
WSN_Node_Security materials																									M	L	L			

Figure 4. Mapping data assets to Angel architecture components

As the next step, the basic protection level is being identified for Angel, inspired by the available mechanisms

(Zigbee, operating system, available middleware) and the recommended good practices (see e.g. [16,18,19]). This level is then treated as the reference for further security analyses. These analyses involve developing the inventory of threats and vulnerabilities (taking into consideration the basic protection level) and then assessing security risks related to the assets exposed to security threats in the presence of vulnerabilities.

The results of the security risk analysis are then used to drive decisions about selection and allocation of additional countermeasures with the aim of additional risk reduction. At this stage, the privacy requirements are taken into account as an additional source of implied security requirements [15,16,17].

The following core security services define the scope of Angel security architecture: identity management, data confidentiality protection, data and services integrity, policy management, auditing, security administering. One of the main problems is key management service in the WSN.

Within each individual WSN, security keys are required for sensor node authentication, authorization and communication protection [20]. Using public keys is unfeasible due to the limited computing, memory and energy resources of the sensor nodes. Symmetric keys however provide the required resource efficiency. In this category, group keys, that are shared among the nodes, are not feasible: In an environment in which the nodes can be captured, the confidentiality offered by the shared symmetric keys is easily compromised. Trust centers for initial sensor node key establishment are not feasible as well, due to the ad-hoc nature of the WSNs. Thus, we deploy keys via a deterministic pre-distribution scheme [21], that provides nodes with pairwise keys, combined with high security and resiliency.

A important element of elaborating the Angel security framework is mapping of the APIs defined in security middleware to services and mechanisms offered by the existing components of Angel platform (for instance, two stacks of network layers: one for IEEE 802.15.4 and ZigBee sensor networks and one for IP networks which coexist in the gateway).

The results of security analyses, design choices and implementation results (in particular in relation to the achieved assurance level) will be maintained in Angel documentation and then used as the evidence to support the claim about Angel trustworthiness with respect to security, in the Angel trust case.

VII. CONCLUSIONS

In this paper we presented the approach to analyzing and demonstrating trustworthiness of health related applications of sensor networks. We first presented an overall approach which is driven by risk analysis and the requirements derived from standards. We explained how the argumentation about trustworthiness and the supporting evidence are integrated and maintained in the form of trust cases. We also provided more detail on particular aspects of trustworthiness, including safety, privacy and security.

REFERENCES

[1] J. Bruynen, M. Nalin, P.Garino, M. Decandia, 'Angel system & platform architecture', in this issue.

[2] J. Górski. 'Trust Case – a case for trustworthiness of IT infrastructures', In: Cyberspace Security and Defense: Research Issues, NATO Science Series II, Vol. 196, Springer-Verlag, 2005, pp. 125-142.

[3] J. Górski, 'Trust-IT – a framework for trust cases', Workshop on Assurance Cases for Security - The Metrics Challenge, DSN 2007 The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, June 25 - June 28, Edinburgh, UK, 2007

[4] J. Górski., A. Jarzębowicz, R. Leszczyna, J. Miler, M. Olszewski, 'Trust Case: justifying trust in an IT solution', Reliability Engineering and System Safety - Vol. 89 (2005), pp. 33-47

[5] L. Cyra, J. Górski, 'Supporting compliance with security standards by trust case templates', International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007, 2007

[6] L. Cyra, J. Górski., 'Supporting compliance with safety standards by trust case templates', ESREL 2007, Stavanger, Norway, 2007.

[7] TCT User Manual, Information Assurance Group, Gdansk University of Technology, 2006

[8] International Standard ISO/FDIS 14971: Medical devices — Application of risk management to medical devices, ISO 14971:2000 Annex A - Medical Devices Safety Questionnaire.

[9] Miler J., 'A Service-Oriented Approach to the Identification of IT Risk', Proc. of 1st IEEE Intern. Conference on Technologies for Homeland Security and Safety TEHOSS'2005, Gdansk, Poland, 2005

[10] RiskGuide tool homepage – http://iag.pg.gda.pl/RiskGuide

[11] EU Directive 95/46/EC - The Data Protection Directive

[12] Directive 2002/58/EC of the European Parilament and of the Council, of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002

[13] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

[14] HIPAA Privacy Rule, Health Insurance Portability and Accountability Act, Part 164, Subpart E, U.S. Department of Health and Human Services.

[15] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson, 'Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process', CMU/SEI-2007-TR-012

[16] M. Howard, S.Lipner, 'The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software', MS Press 2006

[17] OWASP, 2006. http://www.owasp.org.

[18] HIPAA Security Rule, Health Insurance Portability and Accountability Act, Part 164, Subpart C, U.S. Department of Health and Human Services.

[19] ISO/IEC 15408-2005-Information technology - Security techniques Evaluation criteria for IT security Part 1 & Part 2

[20] D. Sanchez, H. Baldus, 'Key Management for Mobile Sensor Networks', Secure Mobile Ad-hoc Networks and Sensors workshop (MADNES 2005), September 20-22, 2005, Sentosa, Singapure.

[21] D. Sanchez, H. Baldus, 'A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks', 1st Intern. IEEE Conf. on Security and Privacy for Emerging Areas in Commu. Networks (SecureComm 2005), Sept. 5-9, 2005, Athens, Greece.