DRAFT

full paper published in:

proc. of 1st IEEE International Conference on Technologies for Homeland Security and Safety TEHOSS'2005
September 28-30, 2005 Gdansk, Poland

Paper published in the proceedings and presented at the conference

A SERVICE-ORIENTED APPROACH TO THE IDENTIFICATION OF IT RISK

Jakub Miler

Gdansk University of Technology, Department of Software Engineering,
11/12 Narutowicza St., 80-952 Gdansk, Poland,
e-mail: jakubm@eti.pg.gda.pl

Summary

This paper outlines an approach to the identification of IT-related risk. The risk is identified from the perspective of the services provided by a software system to the users. The approach assumes the investigation of the service failures with the use of failure mode keywords. The service-based risk identification is supplemented with checklists extracted from standards and classical techniques of security analysis. The approach has been used in two case studies also reported in the paper.

1. Introduction

Faulty software systems have already led to some significant accidents in the past and are likely to keep being a cause of accidents in the future. Probably the most spectacular and well-known accident happened to the Ariane 5 rocket, which exploded shortly after launching due to a controller software bug [11]. This catastrophe, and many others, has shown that software-based solutions can introduce serious risk to their operating environment [13]. The investigation and control of this risk becomes increasingly crucial with rapidly growing number, extent and diversity of software systems put into operation every day.

The software systems are designed and built to deliver services to their users. A service is not *any* performance of a system – it is such performance that presents added value to the users. The users assess the system output against their success criteria that define what added value they expect from the service. A system's service is considered

correct if it meets all the success criteria of all the service users. Otherwise, that service exhibits a failure, which reduces its utility. Service utility is a subjective user's estimate of the actual value delivered by the service to the user.

The system's users already own some values, which they expect to be preserved. Key users' values are their safety and privacy. The loss to these values ultimately affects the users. From this point of view, security is not a users' value by itself – it is a feature of the system, which is a strong prerequisite for that system to preserve the real users' values like safety and privacy. To add value, a system must at least maintain the users' values or provide enough benefit to compensate for potential loss to these values.

The IT risk (or service risk) of a software system is the risk to the users' values posed by that system. The system negatively affects the users through failures of its services. A failed service reduces the overall benefit from the system, which may eventually be nullified by the loss resulting from the failure. The investigation of the service failures seems a good start to the identification of the IT-related risk. The focus on services and their failures is the key aspect of the presented approach.

2. Approach

The service-oriented approach to the IT risk identification aims at building a list of risks posed by the system's service failures to the users. The system definition and design documentation such as the requirements specification, the business models and the use cases is the major input to the analyses. The risk identification is carried out in 5 steps:

1. selection of target users' values threatened by the IT risk,
2. identification of system's context of use, services, scenarios and use cases,
3. building a map of service failure modes with supplementary helper questions,
4. actual identification of risk,
5. review and documentation of identified risks.

The steps are detailed in the next sections, followed by an overview of the tool support.

2.1. Selection of target users' values

In the first step, the users' values taken into account in the risk identification are selected. As already said in the introduction, the key users' values are the safety and the privacy. They should always be considered when investigating the IT risk. There are, however, other values such as independence (the freedom of choice of using or not using the system; see the concept of dependence in [1]) that could be included in the analyses. The actual choice of the users' values depends on the intended coverage of the risk identification. The users' values can be used to control the scope of the analyses.

2.2. Identification of system's services

The next step involves the investigation of the system's context of use and aims at the identification of the system's services, which could be further analyzed for the potential failures. As defined earlier, a service is a system's performance that provides users with observable added value. Practically, unless explicitly designed, a service can be mapped

to a step in a system's usage scenario (involving the system and the users) or a business or system use case.

2.3. Building a map of service failure modes

In this step, a working material for the actual risk identification is prepared. First, the set of studied failure modes is composed. The concept of a failure mode is taken from the FMEA method [7]. Avižienis et al. have defined a set of the most general failure modes: *no service* (*halt*), *incorrect timing*, and *incorrect content* [1]. Incorrect timing failure mode may be further split into *early timing* and *late timing* giving four basic failure modes. A more comprehensive list of 10 failure modes can be adopted from the HAZOP method [5, 8]. The actual choice of the failure modes is left to the analyst.

The selected failure modes are mapped at the system services (with a Cartesian product) forming pairs of a service and a failure mode. Additionally, helper questions are built according to a scheme: "Does *failure mode X* of *service Y* affect stakeholders' *value Z*?". The idea of pairing the services with the failure modes and the structure of the particular helper questions is presented in Fig. 1.

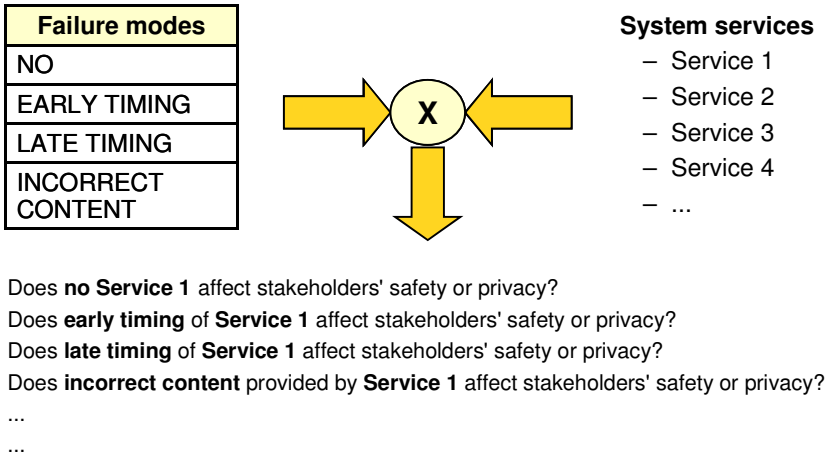

Figure 1. Building helper questions from failure modes and services

2.4. Identification of risk

In this step, the essential effort towards the identification of risk is made. The risk is identified by reviewing the list of services and their failure modes, reflecting on the helper questions and deciding on the possible loss from a service failure. The helper questions are intended to stimulate the analyst's imagination and focus his/her attention on a particular case. A negative answer to a helper question means that there is a risk associated with a particular service. The questions can be answered by a single analyst or by a group of independent analysts providing for better objectivity. The raw identified risks are noted in a preliminary risk list.

The service-oriented risk identification should be supplemented with other sources such as IT standards and dedicated techniques of security assessment such as the CORAS

framework [2]. In case of risk to safety, the ISO 14971 standard offers a questionnaire dedicated to medical devices but partially applicable to other types of IT systems [4]. A key standard covering the IT safety risk is the IEC 61508 standard [9]. As for privacy, the HIPAA US standard provides a number of comprehensive guidelines [6]. Additionally, the identified risks can be further investigated for their causes and, once discovered, these causes can be analyzed for other consequences.

2.5. Risk documentation

The last step aims at building a tangible list of risks for further analysis and mitigation. In this step, the raw risks identified with both service-oriented approach and other sources (e.g. standards) are reviewed, rephrased, merged together and finally documented in the form of a risk list.

2.6. Tool support

The service-oriented risk identification as presented above is supported by an internet-based software tool RiskGuide [10]. The tool offers a Knowledge Base with custom-built helper questions (see section 2.3) and questionnaires extracted from the IT-related standards as well as supports distributed risk identification and analysis. Finally, the tool can publish the results of the IT risk assessment in an on-line risk assessment report or export these results to an XML file for further off-line analysis.

3. Application case studies

The presented approach has been used in two case studies of service risk identification of an IT system for e-health. The first application concerned the system prototype with only one usage scenario (with three sub-scenarios) of about 15 steps in total. The scenario involved two categories of users: the patients and the doctors. Apart from the service-oriented approach, two standards were also referred to: ISO 14971 [4] and HIPAA [6]. In total, some 42 risks to safety, privacy and independence were identified. The examples of identified risks to safety and privacy are given below.

Safety:

- Wrong Patient's interpretation of information from PIPS
  source: ISO 14971 question A.2.11: Is the medical device interpretative?
- Patient neglects schedule of measurements
  source: Failure modes - services: ***early timing****,* ***late timing*** *of* ***Measuring vital signs***
- Incorrect or unavailable Patient's record
  source: Failure modes - services: ***no****,* ***incorrect content*** *of* ***Access to Patient's record***

Privacy:

- No access to Patient record by owning Patient
  source: HIPAA Privacy Rule § 164.524
- Patient is not notified of required and possible disclosures of his/her record
  source: HIPAA Privacy Rule § 164.520

- Patient's PHI is disclosed
  source: Failure modes - services: ***incorrect content*** *of* ***Access to Patient's record***
- Patient's interest in product is disclosed
  source: Failure modes - services: ***incorrect content*** *of* ***Getting product code***

The approach application effort in the first case study amounted to 8 person-hours, 4 of which were used to prepare the working material (steps 1, 2 and 3) and the remaining 4 to actually identify and document the risks (steps 4 and 5).

The second case study involved a pilot implementation of the system already analyzed in first case study. This time, the documentation defined three scenarios (including the one retained from the prototype) of about 40 steps in total. The users remained the same: the patients and the doctors. The risk identification focused on differences as to the prototype: the changes in the retained scenario and the two new scenarios. The standards were not consulted again. Finally, 31 new risks to safety and privacy were identified. The examples are given below.

Safety:
- False Patient's answers to questionnaires stored in the system
  source: Failure modes - services: ***incorrect content*** *of* ***Filling questionnaires***
- Unavailable or incorrect system's recommendations to Patient
  source: Failure modes - services: ***no, incorrect content*** *of* ***Suggestions and advices from system***

Privacy:
- System's diagnosis of Patient's health state is disclosed
  source: Failure modes - services: ***incorrect content*** *of* ***Vital signs assessment***
- Patient's answers to questionnaires are disclosed
  source: Failure modes - services: ***incorrect content*** *of* ***Filling questionnaires***

The application effort in the second case study was 4 person-hours. Compared to the first case study, the effort was reduced due to excluding the standards, reusing some of the working material as well as some experience acquired in using the approach.

4. Conclusions

The paper presented an approach to the identification of risk of failing system's services threatening the crucial values of that system's users such as safety and privacy. The approach adopts the investigation of failure modes and their consequences from the FMEA method [7] and the keywords-based identification of risk from the HAZOP method [5, 8]. The analyses are supplemented with an input from standards and security-dedicated techniques.

The service-oriented approach to IT risk identification has been applied in two case studies of a software system for e-health. In total, some 73 risks to safety and privacy were identified with an effort of 12 person-hours. The identified service risk has been used as a key driver in building a trust case (a structured clear argument for the system's trustworthiness extending the concept of a safety case [12]) for the analyzed system with the IT-Trust method [3]. The results so far are quite encouraging.

References

[1] A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: *Basic Concepts and Taxonomy of Dependable and Secure Computing*, IEEE Transactions on Dependable and Secure Computing, **1** (1), 2004

[2] CORAS: A platform for risk analysis of security critical systems. IST-2000-25031, 2000, http://www.nr.no/coras/

[3] J. Górski, A. Jarzębowicz, R. Leszczyna, J. Miler, M. Olszewski: *Trust case: justifying trust in IT solution*, Reliability Engineering and System Safety **88**, 1 (2005)

[4] ISO/FDIS 14971:2001 International Standard: *Medical devices -- Application of risk management to medical devices*, International Organization for Standardization, 2001

[5] *HAZOP Studies on Systems Containing Programmable Electronics*, MoD Defence Standard 00-58, Issue 2, 2000

[6] *Health Insurance Portability and Accountability Act, Privacy/Security/Enforcement Regulation Text, 45 CFR Parts 160 and 164*, U.S. Congress Act, with amendments, 2003

[7] IEC 60812, *Analysis techniques for system reliability — Procedures for failure mode and effects analysis (FMEA).*

[8] IEC 61882, *Guide for hazard and operability studies (HAZOP studies).*

[9] International Electrical Committee Standard 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems.*

[10] J. Miler, J. Górski, *An Environment Supporting Risk Management in Software Projects*, proc. of 1st National Conference on Information Technologies, Gdansk, Poland, 2003, in Polish

[11] J. L. Lions et al., *Ariane 5 Flight 501 Failure - Report by the Inquiry Board*, European Space Agency, Paris, 19 July 1996

[12] *Safety Management Requirements for Defence Systems*, MoD Defence Standard 00-56, Issue 3, 2004

[13] W.W. Gibbs: *Software's Chronic Crisis*, Scientific American, **271** (3), September 1994, pp. 86-95