COMPUTERS & SECURITY 63 (2016) 45–66

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# A multifaceted evaluation of the reference model of information assurance & security

Yulia Cherdantseva [a,*], Jeremy Hilton [b], Omer Rana [a], Wendy Ivins [a]

[a] School of Computer Science and Informatics, Cardiff University, Cardiff, UK
[b] Centre for Cyber Security and Information Systems, Cranfield University at the Defence Academy of the UK, Cardiff, UK

ARTICLE INFO

*Article history:*
Received 14 June 2016
Received in revised form 14 September 2016
Accepted 20 September 2016
Available online 23 September 2016

*Keywords:*
Information Security
Information Assurance
Conceptual model
Reference model
Analytical evaluation
Empirical evaluation

ABSTRACT

The evaluation of a conceptual model, which is an outcome of a qualitative research, is an arduous task due to the lack of a rigorous basis for evaluation. Overcoming this challenge, the paper at hand presents a detailed example of a multifaceted evaluation of a Reference Model of Information Assurance & Security (RMIAS), which summarises the knowledge acquired by the Information Assurance & Security community to date in one all-encompassing model. A combination of analytical and empirical evaluation methods is exploited to evaluate the RMIAS in a sustained way overcoming the limitations of separate methods. The RMIAS is analytically evaluated regarding the quality criteria of conceptual models and compared with existing models. Twenty-six semi-structured interviews with IAS experts are conducted to test the merit of the RMIAS. Three workshops and a case study are carried out to verify the practical value of the model. The paper discusses the evaluation methodology and evaluation results.

© 2016 Elsevier Ltd. All rights reserved.

## 1. Introduction

Evaluation is critical for any qualitative research claiming plausibility. The evaluation of a conceptual model, which is an outcome of a qualitative research, is an arduous task due to the lack of a rigorous basis for evaluation: "*a conceptual model exists only as a construction of the mind, and therefore quality cannot be as easily assessed*" (Moody, 2005). Clear methods for the evaluation of conceptual models are still lacking and evaluation is often subjective and/or hard to formalise despite the fact that there are multiple proposals, originating both from research and practice, suggesting methods for the evaluation of the quality of conceptual models (at least fifty proposals are identified and analysed in Moody, 2005). Overcoming these challenges, in this paper, we present a concrete and detailed example of multifaceted evaluation of a Reference Model of Information Assurance & Security (RMIAS) (Cherdantseva, 2015; Cherdantseva and Hilton, 2013a).

A reference model is a sub-type of a conceptual model, which strives to represent a problem at the industry level and to capture the entire domain knowledge (Moody, 2005). Despite all discrepancies regarding the clear definition of the term reference model, it is generally accepted among academics that reference models are "*aggregated models, generic models, or theoretical models that have to be adapted to the specific conditions of enterprises and projects*" (Jede and Teuteberg, 2016).

Information Assurance & Security (IAS), as with any other knowledge area, has either an explicit or assumed conceptual model, which describes the phenomenon being investigated, "*maps reality, guides research and systematizes knowledge*" (Järvelin and Wilson, 2003). Conceptual models convey the knowledge

* *Corresponding author.*
*E-mail address:* CherdantsevaYV@cardiff.ac.uk (Y. Cherdantseva).
http://dx.doi.org/10.1016/j.cose.2016.09.007
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

of IAS in a human-intelligible way and are usually graphically represented (Fettke and Loos, 2007). The pivotal purpose of a conceptual model is to facilitate understanding and communication among interested parties of the domain (Moody, 2005, p. 244).

The importance of a conceptual model of the IAS domain is demonstrated via multiple implications. As often acknowledged, many security issues are caused by incorrect security decisions being taken on the basis of incomplete knowledge or misunderstanding of the security domain: threats, security goals and available countermeasures (Ekelhart et al., 2006). In order to overcome this issue, the main entities of the knowledge area as well as the relationship between them should be defined and brought together in a conceptual model. A conceptual model of the IAS domain structures the acquired body of knowledge, creates a common ground for Information Security and Information Assurance professionals, and serves as a conceptual framework and a theoretical background for the researchers. A model clearly visualises the IAS domain, and enables newcomers to get a quick appreciation of its diverse and complex nature. A reference model of IAS plays a crucial role in the context of the information system development as it serves as a blueprint for the design of a *secure* information system. It provides a basis for the elicitation of system security requirements and for the development of an Information Security Policy Document (ISPD) (ISO/IEC, 2005, Sec.5).

IAS is a constantly developing domain, which changes shape following the evolution of society, business needs and ICT. Many studies highlight continual changes of IAS (Anderson, 2001; ISACA, 2009; Lacey, 2009; Parker, 1998; Pipkin, 2000). A conceptual model of a discipline often becomes debatable and requires a revision when the area of knowledge evolves and broadens (Järvelin and Wilson, 2003). As a result, the conceptual model of IAS is regularly revised reflecting the changes in the domain (Parker, 1998, p. 228).

The broadening of the scope of IAS and its multi-disciplinary nature led to the growth of a number of experts who should be involved in the discussion of IAS. The knowledge of experts with different, often non-technical, backgrounds which relates to the various aspects of IAS such as legislation, human-factor, economy, administration, etc. should be captured in order to produce an holistic picture of IAS in an organisation. A group of experts discussing IAS issues may include, but is not limited to business experts (manager or business owner), IAS officers, computer and network experts (system administrators), legal advisers and Human Resources (HR-) experts. Hence, the model of the IAS domain should be expressed at the level accessible to this broad audience and should aid in engaging non-technical and non-security experts in security discussion and decision-making.

The RMIAS, which we discuss in greater detail in Section 3, is one of the recent reference model of the IAS domain. It summarises the knowledge acquired by the IAS community of academics and practitioners to date in one all-encompassing model. It presents the key concepts of IAS and the interrelationships between them at a high level of abstraction in a form suitable for a wide range of experts with different backgrounds. The RMIAS approaches IAS holistically as a complex multi-disciplinary issue. The RMIAS was developed based on the analysis of the existing conceptual models described in Section 2 and on the extensive analysis of IAS literature summarised in Cherdantseva and Hilton (2013b). The RMIAS was originally presented in Cherdantseva and Hilton (2013a) with a detailed description available in Cherdantseva (2015).

The ultimate aim of this research is to verify the following hypothesis:

*The RMIAS provides more complete and accurate representation of the IAS domain, than the existing conceptual models of the IAS domain. The RMIAS reflects how the IAS domain is understood by IAS domain experts. It represents the domain in the form accessible by the experts with the different backgrounds and with the different levels of experience in IAS. Due to the above, the RMIAS helps to build a congruent understanding of the IAS domain in a multi-disciplinary team of experts.*

Summing up, our intention is to test whether the RMIAS corresponds with the vision of IAS possessed by the experts of this domain and whether the RMIAS meets the quality criteria of a conceptual model.

The remainder of the paper is organised as follows. In Section 2, we discuss the related literature. Section 3 provides the reader with the descriptions of the RMIAS. Next, in Section 4 we outline the evaluation methodology and justify the choice of the evaluation criteria. Then, Section 5 analytically evaluates the RMIAS and analyses the responses of the interviewees. Sections 6 and 7 contain the description of the arrangement and the feedback from the workshops and the case study respectively. Section 8 discusses the evaluation results and the limitations of the evaluation methodology. Finally, in Section 9 we draw concluding remarks.

## 2. Related work

In order to identify related work, we conducted a systematic review of the proposed models and frameworks of IAS following the methodology used in Blanco et al. (2011) for the analysis of security ontologies. The search was conducted in the following sources: Google Scholar, ACM Digital Library, IEEE Xplore Digital Library, SCOPUS.

Initially, 52 proposals were selected based on the title, keywords and abstract. The papers were examined and out of them closely related proposals were selected according to the following criteria:

- A model describes the IAS domain. Maturity models were excluded from the analysis because rather than describing the domain, they describe various stages of the Information Security (InfoSec) maturity of an organisation;
- A model addresses the IAS domain in general at a high level of abstraction. Two domain-specific models (e.g. models for governments and e-business) were also selected as they exploited a comprehensive approach to IAS;
- A model/framework has a visual representation (although the absence of a visual representation alone was not a reason for exclusion);

Finally, seventeen models and frameworks of IAS were selected for the analysis. Tables 1 and 2 summarise the analysis of the selected for review models. Table 1 gives an overview of the models and outlines (1) the basis for the development of a model, (2) model evaluation methods used, if any, (3) the

Download English Version:

https://daneshyari.com/en/article/4955592

Download Persian Version:

https://daneshyari.com/article/4955592

Daneshyari.com