Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Information assurance techniques: Perceived cost effectiveness

*Jose M. Such, Antonios Gouglidis, William Knowles *, Gaurav Misra, Awais Rashid*

Security Lancaster, School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, United Kingdom

ARTICLE INFO

Article history:
Received 7 September 2015
Received in revised form 16 January 2016
Accepted 28 March 2016
Available online 14 April 2016

Keywords:
Security
Assurance techniques
Perceptions
Security assessment
Effectiveness
Cost-effectiveness

ABSTRACT

The assurance technique is a fundamental component of the assurance ecosystem; it is the mechanism by which we assess security to derive a measure of assurance. Despite this importance, the characteristics of these assurance techniques have not been comprehensively explored within academic research from the perspective of industry stakeholders. Here, a framework of 20 "assurance techniques" is defined along with their interdependencies. A survey was conducted which received 153 responses from industry stakeholders, in order to determine perceptions of the characteristics of these assurance techniques. These characteristics include the expertise required, number of people required, time required for completion, effectiveness and cost. The extent to which perceptions differ between those in practitioner and management roles is considered. The findings were then used to compute a measure of cost-effectiveness for each assurance technique. Survey respondents were also asked about their perceptions of complementary assurance techniques. These findings were used to establish 15 combinations, of which the combined effectiveness and cost-effectiveness was assessed.

1. Introduction

At the heart of the information assurance process lie the "assurance techniques" that are used to evaluate and measure security. Despite this, and against the backdrop of the trend of year-on-year annual increases of security expenditures for organisations of all sizes (Department of Business Innovation and Skills, 2014; PricewaterhouseCoopers, 2014), the characteristics of assurance techniques remain largely unstudied. This leaves a lingering question unanswered: how do we ensure that the increasing number of trained professionals, products, and services in the information assurance space are deployed and utilised in a cost-effective manner? The necessity of such knowledge increases through the growing number of certifications and legal regulations for organisations of all sizes that mandate a "level" of assurance that must be met.

This study intends to address this gap through a large-scale study on the perceptions of industry practitioners on the value of such assurance techniques. This work is intended to facilitate the economic use and procurement of assurance techniques by entities seeking to evaluate their security posture, inform the design of future assurance schemes which mandate particular assurance techniques, and provide a resource for academic research on cost-effective approaches to assessing security. The key contributions of this paper are:

* *Corresponding author.*
E-mail address: w.knowles@lancaster.ac.uk (W. Knowles).

http://dx.doi.org/10.1016/j.cose.2016.03.009
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

1. A consistent and coherent assurance terminology to clearly define assurance schemes, targets, techniques, and evidence along with their relationships.
2. The definition of an assurance technique framework consisting of 20 assurance techniques classified across 5 categories, along with the relationships between them.
3. An analysis of the perceptions of 153 industry practitioners about the characteristics (e.g., the effectiveness) of the assurance techniques defined within the framework, both as individual entities and as combinations, along with how perceptions differ between practitioner and managerial roles.
4. The synthesis of perceptions to derive measures of assurance technique cost-effectiveness.

The remainder of this publication is organised as follows. Related literature is introduced in Section 2. Section 3 describes the methodology used within this study. Terminology for the assurance ecosystem is then defined in Section 4, along with the framework of 20 assurance techniques across 5 categories in Section 5. Data on the survey and composition of respondents are presented in Section 6. Section 7.2 then examines the perceptions for individual assurance technique characteristics. A metric for cost-effectiveness is introduced in Section 7.3 along with the results of the analysis. Combinations of assurance techniques are then established, and analysed for their effectiveness and cost-effectiveness in Section 7.4. Section 8 concludes the paper.

2. Related work

Despite the extensive body of research for information assurance, the techniques with which we measure security have largely escaped rigorous analysis. Two dimensions of existing literature are explored below: the effectiveness of assurance techniques themselves and the economics of effectiveness.

The discussion of assurance techniques within existing literature has largely fallen on their role within software assurance. In particular, assurance techniques and their use within the software development life cycle (SDLC) (e.g. Arkin et al., 2005; Davis, 2013; Jones and Rastogi, 2004; McGraw, 2004, 2012), or in rare cases, their use within specific product-focused assurance schemes (e.g., the classification of assurance techniques for use within Common Criteria (Jackson and Cooper, 2005)). The predominant body of work in this area has been instigated by the National Institute of Standards and Technology (NIST) project, Software Assurance Metrics And Tool Evaluation (SAMATE[1]), which is sponsored by the U.S. Department of Homeland Security (DHS). An abundance of publications have been produced under this umbrella[2]; in particular around the topic of source code analysis, with the predominant focus on static analysis (e.g. Black, 2011, 2012). SAMATE also performs comparative analyses of static analysis tools as part of its Static Analysis Tool Exposition (SATE) project. The fourth iteration is published as NIST Special Publication 500-279 (NIST, 2013). Beyond SAMATE, static analysis is notable for receiving wider interest as a topic of academic security research (e.g. Bessey et al., 2010; Chess and McGraw, 2004), along with its counterpart, dynamic analysis (e.g. Schwartz et al., 2010). More broadly, a comprehensive review of existing software security assessment tools is presented in (DC Washington Navy Yard and Hamilton, 2009), focusing on when they can be used, their required skills, and their benefits and drawbacks. One assurance technique that has seen research that includes but spans beyond software assurance, is that of penetration testing (which is also frequently used as a misnomer to describe other assurance techniques, such as vulnerability assessments). Little of this research has looked at measuring the effectiveness of penetration testing; however, the core themes have centred on its potential effectiveness to organisations and the motivations for procuring them (e.g. Bishop, 2007; Geer and Harthorne, 2002; Midian, 2002), ensuring that those who conduct penetration tests are appropriately skilled, which has a direct relationship with the resulting effectiveness (e.g. Tang, 2014; Xynos et al., 2010) and the methodologies for conducting a successful penetration test (e.g. Thompson, 2005).

The cost-effectiveness of assurance technique usage is one component within the larger domain of research surrounding the economics of information assurance. Although a marked increase in research activity has been seen here over the past five years (see Anderson and Moore, 2006 for an early survey), the emphasis has predominantly fallen on topics such as incentives (e.g. Anderson et al., 2007), the related topic of cyber insurance (e.g. Pal et al., 2014), and cyber crime (e.g. Anderson et al., 2013; Kshetri, 2006), while limited attention has been paid to the economic aspects of assurance techniques – in particular, their cost-effectiveness. Where this exists, the focus has again fallen on software assurance. For instance, Tassey (2002) investigated the economic impact of inadequate infrastructure for software testing and Drommi et al. (2007) elaborated on existing approaches to model and assess the cost and value of software.

The scope of assurance techniques falls beyond software assurance, however, and it is in this broader application that this study is concerned: the multitude of assurance techniques, both non-technical (e.g., interviews and observation) and technical (e.g., penetration tests), which can be used in the assessment of security controls (be they technical, organisational or physical). To the authors' knowledge, existing literature has not yet covered such a comprehensive analysis.

3. Methodology

This study presents the first comprehensive study of the characteristics of assurance techniques from the perspective of industry stakeholders. The methodology is illustrated in Fig. 1. It can be seen to span two phases, with information gathered from three sources: first, desk research examined existing literature and the definition and usage of assurance techniques within 17 assurance schemes (e.g., within standards); second, 14 targeted interviews (i.e., for particular assurance schemes or scenarios) to understand the role of assurance techniques in practice; and third, an online survey that received responses from 153 industry stakeholders.

[1] http://samate.nist.gov/Main_Page.html.

[2] A comprehensive list of SAMATE publications can be found at: http://samate.nist.gov/index.php/SAMATE_Publications.html.