Author(s): Ouedraogo, Moussa; Mouratidis, Haralambos; Khadraoui, Djamel; Dubois, Eric; Palmer-Brown, Dominic.
Title: Current trends and advances in IT service infrastructures security assurance evaluation
Year of publication: 2009
Citation: Ouedraogo, M. et al. (2009) 'Current trends and advances in IT service infrastructures security assurance evaluation' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 4th Annual Conference, University of East London, pp.132-141
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

CURRENT TRENDS AND ADVANCES IN IT SERVICE INFRASTRUCTURES SECURITY ASSURANCE EVALUATION

Moussa Ouedraogo[1,2], Haralambos Mouratidis[2], Djamel Khadraoui[1], Eric Dubois[1] and Dominic Palmer-Brown[2]
[1]Public Research Center Henri Tudor - 1855 Kirchberg/Luxembourg
{moussa.ouedraogo, djamel.khadraoui, eric.dubois}@tudor.lu
[2] Innovative Informatics, School of Computing and Technology, University of East London, England
{haris, D.Palmer-brown}@uel.ac.uk

Abstract: The term security assurance has been used in the computer science literature to express the confidence that one has in the strength of the security measures. The need for a methodology to measure current security assurance levels of a system has been reported in the literature as vital in order to maintain and improve the overall security. However, a scrutiny of the literature reveals that in the area of IT security assurance, a large number of research questions still remain without an answer. Although a number of works have been presented in recent years, especially with respect to assurance metrics development, little effort has been made in developing a robust operational methodology for the evaluation of IT service infrastructures security assurance. This paper captures the current status of research efforts made in the field of security assurance evaluation. It collects previous and current academic, normalization and commercial work on security assurance, and establishes a comprehensive state of the art in the domain. In addition, the paper outlines the general features of an ongoing work aiming at the development of a security assurance evaluation framework that takes into account the evolving and ubiquitous IT infrastructures. The novelty of this ongoing work lies not only on the adaptability of the security assurance evaluation system to the evolving infrastructure model but also on the use of a "bottom-up" approach in evaluating the security assurance level of a service using aggregation techniques. The methodology is intended to assist network managers in addressing more promptly security failures within the infrastructure as well as to increase the trust of end users in using IT systems.

1. Introduction:

It has been acknowledged that building "totally" secure systems is desirable, but yet unachievable mainly due to the difficulty in anticipating, during the system development process, all the potential future threats to the system and the evolution of systems' environment parameters.
Organizations routinely connect mission-critical systems and data to the Internet and use the World Wide Web to create efficiencies and meet customer expectations and competitive demands. However, this does come at a price, as evidenced by the soaring number of incidents related to computer hacking, and ID thefts. Faced with the routinely failure of Information Technology (IT) systems and their sometimes inherent vulnerabilities, which in turn provide suitable avenues to compromise organizations systems' security, end users have become apprehensive and suspicious towards the use of IT systems.

In addition to the incommensurable efforts made from across computer science disciplines that have and are providing solutions to the growing problem of IT security, *Security Assurance Evaluation* is a field that is gaining momentum. The objective of security assurance is to establish a basis for gaining justifiable confidence that systems will consistently demonstrate one or more desirable properties such as quality, reliability, conformity and more importantly security.

To that extent, recent efforts within the field have been directed towards utilizing quantitative indicators in a more systematic and coordinated fashion to capture the security state of a particular IT infrastructure. The challenge, however, in developing accurate and reliable indicators, similarly to the once developed by the financial market, resides in developing good metrics that will be used to compute these indicators. Until recently the focus was mainly on developing qualitative metrics that usually lead to security assurance levels that are either not accurate and/or not repetitive. Thus the assurance level of a particular piece of IT infrastructure is arrived at via subjective or intuitive considerations of the experts who are familiar with the protocols, architecture and systems utilized in the network (Seddigh et.al, 2004).

Although recently we have witnessed a surge in the number of works dedicated to the field of security assurance evaluation, the literature still fails to provide evidence of a methodology for the evaluation of IT system infrastructure security assurance at runtime, which can be easily adapted to the evolving nature of the IT infrastructure model in addition to helping increase end users' trust in systems by providing sensible and almost real time insights of the system operation nodes.

The main research approach [Ouedraogo et. al, 2008][Pham et. al, 2008], which underpins techniques developed to support security assurance evaluation at operational level, assumes that (i) system operators must identify the set of security functions to be monitored; and (ii) specify assurance metrics for each of them before performing the measurements through the use of probe agents. Other approaches are simply products, which identify the security state of a given system, usually by detection of intrusion and potential attacks that can be made against the system by updating security vulnerabilities databases.

Moreover, current techniques assume that infrastructures are static and they model them that way. When, however, changes do occur, and this is more and more the norm rather than the exception, existing techniques fail to adequately deal with the complications that arise within continuously changing infrastructure models and either become obsolete or at best they require major updates that are costly.

Covering for dynamic infrastructures requires techniques that will allow for the automatic alignment between the changing IT infrastructures and the security assurance evaluation system or the addition on-the-fly of new security functions to be evaluated as similarly done in fields such as requirements monitoring (Feather et. al, 1998),(Robinson, 2003)(Mahbuk, 2004).

This paper provides a step towards the solution of this issue. Firstly, we provide a comprehensive review of the current state of the art in IT security assurance evaluation in section 2. Secondly, in sections 3 and 4, we highlight the requirements for a framework aiming to overcome the above discussed limitations and support the evaluation of IT infrastructure security assurance. Finally, section 5 concludes the paper and discusses some areas for future work.

2. Existing studies, trends and tools:

Works undertaken in the area of IT security assurance evaluation can be classified into three major groups: (i) commercial services and products; (ii) standards, and (iii) academic / governmental research.

2.1 Some Commercial Offers:

IT Security has become a profitable business for consulting companies claiming they are the only specialists able to provide security evaluations. Although the existence of dedicated security assurance products in the market is quite recent, the brief state of the art on commercial offers demonstrates that security assurance evaluation methodologies and tools offer promising market opportunities.

Intellitactics (Intellitactics, 2008) is providing a tool called **Security Assurance Metrics™**. This tool provides a dashboard that allows the creation of multiple views of enterprise security based on physical location, business unit or domain interest. Each dashboard template stored in the library can be configured with any number of **security assurance metrics™** that are dynamically updated to provide relevant and appropriate information to each recipient. Security reports and summarized information are intended to be understood by executives and used for decision-making. The information obtained helps for instance to compare a point-in-time measure to organizational benchmarks, or to identify deviations from normal behavior.

The Security Assurance Group (2008) is a security-consulting firm that provides various assistance services regarding security aspects, especially on Operational Security Assessment. Under this broad term, the company is proposing services on security reviews, vulnerability assessment with the objective of formal certification process or regulation compliance.

The Skybox security company is delivering products for risks assessment. We have looked in more details at their new product called Skybox Assure™ (Skybox security, 2008). Designed for IT operations team, Skybox Assure™ helps organizations proactively analyze, compare, validate and optimize planned network changes. The entire access and connectivity environment is modeled in order to assess the connectivity profile of the network and compare network control information against defined policies.

The ISMS Tool Box offers varied praxis-based facilities for the development, operation and maintenance of an Information Security Management System (ISMS, 2008). It allows you to create rules and regulations quickly and easily and to communicate them in different languages through the intranet. In a working group the rules and regulations can be reviewed and validated and their implementation planned and continuously monitored. The ISMS Tool Box supports not only the Ownership Model, but Inventory and Classification of assets as well. The Functions responsible for the protected assets can be clearly displayed. The ISMS Tool Box also supports business Continuity activities effectively. Alongside the possibility of running a glossary with a collection of relevant links on the intranet, a security incident management system which conforms to Basel II can also be created.

ASPECT (Aspect security, 2008) verifies critical applications for the largest financial, utility, media, e-commerce, and entertainment companies in the world. ASPECT' s Assurance Services provide understanding of the security of an applications via clear, structured, and actionable scorecards supported by comprehensive detailed findings. The

evaluation approach combines security code review and penetration testing to ensure completeness, accuracy, and cost-effectiveness in identifying vulnerabilities, determining related risks and impacts, and ascertaining root causes. ASPECT provides services to verify the security of entire application portfolios or of individual applications.

2.2 Existing Standards:

The most recognized security assurance assessment methodology in the industry is defined by the ISO/IEC 15408 standard, also known as Common Criteria (CC). The CC describes a framework in which developers can specify their security requirements and testing laboratories can evaluate the products to determine if they actually meet the claimed security. In other words, CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. The CC evaluations are performed on computer security products and systems and consist of four documents:

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements
- CEM: Common Evaluation Methodology

The first part defines the general concepts and presents a global model of evaluation: evaluation of Protection Profile (PP), Security Target (ST) and the product itself or Target of Evaluation (TOE). This part also provides the description of the contents of a PP and ST.

The second part defines a collection of generic security functional requirements split up into classes, themselves broken up into families of components, which cover access control, identification, authentication, physical protection, etc The developer selects the best adapted requirements for their product and instantiates them in the Security Target. CC also allows stating requirements for families of products within Protection Profiles.

The last part defines the assurance requirements both for the development environment and for the product itself as well as the tasks for the evaluator. These assurance requirements are organized in classes, then in families of components, which cover functional specification and design descriptions, testing, life cycle management, delivery procedures, security of the development environment, vulnerability analysis, etc. Developers can either build up their own consistent assurance package or use one of the seven predefined Evaluation Assurance Levels (EAL). EAL1 to EAL7 provide an increasing scale that balances the level of assurance obtained on the product security with the cost and feasibility of acquiring that degree of assurance. Each of these levels can be augmented with one or more additional components in order to meet specific objectives.

However, the Common Criteria defines security assurance evaluation requirements for the development and design phases and is not directly applicable for an evaluation of the security assurance of a system in operation. CEM defines how the system must be developed, but not how to maintain it in the “correct” (i.e. intended) state.

ISO/IEC 27004 (ISO, 2008) is a new standard, part of the ISO/IEC 27000- series numbering, being developed for Information Security Management Systems (ISMS). This new standard is being designed to cover information security management measurement and metrics. It is intended to help an organization establish the effectiveness of its ISMS implementation.

Currently, the standard development is still underway.

Similarly to the Common Criteria, ISO 27004 will not be applicable to large deployed systems. The focus remains mainly organizations or small systems.

2.3 Academic and Government Agencies Research:

Several government and academic researches have been dedicated to the evaluation of IT security assurance and mainly to the development of security assurance metrics.

The WISSRR 2001 workshop (WISSSR, 2001) came with the perspective of addressing the challenges in developing metrics or measures for systems requiring security or assurance, but failed to reach an agreement on a set of measures to be used or even a consensus in any particular approach. The workshop organizers agreed the problem domain might be best viewed using a non-disjoint partitioning into technical, organizational, and operational categories. However, there were some useful observations that emerged from this workshop that have been listed as a conclusion:

- There will be no successful single measure or metric that one can use to quantify the assurance present in a system.
- Quality of the software delivered, the architectures and designs chosen, the tools used to build systems, the specified requirements and more are all related to the assurance being quantified.
- There are differences between the Government and the Commercial sectors. This may result in different values placed on metrics or measures between the two sectors.
- Attempts to quantify and obtain a partial ordering of the security attributes of systems in the past have not been successful to a large degree (e.g. the TCSEC and the Common Criteria).
- Processes, procedures, tools and people all interact to produce assurance in systems. Measures that incorporate all these are important.

An interesting characterization of information security metrics was proposed by Bodeau (Bodeau, 2001) of the MITRE Corporation (sponsor of the workshop) according to whom a proper view of metrics might best be viewed as a cross-product involving what need to be measured, why you need to measure it, and who you are measuring for.

Vaughn et.al. (2002), proposed a taxonomy that is divided into two distinct categories of metrics. The first category (organizational security) of metrics aims at assessing the "Information Assurance (IA) posture" (i.e. the actual state) of an organization while the second category is for assessing the IA capabilities of a product or system (Technical Target of Assessment - TTOA).

The second category of metrics is for the Technical Target Of Assessment (TTOA). This type of metric is intended to measure how much a technical object, system or product is capable of providing security in terms of protection, detection and response. This category is often used in comparing or differentiating between alternative and competing TTOA, e.g. the EAL ratings of the Common Criteria. The authors further divide the metrics for the TTOA into two sub-categories – metrics for measuring a TTOA's strengths and metrics for measuring a TTOA's weaknesses.

The Security Metrics Guide for Information Technology Systems (Swanson, 2001) is a

special publication of the National Institute of Standards and Technology (NIST). The publication provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It describes the metric development and implementation process and how it can be used to adequately justify security control investments. This process is called a *Security metrics program* and is to be employed as part of an *Information Security Program***.** The work of the NIST identified 17 metrics groups, which are classified in three categories: management, operational and technical. The new version (NIST SP 800-55) (Swanson, 2003), however, provides a recommended methodology for quantifying the critical elements and for validating the implementation and effectiveness of the system security control objectives and techniques.

Sedddigh et al. (Seddigh et.al, 2004) propose a novel definition for Information assurance that is broader than commonly assumed. The authors suggest that the three key elements that are security, quality of service and availability should constitute the bedrock of a comprehensive definition of Information assurance when applied against IT infrastructure. Fig.1 (Seddigh et al, 2004) provides an illustration of the three key elements with examples of metrics and indicators for each of them. The definition is then used to develop a taxonomy of Information assurance metrics group which can be used for the measurement of IT information assurance.

However, all these contributions only provide means to find the metrics and do not indicate how to combine them into system-wide values in addition to lacking modeling technique which is crucial for building a tool evaluating the assurance of a system.

More recently, some initiatives have been taken towards developing operational methodologies for the evaluation of IT infrastructure security assurance.

Pham et.al (Pham et. al, 2008) introduce an attack graph based security assurance assessment system based on multi-agents. In their approach, the authors use attack graph to compute an "attackability" metric value (the likelihood that an entity will be successfully attacked) for static evaluation and define other metrics for anomaly detection at run time.

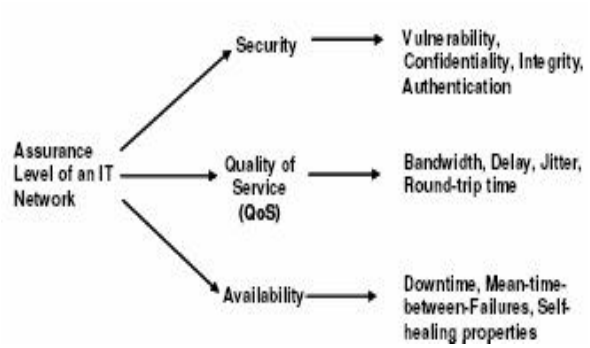

Figure1. Elements of Information Assurance

Only recently, we described the research prototype of a security assurance monitoring framework (the methodology and an example application) that results from a research project called BUGYO (Ouedraogo et.al, 2008). Building on the Common Criteria, security assurance, in the context of BUGYO, is understood as the ground for confidence that an entity meets its security objectives. In another word, the aim is to make assertions on the protection of systems (here: telecom' systems) regarding availability, compliance and vulnerability. Different from the approach known in the Common Criteria, the security assurance is measuring and probing defined criteria of running systems, not specifications, thus having lower latency in the evaluation.

Unfortunately, these later contributions do not account for the dynamicity of the infrastructure model.

3. Building the foundation of an assurance evaluation methodology:

The perpetual changes in the requirements that define the properties that software is required to have, arise from many sources. Users have new or changed needs, development organizations seek to increase revenue or enlarge the customer base while developers often wish to incorporate new concepts or ideas and so on. In that context, the observing system implemented to evaluate such systems security assurance should take notice of the changes being perpetrated and adapt accordingly if one is to expect security assurance measures that are accurate. In an attempt to translate this in mathematical terms, let us assume that a change in the "observed system" model is automatically detectable and can be represented as ΔX. ΔX can symbolized any changes ranging from the addition, update to the removal of a component from the infrastructure model. This change ΔX within the system should command some corrections within the evaluating system to ensure the permanent alignment between the two entities. We note that latter adaptation in the observing system as ΔY. In a security assurance evaluation context where it is assumed each component, or entity in a more general term, requiring some measurements is assigned assurance metrics, ΔY could be the addition, suppression or update of metrics necessary for the handling of the component that has originated the change. Figure 2 illustrates the adaption of the observing system to the changes in the observed system.

More importantly, let us assume that the initial system (before the changes) is represented by X and that SAv is a function used for the determination of the system security assurance level.

Security assurance level of X = SAv (x1, x2,..,xn), where xi is a component of the system.

Before going further, it is important to stress that the notation used here purely purposes the reader' understanding of the scope of the problem rather than representing any formal language syntax, although we intend in future work to capture all these aspects using mathematical representation. Assuming that the system composition after the change has taken place is (z1, z2,..,zp), with possibility that xj=zk (some component may have remained unchanged) and (p>n, p< n or p=n) depending on whether there has been addition, removal or just an update of a component, respectively. The whole problem can be summarized as the determination of the security assurance of the new system represented by the set of system component (z1, z2,.., zp).

The addition or suppression of an entity within a system can have considerable impact on computing the security assurance of a system as it could even lead to amendments with respect to the choice of the initial function used for the security assurance evaluation. For instance, considering systems with several critical points, implying a failure of only one component could culminate in a system total failure, the "minimum operator" i.e. SAv = min may be appropriate. Now, should the system protection measures be restructured in a way that no more critical component exists then using the minimum operator could reveal inadequate. Furthermore, other systems can be formed of subsystems with overlapping functionalities. Let us consider the following case for instance: considering two anti-viruses applications AV1 and AV2 are used among a wide range of system

protection measures with the AV1 being effective in containing viruses v1, v2 and v3 while the AV2 is only effective in containing v1. Without loss of generality, we can assume that the importance of each virus is equal. The resulting security assurance level provided by these two anti-viruses can be considered as *max (AL1, AL2) i.e. SAv= maximum function* where *AL1* and *AL2* are the security assurance values of AV1 and AV2 respectively. If we imagine a situation where AV1 and AV2 are reconfigured in a way that they play different but complementary role in removing v1, then we could consider the weighted sum function as more representative of the security assurance provided by their mutual action.

Both cases illustrate that the removal or addition of a critical component, added to the architectural change of the system, may result in the change of the security assurance function used to compute the assurance level of the system or subsystem.

4. Desiderata for the Proposed Security Assurance Evaluation Methodology:

As we have already mentioned in the previous section, changes in the observed system could culminate in more complex changes within the security assurance evaluation system. The relation between the two entities could be better appreciated by the formalization of the problem we have tried to specify in the previous section using well a established language syntax and semantic. In practice, we believe the changes perpetrated at the observed system level can be accounted for by acting on the metrics at the observing system level. In other words, adding, removing or updating a component in a system model could be handled by adding, deleting or updating metrics on the evaluator system side.

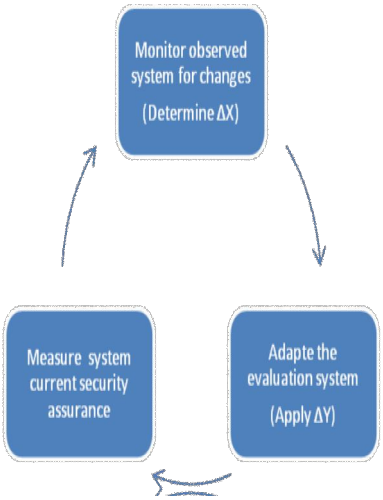

Figure 2. Adaption of the security assurance evaluation

The reliability of IT infrastructure and end-users trust in using the very same systems would be increased if methodologies for the evaluation of security assurance of IT system at operational time were to meet the following desiderata:

Automatic detection: The possibility to detect changes taking place in the model. One way of making the detection more systematic would be to recommend that software component be tagged with sensors or other devices which could be used to determine the status of the component in the system. These expressed security assurance metrics should be automatically compiled into runtime monitoring code.

Flexibility, convenience and incremental: the possibility for users to readily express instructions that will be used to account for the changes that have taken place without having to bring the observed system to an halt.

Use of a bottom-up technique in determining the security assurance level of a system:
Security assurance should be calculated in a hierarchical way i.e. security assurance level of every component is computed by taking into account the assurance level provided by all the subcomponents of that entity.

5. Conclusion and future work:

In this paper, we have provided a review of the current state of the art in security assurance evaluation as well as introducing an ongoing work that aims the development of a security assurance evaluation framework for operational system. We are currently working on formalizing the alignment between the observed system and the security evaluation system. The methodology can be of paramount relevance in area such as wireless networks where it can be adopted as a security application to face up to the growing problem of security. To that extent, it can be adopted as a complementary methodology to the several and diverse applications and technologies (essential to making wireless computing more secure) explored in "Handbook of Wireless Security: From Specifications to Implementations" (Sklavos et. al, 2007).

6. References:

Aspect Security, Available at http://www.aspectsecurity.com/aboutaspect.htm [Accessed 17 April 2008]

Bodeau D., Information Assurance Assessment: Lessons-learned and Challenges,proceeding of WISSR 2001, Williamsburg, VA, May 2001.

CC, Common Criteria for information Technology, part 1-3, version 3.1, September 2006.

Feather M.S., Fickas S., Van Lamsweerde A., and Ponsard C., Reconciling System Requirements and Runtime Behaviour. Proc. of 9th Int. Workhop on Software Specification & Design, 1998.

Intellitactics, Available at : http://www.intellitactics.com/int/products/sam.asp [Accessed 17 April 2008]

Information Security Management System (ISMS),Available at http://www.ismstoolbox.com/ [Accessed 17 April 2008]

ISO/IEC27004, Available at: http://www.iso27001security.com/html/27004.html [Accessed 17 April 2008]

Mahbub K. , Spanoudakis G., A Framework for Requirements Monitoring of Service Based Systems, Proc. Of the 2nd Int. Conference on Service-Oriented Computing (ICSOC '04), New York, November 2004.

Ouedraogo M. ,Khadraoui D., De Rémont B., Dubois E. , Mouratidis H., Deployment of a security assurance monitoring framework for telecommunication service infrastructures on a VoIP system , NTMS'2008, The 2nd International Conference on New technologies, Mobility and Security, 2008, Tangier, Morocco. IEEE Explore (To appear)

Pham N., Baud L., Bellot P. and Riguidel M., Towards a security cockpit, proceeding of the 2nd International Conference on Information Security and Assurance (ISA 2008), Busan, Korea, 2008

Pham N., Baud L., Bellot P. ,Riguidel M., A near real-time system for security assurance assessment , the third International Conference on Internet monitoring and protection pp. 152-160, Bucharest, Romania 2008.

Robinson W.N., Monitoring Web Service Requirements, Proceedings of 12th International Conference on Requirements Engineering, 2003.

Seddigh N., Pieda P., Matrawy A., Nandy B., Lambadaris l., Hatfield A., Current Trends and Advances in Information Assurance Metrics. PST 2004: 197-205

Sklavos N.,Zhang X., Handbook of Wireless Security: From Specifications to Implementations, CRC-Press, A Taylor & Francis Group, 2007.

SkyBOX Assure, Available at http:// www.skyboxsecurity.com/products/ assure.htlm. [Accessed 17 April 12008]

Swanson M., security Metrics guide for Information Technology System, National Institute of Standards and Technology Special publication#800-26.

Swanson M., Nadya B., Sabato J, hash, Graffo L., Security Metrics Guide for Information Technology Systems, National Institute of Standards and technology Special publication #800-55

Vaughn RB, Henning R, Siraj A., Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, in *Proceedings of the IEEE/HICSS'03*, Hawaii, Jan. 2002

Workshop on Information, Security System Scoring and Ranking (WISSSR, 2001) Information System Security Attribute Quantification or Ordering (Commonly but improperly know as security metrics)-Workshop Proceedings-May 21-23, 2001, Williamsburg, VA.