Secure Systems Development – The Evolving Integration of Validation and Verification

Klaus P. Jantke & Oliver Keller
German Research Center for Artificial Intelligence Ltd.
Stuhlsatzenhausweg 3
66123 Saarbrücken, Germany
{jantke,keller}@dfki.de

Abstract

The paper is aiming at a step towards a process model for the development of systems that are *valid* in the sense of meeting both specified security requirements and diverse user needs and expectations. The ultimate goal is to certify a system's validity.

Derived from IT security evaluation criteria, the paper is outlining a certain integration of two independently developed process models in a way that validation and verification are becoming truly dovetailed.

The discussed evaluation process model is currently being developed and implemented in the authors' IT security evaluation facility (ITSEF). It is one of the targets of this publication to bring academic research and development on validation and verification closer to the IT security evaluation practice.

The Message and the Goal of the Paper

What is the message the authors want to deliver by means of the present paper? And in case the message is reaching its audience, what is the goal, what are the implications, what to do next . . . ?

In the paper (Gonzalez & Barr 2000), the authors aim at the clarification of the meaning of the terms validation and verification as these terms apply to intelligent systems, and to describe how several researchers are implementing these. Furthermore, they detail some techniques that can be used to perform the verification and validation of complex systems. The authors of (Gonzalez & Barr 2000) claim that they *strongly believe that there are in fact two separate and independent processes, and that there is inherent value in performing the two processes in sequence (first verification, then validation)*.

The authors of the present contribution go a little further in saying that we do need a *dovetailing* of validation and of verification, and that we do need some systematic way (something like a guideline or guidebook) of doing so: *a process model of secure systems development*.

The need for a proper and well-organized dovetailing of validation and verification – at least in those cases where the quality expectations are very high due to the system's criticality – derives from the requirements of systems certification (cf. Common Criteria for Information Technology Security Evaluation, (Common Criteria 1 1998; Common Criteria 2 1998; Common Criteria 3 1998)).

Generally speaking, the basic message is that dealing with systems certification leads to a new perspective of validation and verification.

In slightly more technical terms, the authors propose a certain synthesis of the two process models found in (Knauf/Philippow/Gonzalez 2000) and (Auerswald 2000), respectively.

Systems' Intelligence and Security for e-Business, e-Commerce and e-Payment

Naturally, not every IT systems can be reasonably seen as an intelligent one. Thus, (Gonzalez & Barr 2000)'s perspective does not always apply.

Naturally, there are many IT systems which do not need any certification. In those cases, we do not need to ponder about the possible implications derived from the necessities of certification.

In contrast to those less ambitious and much less critical IT application areas, there is the rather exciting domain of world-wide business, especially commerce on the Internet including electronic payment systems.

E-commerce is booming, but a true break-trough is still pending. Key reasons are that a majority of potential users are worrying about the security of transactions in open networks; they simply do not trust in e-business, e-commerce and e-payment, in particular. Furthermore, they consider most interfaces too difficult to handle and do not want to download and install applications like fat wallet software, for instance.

There exists, naturally, a certain tradeoff between security and simplicity. What we do need are systems as secure as necessary and as simple and intuitive as possible.

We do need simplicity which is based on flexibility and adaptivity, i.e. on machine intelligence. And we do need security that is based on sophistication which is hidden to the user.

Original ideas and systems implementing those ideas are mushrooming in the area, and we do need a methodology to separate the winnow from the wheat.

Validation and Verification Concepts for Simplicity and Security in e-Commerce

There is a large variety of perspectives at systems validation and verification (cf. (O'Keefe & O'Leary 1993), for a frequently cited basic conceptualization, and (Gonzalez & Barr 2000), for a comprehensive discussion). The authors are aware of the quite different approaches which range from cognitive psychology (cf. (Schaad 1993) to formal methods (cf. (Autexier, Hutter, et al. 2000) and (Hutter, Langenstein, et al. 2000)) including automated logical reasoning. In dependence on the particular framework assumed, one might even be able to exhibit the enormous strength of necessary prerequisites of complex systems' validation resp. verification and, in special situations, come up with provably unsolvable tasks (cf. (Grieser, Jantke, & Lange 1998)).

Thus, the authors decided to narrow their attention to those application domains where security requirements meet the need for system intelligence. Validation and verification deal with the problem whether or not a given system or a system under development meets resp. will meet the needs of simplicity and security.

The authors' working hypothesis is, first, that there are good reasons for invoking rather different methodologies and tools, and second, that established IT evaluation criteria provide a useful guideline for validation and verification.

The development and publication of evaluation standards has been driven mainly by safety and security reasons. Thus, a discussion of these issues is suitable here.

Information held by IT products or systems is a critical resource that enables organisations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private, be available to them as needed, and not be subject to unauthorised modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards.

Many consumers of IT lack the knowledge, expertise or resources necessary to judge whether their confidence in the security of their IT products or systems is appropriate, and they may not wish to rely solely on the assertions of the developers. Consumers may therefore choose to increase their confidence in the security measures of an IT product or system by ordering an analysis of its security (i.e. a security evaluation).

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform. Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve.

There have been developed so-called *Common Criteria for IT Security Evaluation* (cf. (Common Criteria 1 1998; Common Criteria 2 1998; Common Criteria 3 1998)) that are widely accepted within the international community. Therefore, the authors adopt these criteria as a launching pad for their endeavour towards validation and verification techniques focussing the security issue of IT systems under evaluation. Finally, a few words about the importance of standardization in this area.

By establishing such a common criteria base, the results of an IT security evaluation is meaningful to a wider audience.

This standard permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

This standard is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions.

Let us briefly merge the security perspective with the system intelligence perspective. The criteria documents mentioned above do not explicitly lay out concepts like validity, e.g. In contrast, the paper (Gonzalez & Barr 2000) provides a very clear conceptualization which is especially tailored towards intelligent systems: *Verification is the process of ensuring that the intelligent system (1) conforms to specifications, and (2) that its knowledge base is consistent and completge within itself.* This is contrasted to the view that *validation is the the process of ensuring that the output of the intelligent system is equivalent to those of human experts when given the same input*. This perspective may be adopted for the type of systems under consideration and may be adapted appropriately. The *verification* concept cited does perfectly fit into the criteria documents where, for instance, higher evaluation assurance levels like EAL5 of CC do require to measure a system against some formally specified security policies. The *validation* concept has to be interpreted appropriately. Tasks of IT systems in e-business are usually somehow different from what humans do. But those system – for e-payment, e.g. – may be seen as software agents performing some job which can be evaluated from the viewpoint of how well they substitute human experts. Note that, in fact, humans are frequently doing such a comparison when, e.g., criticizing systems by comparing the system's appearance to a clerk's performance in a bank office.

To sum up, the conceptualization of (Gonzalez & Barr 2000) does meet our needs.

It's only that we do not agree with the approach of *performing the two processes in sequence (first verification, then validation)*.

Towards a Development Process Model

The authors' work is aiming at a generic process model for the development of secure IT systems with collateral validation and verification. They are currently involved in a

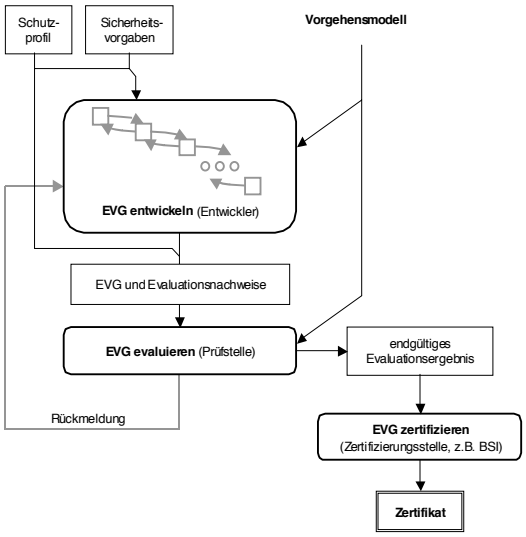

Abbildung 1. Entwicklung, Evaluation und Zertifizierung

Figure 1: Illustration from AUERSWALD

larger project where such a process model is under development[1] for the particularly exciting domain of electronic payment systems.

A first step towards such a process model has been published in (Auerswald 2000) and is illustrated here by a figure directly taken form the publication mentioned.

Due to Knauf, there is a family of validation approaches (cf. citeKnauf/Gonzalez1997, e.g.) motivated by Turing's influential paper (Turing 1950). These approaches lead to some process model of validation taken from (Knauf/Philippow/Gonzalez 2000):

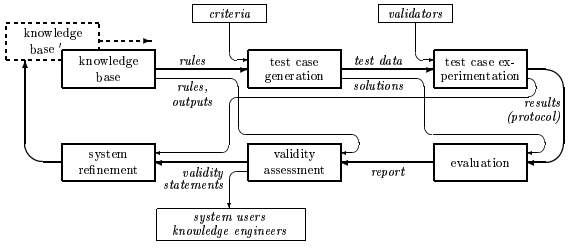

Figure 2: Illustration from KNAUF et al.

[1]Even for such a specific domain, the targeted process model does not yet exist. Therefore, the present paper necessarily reports about unfinished work, only. However, it seems already clear that this work in progress has some implications to be discussed in the sequel.

Last but not least, in the authors' institute there has been developed, implemented and tested some comprehensive method for system verification (cf. (Autexier, Hutter, et al. 2000) and (Hutter, Langenstein, et al. 2000)) which is based on automated logical reasoning. The key paradigm is named "invent and verify" and means that humans are entitled to design system properties and target security functions, and the computer systems is used for proving the desired properties.

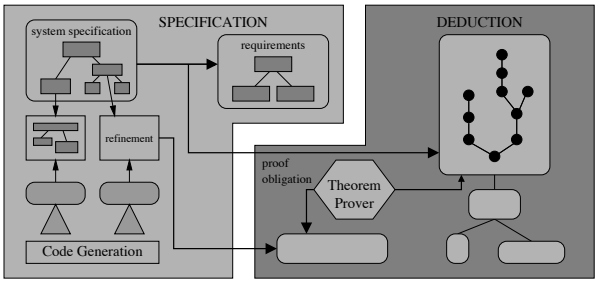

Figure 3: Illustration of Invent & Verify

According to the verification concept adopted from (Gonzalez & Barr 2000) above, this is computer-supported verification. Thus, the system VSE (cf. (Autexier, Hutter, et al. 2000) and (Hutter, Langenstein, et al. 2000)) is a verification tool, though it may be also seen as a CASE tool.

The VSE system allows for the automated proof of formalized system properties. The authors are very much in favor of automated verification, but ...

Integrating Validation and Verification

... formalizations are not always possible or appropriate. Formal descriptions of system properties and target functionalities might be not available or simply too expensive. In realistic evaluation tasks, consequently, one meets a certain mixture of formal and informal descriptions.

This is nicely reflected in (Common Criteria 3 1998), where a certain level[2] *provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a structured presentation of the implementation, to understand the security behaviour. Assurance is additionally gained through a formal model of the TOE security policy, a formal presentation of the functional specification and high-level design, a semiformal presentation of the low-level design, and formal and semiformal demonstration of correspondence between them, as appropriate. A modular, layered and simple TOE design is also required.*

[2]The criteria for IT security evaluation (the already mentioned CC as well as other comparable standards) determine certain evaluation assurance levels. These levels provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach (cf. (Common Criteria 3 1998), in particular) identifies the separate concepts of assurance in a target of evaluation (TOE, for short) at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

In the methodology circumscribed within the Common Criteria documents, especially (Common Criteria 3 1998), one is required to use validation and verification "as appropriate". The authors of these criteria documents are obviously aware of the difficulties of thoroughly formalizing system properties and target behaviors. They leave it open where to draw a demarcation line between formal and informal knowledge representation and reasoning,

This motivates the authors of the present paper to illustrate their proposal by the following figure which is intended to visualize that system evaluation may go through loops of repeated and possibly dovetailed validation and verification activities.

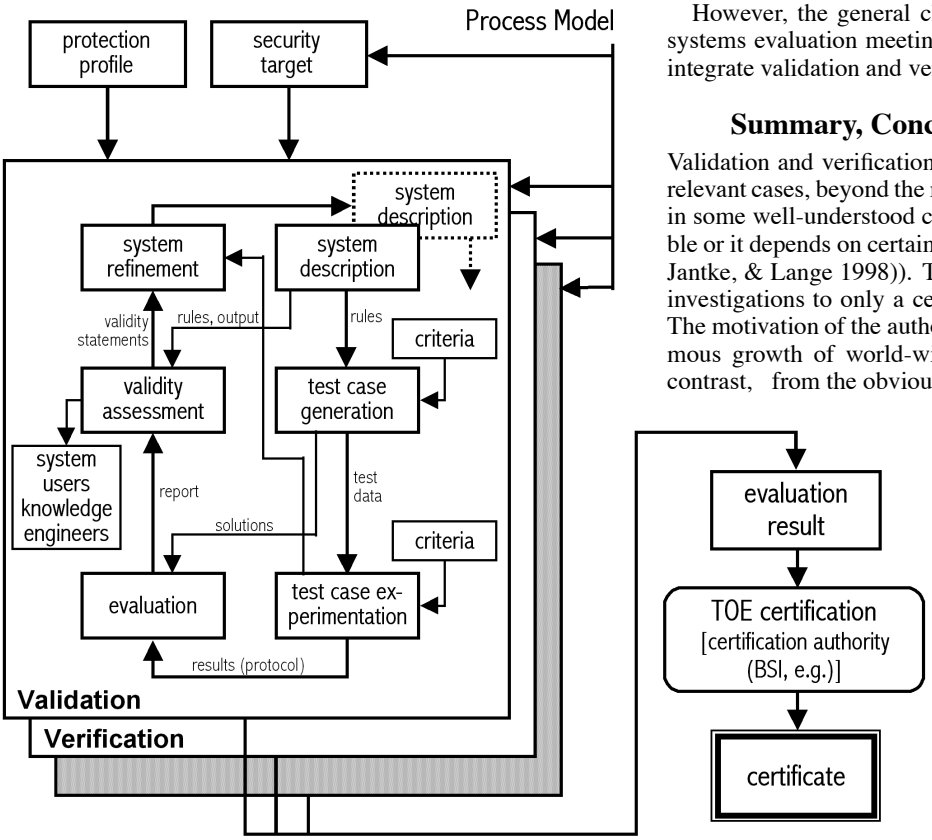

Figure 4: The Evolving Integration of V & V

This figure is intended to illustrate practically occuring evaluation activities which, roughly, proceed as follows:

Evaluators get presented some IT system (an integrated circuit card with digital signature functions constitutes a recent example from the authors' work) together with a large collection of documents according to the requirements specified in criteria documents like (Common Criteria 1 1998), (Common Criteria 2 1998), and (Common Criteria 3 1998). A certain evaluation assurance level is specified. Normally, evaluation starts with informal investigations and with some interviews of experts more or less analogous to Knauf's approach (cf. (Knauf & Gonzalez 1997)). When required, certain points are identified which need more formal reasoning. When facing the requirements of CC EAL5, for instance, formal specifications are taken as a basis. Target properties are formally specified, and the authors invoke the VSE system for proving the target properties, if possible at all. This is clearly verification as defined by (Gonzalez & Barr 2000).

The management of the sketched dovetailing is currently done intuitively and according to the possibilities of invoking the one or the other methodology or tool. Future work has to be invested into a suitable control of switching between the different paradigmatic ways (which are illusttrated above by overlapping rectangels) of how to evaluate a system.

However, the general claim of the present paper is that systems evaluation meeting the needs of modern IT has to integrate validation and verification appropriately.

Summary, Conclusions, and Outlook

Validation and verification of complex systems is, in many relevant cases, beyond the reach of current technologies, and in some well-understood cases, it is even provably impossible or it depends on certain strong assumptions (cf. (Grieser, Jantke, & Lange 1998)). Thus, the authors did narrow their investigations to only a certain aspect of systems' validity. The motivation of the authors' choice derives from the enormous growth of world-wide web communication and, in contrast, from the obvious lack of trust in e-commerce and in e-payment, in particular. The authors' focus is on secure and simple systems. Their work in an IT security evaluation facility lead to the observation that practical system evaluation needs both formal and informal representation and reasoning.

For validation and verification of IT systems under the perspective of IT security, there do exist comprehensive guidelines like CC which, interestingly, suggest a dovetailing of "formal and semiformal" methods, "as appropriate".

In the authors' opinion, there is no other way from the ivory tower of academic research on validation and on verification to commercially relevant applications on a big market than getting closer to each other and, in the very end, getting dovetailed.

Furthermore, there is some hope that the present contribution might encourage scientists both from the validation community and from the verification community to invest into some co-operative work within a certain project to exemplify the evolving integration of V & V. First stepts have been done in the area of human behavioral representation technologies.

References

Auerswald, M. 2000. Common criteria for IT security evaluation - Ausgangspunkt für Zuverlässigkeit im E-Commerce. WIWITA 2000, 2. Wismarer Wirtschaftsinformatiktage, 15./16. Juni 2000, 63–71

Autexier, S.; Hutter, D.; Langenstein, B.; Mantel, H.; Rock, G.; Schairer, A.; Stephan, W.; Vogt, R.; and Wolpers, A. VSE: formal methods meet industrial needs. *Int. J. STTT* 3, 66–77

Common Criteria, Part 1. 1998. Common criteria for information technology security evaluation. Part 1: Introduction and general model. Version 2.0.

Common Criteria, Part 2. 1998. Common criteria for information technology security evaluation. Part 2: Security Functional Requirements. Version 2.0.

Common Criteria, Part 3. 1998. Common criteria for information technology security evaluation. Part 3: Security Assurance Requirements. Version 2.0.

Gonzalez, A. J.; and Barr, V. Validation and verification of intelligent systems – what are they and how are they different? *Journal of Experimental and Theoretical AI* 12 (4), 407–420

Grieser, G.; Jantke, K. P.; and Lange, S. 1998a. Characterizing sufficient expertise for learning system validation. In Cook, D. J., ed., *Proc. 11th International Florida AI Research Society Conference*, 452–456. AAAI Press, Menlo Park.

Hutter, D.; Langenstein, B.; Rock, G.; Siekmann, J. H.; Stephan, W.; and Vogt, R. Formal software sevelopment in the Verification Support Environment (VSE). *Journal of Experimental and Theoretical AI* 12 (4), 383–406

IuKDG. 1997. The German Information and Communication Services Act: *Gesetz zur Regelung d. Rahmenbedingungen für Informations- und Kommunikationsdienste*.

Knauf, R., and Gonzalez, A. 1997. A TURING test approach to intelligent system validation. In Wittig, W., and Grieser, G., eds., *Proc. 5. Leipziger Informatik-Tage, Leipzig, 25./26. September 1997*, 71–76. FIT Leipzig.

Knauf, R.; Jantke, K.; Abel, T.; and Philippow, I. 1997. Fundamentals of a TURING test approach to validation of AI systems. In Gens, W., ed., *IWK–97, 42nd International Scientific Colloquium, Ilmenau University of Technology*, volume 2, 59–64. TU Ilmenau.

Knauf, R.; Philippow, I.; and Gonzalez, A. J. 2000. Towards validation and refinement of rule-based systems. *Journal of Experimental and Theoretical AI* 12

O'Keefe, R., and O'Leary, D. 1993. Expert system verification and validation: A survey and tutorial. *Artificial Intelligence Review* 7:3–42.

Schaad, G. 1993. Psychological aspects of human factor testing and evaluation of military human-machine systems. In Wise, J.; Hopkin, V.; and Stager, P., eds., *Verification and Validation of Complex Systems: Human Factors Issues*, volume 110 of *NATO ASI Series, Series F: Computer and Systems Sciences*. Springer–Verlag. 453–455.

Turing, A. 1950. Computing machinery and intelligence. *Mind* LIX(236):433–460.