LICENTIATE THESIS

Designing the Online Educational Information Security Laboratories

Sarfraz Iqbal

LULEÅ UNIVERSITY OF TECHNOLOGY

LICENTIATE THESIS 2014

DESIGNING THE ONLINE EDUCATIONAL INFORMATION SECURITY LABORATORIES

Sarfraz Iqbal

Luleå, February 2014

Division of Computer and Systems Science
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
SE - 971 87 LULEÅ
www.ltu.se/org/srt

Printed by Luleå University of Technology, Graphic Production 2014

ISSN 1402-1757
ISBN 978-91-7439-850-2 (print)
ISBN 978-91-7439-851-9 (pdf)

Luleå 2014

www.ltu.se

Abstract

Distance education and e-learning in the field of information security is gaining popularity. In the field of information security education, virtual labs have been suggested to facilitate hands-on learning in distance education. An internet-based information security lab is an artifact which involves a collection of systems and software used for teaching information security, and which is accessible through the Internet. This research is motivated from an on-going information security lab development initiative at Luleå University of Technology. A literature review on the online educational information security laboratories (InfoSec labs) in the academic literature was conducted. The current literature about online InfoSec labs still lacks well-specified pedagogical approaches and concrete design principles. It hinders the accumulation of technically and pedagogically rigorous knowledge for the implementation and use of online educational InfoSec labs. Moreover, the literature focused mainly on details of technical lab implementations whereas the pedagogical elements of the curriculum and rationale behind them were ignored. This leads to inadequate guidance about how the instructor and the learner can make use of the lab to pedagogically align the course objectives, teaching / learning activities and assessment methods.

A theoretical framework comprising the Constructive alignment theory (Biggs 1996) and Conversational Framework (Laurillard 2002) was proposed to further guide the research process and analyze the case of an internet security course and e-learning platform. The framework suggested that the MSc program and individual courses in information security should be developed based on specific pedagogical principles in order to improve the quality of teaching and enhance the e-learning platform for flexible hands-on security education. Therefore, to design an online InfoSec lab to improve flexible hands-on education and security skills development in the courses; Action

design research (ADR) was chosen as the whole approach to continue with this research project. The ultimate goal is to design an ensemble IT artifact as a result of emerging design, use, and refinement in context through continuous interaction between technology and organization during design process. This licentiate thesis is mainly focused on the 1st stage (Problem Formulation) of the ADR method where the trigger for the first stage is the problems perceived in the teaching of information security, i.e., how to improve students' security knowledge, how to provide the students with flexible online educational information security lab.

The review of prior research, observations, interviews with teachers and program management and reflection on pedagogical approaches lead to formalize five initial design principles (Contextualization, Collaboration, Flexibility, Cost-effectiveness and Scalability). These initial design principles have been derived keeping in view the requirements of an information security course in the degree program. A conceptual design for the information security course based on Personalized System Of Instruction (PSI) approach including online InfoSec lab design to promote student's hands-on security knowledge level and to provide them flexibility to study at their desired speed has been proposed. The anatomy of design theory framework by Gregor & Jones (2007) is used for outlining a few first components of a design theory for an online-InfoSec-lab course. In its current form, this study makes a contribution to the literature by identifying and discussing about hitherto scattered research reports of educational online InfoSec labs in a common frame of reference, which will help other developers and researchers of information security pedagogy as an index of previous literature. The theoretical framework will be used to provide further guidelines to develop theory-ingrained artifact which will not only help to provide the necessary justification for elements of curriculum and the rationale behind its selection but also it will help to align the course objectives with teaching / learning activities in a specific teaching context for better hands-on education of information security. The initial design principles suggested in this study will provide help to start the next phase of ADR, Building, Intervention and Evaluation (BIE), which will support us to achieve a refined set of more concrete emergent design principles. The proposed conceptual design of online information security course will be implemented including development, implementation and use of online InfoSec lab. The future research will be focused on IT-dominant BIE (building, intervention and evaluation phases of the ADR method). Further research work after the licentiate phase will cover the rest of the phases of ADR.

Contents

Acknowledgement

The research presented in this thesis was carried out in the division of Computer and Systems Science at the department of Computer Science, Electrical and Space Engineering, Luleå University of Technology (LTU). It has been a very interesting journey so far while I am trying to improve my competence in the research field. My initial work as assistant teacher and research engineer in the division of Computer and Systems science since 2008 gave me the necessary motivation to pursue research in the field of hands-on education in information security. Foremost, I would like to thank my supervisor Prof. Tero Päivärinta whose support and guidance was instrumental in finishing this work. I would also like to thank Ann Hägerfors for giving me the opportunity to work on it in the first place. I would extend my gratitude to my Assistant Supervisor Devinder Thapa, who was very forthcoming with his valuable comments. I would also like to thank all my other colleagues in the research group, past and present, for their support and kindness.

I have travelled all the way from Lahore to Luleå, Sweden (almost in the arctic circle) to pursue my studies. This urge to seek knowledge has stretched distances between me and my near & dear ones (my parents, sisters and my best friend my only brother Aijaz Iqbal) but I feel that this suffering is worth to bear to enhance my capabilities. I also admire the love and support of my wife and kids (Aashir & Hamna) who suffer sometimes due to my busy schedules. In the end, I would like to thank my family for their untiring support, best wishes and prayers over all these years.

Luleå, February 2014

Sarfraz Iqbal

1 INTRODUCTION

This chapter describes the background of the research, the research problem area, research questions, delimitation and the structure of the thesis.

1.1 Background

Information Security is considered as a necessity for all information users (Reid & Niekerk 2013) but as the advancements in the information technology are increasing so as the problems associated with information security are increasing. The role of information security is described (El-Khatib et al 2003) to include user authentication / authorization, protection of private information from unintended access, and protection of data integrity. The organizations worldwide are concerned about the information security due to the high rate of breach of information security (Baker et al, Verizon data breach investigation report 2011).

There is a shortage of approximately 20,000 to 30,000 qualified cyber-security specialists in the US public sector alone despite being one of the best technology related domains (Dale et al 2011). There is always a growing need of skilled workforce to protect the critical information systems of organizations around the world. Researchers (Yurcik & Doss 2001) have pointed out that the duty to provide well-educated and trained graduate students to fight with the cyber threats is on the shoulders of academic institutes. The educational institutes are now broadening the area of distance education, which is also desired by the students as well. Some students still prefer taking courses on campus whereas other students are taking online courses that do not require them to visit campus.

There is a clear trend showing that the percentage of online students is increasing. Yurcik & Doss (2001) are of the opinion that more educational development work is needed to improve information systems security education. An educational curriculum should guide and prepare security professionals to master and acquire ever-changing security solutions (Woodward & Young 2007, paper-A). Therefore, the syllabus of information security needs appropriate pedagogical tools, which support a holistic approach to learning (Yurcik & Doss 2001, Woodward & Young 2007, Yngström & Bjork 1998). In order to prepare a trained information security workforce at an educational institute, the students need to be educated not only theoretically but practically as well. The students should master the hands-on skills in addition to plain theoretical education. However, according to the researchers (Crowley 2003) development of curriculum for information security education is noticed as a rather recent phenomenon. For example, less than a decade ago, the ACM (Association for Computing Machinery) guidelines for computer science – related educations specified no topics, courses, or course sequence for information security topics (paper-A, Hentea et al 2006). On campus, isolated laboratories have been used mostly to conduct hands-on education of information security since the mid-1990s to allow the students to practice attacks and defenses in well-secured server environments (Yurcik & Doss 2001, Woodward & Young 2007). Blended or e-learning approaches have also been considered suitable for end user security education and training (Niekerk & Thomson 2010). The instructors and students can communicate on-line from anywhere in the world using the web-based tools (Khan, B. H 1998).

The on-line learning approach targeted for educating information security professionals (in addition to end-users) has also been regarded desirable in a number of educational institutions (Paper-A). On one hand information security students find it more convenient to take online classes without constraints (expense and time) involved with commuting to a campus facility whereas on the other hand university administrators are seeing the online trend as a major revenue and recruitment tool with less staff and more student policy (ibid, Kosak et al 2004). Online education in the field of information security is gaining popularity as some organizations in the field of information technology place the responsibility of career training in the hands of employees, with the understanding that employees must be able to keep ahead of technological change and perform innovative problem solving (El-Khatib et al 2003). The security landscape keeps changing constantly and therefore, the employees need to retool with latest training (Hentea 2005, Wilson & Hash 2003, Ayyagari & Tyks 2012). According to researchers Ayyagari & Tyks (2012) security education is identified as top Information Technology (IT) required skill that needs to be taught in Information Systems (IS) curriculums. Furthermore, information security is considered among core concepts in information systems education (Ayyagari & Tyks 2012). Thus online education in the field of information security requires that educational institutes provide the distance students of information security with flexible, hands-on skills development environment.

1.2 Problem Area

Educating the information security professionals at University level cannot be considered as a trivial subject (Yurcik & Doss 2001). An information security student at Master's level is supposed to be capable of analyzing security flaws, proposing proper solutions and learning in-depth analytic / experimental techniques (Paper-D). Many educational courses in the field of information security provide little hands-on practice that can be applied to thoroughly securing real world applications from various threats that exist today (Crawford & Hu 2011). Similarly, an online information security program is supposed to include plenty of hands-on exercises but in most cases the lab experiments are often not available to distance students that represent a critical challenge in offering online education in the field of information security (Lahoud & Tang 2006). Therefore, in order to match the benefits with traditional learning environments, a successful e-learning system must be designed and constructed carefully based on pedagogical principles and robust design guidelines (paper-C).

Several key elements need to be considered with regard to an online education system for information security, including the security curriculum and technology needed to deliver the education. Distance learning classes have unique requirements if compared to campus-focused education, and accordingly, the information security curriculum needs to keep up with new teaching methods (paper-A, Hentea et al 2006).

Hence, a vital element of information security curriculum is hands-on laboratory experiences, implemented in information security labs. An internet-based information security lab is an artifact which involves a collection of systems and software used for teaching information security, and which is accessible through the Internet (paper-A). The lab provides the practical experience to students studying topics in cyber security with lab exercises to learn and test their practical knowledge about security vulnerabilities, security testing, and defenses (ibid, Stewart et al 2009). An educational information security lab includes at least four kinds of entities: servers, sources and targets of attacks, and exercises (ibid, McDermott & Fox 1999). The practical exercises are an unavoidable segment of educational curriculum of future information security experts. In a situation where the students are seeking to study from distance in majority compared to on-campus students (see figure 2), it becomes a challenging responsibility for an educational institute to provide the distance students a reliable e-learning platform to practice their hands-on skills using the laboratory resources. The introduction of online InfoSec lab at an early stage in the MSc program will enable the students to get acquainted with the lab resources and in the next courses of information security program they don't need to learn basic things as how to get access to the lab etc.

1.3 Research Questions

Information security is considered among one of the core concepts in information systems education and researchers emphasize to enhance hands-on education and active learning of information security students (Hentea et al 2006, Kroenke 2012, Laudon & Laudon 2010, Ayyagari & Tyks 2012).

Online hands-on education of information security students is a very interesting and important research area and this licentiate thesis seeks answers for the following questions:

- What has been theorized about designing online information security laboratories?
- How to design an online InfoSec lab to improve flexible hands-on education and security skills development in the courses?

1.4 Delimitation

This research work is in the realm of Information Systems (IS) where the focus is not only on the development of an IT artifact (online InfoSec lab) based on pedagogical principles but also how it can be used by instructor / learner in a better way for educational purposes to train the information security students. The researchers assert that theory and theorizing should play a key role in Design Science Research and in this context the theory can be viewed as the link between researchers and different research activities over time (Venable 2006). The theorizing or theory building has been explained as an activity that can take place before, during throughout and at the end as a result of Design Science Research. In this study the anatomy of design theory framework by Gregor & Jones (2007) is used for outlining a few first components of a design theory for an online-InfoSec-lab course. This study has presented the first set of initial design principles as the result of primary investigations for the development of an online educational InfoSec laboratory. This licentiate thesis is mainly focused on the 1st stage (Problem Formulation) of the ADR method. The problem formulation stage draws on two principles (practice-inspired research and theory-ingrained artifact). The conceptual design of an information security course based on online InfoSec lab is presented in the form of a research in progress case and further extension of this study will help to concretize the design principles based on the emergent knowledge through building, intervention and evaluation.

1.5 Structure of the Thesis

The rest of the thesis is structured as follows: Chapter 2 provides an introduction to the research methodology used, as well as data collection and analysis. Chapter 3 offers a summary of the appended papers. Chapter 4 provides discussion about the results. Chapter 5 offers discussion and contribution whereas chapter 6 concludes the thesis and offers some suggestions for future research.

This thesis comprises of an introduction and summary of the following papers:

1.6 List of publications

Paper A:

Iqbal, S., Päivärinta, T. Towards A Design Theory For Educational On-line Information Security Laboratories. In: Popescu, E., Li, Q., Klamma, R., Leung, H., Specht, M. (eds.) ICWL 2012. LNCS, vol. 7558, pp. 295–306. Springer, Heidelberg (2012).

Paper B:

Iqbal, S. Applying The Analytical Lens Of Constructive Alignment and Conversational Framework For Course and E-learning Platform Development. In proceedings of Norsk konferanse for organisasjoners bruk av informasjonsteknologi, NOKOBIT -2013. pp.159-172

Paper C:

Iqbal, S., Thapa, D. Initial Design Principles for an Educational, On-line Information Security Laboratory In J.-F. Wang and R. Lau (Eds.): International Conference on Web-based Learning 2013, LNCS 8167, pp. 89–100. © Springer-Verlag Berlin Heidelberg 2013.

Paper D:

Iqbal, S., Booth, T., Päivärinta, T. Towards Personalized System of Instruction For Educational Online Information Security Lab Exercise: Research In Progress. In proceedings of Norsk konferanse for organisasjoners bruk av informasjonsteknologi, NOKOBIT -2012. pp.133-144

The layout of each individual paper has been revised to fit the layout and formatting of the thesis work, but no changes have been made into the content.

2 METHODOLOGY

This chapter provides overview of the overall research methodology used in this data collection and analysis.

2.1 Action Design Research

My research work is within the field of Information systems. In this field the researcher not only focuses on the IT artifact but also on the confluence of people, organization and technology (Hevner et al 2004). The information systems are considered as social systems where people participate in the construction and interaction with the system during performing different activities. Organizations implement information systems to improve the effectiveness and efficiency of that organization (Hevner et al 2004). The researchers (ibid) further elaborate that capabilities of the information system and characteristics of the organization, its work systems its people, and its development and implementation methodologies together determine the extent to which that purpose is achieved. It is then the researcher in the information systems discipline who not only seeks to further the knowledge that aids in the productive application and management of information technology but also attempts to develop and communicate the knowledge that how the technology should be managed and used in an organization for some specific purposes (ibid).

According to the researchers (Hevner et al 2004, March and Smith 1995) Design research (DR) helps in the development of design knowledge by construction and evaluation of IT artifacts with the purpose to solve an identified class of problems. The Information Systems community has debated Design Science Research methods a lot regarding outcome and research process in guiding the Design Science Research projects aimed at developing scientific knowledge about artificial artifacts or processes as well as attempting to provide appropriate practical solutions to organizations (Harnesk & Thapa 2013).

According to the framework (Harnesk & Thapa 2013) two common design research approaches have been discussed after considering the work related to Design Science, Action Design Research, Action Research, Dialogical Action Research and Engaged Scholarship (Harnesk & Thapa 2013, Hevner et al, 2004, Sein et al 2011, Van de Ven 2007, Baskerville & Wood-Harper 1998, Mårtensson & Lee 2004)

1. When design research typically proceeds along a priori defined software engineering approach which comprises a set of activities to solve a known problem and
2. When design research deals with a mixture of technical and organizational properties that dynamically and iteratively emerge from design, use, and on-going refinement in context.

A classification framework has been proposed (Harnesk & Thapa 2013) which provides different perspectives on design research process by making use of traditional two-dimensional typology diagram (type-1 Deductive – a priori, type-II Abductive – a priori, type-III Abductive - Emergent, type-IV Deductive – Emergent).

The type-III Abductive – Emergent design research methods seem appropriate for my research project where the goal is to conceptualize an ensemble IT artifact as a result of emergent perspective on design, use, and refinement in context through continuous interaction between technology and organization during design process. The type III design research methods provide continuous stakeholders / client’s contextual participation in the project which helps the researcher to obtain a broad variety of requirements. This framework provides insight to select ADR (Action Design Research) as a research method for this design research project.

Action design research (ADR) has been proposed as a new design research method to address the problems in this field (Sein et al 2011). Action design research mainly deals with two challenges as follows:

a. Addressing a problem situation encountered in a specific organizational setting by intervening and evaluating.

b. Constructing and evaluating an IT artifact that addresses the class of problems typified by the encountered situation.

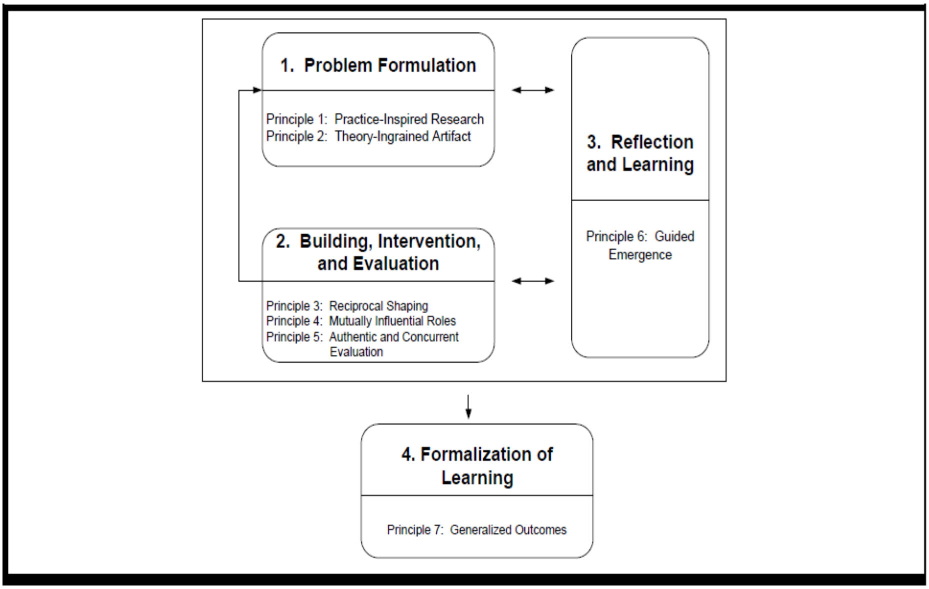

1. Problem Formulation
Principle 1: Practice-Inspired Research
Principle 2: Theory-Ingrained Artifact
2. Building, Intervention, and Evaluation
Principle 3: Reciprocal Shaping
Principle 4: Mutually Influential Roles
Principle 5: Authentic and Concurrent Evaluation
3. Reflection and Learning
Principle 6: Guided Emergence
4. Formalization of Learning
Principle 7: Generalized Outcomes

Figure 1: ADR method: stages and principles (Sein et al 2011)

This licentiate thesis is mainly focused on the 1st stage (Problem Formulation) of ADR method (Sein et al 2011) where the trigger for the first stage is the problems perceived in the teaching of MSc program of information security i.e. how to improve students security knowledge, how to provide the students with flexible online educational information security lab which can help them to learn and practice security skills from distance freely without the time and place constraints, and to improve the throughput in different courses. In this research following activities have been performed in order to collect data for the problem formulation stage:

- Literature review
- Perusal of University's documents related to vision and strategy
- Interviews with teaching staff and management
- Case analysis of an internet security course

The above-mentioned activities have been conducted in light of the suggestions (Sein et al 2011) that the input for problem formulation can come from practitioners, end users, the researchers, existing technologies and or review of prior research. Furthermore, the initial empirical investigation which in this case has been performed through case analysis of an internet security course, initial interviews with teaching staff and management and through survey questionnaire with students (end users of the lab) helped to determine the initial scope of the lab for practitioner participation and deciding roles of the ADR team. The problem formulation stage draws on two principles; practice-inspired research and theory-ingrained artifact.

Practice-Inspired Research. This principle highlights viewing the field problems (such as low hands-on exercises, absence of productive media, flexible e-learning system, absence of pedagogical approaches in teaching of information security, low throughput and mastery of course topics) as knowledge creation opportunities. ADR seeks these opportunities at the intersection of technological and organizational domains. For instance, in this case the technical design and development of online information security lab will not only provide the students opportunity to conduct exercises from distance but also issues of personal flexibility and student & teachers efficacy require equal importance and attention for systematic development (paper-D).

Theory-Ingrained Artifact. This principle emphasizes that the ensemble artifacts created and evaluated via ADR are informed by theories. To concur to this stance, an analytical framework consisting of Anatomy of design theory (Gregor & Jones 2007) was used for literature review (paper-A). Moreover, a theoretical framework (paper-B) consisting of Constructive alignment theory (Biggs 1996) and Conversational framework (Laurillard 2002) was proposed for case analysis of Internet Security course. Furthermore, Personalized system of Instruction approach (Keller 1968) has been used as a kernel theory in paper-C & paper-D to support initial design principles and to propose a conceptual design of an online educational information security lab for an information security course.

2.2 Literature Review and Analysis

Google Scholar was used as a major tool for the literature search by using key words such as “information security laboratory”, “information security lab”, “virtual information security lab”, “information security curriculum”, “information security education”, “information security course” and “information security pedagogy” in the article title. These terms generated a lot of results. Keeping in view the relevance to research area a total of 181 articles were selected for further inspection. All the articles were examined one by one and 13 relevant articles (paper-A) were sorted which specifically discuss information about the security lab concept in an on-line context. The articles discussing the campus-located, isolated laboratory concepts, as well as purely curriculum-related discussions without a lab were omitted.

The research focused on design knowledge with regard to the development of online information security laboratories, and on how related knowledge was captured and communicated to the community researchers and educators of information security. It was assumed that it's beneficial to examine the existing knowledge of on-line information security labs in light of the "anatomy of design theory" (Gregor & Jones 2007), in order to summarize what is currently known about designs and experiences from previous on-line labs. The design theory based framework (table-1) helped to reveal gaps in the existing knowledge in terms of a common framework. In general, we share Hrastinski's justification for such research in the field of e-learning, according to which "the rationale of developing design theory for e-learning is that such theory can support practitioners to understand which mechanisms that may lead to desired outcomes" (Hrastinski et al 2010). Table 1 summarizes the design-theory-based framework used to define the questions that guided the literature analysis (paper-A).

Design theory issues (Gregor & Jones 2007)	**Issues to analyze from the literature concerning on-line information security labs.**
Purpose and scope of interesting designs	Any academic article, which discusses about the implementation of an on-line information security lab was considered relevant for our review.
Constructs	• Technological challenges to implement the laboratory (servers, sources, targets (McDermott & Fox 1999))? • Designs of exercises (McDermott & Fox 1999)?
Principles of Form and Function	• Technological requirements and solutions available for labs? • Elements of curriculum and their rationale? • "Best practices" suggested for collaboration through the lab and on-line communication tools?

	• How do all these relate together, if that has been studied at all?
Artifact mutability	• Description and suggestions for improving the current methods of utilizing lab facilities for distance education? • Lab utility claims?
Testable propositions	• Measures for improvements and utility used for evaluating the existing labs in the literature, if any? • Claims for lab design adaptability for other organizations? • Are any design exemplars (Hrastinski et al 2010) proposed?
Justificatory knowledge	• Do the improvement statements relate to any given theory / theories? (Kernel theories from social sciences governing the design process to provide the foundation knowledge on which other aspects of the ISDT are built (Jones & Gregor 2004, Walls et al 1992) (Or is knowledge still in the form of technical/practical "lessons learned", or even in the form of contextual suggestions only)
Principles of implementation	• Implementation guidelines observed for the servers, sources and targets, exercises?
Expository instantiation	• Where and how has the lab in question been implemented? (Conceptual idea, prototype, system in production – how long it has been in use?)

Table 1. A design theory analysis framework for literature review (paper-A)

The analysis of the articles selected for this study suggests that many articles lacked a clear purpose and scope aiming simply to improve student's access to university resources. The reviewed academic reports were not referring to each other in most cases, such an approach to report IT artifacts is in contrast to the design theory approach of research. None of the article presented a full fledge design theory for the design and development of online information security laboratories. The reviewed articles demonstrated little, if at all, how are these lab ideas connected with the course and program goals. The fundamental issues of elements of curriculum and the supporting rationale behind it were also ignored which clearly revealed a knowledge gap that how are the practical lab activities aligned with the rest of the course content and objectives. Only one article referred to cooperative learning strategy, whereas the rest of articles did not provide any such kernel theory, which could be further used to shed light on the designed labs assessment in a larger context of knowledge claims. Testable design exemplars for online InfoSec labs were absent and only two articles made utility claims for the labs, which provide remote access to students. Hence, it was unclear which approaches would be superior for which particular purposes and whether knowledge and any guidelines for implementation of online InfoSec labs yet would involve any verifiable components. Overall, the review shows that disciplinary literature of online hands-on education of information security is still in its early stages of development (paper-A).

2.3 Case Organization

The case of Msc in information security program offered at department of Computer Science, Electrical and Space Engineering at Luleå University of Technology is considered to proceed with this study in order to illustrate the systematic process of building and implementing information security laboratory (InfoSec lab). The University is situated in Luleå, Sweden.

The department lately noticed an increase in the number of distance students who want to study Msc in information security (see figure-2). Most of the distance students are professionals who also want to work and practice their study individually at times and in places which suit them.

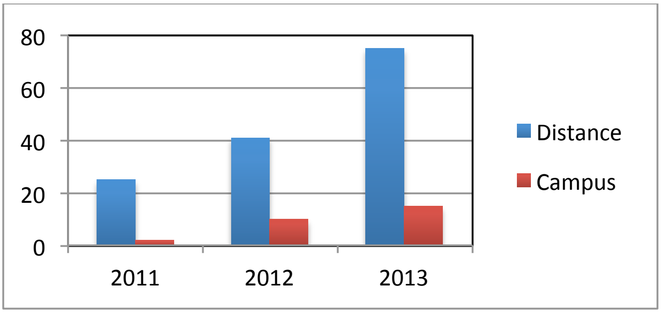


Figure-2 Student history chart showing distance and on-campus students

Different perspectives of e-learning on various levels of analysis has been discussed (paper-B), which include course, institute and society level. As suggested in paper-B the department of Computer Science, Electrical and

Space Engineering should focus on our e-learning environment at course level, which includes following four perspectives:

- Pedagogy with learning theories and models (learning process, learning content, learning outcomes, learning models)
- Community and social relations with learning related social theories and models (groups with relations between and within learners, teachers, technologists, ICT related artifacts, and other learning supportive environment)
- Organization and the overall management with learning related organization theories and models (organization and management of the course by learners, teachers and technologists)
- Information and communication technology in relation to learning (ICT related learning environment with hardware, software, platforms, technical standards and human ICT skills enabling and constraining learning).

The fundamental notion in this study is to improve different courses of MSc program of information security to promote hands-on education of information security through pedagogical improvements both in teaching and development and use of technology. The unit of analysis is the individual courses and how the e-learning platform is being used for teaching / learning activities and communication.

2.4 Empirical Data Collection and Analysis

Empirical data was collected using different sources such as interviews, course analysis and documents related to the vision and strategy of Luleå university of Technology. The university stated in its vision and strategy of 2020, “Our programs are conducted on the campus and as distance courses, and we work for flexible learning that makes use of modern technologies. Independent, active learning that challenges every individual’s capacity to meet the future.”

As a process of program improvement in the department of Computer Science, Electrical and Space Engineering and also to fulfill educational objectives in the light of University’s vision and strategy statement for 2020, the researcher planned interviews with all the staff members (teachers) involved in teaching different courses in Msc information security program and the program management (to obtain the organizational perspective). The researcher conducted semi-structured open-ended interviews (Leedy & Ormrod 2005) with the teachers and the management to gather details about their teaching experience in the field of information security as well as focusing on the practical needs of the degree program. The interviews included discussions on issues such as:

- Instructional strategy, or tactics for teaching
- Need of any specific pedagogical approaches for teaching InfoSec courses
- Major challenges related to teaching courses in InfoSec education program
- Use of any lab for hands on education in information security
- Practical demands of the Information security degree program
- Challenges related to practical needs of the program
- Suggestions for the program improvement

In total 8 staff members were interviewed individually. The researcher provided an overview of the background of the research to interviewees and handed over the interview guide to the interviewees beforehand. The interviews lasted between 25-35 minutes. The interviews were recorded after seeking permission from all the interviewees and ensuring them that the data will solely be used for research purpose at the department of Computer Science, Electrical and Space Engineering. Although some participants can become shy or cautious due to recording which could hinder the interviewee to reveal confidential information. A good reason to record the interviews is that in comparison to note taking, if the researcher is recording the interviews he/she can focus more on the interview process to make discussion meaningful (Miles & Huberman 1994, Blaxter et al 1996).

The interviews were transcribed afterwards for the purpose of analysis. As the researcher is also an employee at the same department, it was of extreme importance to not influence any interviewee or to promote researchers own ideas. To adhere to this stance the researcher avoided any direct input into the interviewee’s answers during interview process and encouraged them to speak to share their own personal experience. The researcher tried to stay neutral (Leedy & Ormrod 2005) and let the discussion flow smoothly making the interviewees comfortable.

The empirical data was also collected through analysis of the case of an “Internet Security” course in the degree program of Information Security (Iqbal 2013). The theoretical framework comprising Constructive alignment theory (Biggs 1996) and Conversational framework (2002) was used for case analysis focusing on the alignment of pedagogical approach used in the course and the e-learning platform. The feedback from the students was obtained through a survey questionnaire (paper-B). The survey was answered by 58 students (ibid).

3 SUMMARY OF APPENDED PAPERS

This chapter presents the summary of the attached papers. A brief summary of the research objectives, main results and the contribution for the licentiate candidate is given as well as the publication details for each article.

3.1 Paper A

Iqbal, S., Päivärinta, T. Towards A Design Theory For Educational On-line Information Security Laboratories. In: Popescu, E., Li, Q., Klamma, R., Leung, H., Specht, M. (eds.) ICWL 2012. LNCS, vol. 7558, pp. 295–306. Springer, Heidelberg (2012).

The aim of this paper was to provide an overview on reported instances of online hands-on education in information security. Web-based instruction allows students and instructors to communicate on-line with providers of resources from all over the world. The importance of providing online hands-on education to students participating in degree programs from distance to learn and master information security skills cannot be ignored. We aimed to integrate the existing knowledge by using the "anatomy of design theory" framework as a basis for the literature analysis. The framework provided a common basis for looking at what has been "theorized" with regard to human-created information technology artifacts such as security labs.

The analysis is based on the anatomy of design theory framework including purpose and scope of laboratory designs, key constructs used for conceptualizing the laboratory implementations, principles of form and function, artifact mutability claims, testable design propositions, justificatory knowledge, principles of implementation, and examples of laboratory instantiations.

The study shows that disciplinary literature on on-line education of information security is in its infancy. The reviewed academic reports seldom referred to each other. Rather, the articles mostly simply presented each laboratory idea as such. Such an approach to reporting IT artifacts is in contrast to the design theory approach of research. The paper suggested that in order to make knowledge of online security labs more cumulative and comparable, the literature should focus more systematically on the design theory viewpoint, with regard to which the framework we used for the literature review gives a starting point.

The main conclusion was that the contemporary literature on the topic is relatively scattered and that there is a need for more systematically formed design theories through which the academia and developers of security laboratories could enhance knowledge sharing and accumulation.

Licentiate candidate’s contribution: My responsibility was to collect the literature and conduct the review. My co-author helped introducing the analytical framework based on anatomy of design theory and to finalize the analysis and discussion.

3.2 Paper B

Iqbal, S. Applying The Analytical Lens Of Constructive Alignment and Conversational Framework For Course and E-learning Platform Development. In proceedings of Norsk konferanse for organisasjoners bruk av informasjonsteknologi, NOKOBIT -2013. pp.159-172

The aim of the paper was to conduct an assessment of educational needs for course and e-learning platform development to teach an online MSc program in information security. In order to improve the quality of teaching and to enhance the e-learning platform based on pedagogical principles, the analytical lens of Constructive alignment theory and Conversational framework was used to examine the case of Internet Security course as well as to evaluate current e-learning platform employed both for distance and campus studies. The theoretical framework based on constructive alignment theory and conversational framework has been used to guide our on-going research process for improvement in our courses as well as for the development and improvement of our e-learning platform. Both the Constructive alignment theory and conversational framework have their pros and cons e.g. constructive alignment presents a holistic view of course development which guides the Instructional designer from stating the course objectives to properly align the course objectives with intended teaching / learning activities and suitable assessment methods whereas it doesn't provide any specific guidelines for the media to be used for communication and interaction between teachers and students in the classroom. The Conversational framework on the other hand discusses in detail about the media types to be used during teaching. The theoretical framework not only helped to understand the categorization of media based on its intended usage in the course such as Fronter (learning management system) has been categorized as interactive whereas Adobe connect (virtual classroom) has been categorized as communicative media for instruction but also pointed out that productive media (such as online InfoSec lab) is missing that can be used for security skills development of students.

The study revealed practical and theoretical problems related to the pedagogical development of the course such as low hands-on education, low flexibility in teaching / learning activities, absence of pedagogical approaches in teaching. The final results of Internet security course also pointed out that procrastination and low throughput is a major challenge for the teachers. The lack of an online information security laboratory also hindered the students to practice their security skills. This situation places the responsibility on the shoulders of the program management and teachers to provide required facilities and infrastructure both for on-campus and distance learning. The study suggests that the management needs to focus on updating and maintenance of e-learning platform in order to provide standardized services for all the distance students.

The main conclusion was that we need to develop the program in information security based on explicit pedagogical approaches to enhance the quality of teaching. Furthermore, an online InfoSec laboratory should be developed on pedagogical principles in order to improve hands-on security skills of students and to align the lab activities with the overall course objectives. In this way we can argue for the benefits of the learning technology being developed for a specific purpose.

3.3 Paper C

Iqbal, S., Thapa, D. Initial Design Principles for an Educational, On-line Information Security Laboratory In J.-F. Wang and R. Lau (Eds.): International Conference on Web-based Learning 2013, LNCS 8167, pp. 89–100. © Springer-Verlag Berlin Heidelberg 2013.

The aim of the article was to promote research based hands-on teaching in the field of information security which will not only benefit the university to have an experienced research based group of teaching staff members but also will help the academic community by continuously adding new information based on educational experiments and experiences with online InfoSec labs. The article proposes initial design principles to design, develop, implement, and test e-Learning platform for information security. E-learning must be rooted in systematic pedagogical approaches in order to make it successful. Furthermore, the importance of creating a link between theory and practice in order to design and develop an instructional system is also emphasized. Keeping in view the strategic objectives and practical demands of the future related to provision of hands-on exercises in different courses in InfoSec program a road map in the form of initial design principles to develop a security lab is proposed. The paper used an example of InfoSec lab to explain the systematic process of the laboratory building, intervention, and evaluation.

A DSR based framework was implied which shows that the technological, pedagogical, and organizational goals interact during design of e-learning platform (online InfoSec lab). The platform in this context is conceptualized as an ensemble IT artifact, because the design outcome is a result of emergent perspective on design, use, and refinement in the actual context. The literature review, observations, interviews with teachers and program management and reflection on the pedagogical approach i.e. Personalized System of Instruction (PSI) to design and develop an online InfoSec lab lead to formalize five initial design principles (Contextualization, Collaboration, Flexibility, Cost-effectiveness, Scalability). These initial design principles will help to collect the necessary information related to the contextual factors such as organizational goals and course goals, practical exercise requirements that in turn are useful to pedagogically align the lab activities with the overall course objectives. Furthermore, the collaboration among the ADR team (including researcher, practitioner, end users) will be enhanced which is important in terms of good input to shape the ensemble artifact. These initial design principles will guide the research process that will ultimately help us to achieve a refined set of emergent design principles. The flexibility based on PSI approach refers to the remote access to lab resources, for instance lab should be accessible for experiments from everywhere any time in order to facilitate the students who are professional, want to work individually and cannot work under a strict schedule (go at your own pace). The principle of Cost-effectiveness refers to the availability of resources, such as fund, technology, and human skills. The existing solutions, such as virtualization technologies can be utilized to make the lab more cost-effective. The scalability depends on factors such as need to extend the lab resources if more students than expected appear in a course, lab up-gradation based on introduction of a new and better technology etc. To accommodate this influx of the student, scalability of the lab facility should be considered while building, intervention and evaluation of the lab.

Licentiate candidate's contribution: My responsibility was to conduct interviews, review the vision and strategy documents of University, analyse data, introducing the PSI approach, my co-author helped in analysis and finalizing initial design principles.

3.4 Paper D

Iqbal, S., Booth, T., Päivärinta, T. Towards Personalized System of Instruction For Educational Online Information Security Lab Exercise: Research In Progress. In proceedings of Norsk konferanse for organisasjoners bruk av informasjonsteknologi, NOKOBIT -2012. pp.133-144.

The aim of the article was to present a PSI-based design of an online information security course, including on-line laboratory, for individual students based on Keller's PSI approach. An information security student at Master's level is supposed to be capable of analysing security flaws, proposing proper solutions, and learning in-depth analytic / experimental techniques. An online lab will allow the distance (as well as the campus) students to perform related hands-on security lab exercises. A variety of pedagogical strategies can be used to develop online laboratories for information security. On the one hand, a cooperative learning strategy for information security classes has been suggested. On the other hand, a good number of the distance students may want to study individually and flexibly. The Personalized System of Instruction

(PSI) is a pedagogical approach, which could help to develop such individual and flexible learning environments.

IT research should develop understanding of how and why IT systems work and do not work so that research in IT could address the design tasks faced by practitioners. In our case the researchers and practitioners thus would benefit from the design theory framework for the design and development of online InfoSec lab aimed at educating students of information security field. The aim of IS design science research is to build practical knowledge for the design and realization of different classes of IS initiatives. Researchers emphasized on the importance of design and development of information system design theories, which could be helpful for the researchers and practitioners in the process of designing products and processes.

The PSI approach which we adopted as the theoretical basis for design will contribute to information security education by providing Graduate level students the path towards in-depth learning (mastery of study topics), giving them the opportunity to work flexibly (go at your own pace), as most of the distance students are professionals, who need a relaxed schedule to study.

The main conclusion was that the lack of systematic research on online InfoSec labs development prompted us to propose a design theory of online InfoSec lab (comprising of purpose and scope of design, constructs, principles of form and function, artifact mutability, testable propositions, justificatory knowledge, principles of implementation and expository instantiation) based on the PSI approach (kernel theory in this particular context), which should be considered as a first step towards accumulation of knowledge in this field. This paper starts to fill this gap by outlining a design theory, and evaluation measures built upon a solid theoretical ground.

Licentiate candidate’s contribution: My responsibility was to prepare whole conceptual design using the anatomy of design theory framework for an online information security course including an online InfoSec lab. My co-authors helped in finalizing the technical details related to lab infrastructure and course design.

4 RESULTS

This chapter provides findings from the literature review, interviews and course analysis in the result section and offers discussion of the research in the next section that is reported in detail in the appended papers.

4.1 Summary Of Results

In order to find the answer for the first research question "What has been theorized about designing online information security laboratories" a literature review was conducted. The articles selected for literature review (paper-A) were initially analysed against the following four important entities of an information Security laboratory:

- Servers
- Source
- Targets
- Exercises

The findings (paper-A) show that most of the articles do not provide discussions about important entities of an InfoSec lab and how these entities interact with each other to activate the learning scenario to achieve specific course and program objectives. Only four articles discussed about above-mentioned entities at a general level not providing detailed descriptions of actual design and implementations. Furthermore, when the articles selected for review were analysed in light of the design theory framework (Gregor & Jones 2007), it was revealed that disciplinary literature regarding online hands-on education of information security professionals is still scattered and is in its infancy. The articles studied for this research (paper-A) neglected to promote a systematic effort towards theory development of an IT artifact as desired in the Information Systems field (Walls et al 1992, Gregor & Jones 2007, Hirschheim, R. & Klein, H. K. 2012). Pedagogical and technological challenges related to the development and use of the InfoSec labs also require specific attention from the research community.

Only one article among all the articles reviewed for this study mentioned about using a pedagogical approach for exercises, which reveals general absence of pedagogical approaches to design and develop online InfoSec labs and related exercises. The review shows that there is a lack of systematic approach in design, development, implementation, and evaluation of InfoSec lab. Likewise, none of the articles studied provided any details of lab development that is based on design science (paper-A, Gregor & Jones 2007).

- The review shows the gap of knowledge in the field of design and development of online InfoSec labs. None of the articles studied for review purpose demonstrated any explicitly described design principles based on a specific design research method (paper-C).
- The review also demonstrates the lack of any pedagogical model, learning theory and scientific method trailed for the design and development of online InfoSec laboratories (ibid).
- The literature does not provide the knowledge how can we use the online information security laboratory as a “productive” learning technology (Laurillard 2002), which is pedagogically aligned with the whole program. The description of relationship between different entities of the online InfoSec lab is vague and somewhat missing, which prevents the instructors and developers to understand how can they make use of the lab for practical exercises.
- The absence of design exemplars proposed for the design, development and use of the online information security labs hinders the contextual information to be conveyed to the practitioners about how and when to manage and use a specific design.
- The articles studied for this research do not reflect properly how the designed labs have been evaluated/validated through specific evaluation methods.

- The elements of Curriculum and rationale behind it to design particular lab exercises and how these are aligned with overall course goals are ignored largely.

The results of the interviews with teaching staff, student survey and case analysis of an Internet security course at Luleå University of Technology revealed following specifics:

- General absence of explicit pedagogical approaches in teaching of information security
- The students were unable to practice their security skills using lab environment.
- There was a gap between the theoretical and practical aspects of the program as the program focused more on the theoretical aspects while not focusing on practical skills at large.
- The current learning technology comprising of Fronter (Learning management system) and Adobe Connect Pro (Virtual classroom) has been used merely as a knowledge-transmitting tool.

There was no productive media (information security laboratory for hands-on education of graduate students) available to refine student's creative security skills.

4.2 Problem Formulation

In order to answer the second research question "How to design an online InfoSec lab to improve flexible hands-on education and security skills development in the courses" the results from literature review, interviews with the program management committee, analysis of an internet security course of Msc program in information security, student feedback and reflection on the pedagogical approaches was considered to proceed with the problem formulation phase. The empirical inputs from all these sources lead towards the development of a conceptual plan for the online InfoSec lab to improve flexible hands-on education and security skills development in the information security course.

The organizational study shows that currently there is no information security laboratory available for students where they can practice their security skills. A campus-based laboratory will restrict the distance students who are in majority compared to on-campus students (see figure-2). The overall goal of the Graduate program is to prepare the students to be "Security managers and Security Engineers". But due to the absence of information security laboratory students are not able to conduct activities such as, installing and configuring firewalls, applying cryptography methods to protect sensitive data, working in teams to develop attack and defence techniques which are considered very important from a security engineering perspective. Keeping in view the educational requirements of the University to offer an MSc program in information security, the study suggests (figure- 3) that in a higher educational institute the educational environment is governed by the educational vision and strategy (paper-b).

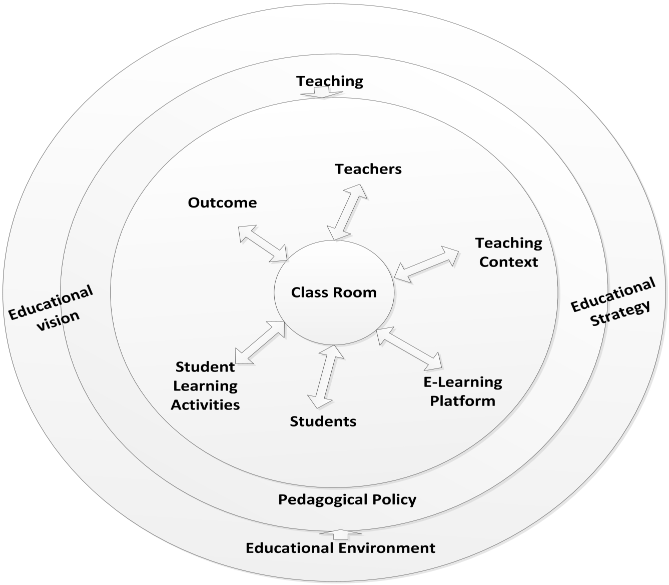


Figure – 3 Educational environment of classroom teaching (paper-B)

The findings (paper-B) suggest that in order to improve the quality of teaching and enhance the e-learning platform, the MSc program in information security should be developed systematically based on specific pedagogical principles. The department of Computer Science, Electrical and Space Engineering should try to formulate its specific departmental pedagogical policy in the light of institutional vision and strategy, which is influenced by several factors such as type of education, mode of education delivery, learning platform requirements etc. The findings (ibid) also portray (figure-3) that in an educational environment the teaching and learning (at classroom level) should be based on a specific pedagogical policy, which is grounded on pedagogical approaches. Different pedagogical approaches could be used in different courses in the degree program based on the overall aim of that program. Every single study course / unit included in the program serves a specific purpose to achieve that specified aim / goal of the program (ibid).

Two levels of pedagogical development are depicted (figure- 3) such as:

- Pedagogical policy at program level
- Pedagogical approach at course level

The decisions regarding the type of e-learning platform to deliver education to students should be made at the program level (ibid). The scholars (Biggs 1996) suggest that in order to improve teaching in an education system, the system as a whole should be subjected to the efforts of improvement and it should not be limited to merely adding "good components" in the form of a new curriculum or method. Hence, in the case under discussion, the university offers an MSc program to both on-campus and distance students at the same time. It requires considering the enhancement of overall e-learning platform for pedagogical improvements. For instance, the pedagogical policy in the department of Computer Science, Electrical and Space Engineering is that the department wants to promote flexible learning. Furthermore, the department also desires to provide flexible hands-on security education to its distance students in order to improve their knowledge level. In light of this pedagogical policy following action plan (paper-C) has been set forth:

- To develop an effective and meaningful e-learning program for the distance as well as campus students.
- To introduce an online InfoSec lab for the students where they can practice their security skills flexibly from distance according to the practical demands of the Course.

The analysis (paper-B) of the current e-leanring platform comprising of Fronter (Learning management system), Wiki, and Virtual Classroom (Adobe Connect

Pro) revealed that the teachers and students make use of Fronter, which is an official tool at Luleå University for different types of interactions such as teacher vs student and also between students' vs students. The teachers mostly use Fronter for delivering:

- Course information
- Course material
- Course assignments
- Comments on assignments
- Maintenance of student portfolio

Whereas the students also make use of the Fronter in different ways:

- Submitting assignments
- Reading comments
- Accessing / downloading course materials

Some teachers also use Wiki instead of Fronter to conduct some of the tasks mentioned above. A chat function is also available in the Fronter course room, which can be utilized for chat between teacher and student etc. The virtual classroom (Adobe Connect Pro) is generally used for:

- Live classes
- Video conferencing
- Project presentations
- Online exams

With the addition of an online InfoSec lab the e-learning platform at Luleå University of Technology, categorized according to the Conversational framework (Laurillard 2002) will appear like this (see table-2):

Learning Management System (Fronter), Wiki	Interactive
Virtual Classroom (Adobe Connect Pro)	Communicative
Online InfoSec Lab	Productive

Table 2. Proposed e-learning platform at Luleå University (paper-B)

The students will be able to conduct individual as well as collaborative tasks using the online InfoSec lab as productive media to practice and implement security solutions studied theoretically. The lab can be used for various purposes and it will facilitate the students to work together and collaborate with each other in the decision-making process concerning different tasks over the network. Lab can be used to prepare a conceptual system against a real world system (paper-B). I adhere to Scholars (Laurillard 2002, Hannafin 2005) that in order to truly benefit from the potential of the technology to serve a different kind of learning an academic community requires a teaching approach that turns academics themselves into reflective practitioners with respect to their teaching instead of just clinging only to what they already know (ibid). This approach stresses that the university teachers must renew and develop their model of the learning process well beyond the traditional transmission model which in turn will shape their teaching, as the new technology requires, as the knowledge industry requires, and as students demand. This approach pushes the academics to become researchers in teaching (long term strategic goal of Luleå University of Technology as part of the vision 2020). Furthermore, this approach will promote the formation of a community that develops a range of designs within which practitioners can craft a variety of contents (ibid).

4.3 Framework For Development Of E-Learning Platform

Design Science research has been used to develop e-learning platforms (paper-C), such as Cybernetic e-Learning management model applied to a (case study of BMW group) (Hilgarth 2011), Business Process Management e-learning program (Kröckel & Hilgarth 2011), user defined and controlled virtual learning environment (Thomas et al 2009), and Synchronous e-learning (Hrastinski et al 2010). Moreover, a framework for the blended learning design arrangements was proposed with a focus on identifying the right blend for the communication component in the context of a distance education program considering expenditures (Kerres & Witt 2003).

However, these frameworks cannot be generalized based on the fact that different stakeholders evaluate communication tools and scenarios differently (Paper-c). Tel and Thomas (2008), analysed technology as a process and as a value-laden system arguing that design-based research can address some of the deficiencies of other research methods in investigating the role of tools and techniques in the classroom to impact educational practice (ibid). This research adheres to the similar stance where general absence of methodically designed online InfoSec labs is evident (ibid).

The literature study showed that in the past the technical implementation of labs was mostly focused in the literature, whereas, the pedagogical elements of the curriculum and rationale behind them were ignored (Paper-A & Paper-B). This situation leads to inadequate guidance about how the instructor and the learner can make use of the platform (ibid). Hence, pondering on the theoretical underpinnings discussed above and keeping in view the strategic objectives and practical demands of the future related to provision of hands-on exercises in different courses in Msc program of information security, a road map in the form of following framework is proposed (see Figure–4) to proceed with this study to develop an Online InfoSec lab.

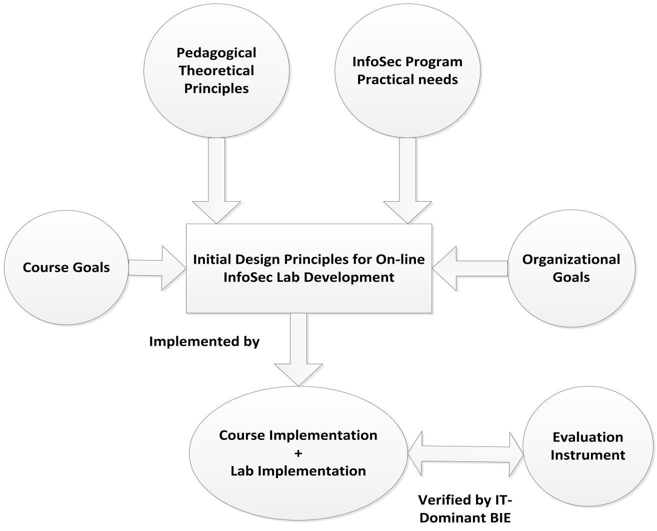

Pedagogical Theoretical Principles
InfoSec Program Practical needs
Course Goals
Initial Design Principles for On-line InfoSec Lab Development
Organizational Goals
Implemented by
Course Implementation + Lab Implementation
Evaluation Instrument
Verified by IT-Dominant BIE

Figure-4 DSR based framework for development of e-Learning platform (paper-C)

The framework (figure-4) portrays that during the design of e-learning platform (online InfoSec lab) the technological, pedagogical, and organizational goals interact with each other (paper-C). The platform in this context is conceptualized as an ensemble IT artifact (Orlikowski 1996), because the design outcome is a result of emergent perspective on design, use, and refinement in the actual context. Hence, considering the emergent nature of e-learning platform (Harnesk & Thapa 2013) the framework proposes employing Action Design Research (ADR) method (Sein et al 2011) for laying the roadmap. ADR is a design research method, which represents the view of continuous stakeholder participation in the research project (ibid). Instantaneously, different stakeholders examine the propositions iteratively together with researchers to define and redefine options for the design (paper-C).

The framework portrays that when the contextual issues are clarified, the resulting initial design principles will guide the initial development of lab based on problem framing and theoretical premises adopted in stage one. For instance, practical needs of information security program, course goals, organizational goals and the pedagogical principles laid down based on a kernel theory will inform the initial design theoretically (ibid). In the next phase of the ADR process, to continue with the Building, Intervention and Evaluation (BIE), there are two different types of BIE processes identified in ADR (a) IT-dominant BIE, (b) Organization dominant BIE (Sein et al 2011, ibid). The IT-Dominant BIE process supports the continuous instantiation and testing of emerging artifact as well as the theories ingrained in it via organizational intervention subject to the assumptions, expectations and knowledge of the participating members.

Therefore, in this context, the framework suggests the IT-Dominant BIE process (ibid) for online information security lab development. The online InfoSec lab is supposed to be implemented in different courses for some specific exercises, which could be based on a variety of pedagogical approaches in order to achieve pre-defined course objectives via testable propositions (ibid, Gregor & Jones 2007). According to the researchers, (Checkland & Scholes 1990, Walls et al 1992, March & Smith 1995, Hevner et al 2004, Hilgarth 2011, Venable et al 2012) Design Science Research projects should establish a clear evaluation strategy via an evaluation component of their Design Science Research that will explain the questions of what to evaluate, when to evaluate and how to evaluate. Evaluation is considered as a crucial and significant part of the research process (Hevner et al 2004, Pries-Heje et al 2008) that plays central role in conducting rigorous Design Science Research. To concur to this stance, the framework portrays that an evaluation instrument will be designed in order to evaluate the implemented design (paper-C).

The evaluation strategy in aforementioned project should be based on the following two purposes in order to evaluate product artifact (online InfoSec lab) and relevant process artifact (methods, procedure to accomplish some tasks) (ibid):

- Evaluate a designed artifact formatively to identify weaknesses and areas of improvement for an artifact under development.

- Evaluate an instantiation of a designed artifact to establish its utility and efficacy (or lack thereof) for achieving its stated purpose.

4.4 Initial Design Principles

The interviews, observations, literature reviews, and reflection on the pedagogical approach i.e. PSI. Consequently, helped to derive five design principles (see table 3), where, principle 1 and 2 along-with ADR principles provide guidelines for the design and development (research process) of the InfoSec lab, and, principle 3, 4 and 5 are the principles of InfoSec lab itself (paper-C) that help to derive attributes for the lab. The design principles are discussed as follows.

Design Principles	Definitions
Contextualization	Organizational Goals, course goals, Teacher goals, constraints, requirements
Collaboration	Researcher (acts as Instructional designer), Practitioners (Developer, IT staff) End users (Teachers, proctor, Students)
Flexibility	Remote access to lab resources Lab Should be accessible to students 24x7.
Cost-effectiveness	Optimal resource allocation for lab development.
Scalability	Lab can be upgraded and easily modified based on practical requirements of different courses.

Table 3. Initial design principles for online-lab development (paper-C)

This study is motivated by an ongoing initiative to design and develop an online InfoSec lab and aims to address the contextual needs of MSc information security program. Keeping in view the challenges related to design, development and use of an online InfoSec lab a road map in the form of a framework was suggested (see figure-4). The findings proposed that e-learning in information security should be based on a theory-into-practice framework as developing such a model for e-learning purposes emphasizes on the interaction between pedagogical models, instructional strategies and learning technologies to facilitate meaningful learning and knowledge development (paper-C).

In order to contribute to this argument the review of the prior research, observations, interviews with teachers and program management and reflection on the pedagogical approach i.e. Personalized System of Instruction (PSI) (Keller 1968) to design and develop an online InfoSec lab lead to formalize five initial design principles:

1. Contextualization
2. Collaboration
3. Flexibility
4. Cost-effectiveness
5. Scalability

These initial design principles have been derived keeping in view the requirements of an information security course in the degree program. PSI has been selected as the underlying pedagogical approach keeping in line with the course goals and student requirements (such as individual flexibility) in this context. The online InfoSec lab that will be developed based on above-mentioned initial design principles following the ADR process will help to fill the knowledge gap such as:

The contextualization principle will help to provide information regarding the contextual factors that are required to be considered while building and implementing InfoSec lab based on pedagogical principles (PSI principles in this case), such as organizational goals (To implement hands-on exercises for distance students, promote flexible learning), course goals (To improve student’s practical knowledge level, provide students individual hands-on exercises) teachers’ goals (Efficiency in terms of consuming less time than traditional teaching method with the help of an assistant / proctor), resource constraints (available funding) and practical requirements. Contextualization provides meaning to goals and communicates the means for interpreting the environment where the activity takes place (Saarinen 2012). The design principle of “Collaboration” refers to the vital requirement of collaboration among researcher, practitioner, and end users to design and develop effective artifact (e.g. researchers, developers, administrative staff, teachers and students). The strong and meaningful collaboration among researchers and practitioners will help shaping the ensemble artifact based on their reflection and the resulting ensemble artifact will emerge through an interdisciplinary and collaborative effort of experts from different fields (paper-C, Iivari 2003).

A conceptual design for the information security course based on PSI approach (Keller 1968) including online InfoSec lab design to promote student's knowledge level and to provide them flexibility to study at their desired speed has been presented (paper-D). Keeping in view the notion of theoretical framework (paper-B), the course objectives, teaching / learning activities and assessment methods have been pedagogically aligned. The anatomy of design theory framework by Gregor & Jones (2007) is used for outlining a design theory for online InfoSec lab course (see table 4).

Components of a design theory for "online information security lab course for distance students"	
The Purpose and scope of design	• Designing "hands-on" online information security course for distance students of information security degree program. Students should be able to conduct lab exercises from anywhere anytime, and individually in order to provide them flexible and reliable learning environment to practice and master their security skills at their own pace.
Constructs	• PSI approach (modularization, automated scripts mastery of topics, student throughput, flexible learning, immediate feedback, teacher's efficiency, less cheating).
Principles of Form and Function	• 24x7 online InfoSec Lab (server, remote access, automated scripts). • The information security course will contain 15 topics. Students have to show specific level of perfection for lower level topics before moving to the next level topics of the course. Each learning topic consists of the following: 1) Reading and watching video assignment 2) General assessment

	3) Security Lab assessment
Artifact mutability	• Suggestions & feedback and evaluation for improving the current lab facilities and their utilization for distance education will be taken into account before the course is offered next time.
Testable propositions	Modularization of course contents leads to: 1. Mastery of course topics (Student's knowledge level) 2. Student throughput (percentage of student who complete the course) 3. Flexible learning (go-at-your-own-pace) Immediate Feedback (provided by the automated computerized system) leads to: 1. Teacher's efficiency in terms of consuming less time than traditional way of teaching. 2. Flexible learning Automated PSI scripts to assign different exercises lead to: 1. Less cheating
Justificatory knowledge	• The proposed course design is based on the Kernel theory known as the Keller plan, PSI (Personalized system of instruction) which was proposed by Fred S. Keller (Keller, 1968). PSI approach has been utilized in different domains e.g. Psychology, Engineering and computer programming. The researchers (Koen, 1971, Pear & Novak 1996, Morita et al 2005 & 2006 and Nilsen & Larsen, 2011) have noted positive results by implementation of the PSI approach in different courses. The PSI approach has different features which make it a unique way of providing education. These features include: • Flexibility (a feature which allows the students to study at their own chosen pace)

	• The course division into smaller units / modules (in our case we will divide the course into smaller topics which will include reading assignments, assessments and exercises) • Mastery / perfection of the studied units, one module at a time (this feature will help our students master each low level topic before they can proceed to the next topic).
Principles of implementation	• The course will be implemented making use of the: • Virtualization techniques for lab development (multiple logical servers on the same physical server) • Learning management system (Moodle) • LMS Server operating system • LMS database system • Web Server • Automated scripts to grade student's work • We will utilize the virtualization techniques to prepare the InfoSec Lab, which is a cost-effective solution (see section 5 for details).
Expository instantiation	• This is a conceptual idea, which we plan to implement in the next semester in the Luleå University of Technology.

Table 4. Design theory framework for course development (paper-D).

5 DISCUSSION

While exploring the answer to my first research question “What has been theorized about designing online information security laboratories” a literature study was conducted. My findings suggest that there is a lack of systematic guidelines to design and develop an online information security laboratory to fulfil the needs of our graduate students of information security. The literature studied for this research (paper-A) doesn’t provide much knowledge how to use the online InfoSec lab to enhance student’s knowledge level in order to achieve the course and program objectives. I identified that there is a lack of details regarding pedagogical alignment of course objectives with teaching / learning activities (including practical lab activities) and relevant assessment methods are largely ignored. For example, the interviews conducted with the teaching and management staff of the graduate program revealed the general absence of pedagogical approaches in teaching of information security also in the core context. It was further analysed that Msc program was focused more on theoretical aspects while ignoring the practical aspects (see section 4.1). In its current form, this study makes a contribution to synthesize the scattered reports of educational online information security laboratories, which will help other developers and researchers of information security pedagogy as an index of previous literature.

In addition to this, A theoretical framework comprising the Constructive alignment theory (Biggs 1996) and Conversational framework (Laurillard 2002) was proposed (paper-B) to further guide the research process and analyse the case of an internet security course and e-learning platform utilized at the department of Computer Science, Electrical and Space Engineering to impart graduate program of information security. The framework was used to analyse how the e-learning platform consisting of Fronter (Learning management system) and Adobe Connect pro (Virtual classroom) was utilized for teaching and training of information security students. The analysis revealed that the productive media (online InfoSec lab) was missing from the current e-learning platform (ibid), which is a vital tool for the hands-on education of information security graduates. The theoretical framework provides guidelines that how we can exploit the narrative, interactive, productive and communicative capabilities of learning technology to meet the specific learning objectives of the course. The framework emphasizes on the interaction between pedagogical model, instructional strategies and learning technologies to develop knowledge and enhance meaningful learning. The framework contributes to the existing literature by providing guidelines to align the theoretical and practical aspects and teaching / learning activities in the course as the online InfoSec lab design will be influenced by type of practical experiments to be conducted based on overall course objectives. Hence, the course goals and the teaching context will define the design of the e-learning platform rather than the capability of technology. Furthermore, in order to improve the e-learning platform to be used in different courses of information security degree program the framework helps to specify what the digital learning technologies should be doing. Exploiting the narrative, interactive, communicative, adaptive and productive capabilities of e-learning platform in carefully integrated combinations can transform the learning experience into one that fits better with the requirements of the digital age. The theoretical framework (ibid) not only provided help to understand and specify the role of e-learning platform in online information security education but it also helped to captures the essence of university teaching as an iterative dialogue between teacher and students (Laurillard 2002) operating on two levels:

a. The discursive, theoretical, conceptual level
b. The active, practical, experiential level

The theoretical framework also guided the ADR team (researcher, developer & teacher) to understand the pedagogical foundations to develop an instructional design for enhanced hands-on education in information security course (paper-D) and the elements needed for the pedagogical alignment of the e-learning platform.

Moreover, the study suggests a first set of design principles (Contextualization, Collaboration, Flexibility, Cost-effectiveness and Scalability) (see section 4.4) to develop an e-learning platform to promote hands-on education in the field of information security. These initial design principles helped to propose a conceptual design of an online information security course (paper-D) including online InfoSec lab based on PSI approach. The initial design principles contribute to the existing literature by providing important contextual information required for initiating a good design of an IT artifact.

The online InfoSec lab design and development based on initial design principles Contextualization, Collaboration, Flexibility, Cost-effectiveness and Scalability contribute in the literature by addressing the issues mentioned in problem formulation stage in a step-by-step manner (section 4.4). The scope and purpose of online InfoSec lab is clarified by considering relevant contextual factors, which range from organizational goals to course goals. For instance, the targeted ensemble artifact which will emerge through the iterative process based on a specific scientific research method of ADR that will not only provide a complete picture of teaching context in which lab will be used, but it will also lead towards the development of specific design exemplars based on different lab experiments in different courses of a degree program of information security. Furthermore, the collaboration among the researchers, developers and end users will help to get a good reflection in different stages of instantiation both regarding lab as an artifact and the different processes and methods used to accomplish some tasks. This reflective knowledge will in turn be used to refine the artifact and the processes and eventually it will lead towards refinement of emergent design principles. The two different types of assessments, Formative and Summative assessments will generate the justificatory knowledge needed to align the lab activities with the overall course objectives and to explain the rationale behind lab activities. This approach will also help the teachers to become researchers through their involvement and collaboration with the ADR team. The iterative process of ADR will help to formalize the learning and defining different stages of artifact mutability during this process of design and development.

Implications for researchers: In its current form the study provides the researchers of information security pedagogy with an index of previous literature regarding design and development of online educational information security laboratories. Moreover, the study suggests initial design principles such as contextualization and flexibility that will provide help to the future researchers about important contextual information to be explored for design and development of e-learning platforms. The study made use of the theories such as anatomy of design theory, constructive alignment theory and personalized system of instruction approach for different purposes. The demonstration of using theories for literature review, analysis and design will help the future ADR researchers to understand the role of theories to develop theory-ingrained artifacts.

Implications for practitioners: The study suggested abstract initial design principles such as collaboration, cost-effectiveness and scalability. These design principles will not only guide the practitioners about the close collaboration among ADR team members needed for initiating a good design of e-learning platform (such as online InfoSec lab) but it will also inform about the current use of virtual technologies to deal with the issues of cost-effectiveness (utilizing less hardware resources for more end users) and scalability. The theoretical framework suggested in this study provides guidelines to the practitioners such as teachers and developers to align the theoretical and practical elements of courses to achieve stated course objectives and to enhance the quality of teaching.

The main aim of this study is to promote research based hands-on education in the field of information security which will not only benefit the university to have an experienced research based group of teaching staff members but also will help the academic community by continuously adding new information based on educational experiments and experiences with online InfoSec labs. Attempting to achieve a full fledge design theory in the field of hands-on education through online InfoSec labs should be seen as the long term goal, as design theories also helps to provide prescriptions for the development of specific applications. "Ultimately a full design theory is often seen as the goal of design research and the key exemplars develop full theories" (Rossi et al 2012).

6 CONCLUSION

This research work revealed that the contemporary literature regarding online InfoSec labs is still in its infancy. The articles studied for this research, mostly focused on technological implementations neglecting pedagogical principles largely with insignificant evaluation measures. This kind of approach hinders the accumulation and sharing of knowledge in the field of hands-on education of information security using online InfoSec labs. This study attempts to explain the systematic process of research regarding the actual design, development, implementation and maintenance of e-learning platform in general and InfoSec labs in particular in order to enhance hands-on education of information security, to promote flexible learning and to improve throughput. The ADR method was utilized to proceed with this research and in this study an important phase “Problem formulation” is reported.

The initial design principles (contextualization, collaboration, flexibility, cost-effectiveness, and scalability) suggested in this study based on the review of the prior research, and interviews with teachers and program management and analysis of e-learning platform in use will provide help to start the next phase of Building, Intervention and Evaluation (BIE), which will support us to achieve a refined set of more concrete emergent design principles. The proposed conceptual design of online information security course will be implemented including development, implementation and use of online InfoSec lab. The future research will be focused on IT-dominant BIE (building, intervention and evaluation phases of the ADR method). Further research work after the actual development and implementation will be reported to really describe the rest of the phases of ADR.

REFERENCES

1. Ayyagari, R. & Tyks, J. (2012). Disaster At A University: A Case Study In Information Security, Journal of Information Technology Education: Innovations in Practice. Volume 11.
2. Baker, W. et al. (2011) (Verizon data breach investigation report) http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
3. Baskerville, R., Wood-Harper, A.T. (1998). Diversity in Information Systems Research Methods. European Journal of Information Systems. 7(2): p. 17.
4. Biggs J. (1996). Enhancing Teaching through Constructive Alignment, Higher Education, Vol. 32 No.3 pp. 347-364
5. Blaxter, L., Hughes, C. and Tight, M. (1996). How to research. Open University press. Buckingham, Philadelphia.
6. Checkland, P., Scholes, J. (1990). Soft Systems Methodology in Practice. J. Wiley, Chichester.
7. Collins, A., Joseph, D., & Bielaczyc, K. (2004). Design research: Theoretical and methodological issues. Journal of the Learning Sciences, 13(1), 15–42.
8. Crawford, E., & Hu, Y. (2011). A Multi-User Adaptive Security Application for Educational Hacking. Proceedings of the World Congress on Engineering and Computer Science Vol-I WCECS, October 19-21, San Francisco, USA.
9. Crowley, E. (2003). Information System Security Curricula Development. Proceeding of the 4th conference on information technology curriculum on Information technology education. pp.249-255.

10. Dale C.R., Barry M.L., Joseph J. E. (2011). The Role of Cyber-Security in information technology Education, SIGITE, west point, New York, USA.
11. EL-kHATIB, K., Korba, L., Xu, Y., Yee, G. (2003). Privacy and Security in E-Learning. International Journal of Distance education. Volume 1, number 4. Idea group publishing. NRC 45786.
12. Gregor, S., & Jones, D. (2007). The Anatomy of a Design Theory. Journal of the Association for Information Systems, 8, pp.312-335.
13. Harnesk, D. & Thapa, D. (2013). A Framework for Classifying Design Research Methods, In proceedings of DESRIST, LNCS 7939, pp.479-485.
14. Hentea, M. (2005). A perspective on achieving information security awareness. Issues in Informing Science and Information Technology, 2, 169-178.
15. Hentea, M., Dhillon, H. S., Dhillon, M. (2006). Towards Changes in Information Security Education. Journal of Information Technology Education, 5, pp.221-233.
16. Hevner, A.R., et al. (2004). Design Science Research in Informtion Systems Research, in MIS Quarterly, MIS Quarterly & The Society for Information Management. p. 75-105.
17. Hilgarth, B. (2011). E-Learning Success in Action! From Case Study Research to the creation of the Cybernetic e-Learning Management Model, IJCISIM Journal, Vol 3, pp. 415–426.
18. Hirschheim, R. & Klein, H. K. (2012). A glorious and not so-short history of the information systems field. Journal of the Association for Information Systems, 13(4), 188-235.
19. Hrastinski, S., Keller, C., and Carlsson, A. S. (2010). Design Exemplars For Synchronous E-Learning: A Design Theory Approach. Computers & Education 55 652-662.
20. Iivari, J. (2003). The IS core-VII: Towards Information Systems As A Science Of Meta-Artifacts. Communication of the association for Information Systems (12:1)
21. Iqbal, S. (2013). Applying The Analytical Lens Of Constructive Alignment And Conversational Framework For Course And E-Learning Platform Development. In proceedings of Norsk konferanse for organisasjoners bruk av informasjonsteknologi, NOKOBIT. pp.159-172
22. Iqbal, S. and Thapa, D. (2013). Initial Design Principles for an Educational, On-Line Information Security Laboratory. In: Jhing-Fa

Wang, Rynson Lau. (Eds.) ICWL. LNCS, vol. 8167, pp. 89–100. Springer, Heidelberg

23. Iqbal, S., Päivärinta, T. (2012). Towards a design theory for educational on-line information security laboratories. In: Popescu, E., Li, Q., Klamma, R., Leung, H., Specht, M. (eds.) ICWL. LNCS, vol. 7558, pp. 295–306. Springer, Heidelberg.
24. Iqbal, S., Booth, T., Päivärinta, T. (2012). Towards Personalized System of Instruction For Educational Online Information Security Lab Exercise: Research In Progress. In Norsk konferanse for organisasjoners bruk av informasjonsteknologi NOKOBIT, Universitetet i Nordland. pp. 133-144.
25. Jones, D., Gregor, S. (2004). An Information Systems Design Theory for e-Learning. Proceedings, Australasian Conference on Information Systems : 15th annual ACIS Conference, Hobart, Tasmania, University of Tasmania, pp.51-61.
26. Keller, F.S. (1968). Good-bye, teacher... Journal of Applied Behavior Analysis. 1(1) 79.
27. Kerres, M., Witt, De. C. (2003). A Didactical Framework for the Design of Blended Learning Arrangements, Journal of Educational Media, 28:2-3, 101-113.
28. Khan, B. H. (1998). Web-Based Instruction (WBI): An Introduction. Educational Media International, 35, pp.63-71.
29. Koen, B.V. (1971). Self-Paced Instruction in Engineering: A Case Study. IEEE Transaction on Education Volume 14(1) p.24-31.
30. Kosak, L., Manning, D., Dobson, E. et al. (2004). Prepared to Teach Online? Perspectives of Faculty in the University of North Carolina System. Online Journal of Distance Learning Administration, 7, pp.1-13.
31. Kröckel, J & Hilgarth, B. (2011). BPM @ KMU – Designing e-Learning for the Introduction of BPM in Small- and Medium –Sized Enterprises, S-BPM ONE, CCIS 213, LNCS pp. 34–47.
32. Kroenke, D. M. (2012). Using MIS. New Jersey: Prentice Hall.
33. Lahoud ABD, H. A., & Tang , X. (2006). Information Security Labs in IDS/IPS for Distance Education. SIGITE’06, October 19–21, Minneapolis, Minnesota, USA, ACM, pp.47-52.
34. Laudon, K., & Laudon, J. (2010). Management information systems. New Jersey: Prentice Hall.
35. Laurillard, D. (2002). Rethinking teaching for the knowledge society. EDUCAUSE review, January/February. Available online: http://www.educause.edu/ir/library/pdf/erm0201.pdf

36. Leedy, P. & Ormrod, J.E. (2005). Practical research: Planning and design. Pearson Education, Upper Saddle River.
37. March, S.T., G.F. Smith. (1995). Design and natural science research on information technology. Decision Support System. 15(4) 251-266.
38. Mårtensson, P. and A. Lee. (2004). Dialogical Action Research at Omega Corporation. MIS Quarterly. 28(3): p. 29.
39. Mason, M. (2010). Sample Size and Saturation in PhD Studies Using Qualitative Interviews. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 11(3), Art. 8, http://nbn-resolving.de/urn:nbn:de:0114-fqs100387.
40. McDermott, J., & Fox, C. (1999). Using Abuse Case Models for Security Requirements Analysis. Proceedings of the 15th annual computer security applications conference (ACSAC'99), Phoenix, Arizona, pp.55-64.
41. Miles, M.B., Huberman, A.M. (1994). Qualitative Data Analysis- An expanded sourcebook. Thousand Oaks, California.
42. Morita, Y., J. Kenne, A. Johendran, Z. Wu, G. Ma, M. Nakayama, A. Nishihara, B. Koen. (2005). Pilot Study of International Web-Based PSI Course between Japan and US. Proceedings of the 21st Annual Conference of Japanese Society of Educational Technology (JSET) September 23rd at University of Tokushima, Japan.
43. Morita, Y., Kenne, J., Nishihara, A., Nakayama, M., Koen, B.V. (2006). Implementation of an International Web-Based PSI Course: A Case Study. 36th ASEE/IEEE Frontiers in Education Conference, San Diego, CA, p.14-18.
44. Nilsen, H., Larsen, E.Å. (2011). Using the Personalized System of Instruction in an Introductory Programming Course. In the proceedings of 18th NOKOBIT Conference, University of Tromsø, p.27-38.
45. Orlikowski, W. J. (1996). Improvising Organizational Transformation Over Time: A Situated Change Perspective, Information Systems Research (7:1), pp. 63-92.
46. Pear, J.J., Novak, M. (1996). Computer-aided personalized system of instruction: A program evaluation. Teaching of Psychology 23(2) 119-123.
47. Pries-Heje, J., Baskerville, R., Venable, J.R. (2008). Strategies for Design Science Research Evaluation, In Proceedings of the 16th European Conference on Information Systems (ECIS) (Galway, Ireland, 9-11 June). National University of Ireland.

48. Reid, R., Niekerk, V. J. (2013). Towards a Brain-Compatible Approach for Web-Based, Information Security Education Proceedings of the European Information Security Multi-Conference (EISMC).
49. Rossi, M., Purao, S., and Sein .M. K. . (2012). Generalizating from design research. International workshop on IT Artefact Design & Workpractice Intervention, Barcelona.
50. Saarinen, L. (2012). Enhancing ICT Supported Distributed Learning through Action Design Research. Doctoral Dissertations, Aalto University, School of Economics
51. Sein, M.K., et al. (2011). Action Design Research. MIS Quarterly. 35(1): p. 19.
52. Stewart, K. E., Humphries, J. W., Andel, T. R. (2009). Developing a Virtualization Platform for Courses in Networking, Systems Administration and Cyber Security Education. Proceedings of the Spring Simulation Multi-conference, San Diego, CA, USA, Society for Computer Simulation International.
53. Tel, A., Thomas, C. R. (2008). Design-Based Research and Educational Technology: Rethinking Technology and the Research Agenda. Educational Technology & Society, 11(4), 29-40.
54. Thoms, B., Garrett, N., Ryan, T. (2009). Online learning communities in the new "U". International Journal of Networking and Virtual Organisations, 6(5), 499-517.
55. Van de Ven, A. (2007). Engaged Scholarship: Creating Knowledge for Science and Practice. New york: Oxford University Press.
56. Van N, J., Thomson, K. L. (2010). Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the Purpose of Information Security Education for Organizational End-Users. In N. Reynolds and M. Turcsányi-Szabó (Eds.), KCKS, IFIP AICT 324, pp.412-423.
57. Venable, J. (2006). The Role of Theory and Theorising in Design Science Research. First International Conference on Design Science Research in Information Systems and Technology, Claremont, California, pp. 1-18
58. Venable, J., Pries-Heje, J., Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. Design Science Research in Information Systems. Advances in Theory and Practice, p. 423-438.
59. Walls, J. G., Widmeyer, G. R., El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. Information Systems Research, 3, pp.36-59.

60. Wilson, M., Hash, J. (2003). Building An Information Technology Security Awareness And Training Pro-Gram. NIST Special Publication 800-50.
61. Woodward, B. S., Young, T. (2007). Redesigning an Information System Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends. Information Systems Education Journal, 5, pp.1-11.
62. Yngstrom, L., Bjorck, F. (1998). The Value and Assessment of Information Security Education and Training. Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, Stockholm, Sweden, pp.271–292.
63. Yurcik, W., Doss, D. (2001). Different Approaches in the Teaching of Information Systems Security. Information Systems Education Conference, Cincinnati OH. USA (ISECON).

Annex

A. Towards A Design Theory For Educational On-line Information Security Laboratories
B. Applying The Analytical Lens Of Constructive Alignment And Conversational Framework For Course And E-Learning Platform Development
C. Initial Design Principles for an Educational, On-line Information Security Laboratory
D. Towards Personalized System Of Instruction For Educational Online Information Security Lab Exercise: Research In Progress.

A TOWARDS A DESIGN THEORY FOR EDUCATIONAL ON-LINE INFORMATION SECURITY LABORATORIES

Sarfraz Iqbal, Tero Päivärinta

Department of Computer Science, Electrical and Space Engineering

Luleå Tekniska Universitet, Luleå, Sweden.

{sarfraz.iqbal, tero.päivärinta} @ltu.se

Abstract. Online learning for educating information security professionals has increased in popularity. The security curriculum and technology, as well as hands-on laboratory experiences implemented in information security labs, are important elements in an online education system for information security. We drew our motivation from an on-going information security lab development initiative in our own institution, and this paper aims to provide an integrated overview on reported instances of online hands-on education in information security. Our review contributes to the existing knowledge by using the anatomy of design theory framework as a basis for literature analysis, as this provides a common basis to examine theories about human-created information technology artifacts such as information security labs and how such knowledge has been communicated to academia. Our results show that none of the articles studied here puts forward a well-grounded and tested design theory for on-line information security laboratories. This hinders accumulation of knowledge in this area and makes it difficult for others to observe, test and adapt clear design principles for security laboratories and exercises.

Keywords: Information security, Information security education, online information security laboratory

1. Introduction

Education of information security professionals is not a trivial issue [1]. An educational curriculum must prepare security professionals for mastering and develop ever-changing security solutions [2]. Hence, the information security curriculum needs dynamic and timely pedagogical tools that support an interdisciplinary and holistic approach to learning [1, 2, 3]. Graduates also need to master the 'hands-on' approach in addition to straightforward theoretical education [1, 2]. However, curricula development for information security education is a relatively recent phenomenon [4]. For example, less than a decade ago, the ACM (Association for Computing Machinery) guidelines for computer science –related educations specified no topics, courses, or course sequence for information security topics [8].

Since the mid-1990s, hands-on education in information security has been largely conducted through isolated laboratories, where the students have been able to practice attacks and defenses in well-secured server environments on campus [e.g., 1, 2]. Beyond campus-located education, however, blended or e-learning approaches have been regarded as even more effective e.g. for end-user security education [5]. Web-based instruction allows students and instructors to communicate on-line with providers of resources from all over the world [6]. Students find it more convenient to take classes online without the expense and time constraints involved in commuting to a campus facility and university administrators are seeing the online trend as a major revenue and recruitment tool involving the use of less staff and more students [7]. As our literature review below will show, the on-line learning approach targeted at educating information security professionals (in addition to end-users) has also been regarded as being desirable in a number of educational institutions.

Several key elements need to be considered with regard to an online education system for information security, including the security curriculum and technology needed to deliver the education. Distance learning classes have unique requirements if compared to campus-focused education, and accordingly, the information security curriculum needs to keep up with new teaching methods [8]. Hands-on laboratory experiences, implemented in information security labs, thus form a core feature of many information security curricula. An internet-based information security lab is an artifact which involves a collection of systems and software used for teaching information security, and which is accessible through the Internet. A lab is used for exercises, which provide the students with practical experience with security vulnerabilities, security testing, and defenses. For example, students studying topics in cyber security benefit from working with realistic training labs that test their knowledge of network security [10]. An educational lab for information security comprises at least four kinds of entities: servers, sources and targets of attacks, and exercises [9].

As we are motivated by the existence of an on-going security lab development initiative in our own institution, the aim of this paper is to provide an overview on reported instances of online hands-on education in information security. We aim to integrate the existing knowledge by using the “anatomy of design theory” framework [11] as a basis for our literature analysis. The framework provides a common basis for looking at what has been “theorized” with regard to human-created information technology artifacts such as security labs. The rest of the paper is organized as follows. The next section summarizes the design theory framework used as the analysis framework for our literature review. Section 3 summarizes the review results, Section 4 presents the analysis in light of the design theory framework while we discuss about the contribution of our review in section 5. The last section concludes with suggestions for future research.

2. Anatomy of Design Theory

In the discipline of information systems (IS), a research stream implies the establishment and evaluation of design theories with regard to promoting systematic research that involves development of information technology artifacts [26, 27] (such as information security laboratories). By articulating and developing design theories, research can guide design, development, maintenance, and improvement of IT artifacts and help individuals accumulate knowledge, as well as learn about the effectiveness and feasibility of IT artifacts in general, in a disciplined way. In connection to a design theory, one or more "kernel" theories (i.e. theories from the reference disciplines through which knowledge of IT utilization and benefits can be justified and evaluated) may help to provide a further foundation for the design theory [26]. Our focus here will be on design knowledge with regard to the development of online information security laboratories, and on how related knowledge is transcribed and communicated to the community researchers and educators of information security. We will assume that it is beneficial to examine the existing knowledge of on-line information security labs in light of the "anatomy of design theory" [11], in order to summarize what we currently know about design(s) and experiences from previous on-line labs. This may potentially reveal gaps in the existing knowledge in terms of a common framework. In general, we share Hrastinski's justification for such research in the field of e-learning, according to which "the rationale of developing design theory for e-learning is that such theory can support practitioners to understand which mechanisms that may lead to desired outcomes" [12]. Design Exemplars are developed through an iterative process (comprising theory and empirical grounding) which involves testing in contextual settings, by which outcomes can be used as an input for further development and knowledge sharing. Design exemplars provide contextual information to practitioners about when and how to manage and use a specific design. Ideally, in our case, design exemplars thus should guide information security educators to choose well-functioning laboratory exercises to be conducted through on-line laboratories, in order to serve the students better. Table 1 summarizes the design-theory-based framework which we used to define the questions that which guided our literature analysis.

Table 2. A design theory analysis framework for literature review

Design theory issues [11]	**Issues to analyze from the literature concerning on-line information security labs.**
Purpose and scope of interesting designs	Any academic article, which discusses about the implementation of an on-line information security lab was considered relevant for our review.
Constructs	- Technological challenges to implement the laboratory (servers, sources, targets [9])? - Designs of exercises [9]?
Principles of Form and	- Technological requirements and solutions available for labs? - Elements of curriculum and their rationale? - "Best practices" suggested for collaboration through the lab

Function	and on-line communication tools? - How do all these relate together, if that has been studied at all?
Artifact mutability	- Description and suggestions for improving the current methods of utilizing lab facilities for distance education? - Lab utility claims?
Testable propositions	- Measures for improvements and utility used for evaluating the existing labs in the literature, if any? - Claims for lab design adaptability for other organizations? - Are any design exemplars [12] proposed?
Justificatory knowledge	- Do the improvement statements relate to any given theory / theories? (Kernel theories from social sciences governing the design process to provide the foundation knowledge on which other aspects of the ISDT are built [26-27]) (Or is knowledge still in the form of technical/practical "lessons learned", or even in the form of contextual suggestions only)
Principles of implementation	- Implementation guidelines observed for the servers, sources and targets, exercises?
Expository instantiation	- Where and how has the lab in question been implemented? (Conceptual idea, prototype, system in production – how long it has been in use?)

We used Google Scholar for our literature search by using key words such as "information security laboratory", "information security lab", "virtual information security lab", "information security curriculum", "information security education", "information security course" and "information security pedagogy" in the article title. This provided us with 181 articles. We went through all the articles one by one and found 13 relevant articles which specifically discuss information about the security lab concept in an on-line context. We omitted articles discussing the campus-located, isolated laboratory concepts, as well as purely curriculum-related discussions.

3. Results

In the review process we have analyzed the articles against four important entities of an information security lab: Servers, Sources, Targets and Exercises [9]. The chosen articles discuss at least one of the entities of an information security lab.

Servers: Security equipment (hardware, software etc.) is costly, which makes it challenging for universities to build and maintain an information security laboratory. This increases the value of server virtualization platforms which provide the opportunity to implement cost effective solutions in order to provide students hands-on experimentation. Virtualization plays an important role in reducing cost providing the opportunity of utilizing same computer resources by many operating systems. A wide variety of servers, operating systems, and virtualization techniques have been demonstrated in the literature [14, 15, 17, 18, 19, 20, 21, 22, 24, 25] (table 2).

Virtualization Benefits for Distance Education: Our review reveals that most of the labs make use of virtualization technologies in one way or another. Virtualization Technologies are an important element of Information Security labs, and provide such benefits as lower hardware cost, increased deployment flexibility, simplified configuration management, customization of software & hardware resources, increased accessibility of computing resources, remote access to multiple single-user & multi-user computer systems and multiple virtual machines, classrooms system administration and ease of isolating the virtual networks [17,19,20-22]. Virtual computing labs are especially helpful for distance students as they can access the software packages hosted on virtual machines remotely instead of going to the university lab physically [15,16]. Virtual and physical labs configuration and cost has been compared [19] which reveals that virtual labs are far less expensive than physical labs which makes it an ideal tool for experimentation. Several virtual technologies have been discussed which have their own pros and cons, depending on how you intend to use them. Some of the popular products that received attention from authors include VNC Server, VNC client, VMware workstation, VMware server, Vlab Manager, VPN Concentrator, Virtual center, Apache Virtual Computing lab, Microsoft HyperV, Xen, and VMLogix Lab Manager [15, 17, 18, 24].

Sources & Targets: Sources and targets are two important entities of an information security lab for experimentation which has been discussed briefly in e.g. [13, 14, 15, 22, 23, 25] (table 2). The sources and/or targets need to be implemented to provide a basis for any information security exercise. For example, one team or individual will use a virtual machine to run some services and use the host operating system to attack. Once the user enters the lab through the server then the sources and targets are put into action to do further activities including attack / defend etc. options.

Exercises: Exercises for the information security lab have also been discussed briefly [13, 14, 15, 16, 18, 22, 23, 25] (table 2). The exercises include usage of tools such as SNORT (traffic monitoring tool), Vulnerability analysis, Firewall configuration, modification & testing, Passwords policies, traffic analysis, security auditing [14, 15, 18], ceaser cipher, Symmetric key encryption/decryption, public and private keys, Ethereal [16], Network Discovery and surveillance, Network Intrusion Detection [22], Attack – Defense exercises[1], SQL and Php injections, host discovery and port scanning, traffic filtering, web security, and intrusion detection [13, 25].

Table 3. Entities of InfoSec Lab

Ref No	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Servers		X	X		X	X	X	X	X	X		X	X
Sources	X	X	X							X	X		X
Targets	X	X	X							X	X		X
Exercise	X	X	X	X		X				X	X		X

Only four articles include discussions about all the four information security lab entities (table 2). However, even these have mainly general-level discussions, involving scarce descriptions of the actual design and implementation. The next section will analyse the reported on-line security laboratories further in light of the design theory framework.

4. Analysis in light of the Design Theory Framework

The analysis below is based on the anatomy of design theory including purpose and scope of laboratory designs, key constructs used for conceptualizing the laboratory implementations, principles of form and construction, artifact

[1] Attack-defense exercises are usually performed by teams to test the skills and develop knowledge about how to detect vulnerabilities in a system and strengthening its security against any intended attack and from learning to counter-attack as in a real-world scenario.

mutability claims, testable design propositions, justificatory knowledge, principles of implementation, and examples of laboratory instantiations [26].

Table 4. Purpose and Scope of Design

Component examples
An application for "educational hacking" [13]. Evaluating IDS/IPS technology and deriving outlines for remote lab [14]. Aim to describe matters of practical importance to instructors, etc to implement Vlab [17]. To improve students access to university resources [16, 19]. To develop a platform to set up logically isolated virtual networks easily [22]. Providing hands on practice to students for defensive/offensive mechanisms [23, 25].

The analysis shows that some articles present aims and goals very clearly e.g. the aim of most of the labs has been to provide hands on practice to network security class students [23, 25] by improving students access to university resources [16, 19] whereas laboratories have also been purposely designed to allow for exploitation that yields desirable results for hackers [13]. Some labs aim at describing matters of practical importance to instructors, administrators etc. [17], while others focus at particular technological exercises (IDS/IPS) [14]. The purpose and scope of design remained slightly unclear in five articles [15, 18, 20, 21, 22] while they discuss more generally about teaching information security classes to distance students and about how to improve their access to university resources for online education.

Table 5. Constructs

Design of Exercises	**Technological challenges**
Design of exercise [13], sample assignments [22] and lab module assignments [25] discussed briefly. Inner team and inter-team tasks described shortly [23].	Technical issues of online lab [14], differences of Plab vs Vlab [19] and challenges regarding configuration, administration etc., discussed briefly [22]. Vlab challenges discussed [17, 24].

The analysis shows that the two major categories have been investigated under the subject of Constructs i.e. technological challenges and design of exercises. Challenges include technical issues like low internet bandwidth for accessing the online lab resources, monitoring network traffic, host communication, durable network configuration [14], browser support for virtual labs (limited active-x browser plug-ins), browser security settings, storage management tasks, practical concerns of accessibility, training, security, configuration flexibility, reliability, resource management, lab network access, sufficient CPU capacity & memory [17, 19], configuration errors and misuse of administrative privilege [22].

Furthermore, management of virtual machines (including software applications and virtualized hardware components), users, isolating the lab network & virtual machines on the operational network [24] to eliminate the danger of contaminating other university resources and also provide the remote access to the students is a challenging issue as are student background and technical skills in using and operating a virtual computing lab. Cost is an economic challenge in terms of buying the necessary equipment and implementing the lab solution [19]. With regard to the design of exercises, some articles discussed design of assignments only briefly [13,22,23,25]. Nine articles provided no clear designs for assignments [14,15,16,17,18,19,20,21, 24].

Table 6. Principles of Form and Function

Technological requirements & solutions for labs	Elements of Curriculum & rationale
Brief technological requirements and solution discussed[14,15,22] VLab technological challenges and solutions described [17, 21, 19, 24].	Three courses as elements of curriculum discussed with some explanations [15]. Exercise modules discussed as elements of curriculum with brief supported reasoning [25].

The analysis revealed that Technological requirements & solutions for labs have been discussed in general level [14, 15, 22] including discussions about virtual technologies [17, 19, 21, 24]. The best practices for collaboration through lab and online communication tools have been largely ignored. Only two articles discussed the courses as elements of a curriculum designed to provide some support for reasoning in favor of a selected approach [15, 25]. Six articles describe no such characteristics or remained relatively unclear about the matter [13, 16, 18, 20, 21, 23].

Table 7. Artifact mutability

Description and suggestions for improvement	Lab utility
Remote lab solutions for IDS/IPS technology for distance education [14]. Virtual lab with remote access eases software availability [15]. Virtual computing environment components suggested for improvement [17].	24/7 remote access for operating systems and applications [15, 24]. Lab utility in terms of saving cost & student access [19, 21].

With regard to artifact mutability, two categories were investigated in the articles; Descriptions and suggestions for improvement and Lab utility. Descriptions and suggestions for improvement has been discussed in terms of lab solutions for a particular technology (IDS/IPS) [14] as well as providing remote software access for distance education [15] and highlighting the virtual computing environment components role for improving the situation [17]. The issue of Lab utility claims shows that some authors claim that their labs provide 24/7 remote access for distance education [15, 24] whereas others consider lab utility in terms of providing students easy access to lab resources with cost saving solutions [19, 21]. Seven articles remained unclear on these issues [13, 18, 20, 22, 23, 24, 25].

Table 8. Testable Propositions

Improvement & utility measures for existing Labs	**Lab design adaptability**	**Design** **exemplars**
Discussion drawbacks of HackQuest, WebGoat etc., [13]. Shift from Physical labs to Virtual labs discussed [19].	None	None

In the testable propositions category [13] has discussed and compared existing applications such as HackQuest and WebGoat, pointing out their drawbacks. Another paper provided measures for a shift from physical lab towards virtual lab infrastructure including cost and configuration [19]. The issues of lab design adaptability for other organizations and concrete design exemplars have been completely ignored.

Table 9. Justificatory Knowledge, Principles of implementation & Expository instantiation

Relevant Theory
Cooperative learning strategy has been discussed [23].
Implementation guidelines
Guidelines discussed briefly regarding exercises [13]. VLab implementation discussed [17, 18, 19, and 24]. Physical +remote networking lab topology implementation discussed [21].

Isolated virtual network lab software implementation with brief discussion about exercises [22].
Place of implementation
Northern Kentucky University [13], North Carolina State University [15], University of New Mexico [17], Columbus State University [18], Anderson School of Management, University of Mexico [19], East Carolina University [21], Michigan Technological University [24], James Madison University USA [25].

In the category of justificatory knowledge, we tried to explore whether any relevant kernel theories had been used, in the light of which the designs could have been assessed in a larger context of knowledge claims. However, only one article referred to cooperative learning strategy [23] whereas the rest of the articles failed to provide any such kernel theory or related concepts, in light of which one could hold further discussions about the designed labs [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25].

We could identify that the implementation guidelines for exercises were, at best, rather briefly discussed by [13, 22]. Virtual lab implementations have been discussed [17, 18, 19, 24] whereas network lab topology [21] and isolated virtual network lab software implementation [22] were mentioned as the technological bases for implementation. Seven articles communicated no such information [14, 15, 16, 20, 23, 25]. Eight articles specifically defined the university context, in which the reported security laboratory is located (table 8).

5. Discussion

All in all, our review shows that disciplinary literature on on-line education of information security is in its infancy. The reviewed academic reports seldomly referred to each other. Rather, the articles mostly simply presented each laboratory idea as such. Such an approach to reporting IT artifacts is in contrast to the design theory approach of research. In order to make knowledge of online security labs more cumulative and comparable, the literature should focus more systematically on the design theory viewpoint, with regard to which the framework we used for the literature review may give a disciplinary basis.

Our review reveals that several articles lacked a clear design purpose and scope. They simply aimed to improve students' access to University resources and to provide them hands on practice for information security classes. Technological challenges pertaining to physical and virtual online labs were discussed briefly [14,17,19,22,24]. However, our analysis revealed that no article discussed a full-fledged design theory [26], and that technological and pedagogical challenges for online information security labs still need to be discussed in a more precise and detailed manner in order to facilitate real sharing and accumulation of such knowledge. Another knowledge gap yet to be filled is the design of actual on-line assignments, which has not been discussed in detail. Elements of the Curriculum and the rationale behind them are fundamental for any information security laboratory. This element was discussed briefly in only two articles [15, 25], revealing a clear knowledge gap that needs to be filled by providing/suggesting suitable elements of the curriculum for on-line lab usage. Any "best practices" of collaboration through the lab and on-line communication tools was largely ignored. Thus, the literature focuses mainly on the technological implementations of the labs, instead of discussing about how the stakeholders could make use of them. None of the articles discussed the relationship between technological requirements and actual solutions for particular exercises, elements of curriculum and their rationale and best practices for collaboration through lab and online communication tools. Artifact mutability is a very important issue for establishing the criteria for the progress of any IT artifact. The utility of a laboratory and its ability to respond to the requirements better than the competing approaches should be measured and reported in order to bring positive changes and to improve the efficiency and effectiveness accordingly. Among the reviewed papers, only two [15, 24] made utility claims about providing 24/7 remote access. However, the articles provided few, if any, specific measurement criteria for validating such mutability claims.

Also, an absence of testable design exemplars for online information security labs was evident. Hence, it remains unclear which approaches would really be superior for which particular purposes, and whether knowledge and any guidelines for implementing the on-line laboratories yet would involve any verifiable components, let alone "best practice" solutions. Only one article [23] referred to kernel theory (i.e., "cooperative learning strategy"), in the light of which any deeper theoretical approach to discuss the usefulness or theoretical implications of the selected lab design could have been used. However, diverging theoretical assumptions, such as varying pedagogical approaches, would surely have had a profound impact on the actual design and evaluation parameters of any exercises and perhaps even the technological laboratory implementations. For example, if we contrast the above-mentioned cooperative learning strategy [in 23] to the pedagogical approach of “mass-customization” [cf. 28], the latter approach might highlight individually flexible interactions with the lab equipment instead of co-operative group efforts. This would, furthermore, have implications on the lab design as well as selection of evaluation criteria of the whole artifact in the first place. The introduction of pedagogical kernel theories would help the researchers and developers of this domain to crystallize the actual contributions of their laboratory concepts and to position them in relation to each other to form a more coherent body of knowledge. The current knowledge exists, at best, on the level of vaguely evaluated, even anecdotal, lessons learned from contextual suggestions.

In its current form, our review makes a contribution to the literature in that it represents the first attempt to locate the hitherto scattered reports of educational on-line information security laboratories in a common frame of reference. The review is thus a useful overview for other developers and researchers of information security pedagogy, providing an index for the previous literature. Our work primarily addresses the general-level absence of design theories for on-line laboratories and, in particular, research opportunities for pursuing such theories about particular on-line laboratory artifacts.

6. Conclusion

This paper provides an overview of reported instances of online educational information security laboratories by providing a literature review of the topic and analyzing 13 relevant articles. Our analysis was based on a framework for defining elements of design theory related to IT artifacts, such as on-line information security laboratories. The analysis showed that the contemporary literature on the topic is relatively scattered and that there is a need for more systematically formed design theories through which the academia and developers of security laboratories could enhance knowledge sharing and accumulation. In the future, our aim is to develop an online information security laboratory for our own educational institution, with a clear purpose and scope to provide on-line information security exercises for the master’s students of our dinstance education program in information security. We will focus on systematic development of a design theory of on-line educational information security laboratories. A solid design theory is expected to form a further basis to introduce methods and techniques of conducting hands-on training based on selected pedagogical approaches, and, furthermore, to develop systematic evaluations for enhancing continuous improvement of our educational products in this field.

References:

1. Yurcik, W., & Doss, D.: Different Approaches in the Teaching of Information Systems Security. Information Systems Education Conference, Cincinnati OH. USA (ISECON) (2001).
2. Woodward, B. S., & Young, T.: Redesigning an Information System Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends. Information Systems Education Journal, 5, pp.1-11 (2007).
3. Yngstrom, L., & Bjorck, F.: The Value and Assessment of Information Security Education and Training. Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, Stockholm, Sweden, pp.271–292, 1998.
4. Crowley, E.: Information System Security Curricula Development. Proceeding of the 4th conference on information technology curriculum on Information technology education. pp.249-255, (2003).
5. Van Niekerk, J., & Thomson, K. L.: Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the Purpose of Information Security Education for Organizational End-Users. In N. Reynolds and M. Turcsányi-Szabó (Eds.), KCKS 2010, IFIP AICT 324, pp.412-423 (2010).
6. Khan, B. H.: Web-Based Instruction (WBI): An Introduction. Educational Media International, 35, pp.63-71 (1998).
7. Kosak, L., Manning, D., Dobson, E. et al.: Prepared to Teach Online? Perspectives of Faculty in the University of North Carolina System. Online Journal of Distance Learning Administration, 7, pp.1-13, (2004)
8. Hentea, M., Dhillon, H. S., Dhillon, M.: Towards Changes in Information Security Education. Journal of Information Technology Education, 5, pp.221-233 (2006).
9. McDermott, J., & Fox, C.: Using Abuse Case Models for Security Requirements Analysis. Proceedings of the 15th annual computer security applications conference (ACSAC'99), Phoenix, Arizona, pp.55-64 (1999).
10. Stewart, K. E., Humphries, J. W., Andel, T. R.: Developing a Virtualization Platform for Courses in Networking, Systems Administration and Cyber Security Education. Proceedings of the Spring Simulation Multi-

conference, San Diego, CA, USA, Society for Computer Simulation International, (2009).

11. Gregor, S., & Jones, D.: The Anatomy of a Design Theory. Journal of the Association for Information Systems, 8, pp.312-335 (2007).
12. Hrastinski, S., Keller, C., Carlsson, S. A.: Design Exemplars for Synchronous e-Learning: A Design Theory Approach. Comput. Educ., 55, pp.652-662 (2010).
13. Crawford, E., & Hu, Y.: A Multi-User Adaptive Security Application for Educational Hacking. Proceedings of the World Congress on Engineering and Computer Science Vol-I WCECS 2011, October 19-21, San Francisco, USA (2011).
14. Lahoud Phd ABD, H. A., & Tang Phd, X.: Information Security Labs in IDS/IPS for Distance Education. SIGITE'06, October 19–21, Minneapolis, Minnesota, USA, ACM, pp.47-52 (2006).
15. Li, P., Toderick, L. W., Lunsford, P. J.: Experiencing Virtual Computing Lab in Information Technology Education. Proceedings of the 10th ACM conference on SIG-information technology education SIGITE'09, October 22–24, Fairfax, Virginia, USA, pp.55-59 ACM (2009).
16. Choi, Y. B., Lim, S., Oh, T. H.: Feasibility of Virtual Security Laboratory for Three-Tiered Distance Education. Proceedings of the ACM conference on Information technology education, pp.53-58 (2010).
17. Burd, S. D., Gaillard, G., Rooney, E. et al.: Virtual Computing Laboratories using VMware Lab Manager. Proceedings of the 44th Hawaii International Conference on System Sciences – IEEE, pp.1-9 (2011).
18. Summers, W. C., & Martin, C.: Using a Virtual Lab to Teach an Online Information Assurance Program. Proceedings of the 2nd annual conference on Information security curriculum development, New York, ACM, pp.84-87 (2005).
19. Burd, S. D., Seazzu, A. F., Conway, C. et al.: Virtual Computing Laboratories: A Case Study with Comparisons to Physical Computing Laboratories. Journal of Information Technology Education, 8 (2009) 24.
20. Gaspar, A., Langevin, S., Armitage, W. et al.: The Role of Virtualization in Computing Education. Proceedings of the 39th SIGCSE technical symposium on Computer science education, New York ACM, pp.131-132 (2008).
21. Li, C.: Blur the Boundary between the Virtual and the Real. Journal of Computing Sciences in Colleges, 24, pp.39-45 (2009).
22. Krishna, K., Sun, W., Rana, P. et al.: V-NetLab: A Cost-Effective Platform to Support Course Projects in Computer Security. Proceedings of the 9th

Annual Colloquium for Information Systems Security Education (CISSE 05), Atlanta, GA, June 6-9, (2005).

23. Chen, F. G., Chen, R. M., Chen, J. S.: A Portable Virtual Laboratory for Information Security Courses. S. Lin and X. Huang (Eds.): CSEE 2011, Part V, CCIS 218, Springer-Verlag Berlin Heidelberg, pp.245-250 (2011).
24. Wang, X., Hembroff, G. C., Yedica, R.: Using VMware VCenter Lab Manager in Undergraduate Education for System Administration and Network Security. Proceedings of the 2010 ACM conference on Information technology education, pp.43-52 (2010).
25. Aboutabl, M. S.: The Cyberdefense Laboratory: A Framework for Information Security Education. Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, pp.55-60 (2006).
26. Jones, David and Gregor, Shirley.: An Information Systems Design Theory for e-Learning. Proceedings, Australasian Conference on Information Systems : 15th annual ACIS Conference, Hobart, Tasmania, University of Tasmania, pp.51-61 (2004).
27. Walls, J. G., Widmeyer, G. R., El Sawy, O. A.: Building an Information System Design Theory for Vigilant EIS. Information Systems Research, 3, pp.36-59 (1992).
28. Friedman, R.S., Deek, F.P.: Innovation and Education in the Digital Age: Reconciling the Roles of Pedagogy, Technology, and the Business of Learning. IEEE Transactions on Engineering Management, 50, 4, pp. 403-412 (2003).

B APPLYING THE ANALYTICAL LENS OF CONSTRUCTIVE ALIGNMENT AND CONVERSATIONAL FRAMEWORK FOR COURSE AND E-LEARNING PLATFORM DEVELOPMENT

Sarfraz Iqbal

Department of Computer Science, Electrical and Space Engineering

Luleå Tekniska Universitet, Luleå, Sweden.

sarfraz.iqbal@ltu.se

Abstract

Assessment of educational needs for offering a master's degree program in Information Security both to campus and distance students is of extreme importance in order to improve curriculum design as well as e-learning platform. The case of an Internet Security course and e-learning platform were analyzed. The theoretical framework based on constructive alignment theory (Biggs, 1996) and conversational framework (Laurillard, 2002) has been used as an analytical lens to analyze the case and guide the ongoing research process for improvement in the courses as well as for the development and improvement of e-learning platform. It is proposed that in order to improve the quality of teaching and enhance the e-learning platform all the courses included in MSc program in Information Security should be developed systematically based on specific pedagogical principles. The systematic development approach will help the instructors to enhance understanding and provide guidelines to incorporate the mindset of constructive alignment. Information Security education benefits greatly from hands-on laboratory oriented exercises. Therefore, e-learning platform including InfoSec lab must be designed and developed based on pedagogical principles. In this way we can argue for the true benefits of the learning technology being developed for a specific purpose. Hence, learning technology is not considered as merely a knowledge-transmitting tool but viewed as an ensemble artifact. This article attempts to put forward a theoretical framework to provide pedagogical guidelines for alignment of courses and for the selection of suitable e-learning platform.

Key words: Internet security, Personalized system of instruction, Constructive alignment

1. INTRODUCTION

The advances in network attack technology including automation of deployment and sophistication of attack tool management has led to situations where a single attacker can employ a large number of distributed systems to launch devastating attacks against a single victim easily (Allen et al, 2002). There is an increased demand for trained network security professionals due to the higher and wide range of attacks on computer networks (Suranjith and Amina, 2005). The researchers (Sukamol & Markus, 2007) argue that the education part of the security has not got the real attention that it deserves. They further argue while good user education can hardly secure a system, we believe that poor user education can put it at serious risk (Srikwan and Jakobsson, 2007). The University teaching is supposed to seek realignment of research and teaching and to teaching methods that support students in the generic skills of scholarship, not the mere acquisition of knowledge (Laurillard, 2002).

In an educational institute teaching has been described as a complex system where different components of this system including teachers, students, the teaching context, student learning activities and the outcome interact with each other at the classroom level (Biggs1993, 1996, Von Bertallanfy 1968). The educational institutes are broadening their scope of educating the future security experts by offering courses and degree programs aimed at preparing an educated work force to secure our valuable information systems. Many educational institutes offer degree programs and courses to campus as well as distance students (Flowers, 2001), which also include professionals.

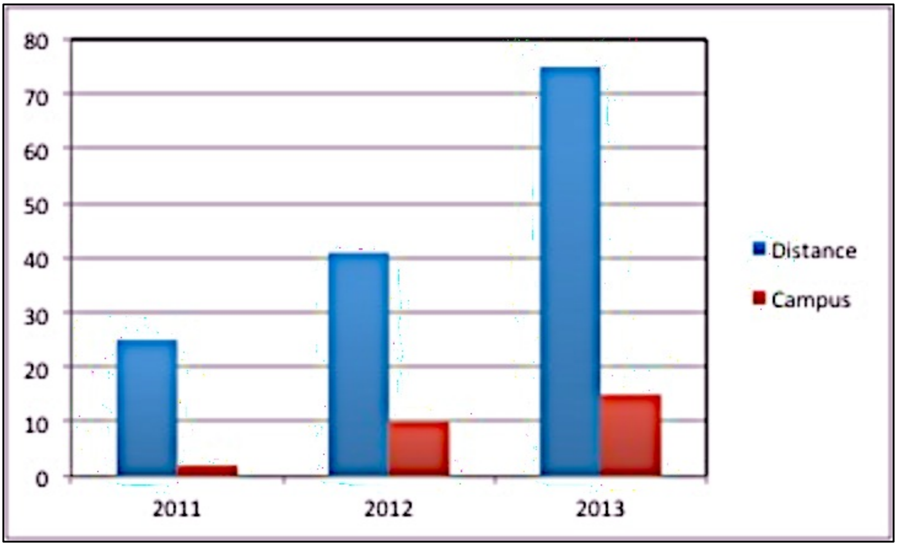


Figure-1 Student history chart showing distance and on-campus students

The Luleå University of Technology also offers an Information Security Master's degree program to campus as well as distance students since 2007. It is noticed that the number of applicants for the MSc Information Security program has increased in past years (see chart-figure-1) with a major increase in number of students who want to study from distance. The department of Computer and Systems Science at Luleå University is endeavoring to improve the quality of teaching in order to develop an effective and meaningful Msc program. This article focuses on the educational needs for course and e-learning platform development to teach an online program in information security. Assessment of educational needs for offering a degree program at campus as well as distance is of extreme importance in order to improve curriculum design (Pratt, 1980, Queeney, 1995) as well as e-learning platform. Recently the author conducted open-ended semi-structured interviews with the whole program management committee and teachers. The interviews revealed general absence of pedagogical approaches in designing and delivering courses in Information Security degree program. The management is interested to find ways to enhance quality of teaching, which lives up to the stated course outcomes "how to promote research based teaching?" The management also wants to find out "how we can improve the knowledge level / understanding of our students?" and "How we can engage students actively in the courses as well as provide them flexible learning opportunities?" Hence, the course of Internet security was designed based on Personalized System of Instruction ((PSI), Keller, 1968) and offered to Master's students of Information Security program at the University. This article aims to use the analytical lens of Constructive alignment (Biggs, 1996) and Conversational Framework (Laurillard, 2002) for assessment of educational needs at the department of computer and systems science at Luleå university to enhance teaching and learning both for campus and distance students of Master's program. The current e-learning platform at the department of computer and systems science will also be assessed for pedagogical improvements.

The rest of the paper is arranged as follows. Section 2 portrays the Theoretical framework. Section 3 describes the case of Internet security course based on PSI approach and also provides an overview of background and key features of the PSI approach. Section 4 provides the analysis of the case under consideration in the light of theoretical framework. The implications for Program development are discussed in section 5 whereas conclusion and further research work is discussed under section 6.

2. THEORETICAL FRAMEWORK

Instructional design literature and constructivist learning theory are considered as popular source of stimulus in higher educational practice (Biggs 1996). Biggs (1996) refers to two major theoretical traditions in higher education, which consists of 1. Objectivist and 2. Constructivism and phenomenography (Duffy & Jonassen 1992, Steffe & Gale 1995 and Marton 1981). Researchers (Steffe & Gale 1995) have recognized various schools of Constructivism with different impact on educational practices such as cognitive, social constructionism and postmodernism. The learner's activities are seen as the central aspect of the Constructivism related theories when it comes to the implications for teaching and assessment. Biggs (1996) suggests that different constructivist theories could emphasize different things but keeping in view the centrality of the learner "a consensus would be that learners arrive at meaning by actively selecting, and cumulatively constructing, their own knowledge, through both individual and social activity". Constructivism promotes a classroom culture where the teacher acts as a facilitator for the development of individual and group meaning instead of being only a traditional lecturer; the constructivist pedagogy (Richardson, 2003) should include following five characteristics: -

- Attention to the individual and respect for student's background and developing understanding of and beliefs about elements of the domain (described as student-centered)
- Facilitation of group dialogue that explores an element of the domain with the purpose of leading to the creation and shared understanding of a topic
- Planned and often unplanned introduction of formal domain knowledge into the conversation through direct instruction, reference to text, exploration of a web site, or some other means.
- Provision of opportunities for students to determine, challenge, change or add to existing beliefs and understandings through engagement in tasks that are structured for this purpose
- Development of students' met awareness of their own understandings and learning process

The above mentioned elements are also utilized differently in different situations depending on several other elements including content domain, age level of the students, student's experiences as learners prior to coming into the specific classroom, school context etc. (Richardson, 2003). Constructive alignment (Biggs, 1996) pushes the teachers to design teaching / learning activities according to the course goals prior to the start of study so that the students are actively engaged in interesting activities individually as well as collaboratively. Constructive alignment theory puts forward following important inferences:

- Attempts to enhance teaching need to address the system as a whole, not simply add "good components, such as a new curriculum or methods".
- When curriculum and assessment methods are aligned, the results of instruction are massively improved.
- Define the teaching objectives at a high cognitive level
- For the teachers to teach for understanding requires them to have a framework of some kind to help them operationalize what "understanding" might mean in their particular case. Solo (structure of the Observed Learning Outcome) provides a systematic way of describing how a learner's performance grows in complexity when mastering many tasks. It includes five levels to denote a hierarchical list of performance of understanding i.e. Prestructural (unsatisfactory), Unistrctural (Barely satisfactory), Multistructural (Moderately satisfactory), Relational (Very satisfactory), Extended Abstract (Most desirable). In sum, a performative notion of understanding enables teachers to specify the things the students need to do in order to

demonstrate particular levels of understanding. The above mentioned objectives form categories from A,B,C,D and F for grading purpose.

- The teaching methods we choose need to engage students in activities that are likely to require them to perform in the way nominated in the curriculum objectives.
- Both individual and social activities play a role in the construction of knowledge. The learner's spontaneous activities are just as crucial in a constructivist instructional framework as those activities that are in reaction to teaching.
- Embed the learning / study skills relevant to learning particular content in the teaching of that content. This must become an increasingly important issue in distance or "flexible learning modes".
- In deciding the assessment tasks, it is necessary to judge the extent to which they embody the target performances of understanding and how well they lend themselves to evaluating individual student performances.
- The main point is that a working version of constructivism can be integrated with instructional design at three crucial points: the curriculum or unit objectives are clearly stated in terms of content specific levels of understanding that imply appropriate performances, the teaching methods require students to be placed in contexts that will likely elicit those performances and the assessment tasks address those same performance.

Laurillard (2002) promotes the idea that knowledge industries create the means by which individuals can acquire the immediate skills and knowledge those industries need. Furthermore, the fundamental design formats for learning technologies can support the practice of elevated cognitive skills and to help ease the complex learning experience. Laurillard (2002) makes some important propositions such as:

- Universities will maintain their competitive edge against the knowledge industries through the maintenance of their core values-including research-based teaching and a curriculum that provides for long-term cognitive needs of individuals.
- Universities are not maintaining a professional teaching approach that parallels their professional research approach, and the curriculum is not sufficiently oriented toward long-term high-level cognitive skills.
- University teaching must aspire to a realignment of research and teaching and to teaching methods that support students in the generic skills of scholarship, not the mere acquisition of knowledge.

- Learning technologies can support students in the learning forms that contribute to the high-level cognitive skills of scholarship and the practitioner-based skills and knowledge of design-like practice.
- Conversational framework provides a framework against which we can specify what the digital learning technologies should be doing. Exploiting the narrative, interactive, communicative, adaptive and productive capabilities of new technologies in carefully integrated combinations can transform the learning experience into one that fits better with the requirements of the digital age.
- Design has to be generated from the learning objectives and the aspirations of the course, rather than from the capability of the technology. All technologies create communities that invent a range of formats within which practitioners can craft a variety of contents; we need the same formats for learning technologies.
- Academics must become researchers in teaching

The Conversational Framework (Laurillard, 2002) for learning promotes an environment where reflective awareness leads to a more progressive model than the transmission model, which is desired by education providers. The framework not only helps to specify what digital technologies should be doing but it also captures the essence of university teaching as an iterative dialogue between teacher and students operating on two levels:

- The discursive, theoretical, conceptual level
- The active, practical, experiential level

The two levels bridged by each participant engaging in the processes of adaptation (practice in relation to theory) and reflection (theory in the light of practice). These ideas are in-line with our views of promoting ties between theory and practice in the department of computer and system science at Luleå University of Technology for enhancing quality of teaching and learning.

The constructive alignment theory (Biggs, 1996) and conversational framework (Laurillard, 2002) has been used as a framework to guide our ongoing research process for improvement in our courses as well as for the development and improvement of our e-learning platform. Both the Constructive alignment theory and conversational framework have their pros and cons e.g. constructive alignment presents a holistic view of course development which guides the Instructional designer from stating the course objectives to properly align the course objectives with intended teaching / learning activities and suitable assessment methods whereas it doesn't provide any specific guidelines for the media to be used for communication and interaction between teachers and students in the classroom. The Conversational framework on the other hand discusses in detail about the media types to be used during teaching. This framework will be utilized to analyze the case of an Internet security course offered to MSc students of Information security program at Luleå University of Technology. It will further analyze the existing e-learning platform used to deliver courses in the information security degree program for an overall program improvement based on specified pedagogical principles in light of the above-mentioned theories.

3. CASE DESCRIPTION OF INTERNET SECURITY COURSE REFLECTING THE PSI PRINCIPLES

The Internet Security course was designed to provide theoretical underpinnings as well as practical knowledge in the field of Internet security, it should help to add more knowledge to student's existing theoretical and practical skills and experiences. According to the pedagogical requirements of the Internet Security course (such as individual learning and Flexible learning that are very important factors for distance students who want to study and work at the same time and cannot follow a strict schedule) and available resources Personalized system of Instruction (PSI) was selected as a pedagogical approach.

The PSI (Keller 1968) originated in the form of programmed instructions in the field of psychology but it has also been used in different other educational domains such as Engineering (Koen 1971, Cumming & McIntosh 1982) and programming courses (Emurian et al 2000, Nilsen & Larsen 2011). Crosbie & Kelly (1993) utilized PSI to teach a course of applied behavior analysis. Some scholars such as Pear & Novak (1996) and Pear & Crone-Todd (1999) described the use of computer-aided personalized system of instruction program in different undergraduate psychology courses. PSI has also been used in the field of Engineering and engineering mathematics. Even a successful experience of an international web-based PSI course was also reported (Morita et al, 2005, Morita et al 2006) facing minor problems related to motivation and network issues. The researchers (Pear & Novak 1996) recognized that this approach is favorable for distance students and the student's reaction reveals that they prefer the convenience of working at their own pace and being free to work on the course when and where they chose. Low rates of procrastination and positive student attitudes were reported (Crosbie & Kelly, 1993) but in some cases procrastination became a problem for weaker students (Nilsen & Larsen 2011). The discussion about the usage of PSI approach in different domains of education exhibits that the PSI approach has potential to produce positive results regarding student's learning. The distinct features of the PSI are as follows: -

- To provide clear study objectives
- Division of course content into smaller modules / units
- Flexibility (study at your own pace)
- Mastery of the course unit / module
- To provide immediate feedback on each course unit / module
- Use of Teacher, Assistant / Proctor

Mastery or perfection of a learning unit is ideal for our plans of improving the knowledge level of students. The basic premise of the PSI is on the flexibility provided to the student where he / she have full control of the speed of study (the go-at-you-own-pace feature). The students have no strict schedule but they can follow the course on their own speed (Keller 1968). These features of PSI were in-line with the pedagogical requirements of the Internet Security course where students were provided flexibility to study at their own pace on the basis of when and where they like it.

A study guide was developed for Internet Security course prior to the start of the course and was delivered to the students. The study guide included following sections:

- Welcome to the course in Internet Security 7.5 HE credits
- Course Outline
- General information about studies and assessments
- The course team
- Aims, goals and literature
- Commented reading list
- Course assignments

The students were informed through the study guide that this course provides a detailed review of the information security field, including essential terminology, the history of the discipline, and practical techniques to manage implementation of security solutions. After an overview of information, network, and web security, students would explore defense technologies and methods, including access controls, firewalls, VPNs, and intrusion detection systems, as well as applied cryptography in public key infrastructure. The course is ideal for those who are interested in helping organizations to protect critical information assets and secure their systems and networks, both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future.

3.1. Objectives and Course Plan

The aim of the course was to develop knowledge and an attitude that contribute to understanding and implementing the fundamental principles of Internet Security with a scientific foundation in education.

On completion of the course students should be able to:

- Understand the nature and scope of the Internet Security
- To be aware of security issues and to analyze any potential outcomes, and consequences to respond and react to security lapses.
- Understanding the safeguarding needs of an organization's knowledge, information systems, and continuity of its ICT-services

The course contained the following activities:

- Individual study of the literature and Reflection
- Live as well as recorded lectures
- Assignments
- Supervision – monitoring and feedback by the teacher and teacher assistant on assignments
- Case study discussion (Mid-term Exam)
- Final Written exam

3.2. Grading and Evaluation Criteria

The course was divided into smaller course modules so that students can get expertise on it. To evaluate their expertise, there were compulsory individual assignments (reflection on the lectures) at the end of each lecture. All the assignments were mandatory, and it was important to complete the previous assignment to get the next one. All the assignments and written exams were inter-connected. For example, students should complete individual assignments to appear in the written exam; likewise, without the completion of initial assignments students cannot appear in the written exam. The assignments should be uploaded into the Fronter (Learning Management System) on the due-date. In case of delay or failure to submit any given assignments on due-date, students should submit the assignments as an email attachment to the teaching assistant who will then upload it in the Fronter.

Written exam was in the form of information security case analysis in the organizational context. The case along with five questions was oriented towards three aspects of information security: technical, formal, and informal. On the successful completion of written exams students will be awarded 5.0 credits. On the successful completion of individual assignments students will be awarded 2.5 credits.

Code	**Type**	**Credits**	**Grade**
0001	Written exam	5.0	U G VG
0002	Individual assignments	2.5	U G#

Table 1. Grading criteria

3.3. Course Results

Total Scores

The total number of students enrolled in the Internet Security course in spring term of 2013 was 94 out of which there were 18 female and 76 male students. The following results emerged. 51 students out of 94 managed to pass the course which included 14 female and 37 male students. Out of 51 passed students 23 got “G” and 28 got “VG” as grades. It shows that 45 % students got “G” whereas 55% students got “VG”. Description of grading criteria is as follows (U = fail, G & G# = Pass, VG = Pass with distinction).

Dropout rates

It is observed that in some cases the focus on mastery of course content produces a negative effect resulting in increased failing rate of students or dropping the course (C.L.C. Kulik et al, 1990, Crosbie and Kelly, 1993). It was noticed that in our course 94 students were enrolled but, those who actually managed to pass the course were 51. Students couldn’t complete the course based on different reasons e.g. Some students left the course because they didn’t find it enough interesting due to lack of social activity in the form of group work. Some students couldn’t follow the deadlines and voluntarily dropped the course.

Feedback & Evaluation

At the end of the course a survey questionnaire was sent to all the students. The survey was answered by 58 students.

- A majority of students in general appreciated this approach of individual learning where they had full freedom of doing the compulsory assignments individually and on their own pace at their own chosen time.

- Some students complained about the overlapping of course content with another course of Information Security. They thought that some part of the course content was almost similar and they expected this course to be more technical instead of theoretical. For example consider following comments "The theoretical part of the course reminded me of the introduction course Information security that we had with another teacher. "
- Many students mentioned that the course has a huge theoretical portion but they expected to have a lot of hands-on practice in this course.
- A lot of students demanded that they should have access to an online lab where they can practice their information security skills individually as well as in collaboration with other students. Some student comments were as follows "I have been thinking a lot about lab's", " hands-on exercises with different programs / devices related to relevant chapters in the course book would be a "paradise", may be you could set up some lab-environment with servers, routers, IDPS, LDAP whatever and make students to get in touch with those. This would be very valuable", "my expectations on the course were that we were to have many practical exercises; unfortunately my expectation on that part were not fully fulfilled."

4. CASE ANALYSIS

The analytical lens of Constructive alignment theory (Biggs, 1996) and Conversational framework (Laurillard, 2002) is used to examine the above-mentioned case of Internet Security course (see section-2) as well as to evaluate current learning platform employed both for distance and campus studies. A lot of teachers aim to improve the understanding of their students through teaching so that their students can act / react properly using their in-depth knowledge in unknown situations or contexts. The Internet Security case based on PSI approach shows that 43 students couldn't complete the course due to different reasons. Lack of social activity in the form of group work was also one of the reasons mentioned in the feedback due to which some students lost their interest in the course. In light of the framework (section 2) it is visible that the learner's activities in the above-mentioned case need to be designed more carefully to keep students interested in the course and to engage students actively.

Practical and theoretical parts of the course were not given equal importance due to which students could not develop deep interest in the course. As students mentioned in the feedback they were hoping to have good hands-on practice sessions. The students even demanded for access to a lab with servers, routers, IDPS etc. where they can practice their security skills. The analysis suggests that not much attention was given to student's background and expectations in this case. The analysis in light of the framework (section 2) suggests that in this particular case an internal framework (such as SOLO) focusing the development and enhancement of student's understanding was lacking.

The course content was overlapped with another course of Information Security, which means that repetition of the same content resulted in frustration among different students. It also points to the fact that in a degree program the different courses should be arranged in a sequenced manner which should consider students knowledge development in an escalating process from one course to the other. The case analysis shows that teaching / learning activities were not planned very well ignoring the issues of deep and surface learning e.g. students should be guided to adopt a deep approach that is directed towards comprehending the meaning of the materials to be learned or students should be motivated to adopt a surface approach for some instances where purpose is to reproduce the materials for the purpose of academic assessment (Hambleton et al, 1998). The analysis also reveals that only individual level assignments were not enough to promote constructivism in the classroom and to keep the students actively engaged.

The current e-learning platform at the department of computer and systems science has been utilized without paying too much attention of how the available technologies can best support the teaching / learning activities needed in the course. The current e-learning platform doesn't include any productive media such as an online information security laboratory is not available for students to practice their security skills.

If the current e-learning resources at department of computer and systems science are categorized in the light of Conversational Framework, it seems that the current available learning resources such as Learning management system (Fronter) and Virtual classroom for lectures delivery (Adobe Connect Pro) has been used for simple interactive and communicative activities (further discussion about media categorization and enhancement in next section).

5. IMPLICATIONS FOR INFORMATION SECURITY PROGRAM DEVELOPMENT

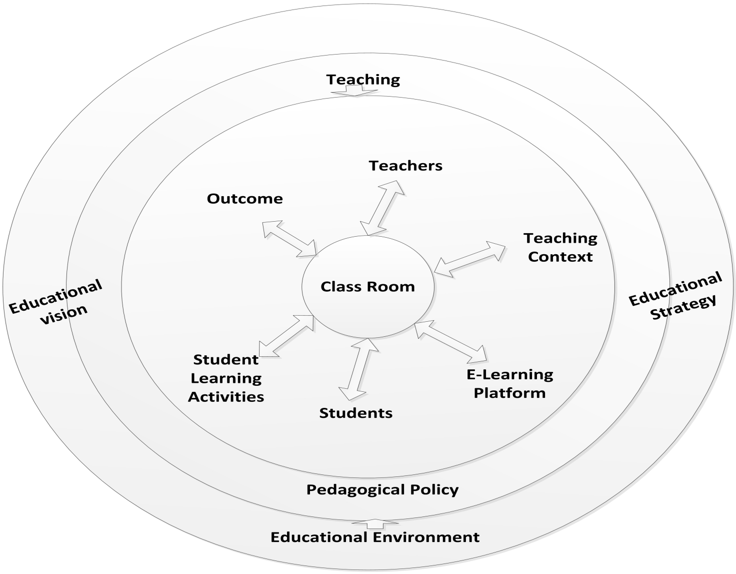


Figure – 2 Educational Environment of classroom teaching

The findings as shown in Figure-2 suggests that an overall educational environment at a higher education institute is governed by the educational vision and strategy of a particular institution. It is proposed that in order to improve the quality of teaching and enhance the e-learning platform the Msc program in Information Security should be developed systematically based on specific pedagogical principles. Figure-2 characterizes teaching based on pedagogical principles at classroom level within an educational system. The pedagogical policy cannot be same for different departments of a university but every department should try to formulate their specific departmental pedagogical policy in the light of Institutional vision and strategy which is influenced by several factors such as type of education, mode of education delivery, learning platform requirements etc. The findings (figure-2) also portrays that in an educational environment the teaching and learning should be based on a specific pedagogical policy / principles. These pedagogical principles, which are based on pedagogical approaches, could be different for different courses in a degree program based on the overall aim of the program. Every single study course / unit included in the program serves a specific purpose to achieve that specified aim / goal of the program. The above figure-2 also depicts that there are two levels of pedagogical underpinnings such as:

- Pedagogical Policy at Program level
- Pedagogical approach at course level

At the program level, it should be discussed and decided what kind of tools and platform is available to deliver the education to students effectively. Biggs (1996) proposes that in order to improve teaching in an education system, the system as a whole should be subjected to the efforts of improvement and it should not be limited to merely adding “good components” in the form of a new curriculum or method. For example, in the case under discussion, the university offers an Msc program to both on-campus and distance students at the same time. It requires considering the overall e-learning platform. The current infrastructure / e-learning platform at the department of computer and systems science can be categorized based on the Conversational Framework for Instruction (Laurillard, 2002) in the following manner (see table-2).

Learning Management System (Fronter), Wiki	(Interactive)
Virtual Classroom (Adobe Connect Pro)	(Communicative)

Table 2. E-Learning platform at Luleå University

The teachers and students make use of Fronter, which is an official tool at Luleå University for different types of interactions such as teacher vs student and also between students’ vs students. The teachers mostly use Fronter for delivering:

- Course information
- Course material
- Course assignments
- Comments on assignments
- Maintenance of student portfolio

Whereas the students also make use of the Fronter in different ways:

- Submitting assignments
- Reading comments
- Accessing / downloading course materials

Some teachers also use Wiki instead of Fronter to conduct some of the tasks mentioned above. A chat function is also available in the Fronter course room, which can be utilized for chat between teacher and student etc. The virtual classroom (Adobe Connect Pro) is generally used for:

- Live classes
- Video conferencing
- Project presentations
- Online Exams

With the addition of an online InfoSec Lab the e-learning platform categorized according to the Conversational framework (*Laurillard*, 2002) will appear like this (see table-3):

Learning Management System (Fronter), Wiki	Interactive
Virtual Classroom (Adobe Connect Pro)	Communicative
Online InfoSec Lab	Productive

Table 3. Proposed E-Learning platform at Luleå University

The online InfoSec lab will offer the opportunity to the students where they can do different tasks individually as well as collaboratively. It will allow the students to work together and collaborate with each other in the decision-making process regarding different tasks over the network. Lab can be used to prepare a conceptual system against a real world system. I adhere to Scholars (Laurillard 2002, Hannafin, 2005) that in order to truly benefit from the potential of the technology to serve a different kind of learning an academic community requires a teaching approach that turns academics themselves into reflective practitioners with respect to their teaching instead of just clinging only to what they already know. This approach demands that the university teachers have to renew and develop their model of the learning process well beyond the traditional transmission model which in turn will shape their teaching, as the new technology requires, as the knowledge industry requires, and as students demand. This approach pushes the academics to become researchers in teaching (long term strategic goal of Luleå university as part of the vision 2020). It will promote the creation of a community that develops a range of designs within which practitioners can craft a variety of contents.

Different perspectives of e-learning on various levels of analysis has been discussed (Koponen, 2009), which include course, institute and society level. It is suggested that department of Computer and Systems science should focuss on our e-learning environment at course level which includes following four perspectives: -

- Pedagogy with learning theories and models (learning process, learning content, learning outcomes, learning models)

- Community and social relations with learning related social theories and models (groups with relations between and within learners, teachers, technologists, ICT related artifacts, and other learning supportive environment)
- Organisation and the overall management with learning related organisation theories and models (organisation and management of the course by learners, teachers and technologists)
- Information and communication technology in relation to learning (ICT related learning environment with hardware, software, platforms, technical standards and human ICT skills enabling and constraining learning)

It is also proposed that the teaching (including lab work plus the theoretical work) in different courses of information security program based on some instructional strategy would help the teachers to gain complete control of the class and achieve course goals. Five main classes of instructional strategies are described (Bednar et al, 1991) which comprises of a. contextualizing instruction, b. activating learning process, c. presenting and cuing content, d. activating and assessing learning outcomes and e. synthesizing and sequencing instructional tactics. The instructional designer needs to understand the instructional situation's demand for the implementation of a strategy by the use of instructional tactics. Even the selection of instructional tactics need to be guided based on the analysis of instructional situation in order to make decisions about different instructional variables, such as learning outcomes, instructional event and the purpose and scope of instruction.

The student feedback from Internet Security course was considered seriously and keeping in view the practical demands of the Internet Security course, following suggestions were made to improve the course in light of analysis using theoretical framework such as:

- The course book of Internet Security is changed to avoid overlapping with any other course in the Information Security Program. The course will focus more on hands-on exercises along-with the theoretical foundations.
- The plan for the lab development is boosted and initially a small ADR team (including a Researcher, Teacher and developer) has been formed which is working for the course development.
- An Online InfoSec lab will be developed based on specific pedagogical approaches, which will be utilized in the Internet Security course.

- The students will be able to conduct their exercises from distance using lab resources.
- To promote active learning appropriate teaching / learning activities should be designed following the notion of constructive alignment to promote constructivism based classroom culture where students will be able to actively participate in different activities both from campus and distance.
- A classroom culture with interactive lectures should be promoted where students should be encouraged to actively participate through different activities such as quizzes which help the students in their meaning making process through collective efforts.

6. DISCUSSION & FURTHER RESEARCH

The graduate program of Information Security offered at Luleå University of Technology is under the process of improvement. In order to evaluate the educational needs for course and e-learning platform development to teach an online program in information security the case of an Internet Security course was considered for analysis. The theoretical framework based on Constructive alignment theory (Biggs 1996) and Conversational framework (Laurillard, 2002) was used to analyze the case. The analysis reveals practical and theoretical problems related to the pedagogical development of the course. The final results of Internet security course also point out that procrastination and low throughput is a major challenge for the teachers. This situation places a huge responsibility on the shoulders of the program management and teachers to provide required facilities and infrastructure both for on-campus and distance learning. Management needs to focus on updating and maintenance of e-learning platform in order to provide standardized services for all the distance students. The situation also demands for the pedagogical alignment and use of e-learning artifacts included in the e-learning program. The course goals were not aligned properly to the teaching / learning activities and assessment methods which hindered the students to achieve those goals properly.

The practical security skills are an important part of the information security curriculum but due to the lack of online information security laboratory students couldn’t keep their interest in the course. The theoretical framework leads our research work for developing our degree program and e-learning platform closely tied to the vision and strategy of Luleå University for 2020, which states that “Our programs are conducted on the campus and as distance courses, and we work for flexible learning that makes use of modern technologies. Independent, active learning that challenges every individual's capacity to meet the future". The theoretical framework provides foundations for pondering on pedagogical development needed to escalate the cognitive skills of information security students in order to enhance their knowledge level. The framework also offers pedagogical guidance for planning and designing courses to keep students actively engaged and at the same time providing them flexible learning facilities. The framework also guides that the "productive" media type could be used to fulfill the demand of students related to practical hands-on experiments by development of an online InfoSec lab, which can be used for constructive purposes. It is proposed that to enhance understanding and providing guidelines to teachers to incorporate the mindset of constructive alignment (Biggs, 1996); the whole program including all the courses should be developed based on explicit pedagogical approaches. All the courses in the MSc information security program should be aligned to the main goal of the program. Following the notion of constructive alignment for good teaching the teachers should specify and align the course objectives, teaching / learning activities and assessments (an assessment method which can realize course objectives). In future the department of Computer and System's Sciences has plans to address all the above-mentioned problems related to Curriculum design and enhancement of e-learning platform which can help to improve quality of teaching, student throughput as well as developing a meaningful and effective e-learning program for Graduate students of Information Security.

The findings suggest that academic community needs to draft the specification for how the new learning technology such as online InfoSec lab should be developed and used in different contexts. For example, as evident from student feedback (see section 4) the practical requirement of a graduate level program such as Msc Information Security requires the development and use of an online InfoSec lab to improve student's hands-on experience. Recently a literature review (Iqbal & Päivärinta 2012) was also conducted to find out how the knowledge regarding online Information security labs has been communicated to the academia and practitioners. The literature review provided an overview of reported instances of online educational information security laboratories. Literature review revealed that articles mostly don't provide any contextualized design exemplars for information security exercises and that technological and pedagogical challenges for online information security labs still need to be discussed in a more precise and detailed manner in order to facilitate real sharing and accumulation of such knowledge. The theoretical framework (section 2) guides us that the online InfoSec lab will act as a productive educational tool for our e-learning platform. It is proposed that the lab must be designed and developed based on pedagogical principles. In this way we can argue for the true benefits of the learning technology being developed for a specific purpose. Hence, learning technology is not considered as merely a knowledge-transmitting tool but viewed as an ensemble artifact (Hannafin, 2005, Sein et al, 2011).

This article attempts to put forward a theoretical framework to provide pedagogical guidelines for alignment of courses and for the selection of suitable e-learning platform. The framework also suggests that exploitation of communicative capabilities (such as narrative, interactive, productive and communicative) of new technologies (such as online InfoSec lab) in different contexts can also help the different stakeholders in an educational institute to provide better input for futuristic design of e-learning platform. According to the researchers (Ton de Jong et al, 2013) physical and virtual laboratories are equally popular in science and engineering education to achieve similar objectives such as developing teamwork abilities, cultivating and promoting conceptual understanding and developing inquiry skills. Looking into the importance of labs the ADR team formed for the design, development and implementation of online InfoSec lab will focus on lab development for different exercises based on different pedagogical approaches such as PSI, CSCL etc. I agree and share the idea with Laurillard (2002) that design of the technology (in this case InfoSec lab) has to be generated from the specific learning objectives and the aspiration of the course rather than the capability of the technology. In the future, specific design exemplars can be developed for enhancing hands-on experiences of students in different contexts and to facilitate different kinds of iterative dialogue between teachers and students. Results of lab based courses will be published in the future which will help to accumulate knowledge in the field of hands-on education of information security.

REFERENCES

1. Bednar, A. K., Cunningham, D., Duffy, T. M., & Perry, J. D.(1991). Theory into practice: How do we link? In G. J. Anglin (Ed.) Instructional Technology: Past, present and future. Englewood, CO: Libraries Unlimited
2. Biggs J. (1996). Enhancing Teaching through Constructive Alignment, Higher Education, Vol. 32 No.3 pp. 347-364
3. Biggs, J.B.(1993). From theory to practice: A cognitive systems approach', Higher Education Research and Development 12, 73-86

4. Cohen, S.A.(1987). Instructional alignment: Searching for a magic bullet, Educational Researcher 16(8), 16-20.
5. Cumming,B., McIntosh, C.(1982). PSI in Engineering Mathematics. Journal of College Science Teaching 12(1) 30-31.
6. De Jong, T., Linn, M.C., Zacharia, Z.C. (2013). Physical and virtual laboratories in science and engineering education. Science 340(6130), 305–308
7. Duffy, T.M. & Jonassen, D. (Eds.), (1992). Constructivism and the technology of instruction: A conversation. Hillsdale NJ: Lawrence Erlbaum Associates
8. Emurian, H., X. Hu, J. Wang, A. Durham.(2000). Learning JAVA: A programmed instruction approach using applets. Computers in Human Behavior. 16(4) 395-422.
9. Hambleton, I. R., Foster, W. H. & Richardson, J. T. E. (1998) Improving student learning using the personalised system of instruction, Higher Education, 35, 187–203.
10. Householder, A., Houle, K., Dougherty, C. (2002).Computer attack trends challenge Internet security, IEEE Comput. 35 (4) 5–7
11. Iqbal, S. and Päivärinta, T.(2012). Towards a design theory for educational on-line information security laboratories. In: Popescu, E., Li, Q., Klamma, R., Leung, H., Specht, M. (eds.) ICWL 2012. LNCS, vol. 7558, pp. 295–306. Springer, Heidelberg
12. Jim Flowers, (2001). Online Learning Needs in Technology Education. Journal of Technology Education volume 13, number 1.
13. Keller, F.S.(1968). Good-bye, teacher... Journal of Applied Behavior Analysis. 1(1) 79.
14. Koen, B.V.(1971). Self-Paced Instruction in Engineering: A Case Study. IEEE Transaction on Education Volume 14(1) p.24-31.
15. Koponen, E.(2009). The development, implementation and use of e-learning: critical realism and design science perspectives. Akateeminen väitöskirja. Tietojenkäsittelytieteiden laitos. Tampereen yliopisto. Verkkojulkaisu http://acta.uta.fi/pdf/978-951-44-7590-0.pdf
16. Laurillard, D.(2002). Rethinking teaching for the knowledge society. EDUCAUSE review, January/February. Available online: http://www.educause.edu/ir/library/pdf/erm0201.pdf
17. Marton, F. (1981). ’Phenomenography – Describing conceptions of the world around us ’, Instructional Science, 10, 177-200
18. Morita, Y., J. Kenne, A. Johendran, Z. Wu, G. Ma, M. Nakayama, A. Nishihara, B. Koen. (2005). Pilot Study of International Web-

Based PSI Course between Japan and US. Proceedings of the 21st Annual Conference of Japanese Society of Educational Technology (JSET) September 23rd at University of Tokushima, Japan.

19. Morita, Y., J. Kenne, A. Nishihara, M. Nakayama, B.V. Koen.(2006). Implementation of an International Web-Based PSI Course: A Case Study. 36th ASEE/IEEE Frontiers in Education Conference, San Diego, CA, p.14-18.
20. Nilsen, H., E.Å. Larsen. (2011). Using the Personalized System of Instruction in an Introductory Programming Course. In the proceedings of 18th NOKOBIT Conference, University of Tromsø, p.27-38.
21. Pear, J., D. Crone-Todd.(1999). Personalized system of instruction in cyberspace. Journal of Applied Behavior Analysis. 32(2) 205.
22. Pear, J.J., M. Novak.(1996). Computer-aided personalized system of instruction: A program evaluation. Teaching of Psychology 23(2) 119-123.
23. Pratt, D. (1980). Curriculum design and development. New York: Harcourt Brace Jovanovich.
24. Queeney, D.S. (1995). Assessing needs in continuing education. SF: Josey – Bass.
25. Richardson, V. (2003). Constructivist Pedagogy. Teachers College Record volume 105, Number 9, pp. 1623-1640
26. Sein M, Henfridsson O, Purao S, Rossi M, Lindgren R.(2011).Action design research, MIS Quarterly, Vol 35 (2)
27. Srikwan, S., and Jakobsson, M. (2007), "Using Cartoons to Teach Internet Security," DIMACS Technical Report 2007-11. www.informatics.indiana.edu/markus/documents/security-education.pdf
28. Steffe, L. And Gale, J. (eds) (1995). Constructivism in Education. Hillsdale, NJ: Erlbaum.
29. Suranjith and Amina, (2005), Internet security games as a pedagogic tool for teaching network security, IEEE.
30. Von Bertalanffy, L.(1968). General Systems Theory. New York: Braziller.
31. Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. Educational Technology Research & Development, 53(4), 5–23

C INITIAL DESIGN PRINCIPLES FOR AN EDUCATIONAL, ON-LINE INFORMATION SECURITY LABORATORY

Sarfraz Iqbal, Devinder Thapa

Department of Computer Science, Electrical and Space Engineering

Luleå Tekniska Universitet, Luleå, Sweden.

{sarfraz.iqbal, devinder.thapa} @ltu.se

Abstract. E-Learning systems should be based on systematic pedagogical approaches and well-designed procedures and techniques. However, current literature on several areas of technology-enhanced learning environments, such as online information security (InfoSec) laboratories still lack well-specified pedagogical approaches and concrete design principles. In information security education, hands-on lab exercises play a major role in learning. Distance education brings in new challenges as the hands-on exercises require now virtual labs, which need to be accessible anywhere and often also anytime. This creates technological and pedagogical challenges, which are not fully understood in terms of explicit design principles that would enhance implementation and use of on-line educational labs. To contribute to this knowledge gap the paper describes five initial design principles: contextualization, collaboration, flexibility, cost-effectiveness, and scalability. The principles are based on a literature review, contextual interviews and observations at a European University. The initial concretization of the principles adopts the pedagogical approach of Personalized System of Instruction (PSI), which is deemed to represent a good fit to the contextual goals for developing on-line security labs in the context of the target university. Further research for actual design of virtual InfoSec labs, adopting the action design-based research tradition to develop learning environments, is needed in order to concretize, to test and to elaborate these design principles.

Keywords: Design Science Research (DSR), Online Information Security Lab, Design Principles, E-learning platform

1. Introduction

To match the benefits with traditional learning environments, a successful e-learning system must be designed and constructed carefully, based on well-grounded pedagogical principles and robust design guidelines [1]. In the field of information security many courses provide little hands-on practice that can be applied to thoroughly securing real world applications from various threats that exist today [2]. Similarly, the lab experiments are often not available to distance students that represent a critical challenge in offering an online information security program which is considered to include plenty of hands-on practices in addition to theoretical lectures [3].

E-learning must be rooted in systematic pedagogical approaches in order to make it effective [4]. Furthermore, the importance of creating a link between theory and practice in order to design and develop an instructional system is also emphasized [4, 5]. However, effective design is possible only if the developer has a reflexive awareness of the theoretical basis underlying the design [6, 7]. To contribute to the similar research strand, the paper proposes initial design principles to design, develop, implement, and test e-Learning platform for information security. The example of information security laboratory is used to explain the systematic process; however the actual installation of the lab will be reported in the future papers.

The rest of the paper is arranged as follows. The next section provides overview of theoretical framework based on Action Design Research (ADR) method. Section 3 summarizes background and problem formulation. Section 3.1 briefly describes the selected pedagogical approach. Furthermore, we discuss the contribution of the research work in section 4. Finally, Section 5 concludes the paper with future research agenda.

2. Design Research for Developing an e-Learning Platform for Information Security Labs

Existing literature shows that most of the literature is focused on the technical implementations of labs, whereas, ignored the pedagogical elements of the curriculum and rationale behind them [8]. It leads to improper guidance about how the instructor and the learner can make use of the platform. There are a few examples of using design science in developing e-learning platforms, such as Cybernetic e-Learning management model applied to a (case study of BMW group) [9], Business Process Management e-learning program [10], user defined and controlled virtual learning environment [11], and Synchronous e-learning [12]. In addition, a didactical framework for the design of blended learning arrangements is proposed with a focus on identifying the right blend for the communication component in the context of a distance education program considering expenditures [13].

However, these frameworks cannot be generalized based on the fact that different stakeholders evaluate communication tools and scenarios differently. Tel and Thomas [14], analyzed technology as a process and as a value-laden system arguing that design-based research can address some of the deficiencies of other research methods in investigating the role of tools and techniques in the classroom to impact educational practice. Our research adheres to the similar stance where general absence of methodically designed online InfoSec labs is evident.

Keeping in view the strategic objectives and practical demands of the future related to provision of hands-on exercises in different courses in InfoSec program a road map in the form of initial design principles to develop a security lab is proposed. The paper will use an example of InfoSec lab to describe the laboratory building, intervention, and evaluation process.

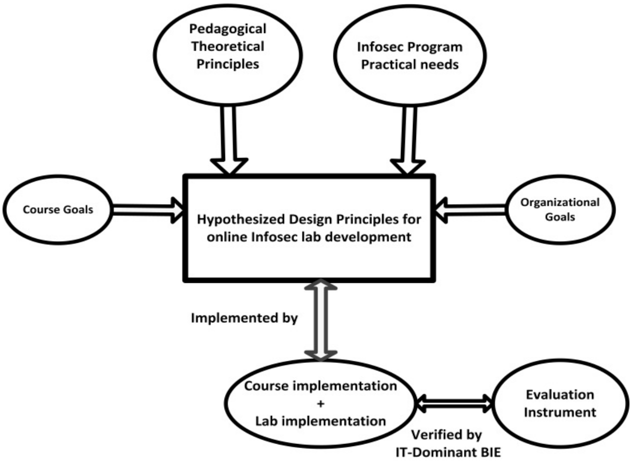

Pedagogical Theoretical Principles
Infosec Program Practical needs
Course Goals
Hypothesized Design Principles for online Infosec lab development
Organizational Goals
Implemented by
Course implementation + Lab implementation
Evaluation Instrument
Verified by IT-Dominant BIE

Figure-1 DSR based Framework for development of e-Learning platform

As shown in the figure-1, the technological, pedagogical, and organizational goals interact during design of e-learning platform (online InfoSec lab). The platform in this context is conceptualized as an ensemble IT artifact [15], because the design outcome is a result of emergent perspective on design, use, and refinement in the actual context. As suggested by [16] and looking at the emergent nature of the platform, the framework suggests employing Action Design Research (ADR) method for laying the roadmap. ADR is a typical design research method representing the view of continuous stakeholder participation in the research project [17]. At the same time, different stakeholders examine the propositions iteratively together with researchers to define and redefine options for the design.

ADR is defined as a research method which generates prescriptive knowledge through building and evaluating ensemble IT artifacts by addressing a problem situation encountered in a specific organizational setting through intervention and evaluation. Moreover, ADR method emphasizes on the development, intervention and evaluation of an IT artifact which also imitates theoretical grounds. Contrary to the traditional design research methods, ADR promotes design and development of IT artifacts based on the organizational context. For example, this research is motivated by an ongoing initiative to design and develop an online InfoSec lab at the University to address the contextual needs of the Msc Information security program.

After clarifying the contextual issues, the hypothesized design principles will guide the initial development of online InfoSec lab based on problem framing and theoretical premises adopted in stage one e.g. InfoSec program's practical needs, course goals, organizational goals and the pedagogical principles laid down based on a kernel theory will inform the initial design theoretically.

Going along the ADR process, the next stage starts with the BIE (Building, Intervention and Evaluation). Two different types of BIE processes are identified in ADR (1) IT-dominant BIE, (2) Organization dominant BIE [17]. The IT-Dominant BIE process supports the continuous instantiation and testing of emerging artifact as well as the theories ingrained in it via organizational intervention subject to the assumptions, expectations and knowledge of the participating members. The organization dominant BIE deploys the artifact early in the organization in the design iterations where ADR team challenges organizational participant's existing ideas and assumptions regarding artifact's specific use context to improve the design.

In this context, the framework suggests the IT-Dominant BIE process [17] for online information security lab development. The lab will be implemented in different courses for some specific exercises which could be based on a variety of pedagogical approaches in order to achieve pre-defined course objectives via testable propositions (cf. Gregor &jones, [18]). The testable propositions will be guided by hypothesized design principles.

Thereafter, an evaluation instrument will be designed in order to have authentic and concurrent evaluation of the implemented design (evaluation details will be reported in the future work). Evaluation is a crucial [19] and significant activity [20] which plays central role in conducting rigorous Design science research. Evaluation puts [21] the science in Design Science by examining its research productions because without evaluation there is no surety that the designed artifacts will work in a useful manner to solve some problems. A research stream [9, 19, 21, 22, 23, 24] suggests that Design Science Research projects should establish a clear evaluation strategy through an evaluation constituent of their Design science research which will explain the questions of what to evaluate, when to evaluate and how to evaluate. The evaluation methods will unfold the rigor hidden in the utility, quality and efficacy of a designed artifact [19].

The evaluation strategy in aforementioned project should be based on the following two purposes in order to evaluate product artifact (online InfoSec lab) and relevant process artifact (methods, procedure to accomplish some tasks) [21]:

- Evaluate a designed artifact formatively to identify weaknesses and areas of improvement for an artifact under development.
- Evaluate an instantiation of a designed artifact to establish its utility and efficacy (or lack thereof) for achieving its stated purpose.

3. BACKGROUND & PROBLEM FORMULATION

To illustrate the systematic process of building and implementing InfoSec lab, we present a case of a European University. The Luleå Tekniska University lately noticed an increase in the number of distance students who want to study Msc in Information Security. Most of the distance students are professionals who also want to work and practice their study individually at times and in places which suit them. As the university stated in its vision and strategy of 2020, "Our programs are conducted on the campus and as distance courses, and we work for flexible learning that makes use of modern technologies. Independent, active learning that challenges every individual's capacity to meet the future." Likewise, the interviews with the management personnel and perusal of the strategic planning documents of University helped to obtain a clear organizational perspective regarding research and education at Computer and systems science department. In addition to the above mentioned strategic objectives and visions the management is also interested in finding ways to address the following issues:

- How to increase the student throughput in different courses of the program?
- How to facilitate flexible learning?

As a process of program improvement in the department of computer and systems science, we planned interviews with all the staff members (teachers) involved in teaching different courses in Msc Information Security program and the program management (to obtain the organizational perspective). One of the authors of this article conducted interviews (semi-structured open ended) with the teachers and the management to gather details about their teaching experience in the field of information security as well as focusing on the practical needs of the degree program. The interviews included discussions on issues such as:

- Instructional strategy, or tactics for teaching
- Need of any specific pedagogical approaches for teaching InfoSec courses
- Major challenges related to teaching courses in InfoSec education program
- Use of any lab for hands on education in information security
- Practical demands of the Information security degree program
- Challenges related to practical needs of the program
- Suggestions for the program improvement

The results of the interviews with the teachers showed that most of them don't follow any specific pedagogical approach or instructional strategy. They are not using any InfoSec lab for practical work in different courses of graduate program, although they assign students different exercises to conduct at their own computers. The students were unable to practice their security skills practically due to the fact that an InfoSec lab is not available at the moment. This fact was also highlighted by the comments given by some of the participants where they stated that there was a gap between the theoretical and practical aspects of the program as the program focused more on the theoretical aspects while not focusing on practical skills at large. The focus of the program has been on management related theoretical issues in the past but now there are plans to address the technical aspects of information security through changes in different course structures. Almost every participant showed interest in the development of an online InfoSec lab to facilitate students regarding practical work in different courses.

The interviews revealed that the university in general and the systems science department in particular, want to improve the graduate program of information security in a systematic manner. To achieve the objectives, the following action plan is set forth:

- To develop an effective and meaningful E-learning program for the distance as well as campus students.
- To introduce an online InfoSec lab for the students where they can practice their security skills flexibly from distance according to the practical demands of the course.

The interviews with teachers as well as program committee suggests that an online InfoSec lab based on explicit pedagogical principles should be developed in order to facilitate students to practice their security skills and also to maintain a balanced situation between the theoretical and practical aspects of the degree program in information security. To address this issue, a literature review is conducted in order to understand the design principles related to online InfoSec labs and how the knowledge regarding design and development of such labs has been communicated to the community (see table-1 and ref[8]). The sample of articles mentioned in table-1 was further scrutinized in order to answer the questions; such as does the existing literature provide any explicit design principles for online InfoSec lab development? What type of pedagogical model, learning theory or scientific method has been used for the development of online InfoSec lab to conduct hands-on education?

The review shows that there is a lack of systematic approach in design, development, implementation, and evaluation of InfoSec lab. Likewise, none of the articles studied provides any details of lab development that is based on design science principles [8, 18]. The review shows the gap of knowledge in the field of design and development of online InfoSec labs. None of the articles studied for review purpose (table-1) demonstrated any explicitly described design principles based on a specific design research method. The review also shows the lack of any pedagogical model, learning theory and scientific method trailed for the design and development of online InfoSec laboratories. Only one article [25] adhered to an explicit pedagogical idea, the cooperative learning strategy. The general absence of scientific methods shows that the systematic development has not been adopted leaving a gap between theory and practice related to the development of e-learning platform for hands-on education of information security. To contribute to this gap we propose that the lab design and development should be based on the design principles in order to truly communicate, justify and accumulate knowledge in the field of hands-on education of information security.

Table 1. Literatur review for Design Principles, Pedagogy, Learning theory and Scientific method.

Ref No.	**Design Principles**		**Pedagogy**	**Learning Theory**	**Scientific Method**
	Implicit Focus	**Explicit**			
[26]	Provision of hands-on practice for security mechanisms	-	-	-	-
[27]	Provision of hands-on practice for computer security	-	-	-	-

	and system administration.				
[28]	A platform to experiment in a networked environment.	-	-	-	-
[29]	Remotely accessible Laboratory teaching environment.	-	-	-	-
[30]	Providing hands-on practice to students	-	-	-	-
[31]	Logical isolation of networks for experimentation	-	-	-	-
[32]	Improve student's access to University resources	-	-	-	-
[33]	Virtual computer lab for teaching online IA classes	-	-	-	-
[34]	Providing remote user access to computing resources	-	-	-	-
[35]	Feasibility of Virtual security lab for distance education	-	-	-	-
[36]	Centralized remote lab services	-	-	-	-

[3]	Remote lab for IDS/IPS education programs	-	-	-	-
[2]	Building a research application that mimics fully functional online bookstore	-	-	-	-
[25]	Developing a portable virtual laboratory	-	CLS	-	-

3.1 Pedagogical Approach to Support Problem Formulation

Based on the problem formulation stage the second stage of ADR leads to building, intervention and evaluation (BIE) of InfoSec lab as described in section-2. As we argued that the InfoSec lab should be based on pedagogical approach; in this context, looking at the course goal and students' requirement, such as individualized flexibility, personalized system of Instruction (PSI) [37] can be utilized as pedagogical approach. PSI is considered a pedagogical approach which can help to develop individual and flexible learning environments. The PSI approach enhances individualized learning by facilitating the students to learn and advance in their studies at their own pace. The distinct features of PSI are:

- Division of course content into smaller modules / units
- Flexibility (study at your own pace)
- Mastery of the course unit / module
- Use of Teacher, Assistant / Proctor

The objective of the InfoSec lab is to provide students with individual and flexible learning environment for hands-on practices in a course of "Information Security". The pedagogical approach however can be varied in various situations. In this paper, the approach is suggested in light of the contextual factors such as organizational goals, course goals, practical needs of the InfoSec program obtained through perusal of organizational policy documents, observation and interviews with program management and teachers.

4. Design Principles

The paper explains how the research regarding the actual design, development, implementation and maintenance of e-learning platform in general and InfoSec labs in particular should be conducted; as we want that the research should be based on a systematic process. The researchers in the field of design research should be responsible to create standards that make design experiments recognizable and accessible to other researchers [38]. The research approach selected here is coherent with [4] that e-learning in information security should be based on a theory-into-practice framework that characterizes the instructional implications of situated cognition and guides the design of e-learning. Developing such a model for e-learning purposes emphasizes on the interaction between pedagogical models, instructional strategies and learning technologies to facilitate meaningful learning and knowledge building. We concur. To contribute to this argument we conducted interviews, observations, literature reviews, and reflected on the pedagogical approach i.e. PSI. Consequently, we derived five design principles (see table 2), in which, principle 1 and 2 along-with ADR principles provide guidelines for the design and development (research process) of the InfoSec lab, whereas, principle 3, 4 and 5 are the principles of InfoSec lab itself that help to derive attributes for the lab. The design principles are discussed as follows.

Table 2. Initial Design principles for Online-lab development

Design Principles	Impact
Contextualization	Organizational Goals, course goals, Teacher goals, constraints, requirements
Collaboration	Researcher (acts as Instructional designer), Practitioners (Developer, IT staff) End users (Teachers, proctor, Students)
Flexibility	Remote access to lab resources Lab Should be accessible to students 24x7.
Cost-effectiveness	Optimal resource allocation
Scalability	Lab can be upgraded and easily modified based on practical requirements of different courses.

Design Principle #1: Contextualization

The principle #1 refers to the contextual factors that we need to consider while building and implementing InfoSec lab based on PSI principles, such as organizational goals (To implement hands-on exercises for distance students, flexible learning), course goals (To improve student's practical knowledge level, provide students individual hands-on exercises) teachers' goals (Efficiency in terms of consuming less time than traditional teaching method with the help of an Assistant / Proctor), resource constraints (available funding) and practical requirements. Contextualization provides meaning to goals and communicates the means for interpreting the environment where the activity takes place [39].

Design Principle #2: Collaboration

The principle #2 refers to the collaboration among researcher, practitioner, and end users to design and develop effective artifact. This principle also contributes to principle #1 in defining the context. By applying ADR collaboration among the community (e.g. researchers, developers, administrative staff, teachers and students) can be promoted. The ensemble artifact in this way will emerge through an interdisciplinary and collaborative effort of experts from different fields [40].

Design Principle #3: Flexibility

The principle #3 based on PSI approach refers to the remote access to lab resources, for instance lab should be accessible for experiments from everywhere any time in order to facilitate the students who are professional, want to work individually and cannot work under a strict schedule (go at your own pace). Most of the literature reviewed (see table-1) implicitly focused on provision of flexibility such as remote access to students. Technologies like virtualization can be applied to provide remote access to multiple single-user & multi-user computer systems and multiple virtual machines [35]. The flexibility principle in this case also refers to the configuration of the information security lab based on the particular context. As we can see the context can be understood through applying principle #1 and #2.

Design Principle #4: Cost-effectiveness

The principles #4 refer to the availability of resources, such as fund, technology, and human skills. Existing literature on InfoSec labs demonstrates that virtualization technologies such as VNC Server, VNC client, VMware workstation, VMware server, Vlab Manager, VPN Concentrator, Virtual center, Apache Virtual Computing lab, Microsoft HyperV, Xen, and VMLogix Lab Manager [27,33,34,36] are considered an important element of InfoSec labs which provide such benefits as lower hardware cost, increased deployment flexibility, simplified configuration management, customization of software & hardware resources, increased accessibility of computing resources, system administration and ease of isolating the virtual networks [28,30,32,34]. The existing solutions, such as virtualization technologies can be utilized to make the lab more cost-effective. Existing researches support this principle by stating that the configuration costs of Virtual labs are far less expensive compared to physical labs [35].

Design Principle #5: Scalability

The principles #5 refers to the scalability, which depends on factors such as need to extend the lab resources if more students than expected appear in a course, lab up-gradation based on introduction of a new and better technology etc. As the observation shows that the information security graduate program is getting popular and the number of students is increasing. To accommodate this influx of the student, scalability of the lab facility should be considered while building, intervention and evaluation of the lab. For example, If there are 30 students in a class and they will work with exercises individually (based on PSI approach), the setting of lab resources will be different from a situation when they are working in groups of 2 or 3 students. Virtualization technologies help to make virtual lab easily scalable compared to physical lab [35].

5. Conclusion

The main objective of this paper is to promote research based hands-on teaching in the field of information security which will not only benefit the university to have an experienced research based group of teaching staff members but also will help the academic community by continuously adding new information based on educational experiments and experiences with online InfoSec labs. In a longer run, attempting to achieve a full fledge design theory in the field of hands-on education through online InfoSec labs should be the goal as design theories also helps to provide prescriptions for the development of specific applications. It is generally accepted that “Ultimately a full design theory is often seen as the goal of design research and the key exemplars develop full theories” [41].

In this paper the review of the prior research and preliminary interviews with teachers and program management on the development of online InfoSec labs lead us to formalize five design principles: *contextualization, collaboration, flexibility, cost-effectiveness, and scalability*. These initial design principles will guide the research process which will ultimately help us to achieve a refined set of emergent design principles.

The paper intended to implement online InfoSec labs for hands-on education in information security. While implementing the lab hypothesized design principles will be tested through testable proposition that will help to validate instructional applications in different perspectives. The lab will be designed and developed in Luleå University that offers an MSc Program in Information Security to both on campus and distance students since 2007. This is our agenda for future research.

References:

1. Gunasekaran, A., Mcneil, R.D. and Shaul, D.: E-learning: research and applications. Industrial and Commercial Training 34, 44-53. (2002)

2. Crawford, E., Hu, Y.: A Multi-User Adaptive Security Application for Educational Hacking. In: Proceedings of the World Congress on Engineering and Computer Science, WCECS 2011, vol. I, San Francisco, USA, October 19-21 (2011)

3. Lahoud, H.A., Tang, X.: Information Security Labs in IDS/IPS for Distance Education. In: SIGITE 2006, Minneapolis, Minnesota, USA, October 19–21, pp. 47–52. ACM (2006)

4. Dabbagh, N.: Pedagogical models for E-Learning: A theory-based design framework. International Journal of Technology in Teaching and Learning 1, 25-44 (2005)

5. Bednar, A.K., Cunningham, D., Duffy, T.M. and Perry, J.D.: Theory into practice: How do we link. Constructivism and the technology of instruction: A conversation 17-34 (1992)

6. Bednar, A. K., Cunningham, D., Duffy, T. M., & Perry, J. D.: Theory into practice: How do we link? In G. J. Anglin (Ed.), Instructional Technology: Past, present and future. Englewood, CO: Libraries Unlimited (1991)

7. Wang, F., & Hannafin, M. J.: Design-based research and technology-enhanced learning environments. Educational Technology Research & Development, 53(4), 5–23 (2005)

8. Iqbal, S. and Päivärinta, T.: Towards a design theory for educational on-line information security laboratories. Advances in Web-Based Learning, 295-306 ICWL (2012).

9. Hilgarth, B.: E-Learning Success in Action! From Case Study Research to the creation of the Cybernetic e-Learning Management Model, IJCISIM Journal, Vol 3, pp. 415–426 (2011)

10. Johannes Kröckel and Bernd Hilgarth.: BPM @ KMU – Designing e-Learning for the Introduction of BPM in Small- and Medium –Sized Enterprises, S-BPM ONE 2011, CCIS 213, LNCS pp. 34–47, (2011)

11. Thoms, B., Garrett, N., & Ryan, T.: Online learning communities in the new "U". International Journal of Networking and Virtual Organisations, 6(5), 499-517 (2009)

12. Stefan Hrastinski, Christina Keller and Sven A. Carlsson.: Design exemplars for synchronous e-learning: A design theory approach. Computers & Education 55 652-662 (2010)

13. Michael Kerres & Claudia De Witt.: A Didactical Framework for the Design of Blended Learning Arrangements, Journal of Educational Media, 28:2-3, 101-113 (2003)

14. Tel Amiel & Thomas C. Reeves.: Design-Based Research and Educational Technology: Rethinking Technology and the Research Agenda. Educational Technology & Society, 11(4), 29-40 (2008)

15. Orlikowski, W. J.: Improvising Organizational Transformation Over Time: A Situated Change Perspective, Information Systems Research (7:1), pp. 63-92 (1996)

16. Dan Harnesk and Devinder Thapa.: A Framework for Classifying Design Research Methods, In proceedings of DESRIST, LNCS 7939, pp.479-485 (2013)

17. Sein M, Henfridsson O, Purao S, Rossi M, Lindgren R.: Action design research, MIS Quarterly, Vol 35 (2) (2011)

18. Gregor, S. and Jones, D.: The anatomy of a design theory. Journal of the Association for Information Systems 8, 312-335 (2007)

19. Hevner, A. R., March, S. T., Park, J., & Ram, S.: Design Science In Information Systems Research. MIS Quarterly, 28(1), 75-105 (2004)

20. Pries-Heje, J., Venable, J. and Baskerville, R.: Strategies for Design Science Research Evaluation. In Proceedings of the 16th European Conference on Information Systems Galway, Ireland, 9-11 June (2008)

21. Venable, J., Pries-Heje, J. & Baskerville, R.: A Comprehensive Framework for Evaluation in Design Science Research. In: K. Peffers, M. Rothenberger & B. Kuechler, eds. Design Science Research in Information Systems. Advances in Theory and Practice, Springer Berlin / Heidelberg: Springer, pp. 423-438 (2012)

22. Checkland, P., Scholes, J.: Soft Systems Methodology in Practice. J. Wiley, Chichester (1990)

23. March, S.T., Smith, G.F.: Design and natural science research on information technology. Decision Support Systems 15, 251–266 (1995)

24. Walls, J.G., Widmeyer, G.R., El Sawy, O.A.: Building an information system design theory for vigilant EIS. Information Systems Research 3, 36–59 (1992)

25. Chen, F.-G., Chen, R.-M., Chen, J. -S.: A Portable Virtual Laboratory for Information Security Courses. In: Lin, S., Huang, X. (eds.) CSEE 2011, Part V. CCIS, vol. 218, pp. 245–250. Springer, Heidelberg (2011)

26. Aboutabl, M.S.: The Cyberdefense Laboratory: A Framework for Information Security Education. In: Proceedings of the IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, pp. 55–60 (2006)

27. Wang, X., Hembroff, G.C., Yedica, R.: Using VMware VCenter Lab Manager in Undergraduate Education for System Administration and Network Security. In: Proceedings of the ACM Conference on Information Technology Education, pp. 43–52 (2010)

28. Krishna, K., Sun, W., Rana, P., et al.: V-NetLab: A Cost-Effective Platform to Support Course Projects in Computer security. In: Proceedings of the 9th Annual Colloquium for Information Systems Security Education (CISSE 2005), Atlanta, GA, June 6-9 (2005)

29. Li, C.: Blur the Boundary between the Virtual and the Real. Journal of Computing Sciences in Colleges 24, 39–45 (2009)

30. Gaspar, A., Langevin, S., Armitage, W., et al.: The Role of Virtualization in Computing Education. In: Proceedings of the 39th SIGCSE Technical Symposium on Computer Science Education, pp. 131–132. ACM, New York (2008)

31. Weiqing Sun, Varun Katta, Kumar Krishna, and R. Sekar.: V-netlab: an approach for realizing logically isolated networks for security experiments. In Proceedings of the conference on Cyber security experimentation and test, Berkeley, CA, USA pp. 1-6 (2008)

32. Burd, S.D., Seazzu, A.F., Conway, C., et al.: Virtual Computing Laboratories: A Case Study with Comparisons to Physical Computing Laboratories. Journal of Information Technology Education 8, 24 (2009)

33. Summers, W.C., Martin, C.: Using a Virtual Lab to Teach an Online Information Assurance Program. In: Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, pp. 84–87. ACM, New York (2005)

34. Burd, S.D., Gaillard, G., Rooney, E., et al.: Virtual Computing Laboratories using VMware Lab Manager. In: Proceedings of the 44th Hawaii International Conference on System Sciences, pp. 1–9. IEEE (2011)

35. Choi, Y.B., Lim, S., Oh, T.H.: Feasibility of Virtual Security Laboratory for Three-Tiered Distance Education. In: Proceedings of the

ACM Conference on Information Technology Education, pp. 53–58 (2010)

36. Li, P., Toderick, L.W., Lunsford, P.J.: Experiencing Virtual Computing Lab in Information Technology Education. In: Proceedings of the 10th ACM Conference on SIG-Information Technology Education, SIGITE 2009, Fairfax, Virginia, USA, October 22–24, pp. 55–59. ACM (2009)

37. Keller, F.S.: Good-bye, teacher... Journal of Applied Behavior Analysis. 1(1) 79 (1968).

38. Collins, A., Joseph, D., & Bielaczyc, K.: Design research: Theoretical and methodological issues. Journal of the Learning Sciences, 13(1), 15–42 (2004)

39. Lauri Saarinen.: Enhancing ICT Supported Distributed Learning through Action Design Research. Doctoral Dissertations, Aalto University, School of Economics (2012)

40. Iivari, J.: The IS core-VII: Towards information systems as a science of meta-artifacts. Communication of the association for Information Systems (12:1) (2003)

41. Matti R., Sandeep P., Maung K. S.: Generalizating from design research. International workshop on IT Artefact Design & Workpractice Intervention, Barcelona (2012)

D TOWARDS PERSONALIZED SYSTEM OF INSTRUCTION FOR EDUCATIONAL ONLINE INFORMATION SECURITY LAB EXERCISES: RESEARCH-IN-PROGRESS

Sarfraz Iqbal, Todd Booth, Tero Päivärinta

Department of Computer Science, Electrical and Space Engineering

Luleå Tekniska Universitet, Luleå, Sweden.

{sarfraz.iqbal, todd.booth, tero.päivärinta} @ltu.se

Abstract

Information Security education benefits greatly from hands-on laboratory oriented exercises. Campus students often have access to security lab equipment. However, remote students, who never visit the campus, often have no laboratory access at all. While previous literature describing designs for information security laboratories are seldom based on specified pedagogical approaches or systematic design theories, this paper contributes by outlining a design theory of online InfoSec labs based on the "Personalized system of instruction" (PSI). We also illustrate the PSI-oriented approach to on-line information security education with help of design suggestions and general level evaluation measures.

Key words: PSI in Information security, PSI security lab exercise, Personalized system of instruction

1. INTRODUCTION

The MSc program in Information Security (InfoSec) at Luleå University of Technology, has been offered to both on campus as well as distance students since 2007. As part of the program improvement, we are planning to introduce course concepts, based on a hands-on, on-line information security lab (InfoSec Lab), starting in August, 2012. An information security student at Master's level is supposed to be capable of analyzing security flaws, proposing proper solutions, and learning in-depth analytic / experimental techniques (Yurcik & David 2000). An online lab will allow the distance (as well as the campus) students to perform related hands-on Security Lab exercises.

A variety of pedagogical strategies can be used to develop online laboratories for information security. On the one hand, a cooperative learning strategy for information security classes has been suggested (Chen et al 2011). On the other hand, a good number of the distance students may want to study individually and flexibly. However, a recent literature review on pedagogical, on-line InfoSec Labs revealed that few of the documented solutions were, in the first place related to any explicitly described pedagogical approaches, whereas none of the reported solutions leaned on a pedagogical strategy targeted for individual and flexible learning processes (Iqbal & Päivärinta 2012). The Personalized System of Instruction (PSI) (Keller 1968) is a pedagogical approach, which could help to develop such individual and flexible learning environments. While the PSI approach has been widely applied to university courses, institutions and disciplines (Price 1999), the focus of this paper is to present a PSI-based design of an online information security course, including on-line laboratory, for individual students based on Keller's PSI approach (Keller, 1968).

A few articles (Krishna et al 2005, Summers & Martin 2005, Aboutabl 2006, Lahoud & Tang 2006, Li et al 2009, Choi et al 2010, Crawford & Hu 2011) include discussions about the exercises for information security labs. These discussions are more or less of general nature, providing little detail of the structure of exercises or designs of the labs. The above mentioned articles rarely provide any detailed discussions about justificatory knowledge (Gregor & Jones 2007) for the pedagogical development of these exercises and the structure of the InfoSec Lab which is an important part of the design theory. They seldom refer to each other's work regarding exercises development which is also in contrast to the principles of design theory. None of the articles discuss about a complete design theory (Iqbal & Päivärinta 2012). This situation implies that researchers and practitioners still need guidance about when and how to use the e-learning techniques in the field of online InfoSec Lab development. We believe that developing a design theory of online InfoSec Lab based on an explicitly described pedagogical approach will provide the basis for the accumulation of knowledge in this field.

Individualized learning based on the PSI approach permits the students to learn and advance in their studies at their own pace. Without the PSI, teachers generally provide classes with general instruction information. With the PSI, teachers provide students with specific instruction information, based on each student's knowledge level. Thus PSI transforms the role of teacher as the facilitator and increases the student's own involvement and participation in study (Keller 1968). Bostow et al (1995) suggest that teachers should arrange more precise and frequent instructional contingencies in order to produce the changes needed to sustain good teaching and learning. Balta et al (2009) suggest that personalization can draw the student's attention and also promises considerable benefits to learning such as improving information security student's cognitive skills to develop good defenses against system vulnerabilities.

The rest of the paper is arranged as follows. The next section summarizes background and key features of the PSI approach. Section 3 provides overview of proposed design theory framework for course development. Section 4 summarizes objectives, details of the design of InfoSec lab and course Topics. Section 5 briefs about evaluation measures for stated objectives. We discuss about the contribution of our research work in section 6, whereas the last part provides conclusion and further research ideas.

2. BACKGROUND AND KEY FEATURES OF PERSONALIZED SYSTEM OF INSTRUCTION

As a behaviorist Keller believed in the teacher's duty to improve student's learning. PSI originated in psychology and has also been used in different other educational domains. In the field of Psychology, Pear & Novak (1996) discussed the use of a computer-aided personalized system of instruction program in two undergraduate psychology courses whereas Pear & Crone-Todd (1999) presented the results of four undergraduate second year courses in the field of Psychology based on Computer-Aided PSI teaching method. The researchers recognized that this approach is highly beneficial for students studying from distance and the student's reaction shows that they like the convenience of "not having to attend classes, being able to work at their own pace and being free to work on the course when and where they chose" (Pear & Novak 1996).

PSI has also been used in the field of Engineering e.g. researchers utilized PSI in the courses of engineering and engineering mathematics (Koen 1971, Cumming & McIntosh 1982). Later on, an international web-based PSI course was proposed by Morita et al (2005) focusing on two major factors affecting presence: 1- the choice of pedagogical strategy and 2- its implementation. The implementation of the PSI in international web-based PSI courses (Morita et al 2006) proved to be successful experience with minor problems related to motivation and network issues.

The PSI approach has also been used in programming courses (Emurian et al 2000, Nilsen & Larsen 2011). The research results show that students learn more with this type of approach but it was also noted that procrastination became a problem especially for weaker students (Nilsen & Larsen 2011). The discussion about the usage of PSI approach in different domains of education demonstrates that the PSI approach has potential to produce positive results regarding student's learning. Literature search using different search engines reveals that the PSI has not been used or implemented before to teach hands-on education in information security to graduate level students.

The distinct features of the PSI (Keller 1968) are as follows: -

- Division of course content into smaller modules / units
- Flexibility (study at your own pace)
- Mastery of the course unit / module
- Use of Teacher, Assistant / Proctor

An important feature of the PSI approach is to divide the course into small units / modules (Keller, 1968). The students need to show a certain level of mastery for lower level modules / units before proceeding to the next level. Mastery or perfection of a learning unit fits well with our plans of improving the knowledge level of students of our information security program.

The basic premise of the PSI is on the flexibility provided to the student where he / she have full control of the speed of study (the go-at-you-own-pace feature). The students have no strict schedule but they can follow the course on their own speed (Keller 1968). We will allow students flexibility; however they still must complete the course by the course deadline or they have to voluntarily leave the course. This flexibility feature is very important for students who are working and who want to also participate in distance courses.

The teaching staff of the course according to Keller's plan (1968) can include an instructor and proctors / assistants. As at the time when the Keller plan has been developed computer aid was not available to the extent where it is today and human roles were needed for streamlining the routine – like feedback procedures; therefore, we have plans to write automated scripts which will grade student's results automatically and this way we plan to improve the feedback procedure.

3. A DESIGN THEORY FOR PSI – ORIENTED INFORMATION SECURITY LABORATORIES

March and Smith (1995) are of the opinion that IT practice is concerned with the development, implementation, operation and maintenance of IT systems whereas development and maintenance are considered as design activities. Design science attempts to create things that serve human purposes. Therefore, design research should conceptualize and signify the real problems related to design tasks in order to develop and lead practitioners towards appropriate techniques for their solution. A stream of researchers proposes that IS research is based on behavioral science paradigm view which should be complemented with the research based on design science paradigm (Carlsson 2006). IT research should develop understanding of how and why IT systems work and do not work so that research in IT could address the design tasks faced by practitioners (March & Smith, 1995). In our case the researchers and practitioners thus would benefit from the design theory framework for the design and development of online InfoSec Lab aimed at educating students of information security field. The aim of IS design science research is to build practical knowledge for the design and realization of different classes of IS initiatives (Carlsson 2006). Researchers emphasized on the importance of design and development of information system design theories which could be helpful for the researchers and practitioners in the process of designing products and processes (Walls et al 1992, Gregor 2006). Gregor & Jones (2007) argue that better understanding of design theories not only provides an avenue for more systematic specification of design knowledge but also it supports the cumulative building of knowledge and it supports our aims to develop a design theory of hands-on education in information security.

Socio-technical design represents an approach that aims to give equal weight to social and technical issues when new work systems such as on-line education are being designed (Mumford, 2000). In our case the technical design and development of online information security lab should give the students opportunity to conduct exercises as well as issues of personal flexibility and student & teachers efficacy require equal importance and attention for systematic development. Socio-technical designers look at the complex systems design as a unified process by recognizing the interaction that is taking place between the technical, economic, organizational and social factors at every stage of the design process and afterwards for improvements in the system (Mumford, 2000). This concept is in line with our approach of design, development, implementation, evaluation and improvement of our online information security lab as well as providing students and teachers a flexible system to not only communicate with each other but also to work individually e.g. having one to one interaction between students and the system (achieved by automating the response using automated scripts).

This field needs to be dealt with a socio-technical approach which demands for a design theory which not only provides support for the design and development of online InfoSec Labs but also to create the relevant necessary pedagogical approaches. The "anatomy of design theory" framework by Gregor & Jones (2007) is utilized for our proposed design theory for online InfoSec lab course.

Components of a design theory for "online information security lab course for distance students"	
The Purpose and scope of design	• Designing "hands-on" online information security course for distance students of information security degree program. Students should be able to conduct lab exercises from anywhere anytime, and individually in order to provide them flexible and reliable learning environment to practice and master their security skills at their own pace.
Constructs	• PSI approach (modularization, automated scripts mastery of topics, student throughput, flexible learning, immediate feedback, teacher's efficiency, less cheating).
Principles of Form and	• 24x7 online InfoSec Lab (server, remote access, automated scripts). • The information security course will contain 15

Function	topics. Students have to show specific level of perfection for lower level topics before moving to the next level topics of the course. Each learning topic consists of the following: 1) Reading and watching video assignment 2) General assessment 3) Security Lab assessment
Artifact mutability	• Suggestions & feedback and evaluation for improving the current lab facilities and their utilization for distance education will be taken into account before the course is offered next time.
Testable propositions	Modularization of course contents leads to: 4. Mastery of course topics (Student's knowledge level) 5. Student throughput (percentage of student who complete the course) 6. Flexible learning (go-at-your-own-pace) Immediate Feedback (provided by the automated computerized system) leads to: 3. Teacher's efficiency in terms of consuming less time than traditional way of teaching. 4. Flexible learning Automated PSI scripts to assign different exercises lead to: 2. Less cheating
Justificatory knowledge	• The proposed course design is based on the Kernel theory known as the Keller plan, PSI (Personalized system of instruction) which was proposed by Fred S. Keller (Keller, 1968). PSI approach has been utilized in different domains e.g. Psychology, Engineering and computer programming. The researchers (Koen, 1971, Pear & Novak 1996, Morita et al 2005 & 2006 and Nilsen &

	Larsen, 2011) have noted positive results by implementation of the PSI approach in different courses. The PSI approach has different features which make it a unique way of providing education. These features include: • Flexibility (a feature which allows the students to study at their own chosen pace) • The course division into smaller units / modules (in our case we will divide the course into smaller topics which will include reading assignments, assessments and exercises) • Mastery / perfection of the studied units, one module at a time (this feature will help our students master each low level topic before they can proceed to the next topic).
Principles of implementation	• The course will be implemented making use of the: • Virtualization techniques for lab development (multiple logical servers on the same physical server) • Learning management system (Moodle) • LMS Server operating system • LMS database system • Web Server • Automated scripts to grade student's work • We will utilize the virtualization techniques to prepare the InfoSec Lab which is a cost-effective solution (see section 5 for details).
Expository instantiation	• This is a conceptual idea which we plan to implement in the next semester in the Luleå University of Technology in the fall term of 2012.

Table 1. Design theory framework for course development

4. OUR OBJECTIVES, COURSE PLAN & LAB DESIGN REFLECTING THE PSI PRINCIPLES

This section concretizes our online InfoSec Lab design, which is based on the PSI-oriented ideas outlined above.

Our major design objective is to implement hands-on exercises on information security for online students. We want to increase the students' knowledge level, without increasing study time. We want the students' limited study time to be more effective. To do this we will create online InfoSec Lab exercises. The implementation is informed by the PSI approach. By increasing the students' knowledge level, we will enhance the students' mastery of the subject. This goal will be achieved by applying the PSI approach (Keller, 1968) according to which a sufficient mastery of a low level course topic needs to be demonstrated before proceeding to the next topic. "The PSI approach is based on behaviorist and cognitive psychology and encourages mastery of course content" (Price, 1999). Other goals of the course design include improving student throughput (percentage of students who complete the course), personal flexibility, immediate feedback, increasing student motivation, and decreasing the ability for students to cheat, all of which involve to specific issues for organizing distance course.

When possible we have attempted to reuse existing solutions and we have attempted to reuse open source solutions which are free. We have implemented the InfoSec Lab via Server virtualization techniques, in order to reduce costs. This will make it easier for other learning institutes to adopt our InfoSec Lab design.

The next subsections are arranged like this:

> **4.1.** Summary of Online InfoSec lab design (Virtualization, Server, Learning Management System (LMS), LMS Server Operating System, Web Server, LMS Database System)
> **4.2.** Remote Access (Flexibility)
> **4.3.** PSI Design Details (Modularization of course content)
> **4.4.** Automated Scripts

4.1. Summary of Online InfoSec lab design

This section contains a brief summary concerning the online InfoSec Lab. Our design required multiple servers. We could run multiple physical servers or run multiple logical servers on a single physical server, via virtualization technology.

Virtualization: It is less expensive to run multiple logical servers on the same physical server. In order to run multiple logical servers (vm guests) on the same physical server (vm host), we were required to choose a virtualization technology. VMware is a leader in the field of virtualization. VMware has a virtualization product VMware vSphere Hypervisor 5 (ESXI5), which is free to use, with certain restrictions (vmware.com). Our InfoSec Lab can be deployed under those restrictions. Therefore we have selected the ESXI 5 VMware virtualization product to support our InfoSec Lab.

Server: We needed to select a physical server to be used, as the vm host, when implementing our Virtual InfoSec Lab solution. Dell servers were reasonably priced and are also certified to be compatible with VMware ESXI 5. Therefore we have selected the Dell PowerEdge R210 II server to support our Virtual InfoSec Lab.

Learning Management System (LMS): We needed to select an LMS. One LMS feature we need is an easy way to update the information in the LMS. Moodle (moodle.org) uses the open source and free SQL database server, MySQL. So Moodle supports this easy update feature which we require. Moodle also has some support in requiring students to pass one instruction unit (which Moodle calls “Topic”) before the students can start the next instruction unit. Therefore we have selected Moodle to support our Virtual InfoSec Lab.

LMS Server Operating System: We needed to install the Moodle LMS onto some server operating system. It costs less money to use a Linux server operating system (which is open source) as opposed to using Microsoft Windows Server. Also, the LMS system Moodle has better support for Linux, as compared to Windows. One popular Linux server operating system which is well supported is Ubuntu, which is available free of charge (ubuntu.com). Therefore we have selected the most recent Linux Ubuntu, version 12.04, to support our virtual InfoSec Lab.

LMS Database System: We needed to install a database system, to be used on our Linux server, to support the LMS. MySQL (mysql.com) is open source and has a free version which meets our requirements. Therefore we have selected the MySQL database system to be used to support our Virtual InfoSec Lab.

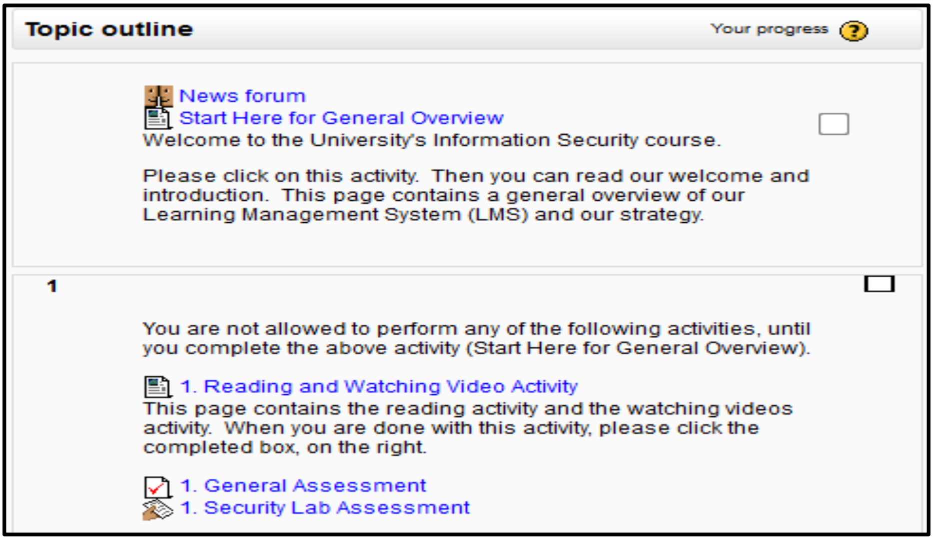
Web Server: We needed to install a web server, to be used with Moodle. Apache is open source free, and easy to configure (apache.org). This meets our requirements. Therefore we have selected Apache to be used to support our virtual InfoSec Lab.

4.2. Remote Access (Flexibility):

The students will have online remote access to their InfoSec Labs 24x7. Most of the time, there will not be any University personnel to monitor or assist. The students will need to remotely access their InfoSec Lab via a (graphical user interface) GUI console application. This will prevent any malware from attacking the student's personal computer, via normal IP networking connections. We also require the student to connect via a VPN (virtual private network), before they are even able to use the GUI console application. One GUI console application that we are considering is Virtual Network Computing (VNC), which we will most likely run over Secure Shell (SSH).

4.3. PSI Design Details (Modularization of course content):

For the purposes of this paper, assume that the information security class consists of 15 learning topics organized as sequenced modules. We've created an LMS course in Moodle, to illustrate our prototype of the PSI design. Each learning topic consists of the following: 1) Reading and Watching Video assignment, 2) General Assessment, and 3) Security Lab Assessment. The following is a screen shot of our general course information and the first topic. All of the following screen shots are the results of actual Moodle LMS configurations. The following is what the student will see, before they perform any activities:



Topic outline

News forum

Start Here for General Overview □

Welcome to the University's Information Security course.

Please click on this activity. Then you can read our welcome and introduction. This page contains a general overview of our Learning Management System (LMS) and our strategy.

1 □

You are not allowed to perform any of the following activities, until you complete the above activity (Start Here for General Overview).

1. Reading and Watching Video Activity

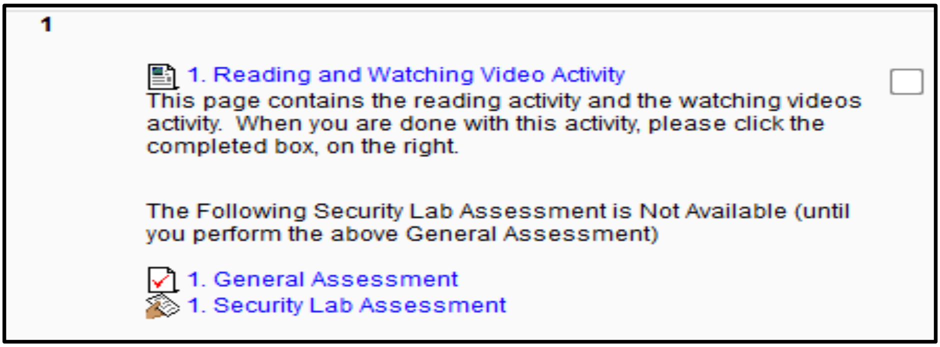
This page contains the reading activity and the watching videos activity. When you are done with this activity, please click the completed box, on the right.

1. General Assessment

1. Security Lab Assessment

FIGURE 1 – PSI approach, topic 1 activities dimmed until previous activity is completed

Notice that it says "You are not allowed to perform any of the following activities, until you complete the above activity". This means that the bottom three activities are not available to the student, at this time. The student must first review the top "Start Here for General Overview" activity before they can perform any of the following three activities. So our LMS does implement the Keller's PSI (1968) approach of completing one topic before starting the next. This ensures that the students have the required general course information, such as how to get support, before they begin the topic 1 activities. Once they review the "Start Here" activity information, the "1. Reading" activity become available and a new checkbox will appear to the right of (1. Reading…). The following screen shot shows this new status.



1

1. Reading and Watching Video Activity □

This page contains the reading activity and the watching videos activity. When you are done with this activity, please click the completed box, on the right.

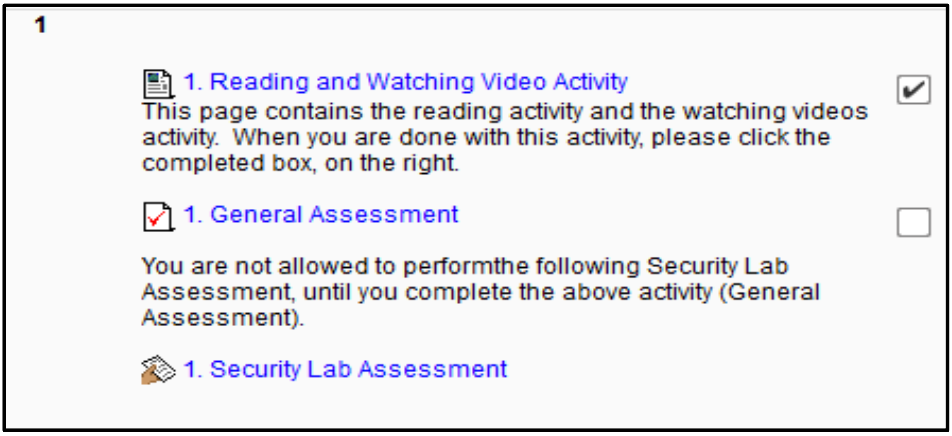
The Following Security Lab Assessment is Not Available (until you perform the above General Assessment)

1. General Assessment

1. Security Lab Assessment

FIGURE 2 – PSI approach, assessment activities dimmed until previous activity is completed

In the above figure, the “1. Reading” activity has a new checkbox on the right. It is now available. Note that the two Assessment activities below it are not available. The student must first indicate that they have viewed the “1. Reading” activity, prior to taking the associated assessments. After they view the “1. Reading” activity, the first General Assessment activity becomes available. Here is the new screen shot:



1

1. Reading and Watching Video Activity ☑

This page contains the reading activity and the watching videos activity. When you are done with this activity, please click the completed box, on the right.

1. General Assessment □

You are not allowed to performthe following Security Lab Assessment, until you complete the above activity (General Assessment).

1. Security Lab Assessment

***FIGURE 3** – PSI approach, 2nd assessment activity dimmed until 1st assessment is completed*

In the above figure 3, for the first time, the “1. General Assessment” is available. This assessment is graded automatically by the LMS Moodle. Only after the student passes the “1. General Assessment” activity, will that student be able to take the “1. Security Lab Assessment”. Only after the student passes both the “1. General” and “1. Security Lab” assessments, will they be able to proceed to the next topic. When the student performs the Security Lab, this lab will be outside the scope of the Moodle LMS. So we will need to perform our own integration with the LMS. We will need to write scripts to automatically grade each student’s security lab exercise. We will also need to write scripts to update the Moodle LMS, after each student performs a security lab exercise. Since the Moodle LMS uses SQL, it is easy for us to automatically update the LMS, with the security lab exercise results.

Immediately after all results are entered into the LMS, our Personalized System of Instruction will then perform an analysis of just that student’s results. A personalized message is then created for just that student. The personalized information is then immediately provided to the student and a copy is sent to the student via email. As shown above, in figure 3, if the student has passed an assessment, the student is then allowed to proceed to the next activity.

Here is an example of the automatically generated PSI message, which is sent to the student (after they complete all topic 1 activities):

FIGURE 4 – PSI Approach, Personalized Status Information Provided to Each Student

> To: Student
> Subject: Information Security Status Update
> Hello John Doe,
>
> This is a short status update, concerning your progress in the InfoSec course.
>
> **Topic 1:** As stated before, you have completed all the activities, and passed topic 1.
>
> **Topic 2:** We see you have read material for topic 2 and have passed both the assessments (General Assessment and Security Lab Assessment) for topic 2. You received a security lab Assessment score of 86. If you wish to take this Lab again, to improve your score, here is some information, to help you.
>
> > Q5. You missed question five. The material for question 5 is found in the course book, on page 37, starting with the title "Title goes here".
> >
> > Q18. You missed question 18. The material for question 18 is found in the course book, on page 37, starting with the title "Title goes here".
> >
> > After you have studied the above material, you can retake the topic 2 lab assessment. When you retake topic 2 assessment, you will only be presented with the questions which you missed. The questions will be different but will cover the same material. Good Luck! To retake the topic 2 assessment, click here.
>
> **Topic 3:** Note that you passed the last topic 2 assessment three days after the deadline. So you are currently behind schedule, by three days. It is very important that you catch up ASAP. The topic 3 deadlines follow:
>
> > Reading and Watching Videos Activity - due in three days (May 7th, noon)

> > Pass General Assessment – due in four days (May 9th, noon)
> >
> > Pass Security Lab Assessment – due in five days (May 10th, noon)
>
> If there is some urgent reason that you can't meet the above schedule, you are required to immediately fill out the following web form, so that we know what the problem is and so that we know when you plan to complete the above. Click here to fill out the form. If you don't have the form, it is absolutely critical, that you catch up and meet the above deadlines.
>
> Thanks and Regards,
>
> Teacher …

The above report will help provide the appropriate pressure for the students to catch up. The reason is that we give them an out (if they immediately fill out the form). Many students will think about this and decide not to fill out the form. This will therefore cause them to implicitly accept the deal that they must now catch up.

4.4. Automated Scripts:

We will be using automated scripts to grade the students' InfoSec Lab exercises. We will use the computer scripts to also give the student their lab exercises. Based on our unique approach instead of giving all students the same identical lab exercise, our automated scripts will give each student a slightly different lab exercise problem. For example, in our Firewall exercise, each student will be given a different server IP address. Our PSI scripts will remember this. Then our PSI scripts will only give a student credit, if that student solves the unique problem, that particular student was given. This way, if a student copies another student's answer, the configured firewall IP addresses will be different (due to different server IP addresses) and our PSI will not give any credit to that student, who has cheated. We were unable to find any research papers which have used our unique approach.

5. EVALUATION PLAN

We share the idea with Bostow et al (1995) that "A learning unit or contingency contains three critical parts. It is composed of (1) the momentary setting in which a student responds, (2) the behavior that the student is to emit, and (3) the consequences that immediately follow the performance”. The learning unit/topic can be measured by noting the behavior emitted and the contingent consequence that follows. The table-2 summarizes roughly what we aim to evaluate and measures of evaluation.

Testable Propositions		Evaluation Measures
Modularization of course contents lead to: -	Mastery of course topic to improve student’s knowledge level	A final exam should be conducted to test the mastery of course topics of students. The final results for passed students compared to enrolment will provide measures for student throughput (it will also be measured against the student throughput of the previous year). A Class Survey in the form of a questionnaire should provide measures for flexible learning.
	Student Throughput	
	Flexible Learning	
Immediate Feedback leads to: -	Teacher Efficiency	Teacher’s interview (experience + time calculation). Class survey regarding system response considering aspects of how quick & useful response student’s received.
	Flexible learning	
Automated PSI scripts to assign different exercises leads to: -	Less cheating	The computerized automated scripts will grade InfoSec lab exercises and verify the IP address to which the exercise was assigned before awarding credits.

Table: 2 Evaluation Plan

We aim at improving the student’s knowledge level through the PSI approach and online InfoSec Lab, which will provide them flexibility to study at their desired speed. The final exam will test student’s knowledge about the work that they have performed utilizing online InfoSec Lab resources and assignments. The teacher/s will be interviewed about their experience with this approach. The time that they spent during this course will provide us with measures of teacher's efficiency. At the end of the course, all the students will answer a survey questionnaire about the performance of online InfoSec Lab, remote access, immediate feedback through automated scripts and overall hands-on experience. This information will be useful for maintenance and improvements in the online InfoSec Lab.

6. DISCUSSION

We are in the process of systematic development of an online InfoSec Lab to provide hands-on education to Msc students of Information Security. Hrastinski et al (2010), suggest that the aim of design research output should be to develop abstract knowledge rather than recipes which can support practitioners in developing a successful system or action. A recent review about online InfoSec Labs (Iqbal & Päivärinta 2012) reveals that the knowledge in this field is still scattered, none of the articles studied provide any details of a well-grounded and tested design theory of online InfoSec Labs. This situation will not only hinder the accumulation of knowledge in this area but also makes it difficult for others to observe, test and adapt clear design principles for online information security laboratories, exercises and relevant pedagogy. The lack of systematic research on online InfoSec Labs development prompts us to propose a design theory of online InfoSec Lab based on the PSI approach which should be considered as a first step towards accumulation of knowledge in this field. This paper starts to fill this gap by outlining a design theory, and evaluation measures built upon a solid theoretical ground.

The PSI approach which we adopted as the theoretical basis for design will contribute to information security education by providing Graduate level students the path towards in-depth learning (mastery of study topics), giving them the opportunity to work flexibly (go at your own pace), as most of the distance students are professionals, who need a relaxed schedule to study. The students will be provided immediate feedback with the help of automated scripts to improve student efficacy. According to our review on previous literature, our work represents one of the first contributions which is explicitly leaning on these pedagogical principles in this field.

We are going to start this online InfoSec Lab course from august, 2012 and after its implementation; we will be ready to collect feedback. We will learn also in practice how the PSI works in hands-on information security teaching. This will help us to further improve the course design, lab facilities and related pedagogical approach. In this sense, our paper outlines a research in progress.

7. CONCLUSION & FURTHER RESEARCH

Hands-on laboratory exercises are an important part of the information security education targeted to prepare a Graduate workforce. Access to the InfoSec labs to conduct security training is equally important for campus and distance students. This article proposed a design theory of online InfoSec Labs based on the Personalized System of Instruction. We argue that a pursuit towards such explicit design theory will provide a basis for the assimilation of knowledge in this field.

In future we also want to look for other pedagogical approaches to design and develop InfoSec Labs e.g. CSCL (computer supported collaborative learning) approach is one of the approaches that we would like to investigate more and see how it impacts the online InfoSec Lab design. CSCL approach is considered as an emerging paradigm (Koschmann 1996) for student’s collaborative learning where the student himself is a part of a studying and learning community that makes use of information and communication technology (ICT) as a mediating tool for social interaction (Päykkänen et al, 2006). Furthermore, when CSCL approach will be adapted for the online InfoSec Lab exercises, it will have impacts on the lab design depending on the structure of the exercises that we aim to develop.

REFERENCES

1. Aboutabl, M.S. 2006. The cyberdefense laboratory: A framework for information security education. Information Assurance Workshop, IEEE, p.55-60.
2. Apache retrieved on 02-05-2012 from http://apache.org
3. Balta, O.C., N. Simsek, N. Tezcan. 2009. A Web Based Generation System for Personalization of E-Learning Materials. WCSET- World Congress on Science, Engineering, and Technology, Dubai, United Arab Emirates, p.419-422.
4. Bostow, D.E., K.M. Kritch, B.F. Tompkins. 1995. Computers and pedagogy: Replacing telling with interactive computer-programmed instruction. Behavior Research Methods 27(2) 297-300.
5. Carlsson, S.A. 2006. Towards an information systems design research framework: A critical realist perspective. Proceedings of the First

International Conference on Design Science Research in Information Systems and Technology, Claremont, CA. p.192-212.

6. Chen, F.G., R.M. Chen, J.S. Chen. 2011. A Portable Virtual Laboratory for Information Security Courses. Advances in Computer Science, Environment, Ecoinformatics, and Education, Springer-Verlag Berlin Heidelberg p. 245–250.
7. Choi, Y.B., Lim, S., Oh, T.H. 2010. Feasibility of virtual security laboratory for three-tiered distance education. Proceedings of the ACM Conference on Information Technology Education. ACM, 53-58.
8. Crawford, E., Y. Hu. 2011. A Multi-user Adaptive Security Application for Educational Hacking. Proceedings of the World Congress on Engineering and Computer Science. WCECS, San Francisco, USA vol. I.
9. Cumming, B., C. McIntosh. 1982. PSI in Engineering Mathematics. Journal of College Science Teaching 12(1) 30-31.
10. Emurian, H., X. Hu, J. Wang, A. Durham. 2000. Learning JAVA: A programmed instruction approach using applets. Computers in Human Behavior. 16(4) 395-422.
11. Gregor, S. 2006. The nature of theory in information systems. MIS Quarterly 30(3) 611-642.
12. Gregor, S., D. Jones. 2007. The anatomy of a design theory. Journal of the Association for Information Systems 8(5) 312-335.
13. Hrastinski, S., C. Keller, S.A. Carlsson. 2010. Design exemplars for synchronous e-learning: A design theory approach. Comput. Educ. 55(2) 652-662.
14. Keller, F.S. 1968. Good-bye, teacher... Journal of Applied Behavior Analysis. 1(1) 79.
15. Koen, B.V. 1971. Self-Paced Instruction in Engineering: A Case Study. IEEE Transaction on Education Volume 14(1) p.24-31.
16. Koschmann, T. 1996. Paradigm shift and instructional technology: An introduction. In T. Koschmann (Ed.), CSCL: Theory and practice of an emerging paradigm New Jersey: Lawrence Erlbaum Associates. pp. 1–24.
17. Krishna, K., W. Sun, P. Rana, T. Li, R. Sekar. 2005. V-NetLab: a cost-effective platform to support course projects in computer security. Proceedings of 9th Colloquium for Information Systems Security Education, Atlanta, p. 44-50.
18. H. A. Lahoud, X. Tang, 2006, Information security labs in IDS/IPS for distance education, Proceedings of the 7th conference on Information technology education, Minneapolis, Minnesota, USA, p. 47-52.

19. Li, P., L.W. Toderick, P.J. Lunsford. 2009. Experiencing virtual computing lab in information technology education. Proceedings of the 10th ACM Conference on SIG-Information Technology Education. ACM, p.55-59.
20. March, S.T., G.F. Smith. 1995. Design and natural science research on information technology. Decision Support System. 15(4) 251-266.
21. Moodle retrieved on 02-05-2012 from http://moodle.org
22. Morita, Y., J. Kenne, A. Johendran, Z. Wu, G. Ma, M. Nakayama, A. Nishihara, B. Koen. 2005. Pilot Study of International Web-Based PSI Course between Japan and US. Proceedings of the 21st Annual Conference of Japanese Society of Educational Technology (JSET) September 23rd at University of Tokushima, Japan.
23. Morita, Y., J. Kenne, A. Nishihara, M. Nakayama, B.V. Koen. 2006. Implementation of an International Web-Based PSI Course: A Case Study. 36th ASEE/IEEE Frontiers in Education Conference, San Diego, CA, p.14-18.
24. Mumford, E. 2000. A socio-technical approach to systems design, Requirements Engineering, 5(2), 125-133.
25. MYSQL retrieved on 02-05-2012 from http://mysql.com
26. Nilsen, H., E.Å. Larsen. 2011. Using the Personalized System of Instruction in an Introductory Programming Course. In the proceedings of 18th NOKOBIT Conference, University of Tromsø, p.27-38.
27. Päykkänen, K., H. Räisänen, H. Isomäki. 2006. Mobile studying and social usability on a wireless campus. Proceedings of the 8th Conference on Human-Computer Interaction with Mobile Devices and Services. ACM, 269-270.
28. Pear, J., D. Crone-Todd. 1999. Personalized system of instruction in cyberspace. Journal of Applied Behavior Analysis. 32(2) 205.
29. Pear, J.J., M. Novak. 1996. Computer-aided personalized system of instruction: A program evaluation. Teaching of Psychology 23(2) 119-123.
30. Price, R.V. 1999. Designing a college Web-based course using a modified personalized system of instruction (PSI) model. TechTrends 43(5) 23-28.
31. Sarfraz Iqbal., Tero Päivärinta.2012.Towards A Design Theory for Educational Online Information Security Laboratories, Advances In Web-Based Learning - ICWL, Springer-Verlag Berlin Heidelberg, LNCS, Volume 7558/2012, 295-306
32. Summers, W.C., C. Martin. 2005. Using a virtual lab to teach an online information assurance program. Proceedings of the 2nd Annual

Conference on Information Security Curriculum Development. ACM, 84-87.

33. UBUNTU retrieved on 02-05-2012 from ubuntu.com http://Ubuntu.Com
34. VMware vSphere Hypervisor 5.1 Download Center retrieved on 02-05-2012 from https://my.vmware.com/web/vmware/evalcenter?p=free-esxi5&lp=default
35. Walls. J.G., Widmeyer, G.R. & O.A. El Sawy. 1992. Building an information systems design theory for vigilant EIS. Information Systems Research 3(1) 36-59.
36. Yurcik, William., David Doss. 2000. Information security educational initiatives to protect e-commerce and critical national infrastructures. Information Systems Education Conference (ISECON) Philadelphia, PA.