2014

Design Principles for Online Information Security Laboratory

Sarfraz Iqbal
Luleå University of Technology, sarfraz.iqbal@ltu.se

Ali Ismail Awad
Luleå University of Technology, ali.awad@ltu.se

Devinder Thapa
Luleå University of Technology, devinder.thapa@ltu.se

IRIS: *Selected Papers of the IRIS*. Nr 5: 65-79, 2014© AIS – IRIS The Scandinavian chapter of the AIS, ISSN 2387-3353 Published online 2 December 2014.

Design Principles for Online Information Security Laboratory

Sarfraz Iqbal, Ali Ismail Awad, Devinder Thapa

Luleå University of Technology
sarfraz.iqbal@ltu.se, ali.awad@ltu.se, devinder.thapa@ltu.se

Abstract. In this paper, we reported an online InfoSec Lab based on initial design principles derived from kernel theories such as Conversational Framework (CF), Constructive Alignment (CA), and Personalized System of Instruction (PSI). The overall research was conducted using the action design research approach. In doing so, the iterative cycles and critical reflections during the process helped to refine a set of existing design principles. The study contributes to the IS community by providing design principles for an online InfoSec Lab that utilizes state-of-the art technology for mixed classrooms.

Keywords: Online InfoSec Lab, Action design research, Pedagogy, Design principles, PSI.

1 Introduction

The recent increase in security breaches around the globe and advances in the methods and technology of network attacks has also increased the demand for trained security professionals (Householder et al. 2002; Suranjith and Amina 2005). In addition, employees in different organizations need to retool themselves with the latest education and training due to continuously changing security solutions (Hentea 2005; Wilson and Hash 2003; Ayyagari and Tyks 2012). Thus, the onus for producing a trained workforce of network security professionals is on the educational institutions (Yurcik and Doss 2001). Hence interventions that encourage educational institutions offering distance education to adopt and use e-learning platforms for hands-on education in information security are of extreme importance for many reasons. For example, using the e-learning platform appropriately based on specific pedagogical principles may help to develop design exemplars for practitioners to understand when and how to manage and use a specific design to improve hands-on education (Iqbal and Päivärinta 2012).

Our previous findings show (Iqbal and Päivärinta 2012; Iqbal and Thapa 2013) that there is a lack of systematic studies of hands-on education in information security using online InfoSec labs. Likewise, existing online InfoSec labs are not built on sound theoretical foundations, in other words there is a lack of design principles and design theory creating systematized knowledge and providing a basis for appropriate design and action (Gregor and Jones 2007; Gregor et al. 2013). This is an important issue and it demands the systematic knowledge necessary to help practitioners understand the mechanisms that may lead to desired outcomes (Hrastinski et al. 2010). Consequently, online InfoSec labs needs to be developed systematically

in order to accumulate hands-on security knowledge as desired by the Information Systems field (Hirschheim and Klein 2012).

E-learning approaches are considered effective for security education/training (Niekerk and Thomson 2010), and educational institutions are extending their areas of security education by offering online courses and degree programmes (Iqbal and Paivarinta, 2012; Dale et al. 2011). It is generally accepted that the online courses provide convenience in terms of time and location, however at the same time they also bring new challenges related to the delivery of education through e-learning artefacts (Hentea et al. 2006). For example, hands-on laboratory exercises are an important part of the information security curriculum, and in most cases are not available to distance students (Crawford and Hu, 2011). In order to address these challenges, we propose an online, pedagogically based information security (InfoSec) lab for hands-on exercises. When exploring for exemplar labs that fulfil the given criteria, it was almost impossible to find any, particularly in the context of IS security courses. Consequently, in this paper, we describe a case in which an Online InfoSec Lab is designed following the pedagogical approaches Personalized System of Instruction (PSI), Constructive Alignment Theory, and Conversational Framework, as kernel theories. The Action Design Research (ADR) approach adopted in this study conceptualizes the IT artefacts as ensembles as a result of emergent perspectives on design, use and refinement in context through continuous interaction between technology and organization during the design process (Sein et al. 2011).

We report on the actual process of development, implementation and evaluation of the Online InfoSec Lab at Luleå University of Technology. The article aims to describe the IT-dominant BIE (building, implementation and evaluation) phase of the proposed framework (see ref. Iqbal and Thapa 2013). The review of prior research (Iqbal and Päivärinta 2012) and preliminary interviews with teachers and programme management at Lulea University of Technology for the development of online InfoSec labs lead us to derive five initial design principles i.e. *Contextualization, Collaboration, Flexibility, Cost-effectiveness* and *Scalability*. The initial design principles will be followed in the BIE process, and concurrently refined and adapted as a set of emergent design principles.

The rest of the paper is organized as follows. In Section 2, we discuss the theoretical framework comprising kernel theories which are incorporated in the InfoSec Lab. Section 3 provides an overview of the ADR research approach. Section 4 discusses the process of lab design and development through the ADR phase of BIE. Section 5 discusses the contribution. Finally, Section 6 concludes the paper with a future research agenda.

2 Theoretical premises (Kernel Theories)

2.1 Constructive Alignment and Conversational Framework

A theoretical framework comprising Constructive Alignment Theory (Biggs 1996) and Conversational Framework (Laurillard 2002) was prepared and applied in the initial phase of the project. The theoretical framework has been utilized as an analytical lens to analyse the current situation and to guide the on-going research process in the Computer and Systems Science

Division in order to enhance quality of the teaching and e-learning platform to deliver a master's programme in information security. Hence, after analysing the current e-learning platform and teaching methods/situation, the theoretical framework suggested the following criteria (see Table 1) for the use of an e-learning platform to enhance the quality of online education, particularly targeting hands-on education in information security courses.

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

Table 1: Integrated E-learning Platform (Iqbal 2013)

Keeping in mind the contextual requirements (course objectives, practical requirements, etc.) of the InfoSec courses, it was suggested that the learning management system (Fronter) could be used for interactive purposes, whereas the virtual classroom (Adobe Connect) could be used for communicative purposes. Likewise, the Online InfoSec Lab could be used for productive purposes, for example to provide InfoSec students with the media to implement security solutions and to test and improve their security skills. The theoretical framework furthermore guided the alignment of the teaching/learning activities, including practical lab activities based on a specific pedagogical approach. Hence, the PSI approach was selected based on server security architecture course requirements in order to provide the students with individual and flexible hands-on education.

2.2 Pedgaogical approach (PSI)

The Personalized System of Instruction (PSI) approach (Keller 1968) was initially in the form of programmed instructions in the psychology field, however it has also been applied in various other educational fields such as applied behaviour analysis, engineering and programming courses (Koen 1971; Cumming and McIntosh, 1982; Crosbie and Kelly 1993; Emurian et al. 2000; Nilsen and Larsen 2011). Although, scholars applying the PSI approach noted positive student feedback (Crosbie and Kelly 1993) in some cases procrastination was identified as a problem for weaker students (Nilsen and Larsen 2011). The PSI approach is considered favourable for distance students (Pear and Novak 1996) where students prefer the convenience of working at their own pace. 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
- Integrated E-learning Platform

The pedagogical requirements of the course, such as individualized and flexible learning, are important factors in general, and for distance students in particular, as the distance students wish to study and work at the same time and cannot follow a strict schedule. The PSI approach also fits well with the course objective that is to enhance the mastery of course topics.

3 Method

The ADR method was selected for this research project mainly because it provides continuous stakeholder participation in the project, which was an important factor in bringing the necessary pedagogical improvements to address the problems identified in this project. Incorporating the design science research elements in this project was important in order to contribute to design theory in the longer run based on continuous reflections during and following the work, and by elucidating some general design principles (Gregor et al 2013). The ADR research process encompasses four stages i.e. (1) problem formulation, (2) building, implementation and evaluation, (3) reflection and learning, and (4) formalization of learning. The summary of the ADR research process for the Online InfoSec Laboratory is highlighted in the following table.

Stages and Principles		**Activities to build, intervene, and evaluate InfoSec lab**
Stage 1: Problem Formulation		
Principle 1: Practice-inspired research	The research was motivated by the problems of low hands-on exercises, absence of InfoSec Lab, need for a flexible e-learning system, absence of pedagogical approaches in teaching of information security and to enhance mastery of course topics.	Recognition: Shortcomings of existing e-learning platforms for hands-on education in information security were recognized as lacking productive media. Official approval was obtained to formally proceed with the project and to seek funding in this regard.
Principle 2: Theory-ingrained artefact	The on-going research process was in the first phase guided by theories such as Constructive Alignment and Conversational Framework. Moreover, in order to proceed with the second phase of building, implementation and evaluation of the artefact, a kernel theory (Personalized System of Instruction) informed the design of the Online InfoSec Lab.	
Stage 2: Building, Implementation and Evaluation		
Principle 3: Reciprocal Shaping	An ADR team was formed with stakeholders concerned such as researchers, developers, teachers and teaching assistants.	Alpha version: Following the criteria of IT-Dominant BIE, the initial version of the Online InfoSec Lab was tested by the stakeholders to overcome weaknesses at this stage before implementing it on the course for end user (Student)

		experimentation. Beta version: The Online InfoSec Lab was developed and implemented in the server security architecture course as an example.
Principle 4: Mutually influential roles	The ADR team created for this project included a Ph.D. candidate (researcher), teachers as practitioners who agreed to undertake the part of the project to pilot test the building and implementation of an Online InfoSec Lab in their courses (in this case the pilot course was Server Security Architecture), the developer also received some help from the technical infrastructure team at LTU and the assistant teacher.	
Principle 5: Authentic and Concurrent Evaluation	The theoretical framework and resulting pedagogical guidelines used to design the courses and to enhance the e-learning platform with the addition of an Online InfoSec Lab as a productive media were discussed in a pedagogical forum and various other seminars with stakeholders in order to gain commitment. Furthermore, a set of initial design principles was developed and presented to stakeholders and was published in order to obtain feedback from the academic community.	
Stage 3: Reflection and Learning		
Principle 6: Guided Emergence	The dynamic complexities of the deliverable artefact and processes to achieve desired objectives began to emerge.	Emerging version and realization: The project deliverables, including the pedagogical model for pilot course and Online InfoSec Lab, were refined for maximal effect.
Stage 4: Formalization of Learning		
Principle 7: Generalized Outcomes	As this was the first iteration of the BIE, further iteration will be used to generalize the problem and solution to address the class of problem i.e. lack of pedagogically- based e-learning platform for hands-on education in IS security.	Ensemble version: An ensemble embodying the design principles used to design the Online InfoSec Lab based on a pedagogical approach in order to enhance hands-on education in IS security.

Table 2: Summary of the ADR research process

4 Building, Intervention and Evaluation of the Online InfoSec Lab

4.1 Online InfoSec Lab Architecture

In order to carry out the first iteration of the BIE of the Online InfoSec Lab, we selected the Server Security Architecture course as a case study. The five initial design principles: *Contextualization, Collaboration, Flexibility, Cost-effectiveness* and *Scalability* were followed in the process. For example, utilizing the contextualization principle, the contextual requirements were gathered from different sources such as organizational goals, course goals, pedagogical requirements etc. while, the collaboration principle was used as a means to motivate all the stakeholders (including researcher, developer, IT staff, teacher etc.) to hold regular meetings to achieve an effective and purposeful design for the Online InfoSec Lab and related activities. Overall, the course was designed keeping in mind the problems perceived in the teaching of the M.Sc. programme in information security i.e. how to provide students with a flexible online educational information security laboratory that could help them to learn and practice security skills from distance, freely without time or location constraints. Another important issue was to enhance mastery of the course topics. The students were informed through the study guide that this course covers the basic concepts, standards, purpose and implementation of server security architectures. The course provides a narrow, but in-depth, focus on server security architectures. For example, it covers how to analyse server security architecture requirements based on an organization's security policy.

Initially, an ADR team was created which included a researcher, a teacher, a developer and a teaching assistant. The organizational and course goals demanded that we should develop an online information security lab providing remote access to our distance students from anywhere in the world. Given the fact that we had limited funding available to develop the lab at this stage, it was decided to make use of virtualization techniques that not only make the lab cost-effective but also help to prepare an infrastructure, which is easily upgradable based on the requirements of the course.

Accordingly, we deployed the information security laboratory in the private network of Luleå University of Technology, with student remote access capability. The design of the Online InfoSec Laboratory dealt with different issues such as flexibility in terms of availability and accessibility, scalability and robustness (a new design principle that emerged during the BIE process). The design layout of the laboratory is shown in Fig.1. The availability of the laboratory represents its operability state during the course. However, the laboratory could be operable most of the time; students had no access to it without the presence of the teacher or the teaching assistant. Thus, in our case, the availability issue was mapped to the availability of the operator. Laboratory accessibility concerns how easy or difficult it is to access the laboratory. We have used two different access routes for the two laboratory assignments shown in Fig.1. These included use of simple Secure Shell (SSH) protocol (Soete 2011), and a fairly complex Virtual Private Network (VPN) tunnel (Fowler 1999, Neumann 2009).

A scalable laboratory can fit different assignments using a limited budget. With the equipment we had, we could build two different assignments by extending the topology of the first experiment. Technically speaking, the laboratory has been built inside the University's infrastructure in order to avoid security attacks. Fig. 1 shows that both laboratory assignments are set behind the University's firewall. We have used individual routers for each assignment in order

to run both in parallel. The router also worked as another security defence as it has been configured to accept SSH and VPN connections with student user name and password. Each router was a configured static external IP address that was linked with the university's Dynamic Host Configuration Protocol (DHCP) (Droms 1997 & 1999) server. In order to facilitate the availability of the laboratory, we built two copies of the first assignment; so two students could work on the same assignment at the same time.

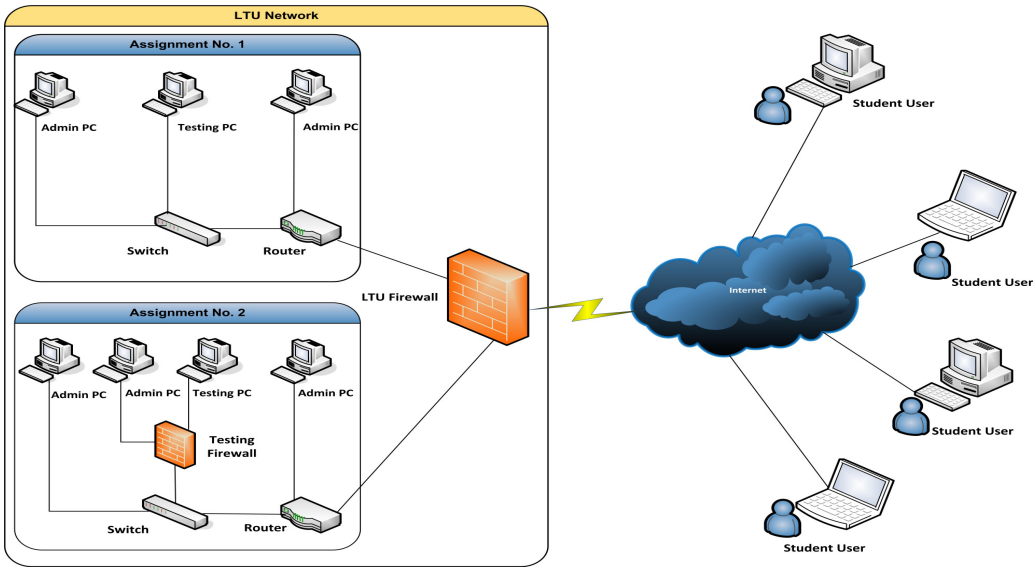

Figure 1: Online InfoSec Lab architecture

4.1.1 Network Topology Configuration Assignment

The main purpose of the network topology configuration assignment, shown in Fig. 2, is to provide students with a means to understanding and configuring simple network topology, and investigating any security issue that comes up in the configuration process. The assignment was constructed using a Cisco 1941 router model, Cisco Catalyst 2690 layer 2 switch model with 24 ports (Stallings 1997), one computer machine with two Ethernet interfaces and one COM port for console connections. The computer machine was connected alternately to the router and the switch console ports for administration purposes. One Ethernet interface was used for testing the network connectivity using ping commands. The router was connected to the university's DHCP server via Gigabit Ethernet port (GE 0/1) with given IP 130.240.2xx.xxx, and was connected to the internal switch via Gigabit Ethernet port (GE 0/0) with granted IP address 192.168.1.1. A Network Address Translation (NAT) option was enabled and configured on the router to provide connectivity between the two sides of the router. In addition, SSH and Telnet protocols were configured on the router to give access to the router itself and to the switch behind. The switch was configured with two Virtual Lans (Vlans) with a management IP address 192.168.1.2. Students carried out the laboratory assignment in two phases. In the first phase, they connected to the router external IP address (130.240.2xx.xxx) using the SSH client installed on their

computers. This way, we increased laboratory accessibility by providing the student with a flexible laboratory access method regardless of the operating system used. The students had full access to the router configurations after making a successful connection. On the router, they created user accounts, checked the encryption of their user account, built different access lists for traffic management, enabled NAT on both router interfaces, and configured a secure Hypertext Transfer Protocol (HTTP) server for accessing and configuring the router via a web browser. In the second phase, the students connected to the switch using the earlier configured Telnet with the switch management IP address (192.168.1.2). Then, they had full access to the switch operating system for configuring Vlans, setting a name to the switch, and creating user accounts. It is worth noting that the student could access the testing computer from the router and the switch using its pre-configured IP address 192.168.1.5 and a ping command.

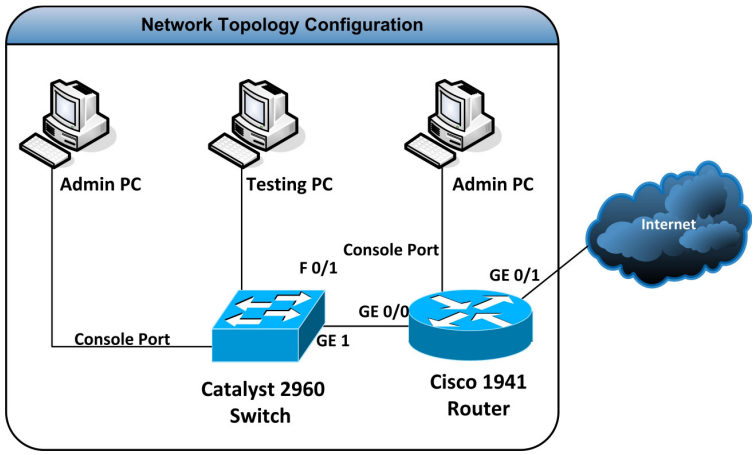

Figure 2: Network topology configurations

4.1.2 Firewall Configurations and Testing

A firewall is defined as a set of rules that can be executed to control network traffic. A physical firewall is a network device that holds and executes a set of rules to control transverse network traffic passing through it (Bellovin and Cheswick 1994). A firewall is an import network device that is used to create a trusted network segment. In order to mitigate the rules' complexity, multiple firewalls can be used with complimentary sets of rules (Yoon et al. 2010). The purpose of this assignment is to enrich the students' technical skills in firewall configuration, using a secure VPN connection, and testing Denial of Service (DoS) attack (Hoque et al. 2013). To achieve the aforementioned purposes, we configured the Cisco 1941 router to work as a VPN server with external IP address 130.240.2xx.xxx, and with the same interfaces and configurations mentioned in the previous laboratory assignment. Fig. 3 shows the network topology of the firewall configuration and testing assignment. A Cisco Adaptive Security Appliance (ASA) 5505 was used as a testing firewall (Hucaby 2007). The firewall was connected to the switch via a firewall Ethernet port (0/0), and to one Ethernet interface of the computer via a firewall port Ethernet (0/1) for testing purposes. The other Ethernet interface of the computer was connected to the firewall port (0/2) for management purposes with assigned IP address 10.10.10.7. The

computer COM port was alternately connected to the router and to the switch console ports for management purposes. Students also conducted this laboratory assignment in two phases. In the first phase, they connected to the VPN server using the router external IP address (130.240.2xx.xxx) and a Cisco VPN client installed locally on their computers. Upon successful connection, the students had access to all the equipment behind the router. In the second phase, the students used the remote desktop connection to access the firewall management computer. Later, the students used Cisco Adaptive Security Device Manager (ASDM) software for firewall configuration and management. It is worth noting that students had access to a limited user account in the firewall management computer in order to avoid any risk of attack on the university network. During the experiment, the students contacted the firewall graphical user interface, configured the firewall external and internal interfaces, and set traffic permit and deny rules to create a trusted network against DoS attack.

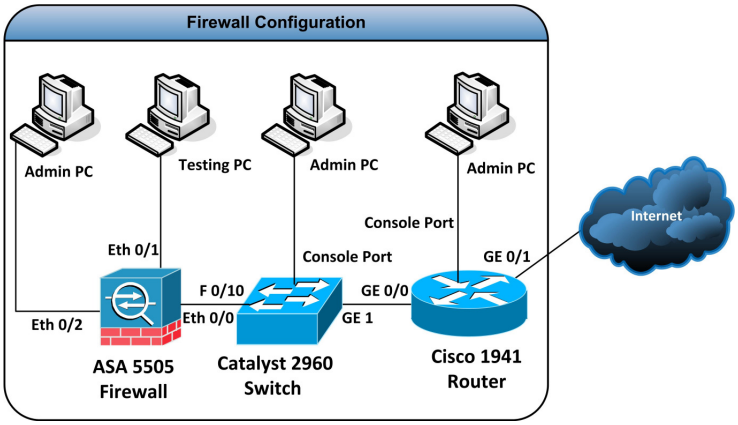

Figure 3: Firewall configuration and testing

4.2 Reflection and Learning

The building of the Online InfoSec Lab, intervening by implementing it in a pilot course on server security architecture and evaluating its effect generated six design principles. These principles are listed in Table 2. The evaluation also disclosed the implications for building an Online InfoSec Lab that are shown in the right hand column of Table 2. The stakeholders identified in the ADR team were researcher, teachers, developer and teacher assistants. As the ADR method suggests during preparation of the alpha version, a formative assessment takes place. Hence, the initial version of the Online InfoSec Lab was tested by the development team to unveil its weaknesses at an early stage and correct them before launching the system for testing by the students. The development team was generally satisfied with several aspects of the Online InfoSec Lab. During the lab development and alpha testing process, it was revealed that it is necessary to make the lab robust to ensure that students cannot damage lab configurations. Thus, the principle of *robustness* (emerged during BIE) was applied. By considering the robustness principle, the laboratory should be able to handle any student misbehaviour that may damage

laboratory software or hardware facilities. The robustness issue could also be managed by providing the students with a clearly stated, step-by-step assignment, monitoring student behaviour, and building backups for the working configurations (Miloslavskaya 2004). During the implementation phase of the ADR process, end users (teachers, assistant teachers and students) were involved in the process for experience and the beta version of the Online InfoSec Lab was put into action. A survey questionnaire was sent to the students to inquire about their experience of using the online information security lab for the first time in the M.Sc. programme on information security. The results show that the majority of the students liked the idea of the personalized instructions provided for them regarding assignment tasks. Lab performance was rated satisfactory where the majority of the students agreed that it was easy to establish a connection remotely. However, some students mentioned minor issues concerning disconnection during lab work.

Design Principles	Impact
Contextualization	Contextual factors need to be obtained from organizational goals, course goals, teacher goals, constraints, and requirements. Pedagogical approach.
Collaboration	Regular meetings should be held between different stakeholders of lab for design, development and implementation purposes. Researcher (acts as instructional designer), practitioners (developer, IT staff) end users (teachers, proctor, students)
Flexibility	Remote access to lab resources. Lab activities should be modularized. Lab Should be accessible without interruption to students preferably 24/7 or at least, when a student books a particular time for lab activities.
Cost-effectiveness	Optimal resource allocation to develop the lab. Virtual technologies can be utilized to keep expenses low.
Scalability	Lab can be upgraded and easily modified based on the practical requirements of different courses.
Robustness (emerged principle)	Handle inadvertent damage by users. Quickly recover configurations. Prepare back-ups of assignment configurations.

Table 3: Design principles for Online InfoSec Lab

5 Discussion

This research contributes by showing the design, development and implementation of an Online InfoSec Lab aimed at the improvement of hands-on education and the evaluation of its use in context. The study also described the ADR process through Online InfoSec Lab intervention in the server security architecture course. The outcome and the student feedback show that the proposed integrated environment is useful as a learning tool. The results show that the project has

been successful with positive outcomes and feedback from stakeholders involved, and from the university administration as a primary stakeholder in this process. The stakeholders are ready for further instantiations of the Online InfoSec Lab in other courses for the next phase of the project. In this BIE process, the researcher developed the initial design principles, which were reciprocally shaped together with other stakeholders. These principles were not given much attention in previous similar works (Choi et al. 2010; Burd et al. 2009; Gaspar 2008 and Li, C. 2009).

Initially, during the problem formulation stage of the ADR method, a theoretical framework based on Constructive Alignment Theory (Biggs 1996) and Conversational Framework (Laurillard 2002) was prepared and used to analyse existing e-learning resources and courses. The theoretical framework was prepared in the light of the principle of theory-ingrained-artefact, which emphasizes that the ensemble artefacts created and evaluated through ADR are informed by theories. Furthermore, the Personalized System of Instruction approach (Keller 1968) has been used as a kernel theory in this article to support the design principles for the development of an Online InfoSec Lab and related exercises.

Existing studies present an InfoSec Lab as a single entity only composed of IT infrastructure, and present other activities and entities as a black box. However this study shows it is necessary to restructure the InfoSec Lab and design it instead as an ensemble artefact. Existing studies rarely suggest any explicit design principles to make the proposed lab adaptable according to the contextual requirements of teachers in different institutions and for different courses. We proposed and applied design principles such as (contextualization, collaboration, flexibility, cost-effectiveness, scalability and robustness) based on empirical study.

The design principles, specifically contextualization, collaboration and flexibility, are important findings that are mostly absent in earlier published work (Choi et al. 2010; Burd et al. 2009; Gaspar 2008 and Li, C. 2009). For instance, following the contextualization principle, the lab experiments must be contextualized based on the input from programme and course goals in order to align the theoretical and practical elements of the curriculum. The contextualization principle guides the teacher to select appropriate lab exercises for security skills development by the information security students. Furthermore, the pedagogical approach required is also selected in the light of the contextual requirements of the course, for example the PSI approach was selected for designing and offering the Online InfoSec Lab exercises to the students in the case under consideration in this article. The PSI approach helped to divide the course content and lab exercises into lower and higher level modules in such a way that student's mastery of course content could be improved. Furthermore, the PSI approach supported the design of individual lab exercises and provided individual feedback to the students, which was an important requirement for distance students on this course. The principle of collaboration guided the researcher, developer, IT staff, teacher, student and lab assistant to collaborate with each other on different occasions during the BIE activities. This collaboration is of extreme importance as it facilitates different stakeholder participation and mutual discussion in the BIE activities of the ADR research process in order to develop an efficient and effective artefact. The principle of flexibility has several implications from the teacher perspective, such as providing a flexible method of remote access to the lab resources, preferably 24/7. In addition, the flexibility principle also

stipulates a flexible lab booking system for the students in order to facilitate their undertaking of lab exercises at their desired time and pace.

In most cases, existing research lacks pedagogical underpinning for designing lab exercises (Iqbal and Päivärinta 2012). Design principles such as contextualization, collaboration, robustness and flexibility offer practical contributions to removing the barrier of time and location, improving mastery of course content and promoting individualized learning by following flexible pedagogical approaches to design lab exercises. The design principle of contextualization helps to clarify the scope and purpose of the Online InfoSec Lab by considering relevant contextual factors. Moreover, the target ensemble artefact will emerge via the iterative process based on ADR methodology that will provide a holistic picture of the teaching context in which the lab will be used. Furthermore, researchers and teachers will be able to develop specific design exemplars based on different lab experiments in the various, separate courses included in an information security programme at graduate level. In addition, the reflective knowledge produced during collaboration among the researchers, developers and end users will help to refine the artefact and the processes for accomplishing some tasks. Finally, this could lead towards refinement of emergent design principles. Overall, the design principles proposed in this study provide guidelines for teachers and developers to align their teaching/learning activities in their courses in order to achieve specified course objectives, and consequently enhance the quality of hands-on teaching.

We agree with Orlikowski and Iacono (2001), and share their view that the IT artefact should be theorized properly in order to unfold the ensemble view of the artefact, instead of merely clinging to using technology as a black box. For example, during the design, development and implementation process of the Online InfoSec Lab, it was realized that there are many different stakeholders involved in this entire process. These stakeholders also collaborate with each other on different occasions based on the contextual needs arising during the design and development process. For example, since the beginning of the project on InfoSec Lab development, different actors have influenced and participated at different stages of BIE process. This situation demands that we describe the different entities of the Online InfoSec Lab in detail in order to understand the role of the different stakeholders in the design, development and implementation process of the lab and its related exercises. Thus, the ensemble version of lab should describe the web of equipment, techniques, applications and people that define a social context, the infrastructure that supports its development and use, and the social relationships and processes that make up the terrain in which people use it (Orlikowski and Iacono 2001). This is the agenda for further research avenues.

6 Conclusions

The problems perceived in the teaching of master's programme in information security include low levels of hands-on exercise availability, mastery of course topics, and absence of an Online InfoSec Lab. Furthermore, we found that an explicit pedagogical approach and design science research method were also undermined in existing works. Hence, in order to provide the students with flexibility in their learning and practicing of security skills from distance, freely without

time and location constraints, we were led to design and develop an Online InfoSec Lab. We employed the ADR approach. The study introduced a learning environment that is designed to meet the active learning preferences of information security students in the mixed classroom, and also support flexible, individual, hands-on learning. In this paper, we assumed that the problem identified in this particular study is the absence of productive media for hands-on education in information security courses at graduate level, and the solution proposed is a pedagogical, Online InfoSec Lab implementation. Further research focuses on generalization of this problem and solution to the class of problem i.e. hands-on learning exercises through an Online InfoSec Lab. Likewise, the abstract problems such as lack of pedagogically-based e-learning platform for hands-on education of IS security, and the abstract solutions such as an Online InfoSec Lab based on a pedagogical approach. In our further iteration, we will continue with the ADR research method and develop other courses in the information security master's programme based on other pedagogical approaches in addition to those defined in this research project. This will also help to verify and capture the emerging design principles in order to produce further systematized knowledge to contribute to the theorizing of the process of building, implementation and evaluation of an Online InfoSec Lab. Future research will also look into the framework of (Lee et al 2011) as an organizational device to structure discussion and terminology in order to distinguish between activities that occur in implementation and activities that occur in abstraction and theorizing (Gregor et al 2013).

References

Ayyagari, R., and Tyks, J. (2012). "Disaster at a university: a case study in information security", Journal of Information Technology Education: Innovations in Practice. Volume 11.

Biggs J. (1996). "Enhancing Teaching through Constructive Alignment", Higher Education, Vol. 32 No.3 pp. 347-364

Crawford, E., and 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.

Crosbie, J., and Kelly, G. (1993). "A computer-based personalized system of instruction course in applied behaviour analysis". Behaviour Research Methods, Instruments, & Computers, 25, 366-370.

Cumming, B., and C. McIntosh. (1982). "PSI in Engineering Mathematics". Journal of College Science Teaching 12(1) 30-31.

D. Fowler. (1999). "Virtual Private Networks: Making the Right Connection", ser. Morgan Kaufmann series in networking. Morgan Kaufmann Publishers.

D. Hucaby. (2007). "Cisco ASA, PIX, and FWSM Firewall Handbook", Second Edition, 2nd ed. Cisco Press.

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.

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.

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

Gregor, Shirley, Ahmed Imran, and Tim Turner. (2013). "A 'sweet spot' change strategy for a least developed country: leveraging e-Government in Bangladesh." European Journal of Information Systems

Hentea, M. (2005). "A perspective on achieving information security awareness". Issues in Informing Science and Information Technology, 2, 169-178.

Hentea, M., Dhillon, H. S., Dhillon, M. (2006). "Towards Changes in Information Security Education". Journal of Information Technology Education, 5, pp.221-233.

Hirschheim, R. and 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.

Householder, K. Houle, C. Dougherty. (2002). "Computer attack trends challenge Internet security", IEEE Comput. 35 (4) 5–7

Hrastinski, S., Keller, C., and Carlsson, A. S. (2010). "Design Exemplars For Synchronous E-Learning: A Design Theory Approach". Computers & Education 55 652-662.

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

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

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 2013. LNCS, vol. 8167, pp. 89–100. Springer, Heidelberg

J. C. Neumann. (2009). "Configuring a VPN using IPSec," in Cisco Routers for the Small Business. Apress, , pp. 81–103.

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

Koen, B.V. (1971). "Self-Paced Instruction in Engineering: A Case Study". IEEE Transaction on Education Volume 14(1) p.24-31

Laurillard, D. (2002). "Rethinking teaching for the knowledge society". EDUCAUSE review, January/February. Available online: http://www.educause.edu/ir/library/pdf/erm0201.pdf

Lee J, Pries-Heje, J and Baskerville, R. (2011). "Theorizing in design science research". In Lecture Notes in Computer Science (JAIN H, SINH A and VITHARANA P, Eds) Service-oriented perspectives in design science research (6th DESRIST) pp 1–16, Springer, Milwaukee, MI.

M. D. Soete. (2011). "Secure shell," in Encyclopaedia of Cryptography and Security, H. C. van Tilborg and S. Jajodia, Eds. Springer US, pp.1252–1253.

M. Yoon, S. Chen, and Z. Zhang. (2010). "Minimizing the maximum firewall rule set in a network with multiple firewalls," IEEE Transactions on Computers, vol. 59, no. 2, pp. 218–230, February.

N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita. (2013). "Network attacks: Taxonomy, tools and systems," "Journal of Network and Computer Applications, no. 0, pp. –,.

N. Miloslavskaya, A. Tolstoy, and D. Ushakov. (2004). "Laboratory support for information security education," in Information Security Management, Education and Privacy, ser. IFIP International Federation for Information Processing, Y. Deswarte, F. Cuppens, S. Jajodia, and L. Wang, Eds. Springer US, August, vol. 148, pp. 101–116.

Nilsen, H., and 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.

Pear, J.J., M. Novak. (1996). "Computer-aided personalized system of instruction: A program evaluation". Teaching of Psychology 23(2) 119-123.

R. Droms. (1997). "Dynamic Host Configuration Protocol," RFC 2131 (Draft Standard), Internet Engineering Task Force, March, updated by RFCs 3396, 4361, 5494.

R. Droms. (1999). "Automated configuration of tcp/ip with dhcp," IEEE Internet Computing, vol. 3, no. 4, pp. 45–53.

S. M. Bellovin and W. R. Cheswick. (1994). "Network firewalls," IEEE Communications Magazine, vol. 32, no. 9, pp. 50–57, September.

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

Suranjith and Amina. (2005). "Internet security games as a pedagogic tool for teaching network security", IEEE.

Van Niekerk, J., and 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 2010, IFIP AICT 324, pp.412-423.

W. J. Orlikowski and C. S. Iacono. (2001). "Research commentary: Desperately seeking the 'IT' in IT research—A call to theorizing the IT artifact", Inf. Syst. Res., vol. 12, no. 2, pp. 121–134.

W. Stallings. (1997). "Data and Computer Communications", 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, Inc.,. www.informatics.indiana.edu/markus/documents/security-education.pdf

Wilson, M., and Hash, J. (2003). "Building An Information Technology Security Awareness And Training Program". NIST Special Publication 800-50.

Yurcik, W., and Doss, D. (2001). "Different Approaches in the Teaching of Information Systems Security". Information Systems Education Conference, Cincinnati OH. USA (ISECON).