Conceptual Model of Online Pedagogical Information Security Laboratory: Toward an Ensemble Artifact

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

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

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

Tero Päivärinta
Luleå University of Technology, Sweden
tero.paivarinta@ltu.se

Abstract

Distance education in information security has unique requirements in comparison to on-campus education. For instance, an online InfoSec lab is required to provide hands-on education to distance students while development and operation of a lab is a non-trivial problem. There is a need to understand the nature of the online InfoSec labs as ensemble artifacts, and just a black-box tool's view is not enough. This article suggests a conceptual model to explain the ensemble view of the online InfoSec lab. In doing so, the paper makes two specific contributions: First, it conceptualizes the online Information Security (InfoSec) lab as an ensemble artifact so that we can unfold the black-box view of an InfoSec lab and understand the important building blocks (entities of the lab) and their interrelationships. Second, it suggests design principles to implement the conceptual model of an InfoSec lab.

1. Introduction

Recent research shows a huge shortage (20,000 to 30,000) of qualified cyber security specialists [1] in the United States, while networking giant CISCO in its report predicts the shortage of more than a million security specialists all around the globe [2]. Following the growing need for skilled InfoSec personnel, many universities offer graduate-level programs in information security to distance students. Distance education has unique requirements in comparison to on-campus education [3]. For instance, an online InfoSec lab is required to provide hands-on education to distance students. However, the provision and maintenance of hands-on laboratory experiences to distance students is very challenging. Furthermore, distance students require a flexible mode of education in terms of time and space, so that they can continue their education in a way that will not hinder their job routines. Previous study advocates that the information security graduates should master hands-on approach in addition to theoretical education [4]. The information security laboratory allows implementation of hands-on laboratory experiences, which are vital elements of information security education at graduate level. Hence, to pursue the ongoing research initiative, the following question was framed, "How to design an online pedagogical InfoSec lab to improve flexible hands-on education in the courses?"

A recent literature review [4] revealed the general absence of specific design methods focused on online InfoSec lab development. The review [4] also shows that the literature studied for this research mostly focuses on the tool view of online InfoSec labs by providing mostly the technical details of the labs. The lack of explicitly described pedagogical approaches and concrete design principles for designing and developing online InfoSec labs in the existing literature hinders the accumulation of technically and pedagogically rigorous knowledge [5]. Hence, there is a need to understand the nature of the online InfoSec labs as ensemble artifacts [6] because just a black-box tool's view is not enough [7]. The ensemble is defined as a "web of equipment, techniques, applications, and people that define a social context including the history of commitments in making up that web, the infrastructure that supports its development and use, and the social relations and processes that make up the terrain in which people use it" [7]. Action Design research (ADR) [6] can be employed to conceptualize the ensemble artifact as a result of emergent perspectives on design, use, and refinement in context through continuous interaction between technology and organization during the process of design [5]. A stream of researchers [6], [8]–[10] propose that information systems research must respond to a dual mission by making theoretical contributions and providing assistance in solving the current and anticipated problems of practitioners.

This article proposes a conceptual model of an online InfoSec lab to be used for pedagogical purposes. The conceptual model intends to clarify the issues related to design, development, implementation and management of online InfoSec labs. For instance, in

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.16

this case, Luleå University of Technology searched for a design exemplar of a pedagogical online InfoSec lab to adapt the design according to our pedagogical requirements. However, the literature review [4] shows there is a general absence of pedagogical approaches in the design and development of online InfoSec labs and related exercises. Problems such as this hinder efforts of information security teachers to adopt ready-made solutions available in the literature due to the lack of theoretical clarifications underlying the available solutions. The important challenge in the online InfoSec lab research has been in the difficulty of understanding the general level of empirical descriptions of online InfoSec lab development into effective Socio-technical design principles that promote their development and management. Design and development of online InfoSec labs requires a socio-technical approach [7] that will help the academic community to understand their complex and fragmented emergence as socio-technical systems. From a technical point of view InfoSec lab design and development requires technical implementation, integration and control of IT capabilities. From a social point of view, it requires organizing the online InfoSec lab and providing a connection for different actors [11] with relevant interests in ways that promote further advancements in the design and development of online InfoSec labs. The ensemble artifact emerges out of this socio-technical confluence [6].

To unfold this ensemble perspective, we draw a conceptual model of the online InfoSec lab in this paper. The ensemble lab consists of four intertwined entities: exercise, exercise processing and management interface, lab infrastructure, and concrete exercise interface. The details of the conceptual model are provided in the Section 4. The paper is organized into six sections. In the next section, Section 2, we briefly discuss the related research work. Section 3 discusses an illustrative example of an online InfoSec lab exercise. Section 4 discusses the conceptual online InfoSec lab model. Section 5 describes the initial design principles. Finally, Section 6 concludes the paper with discussion and future research agenda.

2. Related research

Orlikowski and Iacono [7] suggest that researchers should theorize about the IT artifacts explicitly and incorporate those theories into their studies to enhance the contribution of their work. Five meta-categories of conceptualizing the technology have been proposed [7] such as the tool view, the proxy view, the ensemble view, the computational view, and the nominal view. The ensemble artifact should show a complete picture of the whole process, including the design and development process of the exercise, the role of stakeholders involved, the structure of different entities of the lab, the pedagogical approaches underlying the exercise design, the pedagogical alignment of lab exercises with rest of the course content, the interconnection of different stakeholders belonging to different entities, and the realization of the exercise design that takes place before the lab activities are actually conducted in the lab environment.

An InfoSec lab can be used for several purposes (tutorials, exercises, demonstrations, simulations, webinars, films and videos), where the teacher plays an important role in deciding lab activities based on specific course goals [12]. Furthermore, the online InfoSec lab is an IT artifact that is composed of a collection of hardware and software components that can be accessed through the Internet or intranet. The lab may be used in two ways, either the teacher or lab assistant can lead the lab activities [12], or the lab could be configured in such a way that it becomes automated. The systematized lab is ready for the students and the exercises that they will do without the presence of a teacher or instructor.

A recent literature review [4] revealed that most of the articles view labs as tools for achieving goals, without paying much attention to the whole package, in other words, thinking little about elements of the curriculum and the rationale behind it. Furthermore, most of the reviewed articles did not explicitly identify the core entities of an InfoSec lab, nor did they define the relationship between different entities of a lab. The articles reviewed also paid little or no attention to the issues of pedagogical alignment of lab activities and pedagogical theories[4]. Thus, the choice of appropriate pedagogical approaches for specific lab exercises remains a challenge, because the teachers do not get enough information on which pedagogical approaches to design exercises will be beneficial for achieving which learning outcomes. The literature reveals that virtual laboratories based on virtual technologies are gaining popularity due to the cost-effective features of virtual technologies [13]–[17]. Remote virtual computing labs have been suggested [16] [17], with a brief discussion of infrastructure and exercises that make use of the lab, yet without a detailed description of any explicit design method or any pedagogical approach adopted to design and develop a lab and relevant exercises. Similarly, virtual security laboratories [13], [14], [18], [19] have been proposed. Some of these laboratory ideas do not include any explicit descriptions of infrastructure [18] [15]. Although, good discussions about physical and virtual computing laboratories [14] have been provided, most of the details include technical

discussions [13]that present just the tools view [7] of InfoSec labs.

Overall, the literature review results show that most focused on the technical details of the labs while ignoring the description of unfolding the black box of the lab to see who the different stakeholders for the different entities of the lab are. The absence of focus on roles of stakeholders, design methods, pedagogical theories and testable design propositions [20] also raises concerns over how these ideas have been validated / evaluated. In the next section we discuss an example of an exercise to briefly illustrate the process of developing an online InfoSec lab exercise.

3. Pilot exercise

A brief background of this ongoing research work follows herein. Luleå University of Technology offers an MSc program in information security to both on-campus and distance students. The Information Systems department of the University is planning to design and develop an online information security laboratory (InfoSec lab) due to an increase in number of distance students (around 70% of total). To find the answer for our research question (see Section 1), we conducted a literature review, semi-structured interviews with teaching and management staff from the MSc program of information security, and case analysis of an Internet security course [4][5] [21]. Furthermore, feedback from students was also obtained. The interviews, observations, literature review, and reflection on the pedagogical approach (personalized system of instruction, PSI [22]) helped us to derive an initial set of design principles to guide the design and development of an online InfoSec lab [5]. The initial design principles (Contextualization, Collaboration, Flexibility, Cost-effectiveness and Scalability) were derived keeping in view the hands-on exercises requirement of an information security course. The design principles incorporate a socio-technical perspective so that the resultant artifact based on these principles should be an ensemble artifact.

Thereafter, in order to get a realistic feeling and in-depth understanding of the whole procedure from planning a lab exercise to designing and implementing a lab exercise in an online InfoSec lab, we have considered a pilot test of the design and development of a simple exercise "Firewall Configuration and Testing." The exercise was selected after the teacher of a course called "Server Security Architecture" volunteered to be a part of the team. The teacher, assistant teacher, developer, researcher, two guest users (to test the system), and the IT support personnel participated and collaborated in this pilot testing. 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 a transverse network traffic passing through it [23]. A firewall is an important network device that is used to create a trusted network segment. In order to mitigate the rules' complexity, multiple firewalls can be used with complementary sets of rules [24]. The purpose of this assignment is to enrich the students' technical skills for firewall configuration and testing for protecting server security architecture against denial of service (DoS) attacks [25]. The firewall exercise module has been planned to match the goals of the server security architecture course.

The exercise processing started when the teacher and assistant teacher prepared the written draft of the lab exercise according to contextual requirements of the course and provided it to the developer. The developer was informed during a meeting with teacher that the exercise is for individual students based on PSI principles [22]. The exercise processing and management unit started to manually select the required facilities from the available laboratory hardware platform. Accordingly, the developer started to configure a Cisco 1941 router to work as a VPN server with external IP address 130.240.2xx.xxx in order to provide a secure access method for the exercise module. Figure 1 shows the network topology of the firewall configuration and testing exercise module. A Cisco Adaptive Security Appliance (ASA) 5505 was used as a testing firewall [26].

The Firewall ((ASA) 5505) 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 purpose. The other Ethernet interface of the computer was connected to the firewall port (0/2), for management purposes, with an assigned IP address 10.10.10.7. The computer COM port was alternately connected to the router and the switch console ports for management purposes. The guest users conducted this laboratory assignment in two phases. In the first phase, they connected to the VPN server using the router's external IP address (130.240.2xx.xxx) and a Cisco VPN client installed locally on their computers. Upon a successful connection, the guest users had access to all equipment behind the router. In the second phase, the guests used the remote desktop connection to access the firewall management computer.

Later, the guests used Cisco Adaptive Security Device Manager (ASDM) software for firewall configuration and management. It is worth noting that guests had access to a limited user account on the firewall management computer, in order to avoid any risk of attack on the university network. During the

experiment, the second step of the exercise Processing and management unit started to monitor the students' behaviors and make any required intervention in order to make sure that the exercise was conducted the same way it was designed for. During the experiment, the guest users got in touch with the firewall graphical user interface, configured the firewall external and internal interfaces, and set traffic permit and deny rules for creating a trusted network against DoS attack.

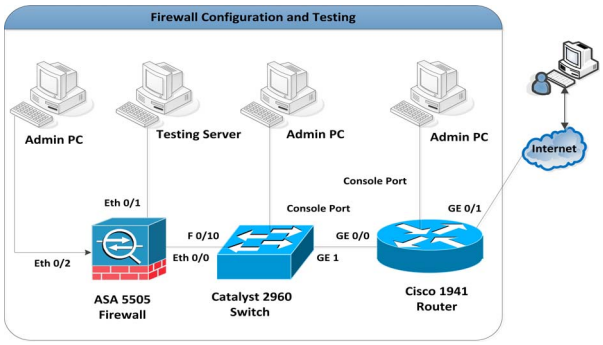

Figure 1. Firewall configuration and testing

The preparation of an exercise design and its pilot implementation and testing with two guest users helped us to understand and propose the conceptual model of an online InfoSec lab as an ensemble artifact (described in detail in Section 4).

4. A conceptual model for an InfoSec lab as an ensemble artifact

The ensemble view of an IT artifact includes interaction between social context, technology, and infrastructure. Following this ensemble view, the scenario of hands-on lab exercises can be considered as the teacher organizes the lab activities based on the desired course goals. The teacher prepares the detailed written lab exercises including descriptions of underlying pedagogical approaches and hands over these exercises to the lab exercise processing and management interface (EPI) administrator / developer. The developer should have a clear written exercise document. In addition to that, the teacher and lab developer will need to have a discussion in order to set clear goals for the lab assignment. This way, the developer will become more aware of the assignment, and can select better resources and the appropriate method for providing access to these resources. Thereafter, the exercise processing and management interface (EPI) works as a bridge between the actual physical resources (lab infrastructure) and the concrete lab exercise topologies (see Figure 2). The lab administrator or developer responsible for the management process takes into consideration the exercise design and decides the physical and virtual resources to be used for preparing every individual lab exercise topology. The design of exercise topology is influenced by the underlying pedagogical approach. Subsequently, different topologies for different exercises are prepared. Each lab exercise has its own interface. The roles of different actors such as teachers, assistant teachers, and students are described and access privileges are designed as required.

This scenario and the observations from the literature review inform us that there are a few important entities (see Figure 2) intertwined in an online InfoSec lab such as the:

- Exercise
- Exercise processing and management interface (EPI)
- Lab infrastructure
- Concrete exercise interface

The subsequent sections further describe each lab entity in detail.

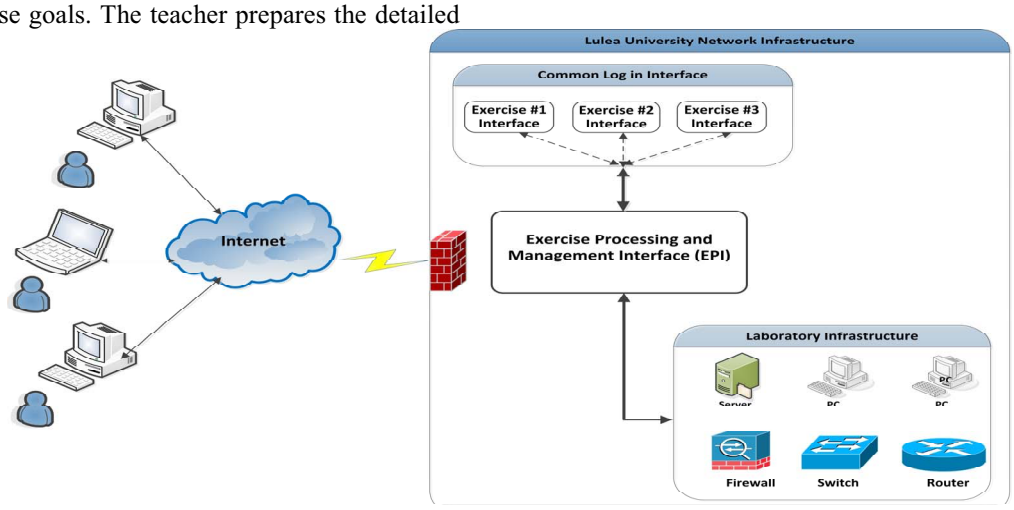

Figure 2. Conceptual model of an online InfoSec lab

4.1. Exercise

In the Oxford dictionary, the word "exercise" is defined as "an activity carried out for a specific purpose," and "a task set to practice or test a skill." The role of hands-on exercises in information security is of a vital nature [12][4] in order to produce and enhance the security skills of information security students. In the existing literature, the design of lab exercises has been discussed briefly [16]–[19], [27]–[30]. A lab exercise is a written plan to carry out some specific tasks to achieve particular goals. The exercise not only guides the students or end users to conduct different lab activities in a step-by-step manner, but it also provides guidelines for the developer to generate the final lab exercise interface for end users. It is very important to understand the nature of the exercise, because it has a direct impact on the students' learning and the interrelationship of different actors in the lab atmosphere.

Hands-on exercises included in a course should guide the student to implement the theoretical principles studied in that course. Thus, the lab exercises should be pedagogically aligned with rest of the teaching and learning activities in that course. The students' learning activities are considered the central aspect of the Constructivism-related theories [31][32]. Constructive alignment theory [31] puts forward the guidelines for the teachers to plan and align the teaching / learning activities and relevant assessment methods in light of the course goals. Hence, the design of the exercise should be guided by a specific pedagogical theory. In fact, an information security student needs to be trained to combat information security threats both individually and as part of security team. There are different pedagogical theories that can be used to design information security exercises to enhance students' individual as well as collaborative security skills. For example, personalized system of instruction (PSI) [22], computer supported collaborative learning (CSCL) [33], and cooperative learning strategy (CLS) [34] are a few to be named. In the illustrative example in Section 3, the PSI approach has been employed to develop an exercise for individual students.

The exercise has its own stakeholders, which may include but are not limited to teacher, assistant teachers, and program coordinator. The role of the teacher in selecting and preparing the suitable lab exercises for students is vital. Assistant teachers also participate in the preparation of lab activities and exercises. The constructive alignment theory [31] provides guidelines to the teachers to prepare the teaching and learning activities prior to the start of the course. From a holistic perspective, the program coordinator should be involved in the decision-making processes regarding the alignment of different course goals to the program goals. In this way, early communication between different teachers and the program coordinator will make sure that all the lab exercises in the individual courses contribute to achieving the overall program goals.

4.2. Exercise processing and management interface

Exercise processing and management interface (EPI) represents an entity that includes the lab developer, administrator, and IT personnel. The EPI unit has many roles in preparing the lab design, development, implementation of exercises, and maintenance. In other words, they take part in: 1) selecting and ordering the required hardware and software resources for lab infrastructure, 2) preparing the individual exercise topologies with their own interfaces and, 3) monitoring the lab functionality and providing the necessary management and maintenance services. A major role of the lab developer in the EPI unit is to initiate the design and development of lab exercises based on the design presented in the written exercise plan provided by the teacher. When the developer reads that document and collaborates with the teacher via further discussions, the real design process starts. Once the developer reads the initial written exercise plan provided by the teacher / teacher assistant, the real hidden challenges of obtaining the desired design of the lab exercise are unveiled. The stakeholders including teacher and developer at this point can mutually agree to make suitable changes in the design of the lab based on available resources and other feasibility constraints. This collaboration in turn will also have an effect on the written exercise plan that might also be updated in order to match it with the actual possible solution with available hardware and software resources in the lab infrastructure.

EPI is also responsible for access management. Access management is possible in different ways. For example, access to a specific lab exercise can be provided via a specific interface designed for that exercise. On the other hand, a common login interface for the online InfoSec lab can be developed. All the users will enter the lab through this common interface with the only difference being that when a user accesses the lab using an authenticated username and password, he / she has access to only those lab exercises which they are supposed to do (this rule is

defined using the pedagogical approach selected for the course and lab activities). For instance, the teacher's plan is to provide three individual lab exercises to the students of a server security architecture course. The teacher's goal in this context is to improve the individual learning skills of the information security students in a step-by-step manner. The pedagogical theory, which matches the goal mentioned above, is a personalized system of instruction (PSI, Keller 1969). Three individual lab exercise modules can be developed following PSI principles in such a way that the students are provided access to a lower-level lab exercise module. The students cannot obtain access to a higher-level exercise module until they pass the lower-level exercise module. This process can be obtained using automated scripts in the lab configuration. Furthermore, EPI is used to set up the servers, resources, and targets according to the requirement of a particular exercise.

4.3. Lab infrastructure

Lab infrastructure consists of the hardware, software, network resources and services required for the development, operation, and management of an information security lab environment. It also includes a specific lab room for all the physical equipment. The lab infrastructure is used to provide access to lab resources for teachers, researchers, and on-campus and distance students of information security programs. Hence, there are a lot of stakeholders involved in the process of defining the required lab infrastructure such as developers, teachers, researchers, IT staff, and management personnel. The feedback from end users such as students is also very important when it comes to updating the lab infrastructure regularly. For instance, in the initial phase of this project, the meetings were held with all the teachers and management staff in the information security MSc program. The decision makers from top management were also engaged in this process. The issues from overall program goals, to individual course goals were discussed to obtain a good picture of how much funding will be needed to initiate this process and finally implement it. Normally, an online InfoSec lab infrastructure will include the following components (as described in Section 3):

Hardware: Servers, client computers, switches, hubs, routers, firewalls, and so forth.

Software: Server operating systems, client operating systems, virtual machines, and so forth.

Network resources: Network deployment, isolated Internet connectivity for remote access, setting up firewall and other security features.

Users: Lab administrators, developers, teachers, students, and researchers.

4.4. Concrete contextual exercise interface

The concrete contextual exercise interface is the fourth entity of an online InfoSec lab. The concrete contextual exercise interface is produced as an output of the process that takes place in exercise management and processing interface. The teacher, assistant teacher, and students are the main stakeholders of this entity. The student or end user accesses the lab via a common lab interface by providing an authenticated user name and password. When the students provide their necessary credentials to enter the lab, they are immediately directed to access the specific contextual exercises that they have been authorized to access. The student accesses the individual exercises that they want to do by clicking the icon of that exercise. Once the actual exercise interface is opened, it will show the student the resources and targets for that exercise. This interface offers the remote student the opportunity to operate the equipment provided or resources in almost the same way as if physically present in the lab.

5. Design principles of an online InfoSec lab

In order to fully grasp the idea of design and development of an InfoSec lab for distance students from an ensemble perspective, the next step was to focus on available resources of the ongoing research project and to prepare a simple pilot exercise. (see Section 3). This further investigation broadened our vision, giving us understanding of the important lab entities, the stakeholders involved, and the underlying invisible interconnection between these actors. Our enhanced understanding in light of the new knowledge that emerged during this design process, based on literature review and pilot exercise testing, lead us to further enhance our initial design principles. As per the emergent knowledge, we identified four interrelated entities of an online information security lab including the exercise (written document), lab infrastructure (hardware, software, network resources, etc.), exercise processing and management interface (EPI), and the concrete exercise interface. Each individual lab entity encompasses its own stakeholders and functionality and thus implies different design principles. Here we present the initial design principles for each entity of the ensemble artifact.

Table 1. Initial design principles for an InfoSec lab

Lab Entities	Design Principles
Exercise	• Contextualization based on course goals • Pedagogical alignment of lab activities • Flexible learning
Exercise processing and management Interface (EPI)	• Isolate the lab network • Flexible configuration management • Ease of remote access • Availability of lab resources • Collaboration
Lab infrastructure	• Contextualization based on program goals • Scalability • Easy Configuration and reconfiguration • Back-up and Recoverability • Hardware integration • Cost-effectiveness
Concrete exercise interface	• User friendly interface with properly arranged resources and targets • Easy to use • Tracking and debugging errors

We will briefly discuss the initial design principles from each category to elaborate their clear meanings.

5.1 Design principles for exercise

5.1.1 Contextualization based on course goals. This principle suggests that at the course level, the classroom environment should be contextualized for specified tasks which will be mainly guided by course goals. This principle refers to the contextual factors including state of the art of technology to be used for lab exercises, the details of how the journey of the student from position "B" will be to the desired position "A." B and A represent the two different cognitive levels of a student, one before (B) starting the lab exercise, and the second after (A) the student has performed the prescribed exercise. The purpose is to conceptualize and plan for the afterwards ideal condition when the student is supposed to be equipped with more skilled knowledge than before. Furthermore, the contextual factors to be considered at this stage include the scope of the exercise (how simple or complicated it will be), individual vs. collaborative student work, how much time should be allocated for exercise, whether the students will be helped by a teacher / teacher assistant or they will get help from the lab resources automatically.

5.1.2. Pedagogical alignment of lab activities. The pedagogical alignment of lab activities with the rest of the theoretical part of the course is vital. This principle guides the teacher and assistant teacher (main stakeholders of the exercise document) to pre-plan the lab activities before the course start. Thus, the hands-on lab exercises will be used to strengthen the core issues studied during the course and the students will be able to implement the practical solutions in the lab in light of the studied literature. Furthermore, the selection and role of the pedagogical kernel theories are also defined in this principle. The teacher selects the pedagogical theories while keeping the learning goal of the exercise in view, for example, sometimes enhancing individual learning skills vs. collaborative learning.

5.1.3. Flexible learning. The flexible learning principle partially depends on the pedagogical approach selected for the exercise. For example, the personalized system of instruction approach (PSI) [22] guides the teacher to break up the practical lab exercises into smaller modules. The modular approach helps to provide a flexible mode of learning to students. The flexible learning approach also refers to the remote access to lab resources; for instance, the lab should be accessible for experiments from everywhere, any time in order to facilitate the students who are professionals, want to work individually, and / or cannot work under a strict schedule (i.e., go at your own pace).

5.2 Design principles for EPI

5.2.1. Isolate the lab network. Lab isolation is a crucial issue in order to avoid any data/packet leakage during an exercise, as in an attack - defense exercise, for example. Moreover, EPI should take care of protecting the lab infrastructure from any outside attack. The EPI should arrange the access to the lab network in such a way that the lab network can still be isolated. The lab and external network should be isolated properly in order to eliminate concerns from the campus network [35].

5.2.2. Flexible configuration management. The EPI should allow flexibility for easy configuration of the concrete lab exercise interface management based on the particular context.

5.2.3. Ease of remote access. Issues related to bandwidth should be considered while planning for providing remote access for distance students. For

instance, bandwidth issues are extremely different for students trying to access the lab resources from developing African or Asian countries compared to those in Australia or Europe.

5.2.4 Availability of lab resources. In an ideal case, the lab resources should be available 24/7 or at least at the time booked by the students to conduct their exercises. The access to available resources should be ensured without any interruptions in order to enhance reliability and authenticity. The availability of lab staff to deal with any upcoming issues during exercises is also of importance.

5.2.5 Collaboration. A high degree of collaboration is required among lab staff, such as between developers, lab assistants, and administrators to provide good lab implementation and management. Similarly, the collaboration of EPI stakeholders such as developers with stakeholders of other entities such as teachers and end users is very important for developing an effective artifact. The ensemble artifact will, in this way, emerge through an interdisciplinary and collaborative effort of experts from different fields [5].

5.3. Design principles for lab infrastructure

5.3.1. Contextualization based on program goals. The contextualization principle in this context suggests obtaining contextual information from all the stakeholders of an InfoSec lab. The requirements from all the stakeholders (including the teachers of all the courses, program management, developer etc.) should be considered in order to align the program goals with the lab activities. Thus, the lab infrastructure should support all the exercises required in different courses of a degree program of information security [5].

5.3.2. Scalability. It is extremely important that the lab infrastructure should be able to support all the exercises required in different courses of an information security program. Additionally, the lab should be scalable to accommodate more students than expected in the lab, and thus should support creation of many replications or copies of the same exercise in order to provide lab resources to all students [35].

5.3.3. Easy configuration and reconfiguration. The lab infrastructure should be easily configurable and reconfigurable. There should be support for changing the configuration of hosts and networks efficiently [35].

5.3.4. Back-up and recoverability. The lab administrator should be able to take back-up of the exercise topology and configurations including all involved equipment. In case of any hardware failure due to any problem, the lab administrator should be able to recover the original configurations easily.

5.3.5. Hardware integration. The lab infrastructure should be extendable using hardware from different manufacturers.

5.3.6. Cost-Effectiveness. The cost-effectiveness principles implies the availability of resources (funds, technology, and human skills) [5]. Virtualization technologies such as VNC server, VNC client, and Vlab manager, are considered important elements of InfoSec labs, which provide benefits such as lower hardware cost, and customization of software and hardware resources [14], [15].

5.4. Design principles for concrete exercise interface

5.4.1. User-friendly interface with properly arranged resources and targets. When the student accesses the exercise and opens it in the lab environment, the concrete exercise interface should guide and support the recognition of resources that students are supposed to use to perform specified tasks. The students should not need to make a large effort (in terms of wasting time) to locate the available resources and the target area when going to complete a task. These principles will improve student efficiency during lab exercises.

5.4.2. Easy to use. The interface for different exercises will change, based on exercise requirements. In this case, we need to make sure that the dependencies that are needed to run the interface such as SSH or VPN are available. Moreover, additional libraries such as Linux, for example, must be available in advance and can be straightforwardly installed by students.

5.4.3. Tracking and debugging errors. The interface should have a good communication with the hardware platform in order to be able to handle errors from the students' and hardware side. The student should have the ability to track a given instruction, identify any erroneous command, and record any response from the hardware platform. Later on, students can check the trace file for better understanding of any mistakes.

6. Discussion and further research

The manner in which an InfoSec lab is viewed has an impact on how the InfoSec lab affects the development of hands-on skills of information security students. Hence, we need to scale up to the ensemble view of the InfoSec lab in order to fully understand challenges related to its design,

development, and use in specific contexts for certain exercises in order to achieve particular goals. This article is an endeavor to do the same in the context of hands-on information security education using online InfoSec labs. In this research article, we argue that an online InfoSec lab should not be considered as a monolithic black box. There is a need to view the online InfoSec lab as an ensemble artifact. Our work at its current status is useful in the sense that it serves two purposes. First, the study conceptualizes the online InfoSec lab as an ensemble artifact. This means that we can unfold the black-box tools view of the lab and identify and understand the important building blocks (entities of lab), and the interrelationships of the entities. This study attempts to provide conceptual clarity given the existing literature on online InfoSec labs, by identifying the stakeholders and their roles for each entity in the proposed conceptual model; this is a view which has not been recognized essentially in earlier similar works. Secondly, the study suggests design principles for implementing a conceptual model of an online InfoSec lab in different contexts.

Furthermore, this study enhances our academic understanding of the role of an InfoSec lab for the development of hands-on education in information security. For instance, the pedagogical approaches and their role in design and development of lab exercises have been mostly absent in the existing literature [13]–[19]; however, our proposed model and design principles reflect that the pedagogical alignment of lab activities is important for achieving specific goals through hands-on education via InfoSec labs. The pedagogical theories influence the design of an exercise from the start and, eventually, the concrete lab interface settings are defined based on the pedagogical theory selected during the initial phase of the exercise development. The ensemble view of online InfoSec labs proposed in this study helps to identify the stakeholders for the design and development of the exercise, the exercise processing and management interface, the lab infrastructure, and the concrete exercise interface. In a similar manner, design and development of a lab as an ensemble artifact [6] will lead us to understand the stakeholders' perspective, their roles, their influences, their collaboration, the role of pedagogy, the impact of pedagogical approaches on the design of the lab, and the socio-technical perspective of the online InfoSec lab. The proposed description of entities and design principles will solve the problems of initiating the design and development of a lab. Practitioners wishing to include lab activities in their courses and programs can utilize this knowledge to understand fully how much human and technical resources are needed to conduct what type of exercises. Furthermore, the lab descriptions as ensemble artifacts will guide the researchers and practitioners toward adopting an existing design exemplar of a lab and to further enhance its growth by overcoming the issues of complexity coordination. Conceptualizing the InfoSec lab as an ensemble artifact has different implications such as, from the practitioners' point of view, where design principles and rules can be formulated that not only highlight the socio-technical perspective, but also address the challenges of adapting the lab idea in a suitable manner for other different contexts. From a research perspective, the researchers should study the lab as an ensemble artifact rather than just a tool or computational technology, and our research provides a starting point for them. In other words, the lab should not be taken for granted, but rather, its actual design, implementation, and use in context should define the utility and usability of the lab while aiming at enhancing the security knowledge of the InfoSec students.

We will proceed further by applying the conceptual model to have a fully functional online InfoSec lab that will support different exercises in different courses for an information security program. The lab will be tested in the classroom environment with students, which will help us in managing emerging challenges. In forthcoming iterations, we will continue with the ADR research method, and keep on developing other courses for information security master's program based on the pedagogical premises defined in this research project. This will also help to verify and capture the emerging design principles that will produce further systematized knowledge that will contribute towards design theory for online InfoSec labs and relevant pedagogy.

7. References

[1] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," presented at the Proceedings of the conference on Information technology education, pp. 113–122, 2011.

[2] B. Karlovsky, "Cisco Predicts Major Global Shortage of Security Professionals," http://www.arnnet.com.au/article/543470/cisco_predicts_major_global_shortage_security_professionals accessed on 25-04-2014.

[3] L. Kosak, D. Manning, E. Dobson, L. Rogerson, S. Cotnam, S. Colaric, and C. McFadden, "Prepared to teach online? Perspectives of faculty in the University of North Carolina system," *Online J. Distance Learn. Adm.*, vol. 7, no. 3, 2004.

[4] S. Iqbal and T. Päivärinta, "Towards a design theory for educational on-line information security

laboratories," in *Advances in Web-Based Learning-ICWL 2012*, Springer, pp. 295–306, 2012.
[5] S. Iqbal and D. Thapa, "Initial Design Principles for an Educational, On-line Information Security Laboratory," in *Advances in Web-Based Learning–ICWL*, Springer, pp. 89–100, 2013.
[6] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action Design Research.," *MISQ.*, vol. 35, no. 1, 2011.
[7] W. J. Orlikowski and C. S. Iacono, "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, 2001.
[8] J. Iivari, "The IS core--vii towards information systems as a science of meta-artifacts.," *Commun. Assoc. Inf. Syst.*, vol. 12, 2003.
[9] I. Benbasat and R. W. Zmud, "Empirical research in information systems: the practice of relevance," *MISQ*, pp. 3–16, 1999.
[10] M. Rosemann and I. Vessey, "Toward improving the relevance of information systems research to practice: the role of applicability checks," *MISQ.*, pp. 1–22, 2008.
[11] O. Hanseth and K. Lyytinen, "Design theory for dynamic complexity in information infrastructures: the case of building internet," *J. Inf. Technology*, vol. 25, no. 1, pp. 1–19, 2010.
[12] H. J. Mattord and M. E. Whitman, "Planning, building and operating the information security and assurance laboratory," presented at the Proceedings of the 1st annual conference on Information security curriculum development, pp. 8–14, 2004.
[13] S. D. Burd, G. Gaillard, E. Rooney, and A. F. Seazzu, "Virtual computing laboratories using vmware lab manager," presented at the System Sciences (HICSS), 44th Hawaii International Conference, pp. 1–9, 2011.
[14] S. D. Burd, A. F. Seazzu, and C. Conway, "Virtual Computing Laboratories: A Case Study with Comparisons to Physical Computing Laboratories.," *J. Inf. Technol. Educ.*, vol. 8, 2009.
[15] A. Gaspar, S. Langevin, W. Armitage, R. Sekar, and T. Daniels, "The role of virtualization in computing education," presented at the ACM sIGCsE bulletin, vol. 40, pp. 131–132, 2008.
[16] P. Li, L. W. Toderick, and P. J. Lunsford, "Experiencing virtual computing lab in information technology education," presented at the Proceedings of the 10th ACM conference on SIG-information technology education, pp. 55–59, 2009.
[17] K. Krishna, W. Sun, P. Rana, T. Li, and R. Sekar, "V-NetLab: a cost-effective platform to support course projects in computer security," presented at the Proceedings of 9th Colloquium for Information Systems Security Education, 2005.
[18] Y. B. Choi, S. Lim, and T. H. Oh, "Feasibility of virtual security laboratory for three-tiered distance education," presented at the Proceedings of the ACM conference on Information technology education, pp. 53–58, 2010.
[19] W. C. Summers and C. Martin, "Using a virtual lab to teach an online information assurance program," presented at the Proceedings of the 2nd annual conference on Information security curriculum development, pp. 84–87, 2005.
[20] S. Gregor and D. Jones, "The Anatomy of a Design Theory.," *J. Assoc. Inf. Syst.*, vol. 8, no. 5, 2007.
[21] S. Iqbal, "Applying the analytical lens of constructive alignment and conversational framework for course and E-learning platform development," *NOKOBIT*, 2013.
[22] F. S. Keller, "Good bye, teacher…1," *J. Appl. Behav. Anal.*, vol. 1, no. 1, pp. 79–89, 1968.
[23] S. M. Bellovin and W. R. Cheswick, "Network firewalls," *Commun. Mag. IEEE*, vol. 32, no. 9, pp. 50–57, 1994.
[24] M. Yoon, S. Chen, and Z. Zhang, "Minimizing the maximum firewall rule set in a network with multiple firewalls," *Comput. IEEE Trans. On*, vol. 59, no. 2, pp. 218–230, 2010.
[25] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, "Network attacks: Taxonomy, tools and systems," *J. Netw. Comput. Appl.*, 2013.
[26] D. Hucaby, *Cisco asa, pix, and fwsm firewall handbook*. Pearson Education, 2007.
[27] E. Crawford and Y. Hu, "A Multi-User Adaptive Security Application for Educational Hacking," presented at the Proceedings of the World Congress on Engineering and Computer Science, vol. 1, pp. 19–21, 2011.
[28] H. A. Lahoud and X. Tang, "Information security labs in IDS/IPS for distance education," presented at the Proceedings of the 7th conference on Information technology education, pp. 47–52, 2006.
[29] F.-G. Chen, R.-M. Chen, and J.-S. Chen, "A Portable Virtual Laboratory for Information Security Courses," in *Advances in Computer Science, Environment, Ecoinformatics, and Education*, Springer, pp. 245–250, 2011.
[30] M. S. Aboutabl, "The CyberDefense laboratory: A framework for information security education," presented at the Information Assurance Workshop, IEEE, pp. 55–60, 2006.
[31] J. Biggs, "Enhancing teaching through constructive alignment," *High. Education,* vol. 32, no. 3, pp. 347–364, 1996.
[32] V. Richardson, "Constructivist pedagogy," *Teach. Coll. Rec.*, vol. 105, no. 9, pp. 1623–1640, 2003.
[33] G. Stahl, T. Koschmann, and D. Suthers, "Computer-supported collaborative learning: An historical perspective," *Camb. Handb. Learn. Sci.*,, 2006.
[34] R. E. Slavin, "Research on cooperative learning and achievement: What we know, what we need to know," *Contemp. Educ. Psychol.*, vol. 21, no. 1, pp. 43–69, 1996.
[35] V. Anantapadmanabhan, P. Frankl, N. Memon, and G. Naumovich, "Design of a laboratory for information security education," in *Security education and critical infrastructures*, Springer, pp. 61–73, 2003.