# *A Virtualization-based Laboratory for Learners' Hands-on Skills of Hacking*

Jung-Lung Hsu, Kainan University, Taiwan
Kuo-Ming Hung, Kainan University, Taiwan
Wu-Yuin Hwang, National Central University, Taiwan
Huey-Wen Chou, National Central University, Taiwan

The Asian Conference on the Social Sciences 2016
Official Conference Proceedings

**Abstract**
This paper describes an ongoing design project that aims to exploit virtualization for enhancing learners' hands-on experience of attacking and defending systems. In this paper we present Experiential Learning Theory as the theoretical framework. The argument of this study is that the design of pedagogic systems should consider an integral view of cognitive domain (knowledge) and affective domain (attitude), particularly for the class concerning information security. Afterwards, we describe guidelines of how to design an interactive system that can sustain learners' hands-on experience in terms of cognitive and affective domain. This study considers that engineering students would learn better if they have hands-on experience of both attack and defense skills in security education. In this regard, having a controlled and well defined environment whereby students can play the role of attackers and defenders is important.

Keywords: Virtualization, Hacking, Learning Style, Affective Learning

## Introduction

It has been recognized that information technology is becoming one of the driving forces that leads contemporary industries to keeping competitive. Despite its benefits, information technology entails the issue of information security, which would probably cause heavy loss. US IC3 (Internet Crime Complaint Center, IC3) released "2013 Internet Crime Report", indicating that the complaint cases increased to 26.2 million transactions, compared to 23.1 million transactions in 2005. Meanwhile, the report stated that the amount of loss caused by information security raised extremely from $ 180 million to $ 780 million. For example, in May 2011, Sony's PlayStation video games were hacked and resulted in a loss of personal data from approximately 77 million users. Furthermore, a "320-Fi terrorist attacks" that occurred on March 20, 2012 in South Korea eventually paralyzed nearly 40,008 thousand computers.

Although information technology brings lots of convenience, it has entailed many potential risks in our daily life. Information security is one of the risks that may incur heavy loss. Instructors of cybersecruity usually teach theories and mathematics in classes. Learners have little chance to obtain practical skills of how to against cyber-attack. The importance of hands-on experience has been proved by an ancient Chinese proverb, saying that "Tell me and I will forget. Show me and I may remember. Involve me and I will understand." Thus, some of researchers devoted to proposing guidelines and frameworks for institutions to build professional laboratories for security testing in a cost effectiveness way (Murty, 2008; Nurmi *et al*., 2009). However, the purpose of these studies focus mainly on the infrastructure of the laboratories. The foci of their attentions were seldom centered on the design of how to effectively enhance learners' cybersecurity knowledge.

Besides, according to taxonomy of learning domains (David, 1986), educational activities include not only cognitive domain (knowledge), but also affective domain (attitude). Our claim is that the acquisition of cybersecurity knowledge shouldn't undergo in a learning process without considering affective education. In terms of designing systems that are specifically aimed at improving learners' achievements, there is very little within the current design literature. Unlike prior research seeking to build professional laboratories for security testing in a cost effectiveness way, this study focus on the design of how to enhance learners' hacking skills, meanwhile, effectively instilling them with correct attitudes and values to prevent abusing this capability.

## Literature review

Based on the tenet of Experiential Learning Theory (Kolb & Kolb, 2005), it is believed that the acquisition of learners' practical cybersecurity knowledge could be enhanced through actual experience. This study considers that learners' would learn better if they have hands-on experience of both attack and defense approaches in a well-design setting.

Through the lens of ELT, it is expected that learners' practical ability and knowledge can be enhanced by the pedagogic activities that emphasize actual experience (Kolb & Kolb, 2005). However, security education shouldn't be taught in a way that correct attitudes and values are not emphasized. In their study, Pashel warned that once a

student acquires the expertise to attack a system, it is probably for them to use the skills for good or bad intentions (Pashel, 2006). Undoubtedly, teaching learners the attack approaches without the ethical or legal constructs to understand their actions would bring the potential risks (Logan & Clarkson, 2005). Thereby, certain pedagogic design dedicated to enhance ethical or legal awareness to prevent students from conducting malicious acts in the future needs to be addressed.

Based on Kearney's definition (Pashel, 2006), affective learning is "an increasing internalization of positive attitudes toward the content or subject matter". It seems that affective education functions like a compass, which points out the right direction of how to use the knowledge and skills (Boyd, Dooley & Felton, 2006). In a nutshell, any type of security technique can be used properly or abused, such as penetration testing can either become "black hat hackers" or "white hat hackers" (Hartley, 2006). "Black hat hackers" perform unauthorized penetration attacks against information systems, which may or may not be illegal in the country they are conducting (Logan & Clarkson, 2005).

**Pilot study**

The first stage while designing an interactive system that serves as an ad-hoc laboratory is to determine whether the infrastructure is public or private IaaS. As the information technology continually advances, the application of virtualization becomes potential and various. Currently, there are many public services announced on the Internet that can sustain the aim of this design project. Amazon EC2, for instance, is a system using Xen Virtualization technology to provide an IaaS service. Through their web services users can create, execute, and terminate dedicated virtual machines to perform needed tasks (Murty, 2008). If the budget is sufficient, Amazon EC2 is reliable and seems a qualified infrastructure service provider.

Alternatively, Eucalyptus, a set of open source packages, seems an affordable solution for system administrators to establish the services based on a private IaaS infrastructure (Nurmi *et al*., 2009). This solution is better than establishing a hardware-based laboratory because of its flexibility. The problem of using Eucalyptus with private IaaS is that it requires system administrators to modify the underlying information architecture before using Eucalyptus. Practically, it is inconvenient and too complicated for instructors and learners in such an environment. After all, using Eucalyptus probably needs reorganizing or modifying the entire campus architecture (Pittman, 2013).

In order to get rid of the infrastructure constraints, many researchers suggested Emulab (White *et al*., 2002) because it serves simply as a testbed. Any users can access the services from Emulab through the Internet connection with a Web-GUI interface. This can be an effective and practical solution because an ad-hoc virtualized laboratory is created as users upload the attempted topologies. Technically, an ad-hoc virtualized laboratory represents a specific network topology. The learners can access and conduct various information security experiments, ranging from single system exercise to multi-system development exercises. The entire ad-hoc virtualized laboratory is just a file, so that it can be easily shared between the learners. This kind of virtualized laboratory operates has the potential to dramatically reduce the need for

physical devices. In addition, the learners would be able to access to the virtualized laboratory in their home.

The second stage is on the design of interactive activities that can enhance learners' cognitive abilities. The learners may switch the roles of attackers and defenders during this step. The aim of this arrangement is twofold. On the one hand, playing the role of defender gives the participant the experience of failing to protect the systems, which is believed to help raising their awareness of information security. On the other hand, as an attacker, it allows the participant to hack the systems, which might give him a better understanding of how security systems fail, and then encourage him to tackle and solve the security flaws.

The final stage is based on Krathwohl's taxonomy of affective domain (Krathwohl, 2002). It is suggested to take forty to sixty minutes for the learners to participate in. Learners are expected to express a series of questions associated with what they have done in the lecture. For example, the questions could be "sharing the experience of setting passwords in daily life." "express your feelings and thoughts when logging on the computer from various aspects." The purpose of this design is to signal the learners that improper forms of hacking are both unethical and illegal. Accordingly, an interactive system that can store and share the learners' responses would be helpful.

**Discussion and conclusion**

In this pilot study, eighteen students majored in Management Information Systems participated. The students were taught three kinds of solutions for building a virtualization-based laboratory: Amazon EC2, Eucalyptus, and Emulab. The concepts of virtualization-based laboratory were first introduced so that the students understand what it means. Next, the students were told the advantage and disadvantages of each solution for them to better understand the limitations of the relevant techniques. Finally, the students were asked to fill out questionnaires to indicate their perceptions towards learning Information Security through virtualization-based laboratory. The purpose of this study was to first collect students' attitude toward virtualization-based laboratory. The results of this pilot study can be helpful while investigating the feasibility of exploiting virtualization-based laboratory.

Table 1 shows the participants' perceptions that were collected by the questionnaire, where "1" stands for "strongly disagree" and "5" stands for "strongly agree". Mathematically, if the mean value is larger than 3, it could be interpreted as that the participants had positive perception toward the pedagogical activity. Overall, participants responded positively to exploiting virtualized laboratory in lecture of Information Security. Regarding the construct of easy to use, participants consistently considered that virtualized laboratory was flexible and easy. The empirical evidence in Table 1 indicates positive perceptions toward the way of learning Information Security through virtualized laboratory.

In a nutshell, while the participants' perceptions were all above-average, the results from the questionnaire indicates that the item related to resolving problems of Information Security was not as high as the other items. The reason might be that learners were only introduced the solutions that can used to sustain a virtualized laboratory. Although the advantages and disadvantages of each solution have been

listed, learners did not have real experience of using a virtualized laboratory in this pilot study.

Table 1. Statistics of the participants' perceptions

| Items | Mean | S.D |
|---|---|---|
| Easy to use | | |
| I think I could easily use virtualized laboratory to learn security. | 3.31 | 0.23 |
| Learning virtualized laboratory can be easy for me. | 3.43 | 0.46 |
| It is easy to construct the needed settings via virtualized laboratory. | 3.61 | 0.59 |
| Usefulness | | |
| Using virtualized laboratory can enhance learners' hands-on skills. | 4.01 | 0.31 |
| Virtualized laboratory helps learners to study scenarios of security. | 3.68 | 0.68 |
| Using virtualized laboratory to learn security is practical. | 3.79 | 0.47 |
| Self-efficacy | | |
| I believe using virtualized laboratory can improve understandings of security. | 4.19 | 0.63 |
| I believe learning virtualized laboratory can enhance hands-on skills. | 3.93 | 0.87 |
| I think I can resolve security problems when virtualized laboratory. | 3.16 | 0.86 |

In this paper we argued that the acquisition of cybersecurity knowledge shouldn't undergo in a learning process without considering affective education. Through this work in progress we hope to make clear the procedure of how to construct virtualization-based laboratories. In addition, we tried to provide guideline of how to enhance learners' hands-on skills of hacking, meanwhile instill them with correct attitude. Once learners understand how attackers work, then they will be able to emulate the attackers' activities if they plan on carrying out a useful security policy in the future. Based on the guidelines of this paper, an empirical research will be conducted in order to collect more useful feedbacks from the learners.

**Acknowledgment**

This study was supported by a grant from the Ministry of Science and Technology, under the grant number: MOST 104-2511-S-424-004.

**References**


Boyd, B. L., Dooley, K. E., & Felton, S. (2006). Measuring learning in the affective domain using reflective writing about a virtual international agriculture experience. *Journal of Agricultural Education*, *47*(3), 24-32.

Hartley R. 2006. Ethical Hacking: Teaching Students to Hack. *INFOSEC Writers, November*, *5*.

Kolb, A. Y., & Kolb, D. A. (2005). Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of management learning & education*, *4*(2), 193-212.

Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory into practice*, *41*(4), 212-218.

Logan, P. Y., & Clarkson, A. (2005). Teaching students to hack: curriculum issues in information security. *ACM SIGCSE Bulletin*, *37*(1), 157-161.

Murty, J. 2008. *Programming Amazon Web Services: S3, EC2, SQS, FPS, and SimpleDB*, O'Reilly Media.

Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009, May). The eucalyptus open-source cloud-computing system. In *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on* (pp. 124-131). IEEE.

Pashel, B. A. (2006, September). Teaching students to hack: ethical implications in teaching students to hack at the university level. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 197-200). ACM.

Pittman, J. (2013). Understanding System Utilization as a Limitation Associated with Cybersecurity Laboratories–A Literature Analysis. *Journal of Information Technology Education: Research*, *12*, 363-378.

White, B., Guruprasad, S., Newbold, M., Lepreau, J., Stoller, L., Ricci, R., & Joglekar, A. (2002). Netbed: an integrated experimental environment. *Computer Communication Review*, *32*(3), 27.