*Information & Security: An International Journal*

Luke Topham et al., vol.35, 2016, 51-80 https://doi.org/10.11610/isij.3503

# CYBER SECURITY TEACHING AND LEARNING LABORATORIES: A SURVEY

Luke TOPHAM, Kashif KIFAYAT, Younis A. YOUNIS,
Qi SHI, and Bob ASKWITH

**Abstract**: Currently there is a great demand for trained cyber security professionals with hands-on skills. The need for these professionals stems from our reliance on technology in many aspects of our daily lives and the smooth running of modern governments, education and health services. These professionals are desperately needed to defend cyberspace from threats such as hackers and malware who threaten to disrupt such services daily. This paper presents an insight into current approaches taken in the practical teaching of cyber security. We also give requirements and best practices for future training platforms based on a defined teaching process.

**Keywords**: Education, training, cybersecurity, computing laboratory, cloud computing, virtualisation, pedagogy.

## 1. Introduction

As the reliance on cyberspace in our daily lives and business grows, the threat and impact of cyber-crime increases. This threat may come from “hacktivists”, criminals, foreign governments or even terrorists who may wish to cause disruptions or make financial gains through such illicit activities. A UK government report estimated that the cost of cyber-crime to the UK was £27 billion per annum,[1] however, this figure does not include crime without a financial motive such as “hacktivism” and terrorism. There is currently a high demand for cyber security professionals and therefore a strong need to train future professionals with the appropriate hands-on skills required to combat these threats.

The weakest link in system security is often the human personnel and their lack of security awareness and skills,[2] this is tied to the significant and growing demand for well-trained cyber security practitioners.[3] Governments are responding to the threat to cyber security and are taking an active role steering the training and organisation of cyber security practitioners.[3]

A growing number of Higher Education (HE) institutions are offering courses in cyber security to help bridge this gap between supply and demand of trained practitioners. However, in these courses there is often a heavy focus on theoretical teaching and a shortage of practical hands-on experimentation conducted by students. It has been long known that practical experience is a useful aid to understanding,[4] as emphasised in the famous quote by Confucius; "I hear and I forget. I see and I remember. I do and I understand."[5] The challenge then is to decide on how to safely offer students the opportunity to experiment with real-world modern technology, tools and techniques, while adhering to constraints such as budgets and physical space.

The weakest link in system security is often the human personnel and their lack of security awareness and skills,[6] this is tied to the significant and growing demand for well-trained cyber security practitioners.[7] Governments are responding to the threat to cyber security and are taking an active role steering the training and organisation of cyber security practitioners.[3]

The growth in the offerings of cyber security courses is also occurring alongside the growth in demand for distance learning courses. Historically, practical experimentation would be confined to a physical laboratory on-campus and therefore, anyone who did not physically attend would be denied this opportunity. A challenge to consider is how to give students an equivalent environment to experiment whilst off-campus which is compatible with the variety of equipment that students may own and also provide it in a way that will require as little support as possible.

There are a variety of solutions to the aforementioned challenges which allow practical experimentation in cyber security.[5,8,9] These solutions can be broadly categorised into physical laboratories, simulation laboratories and virtual laboratories as shown in Figure 1. This paper provides a review of the existing literature on the variety of approaches to providing cyber security students access to hands-on experimentation, both on and off-campus.

A considerable amount of work has been published in this area with many papers detailing a number of platforms covering the full range of laboratory types.[10,11,12]

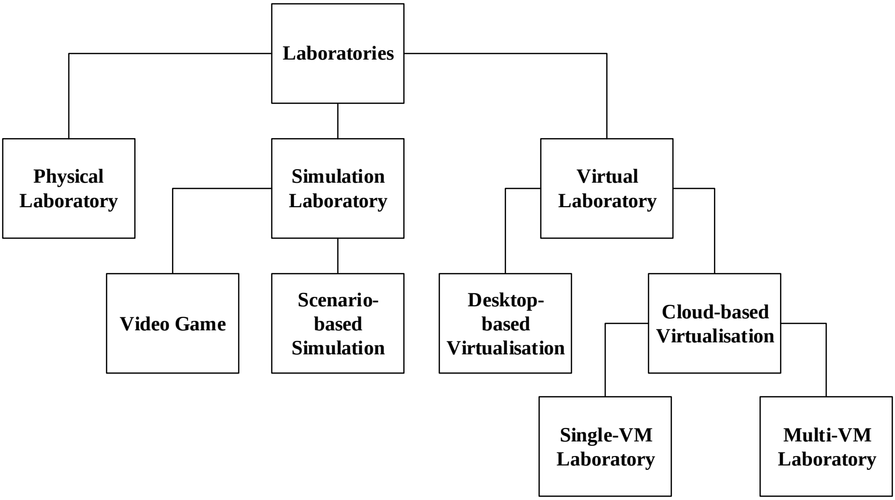

**Figure 1: Laboratory Type Hierarchy.**

The remainder of this paper is organised as follows: Section 2 provides a background to cyber security education and approaches, Section 3 describes each type of laboratory and discusses some examples for each, Section 4 compares the laboratory types, Section 5 provides suggestions and requirements for future platform and Section 6 provides a conclusion to the paper.

## 2. Background

Cyber security education and training is becoming ever more imperative. Cyber-attacks are experienced daily, and high profile attacks such as the highly publicised breach at SONY and the Stuxnet worm's attack on the Iranian nuclear program highlight and confirm the dire need for improved cyber security world-wide.[13]

Focusing on HE offerings of cyber security, such courses may include topics on ethical hacking, malware, security auditing, digital forensics and secure software development. All of these topics could be complemented by offering students hands-on laboratory based exercises. Locasto suggests that practical training is the only way to achieving a sufficient cyber security education.[14] ACM has recognised the need for experiential learning and has incorporated it in their proposed standards for IT curriculum,[15] to achieve this recommendation, students must be provided with an environment for practical experimentation.

## 2.1. Teaching Process

The most common teaching process in HE, revolves around a tutor imparting their knowledge upon students through a variety of activities. This teaching process is modelled in Figure 2. Traditional academic activities such as lectures and seminars are used in conjunction with selected reading to impart the tutor's theoretical knowledge upon the student. For practical learning activities a tutor will use their theoretical knowledge and possibly any access to industry that they may have to develop exercises replicating real-word problems and scenarios, these are commonly delivered through workshops, laboratory sessions and tutor-lead demonstrations. Configuring networks for exercises is a time consuming and problematic task especially when using a multi-purpose laboratory which may be needed for other purposes.

In cyber security education, a number of taught modules can be expected including: ethical hacking, security auditing, digital forensics, network security, cryptography, malware analysis, secure software development and ethical training, this is likely to be in addition to computing topics.

To meet the needs of these modules, students will require access to a variety of machines and networks to experiment. For example, to model a realistic security audit, it is not practical to give each student a business size network instead a network with a sufficient variety of machines and services will be required is required to create an abstract network of appropriate complexity. The purpose of these scenarios is to give access to the variety of machines and services that may be found in a business. In Figure 2 below two modules marked as “Platform” will be provided by a laboratory, teachers will need administration tools to create and grade exercises and students will require a way to interact with these exercises and complete them.

## 2.2. Requirements

Any cyber security laboratory must meet the needs of the teaching process shown in Section 2.1.

1. In order for tutors to be able to develop realistic scenarios and exercises the laboratory must provide them with the flexibility to implement creative exercises.

2. Teaching staff should be able to quickly and easily deploy exercises to multiple students.

3. Any machines and software within the laboratory should be isolated from outside networks.

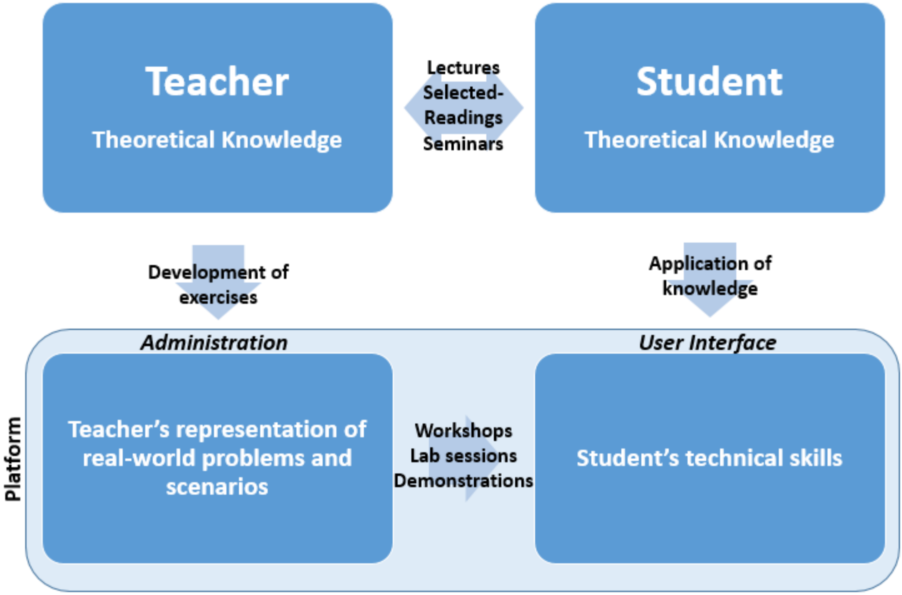

**Figure 2: Teaching Process Model.**

4. In the laboratory, it should be possible to give students administration rights for any machines which are assigned to them, this is important for certain experiments.

5. Storage and backup should be provided to allow students to make continual progress of their work as well as restore systems should there be any errors.

Quick recovery is important due to the nature of cyber security exercises which will test the reliability of systems to the extremes, failure to provide this will reduce learning time. Requirements 2 and 5 are satisfied well by cloud computing approaches, snapshots can be stored allowing for the quick restoral of Virtual Machines (VMs) and can also be used to easily deploy exercises. Also, solutions such as RAID can provide redundancy in the case of hard disk failures, without interrupting services.

### *2.3. Laboratory Isolation*

In a laboratory that will host ethical hacking and malware analysis experiments, isolation of the laboratory from outside networks including the Internet is imperative for their protection and thus for legal reasons. Isolation can be achieved with various techniques such as SSH tunnelling, VLANs and firewall restrictions.[16,17]

Isolation must prevent malware from escaping the laboratory, both accidentally and deliberately. Machines inside the laboratory should only be able to attack authorised machines within the laboratory during such activities. Machines within the laboratory must never be able to communicate with or attack a machine outside of the laboratory. Students should only be able to practice with machines that are assigned to them, they should not be able to interfere with other students' work.

Laboratory isolation may lead to restrictions on availability and usability, for example, laboratories may not be remotely accessible if they are completely isolated. However, it is possible to retain isolation whilst still allowing remote access. The Deter project does so by ensuring that network traffic can only exit the laboratory through a designated SSH tunnel, all other external traffic is blocked.[18] In cases such as malware analysis, the use of external storage devices may be forbidden, this may prevent physical security exercises for exercises such as cyber-warfare challenges.

### 2.4. Unique Requirements

Outside of HE other training platforms exist in industry and military but laboratories in Universities are subject to specific restrictions and requirements. Universities are often limited by resources in terms of equipment, budgets and physical space. Universities have a duty to impart industry-level skills and knowledge upon students. These restrictions must be adhered to, whilst also providing an adequate level of education for students to allow them to develop the necessary skills for required by industry.

### 2.5. Generic Requirements

When developing a laboratory a number of factors need to be considered, this includes when estimating server requirements for cloud-based laboratories. The number of users expected at peak times should be estimated, this is likely to be the full cohort of students signed up for relevant modules. This figure will be used to estimate memory and processing requirements. Similarly, the total number of users will also be required to estimate storage requirements. Other networking considerations, both virtual and physical, will include estimated network traffic and application load. Accurate estimations are important to ensure that the network will handle peak traffic without degraded performance.

## 3. Laboratory Approaches

This section introduces the three main types of computing laboratories; physical, simulation and virtual (single VM or multi-VM), also shown in Figure 1. Further comparisons are provided in Section 4.

**Table 1: Summary of Laboratory Types.**

| Lab Type | Virtualisation Type | Remote Access | Lab Scheduling | Persistent Storage | Configuration Level |
|---|---|---|---|---|---|
| **Physical Lab** | None | No | Restricted time and space | Problematic | Limited and expensive |
| **Simulation Lab** | None | Yes | No restriction | Depends on the type of simulation | Application level |
| **Single VM Lab** | Single-VM | Yes | May be reservation based | Yes | VM-level |
| **Multi VM Lab** | Multi-VM | Yes | May be reservation based | Yes | VM-level |

Before reviewing the current literature on cyber security educational platforms, it is worth noting some of the aspects that are important to institutions and students, summarised in Table 1. For students, remote access and lab scheduling are important, students would ideally prefer to work and experiment when and where it best suits them. Students often have other commitments alongside their studies, so flexible lab access would be beneficial. Tutors are expected to keep their course materials and experiments as up to date as possible, therefore the ability to reconfigure a lab easily is necessary. Persistent storage is important for students and tutors. Students need to maintain their progress for experiments and tutors are likely to want to see evidence of completed work and assessments.

### *3.1. Physical Laboratories.*

The traditional approach to educational laboratories has been the physical laboratory. Most institutions will have general purpose computer laboratories which are shared by a variety of modules and courses, however, sharing these labs with a cyber security module can become problematic. Cyber security modules may include experiments involving ethical hacking and the analysis and observation of malware, the risk of such experiments to the campus network and the Internet is too great to not isolate these labs.[19] This fact, along with the point that the tools used in cyber security experiments are often prohibited from traditional laboratories means that there is little choice but to create a dedicated cyber security laboratory.[20,21]

Arguably, a dedicated traditional physical laboratory for cyber security would offer students the best and most realistic environment in which they can experiment,[11] as they are able to practice with real equipment and tools. Students are able to experiment safely under the supervision of a tutor, who will be on hand for immediate support and guidance, a benefit that is not available to distance learning students.

The aforementioned benefits come at great effort and cost.[19] Purchasing and maintaining cutting edge equipment for the lab is expensive[11,22] especially when this lab may only be used for one module. Dedicated room space is required by this lab, again if this lab is used for only one module then when it is not in use, it is wasting space which could otherwise be used for another module.[19] A particular issue is that a member of staff with technical skills may be regularly required to set up different experiments, it is often time consuming to configure and to reconfigure networks for different experiments, each of which can vary greatly.[23]

A team at Georgia Tech developed an isolated physical laboratory for cyber security classes to complement the theoretical teaching at an introductory level.[20] This project claims novelty for the fact that it provides a simplified model of the Internet and enterprise networks whilst using a small number of physical machines. An external administration portal is available via the Internet, however, students are not able to complete exercises online. With this laboratory there are scheduling issues as there are only 25 machines which students are able to use within the laboratory, this limits the times when students can work. Perl scrips have been utilised in this project to allow the restoration or configuration of exercises and assignments, effectively removing the need to rewire the network for different experiments. Although efforts have been taken to minimise the amount of reconfigurations that are needed, the laboratory still requires a significant amount of effort to maintain.

The ASSERT computer security laboratory[24] was created using only surplus equipment available in storage at many universities, the laboratory was later used to leverage additional funding for further development. This approach was taken to minimise costs, as academic budgets are often restrictive. The laboratory uses virtualisation and host based images stored on a server to recreate exercises with a known configuration. Users are bound to a physical workstation as they can only save images containing their progress to the local machine. Monitoring this laboratory was found to be limited as the exact state of the system at any given time cannot be known for certain. Another major short-coming of this platform is that students must be present in the laboratory and are unable to perform any work remotely. Due to the lack of remote access there is no opportunity for distance learning and the students’ opportunities to do work outside of the scheduled class is limited.

InfoSec Lab, an information security laboratory, was successfully used to support a cyber security course following a standard of curriculum set by the USA government.[25] By aligning the curriculum with the NSTISSI 4011 and 4012 standards this platform was used to leverage additional funds from the National Science Foundation (NSF) to purchase more hardware. As with other physical laboratories, InfoSec Lab users were limited to a set number of workstations which they could work from, 16 for this laboratory. To improve the availability of the laboratory, students were given access codes to the door and were allowed to work in their whenever the building was open and the room was free from scheduled classes. This laboratory suffered from a lack of flexibility, a member of staff was required to manually install and configure experiments. Future plans for this laboratory included the introduction of virtualisation to provide greater flexibility for experiments.

At the University of Wisconsin-Eau Claire a cyberwar exercise was developed using an isolated laboratory reserved only for cyber security students.[26] This exercises involved groups of students tasked with securing their own computer systems whilst attacking the systems belonging to opposing groups, this was used a method of demonstrating the students' understanding of the theory taught throughout the academic year. The laboratory includes six Redhat Linux servers which are purposely vulnerable to attack for the group activities and further vulnerable Windows and Linux machines were available for exercises. A secure laptop was also attached to the network to monitor activity, this required assistance from technical staff. One of the main issues with this exercise was deciding how to limit physical access to opposing team's machines, this was a problem because all of the machines were present in the same room and couldn't be locked away.

Security and Information Assurance Lab (SAIL) is an online information assurance platform.[27] This is a remotely accessible physical laboratory which contains a number of different machines and a VPN authenticator for authentication. Traffic inside the laboratory is isolated to avoid damage to any machines outside of the laboratory. There were a number of issues with this laboratory, when a student accidentally shut down the machines, someone would have to physically power the machines back on. Another issue was that there were a limited number of physical machines and if they were all in use then other students would not be able to do any work. This approach does fix some of the accessibility and availability issues found with physical laboratories, but it does not solve all of them.

A particular limitation of the physical laboratories mentioned above is the fact that they often focus too heavily on a narrow scope of teaching, most often penetration testing. As mentioned previously, these laboratories are expensive and time consuming to maintain, it is therefore difficult to justify this expense for such a narrow range of learning outcomes. This cost would be more justifiable if the laboratories were expanded to include other taught modules such as information assurance and security auditing, this would also improve the practical skills range of the students.

### *3.2. Simulation Laboratories*

In the case of a simulation laboratory, a simulation is a digital representation of a scenario or piece of equipment which can be used as a tool to give users some hands-on practice and have been used successfully in different areas such as pilot training. Simulations are a useful training tool offering hands-on experience and user interaction, which is much more stimulating for the user,[5] as compared to having no practical sessions.

Simulated labs can be used in cyber security training where access to real equipment isn't feasible for whatever reason, such as where there are budget or space limitations. It provides students with the opportunity to practice their skills in preparation for real-world problems,[5] but they often vary in their realism and effectiveness. Simulations may be used to give students experience in specific domains, such as configuring Intrusion Detection Systems (IDS). However, in such cases students are confined to the scope of the simulation.[23] Therefore, in simulation labs, students are unable to try out new ideas and experiment with the real tools. When students find a real-world job they may also find it more difficult to apply their skills and knowledge to the real situation, especially if the simulations are not realistic.

As mentioned previously, the scope of simulations are limited and in most cases there is also a lack of flexibility and application-level reconfigurations. For example, new scenarios can often only be created by the original developer.[5,23,28,29]

Simulation software may be delivered via the Internet or via portable media,[30] often with minimal resource requirements. As simulations are highly accessible, they are easily distributed and available for distance learning which is particularly useful for regular training and practice. Simulations are useful for giving users regular training with minimal effort to set up.[5]

As previously, security is often a major concern when students are experimenting, especially with ethical hacking and malware. This is not a problem with simulations as the experiments are not real and no real tools or networks are involved.[31]

Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL) provides safe experimentation in computer and network security.[31] This simulator aimed at demonstrating attack scripts and malware and was developed internally at relatively low cost.

The Real-time Immersive Network Simulation Environment for Network Security Exercises (RINSE) aims at improving preparedness and training in the protection of large-scale networks.[32] RINSE involves hundreds of users and simulates a complex network comprising hundreds of Local Area Networks (LANs). The RINSE simulation software runs across multiple servers and is made available across the Internet, this approach differs from most simulators which are commonly run as desktop or web applications and don't involve any multi-user interactions. This multi-user interaction gives a more realistic and complex environment where users can attack each other. The RINSE simulation was found to rely heavily on the local CPU which caused traffic delay, interference between different CPU intensive tasks and possible packet loss.[32]

A Windows Attack intrusion Emulator (AWARE) emulates attacks on Windows machines with the aim of teaching casual users how to detect potential attacks.[33] AWARE gives the user the experience of specific attacks against a specific Operating System and as such there is very little room for experimenting outside of the given tutorials. The two main challenges in the development of RINSE were to firstly create an extensible platform so that new challenges could be developed and secondly, the platform had to be reliable as competitions based on this platform would involve many players with events spanning many days.

Overall, simulations can give the users at least some hands-on experience where it may otherwise be difficult. However, simulations do not provide experience of real technologies and deny the student the opportunity to experiment and see the consequences of their actions.[30] Simulations are limited and therefore access to the real tools and equipment would be preferable for a broader and deeper learning experience.[30]

### 3.3. Educational Games

Video games are increasingly used in education and can be considered as a special case of simulation software discussed in Section 3.2.[13,29] Defending against a real-time attack is a stressful task which requires the accurate application of relevant knowledge. In stressful work environments such as these, humans are more prone to errors, and for this reason these people should be well trained with practical exercises which simulate varying levels of stress.[13] Training should be a continuous process; in some cases daily training may be essential to change the habits of users,[13] and the use of video games can achieve this.

CyberNEXS is a cyber security training video game which teaches a range of topics including password usage and management, protection from malware and spam, patch management, social engineering and phishing techniques.[13] Nagarajan raises a key limitation of many training platforms in the fact that they often do not require users to apply knowledge in real-time as though they were defending an attack for real.

CyberCiege is a game that has been developed for information assurance education.[29] CyberCiege takes inspiration from games such as The Sims and Roller Coaster Tycoon which task the user with managing resources.[29] CyberCiege tasks users with using the available resources to plan and construct a network. The effect that the network has on the virtual users' productiveness and the ability of attackers to attack the network is then simulated.[29]

I-SEE, a game-based training environment for information security training, promotes a high level understanding of cyber security concepts and makes use of 3D and web-based technologies.[34] Once students have learned the basic concepts, they can put them to the test in competitive group activities. Although I-SEE aims to give students training without overwhelming them with complex configuration or difficult technical content, this means that students are given a less realistic set of skills.

A team from the University of Washington took an alternative approach to raising the awareness of cyber security education through the development of a board game which was given to 150 educators for free.[35] Pedagogic research results suggested that students had an increase in their awareness of cyber security issues and that material was covered that educators would not have otherwise covered. This game has a high level of engagement however this is at the expense of technical teaching and would therefore suit an earlier stage of education rather than HE.

Many of the video games used in cyber security education do not teach the more technical topics such as networking security and encryption, instead they focus more on raising awareness of high level issues. Video games are therefore more likely to be useful for raising awareness in computer users or at an earlier stage of education. However, inspiration from video games can be used to make education more engaging and to improve cyber security training platforms such as the multi-user competition, scoring and progression paths.

### *3.4. Virtual Laboratories*

This subsection explores the two main types of virtual laboratories; desktop virtualisation and cloud based virtualisation.

Virtualisation refers to the creation of a virtual version of a device, operating system or a network. Virtualisation is useful as it allows the use of different operating systems simultaneously on a single physical machine and it can also reduce hardware and software costs for an institution, through more efficient usage. Virtualisation is useful for HE institutions as it can allow cyber security classes to be taught in general purpose physical laboratories used by other classes.[22]

Virtualisation can be offered in two forms; desktop virtualisation and cloud-based virtualisation. Desktop virtualisation software is installed and remains solely on the user's machine and VMs share the host machine's resources.

### *3.4.1. Desktop Virtualisation VS Cloud-based Virtualisation*

Desktop virtualisation software is installed and remains solely on the user's machine, VMs share the host machine's resources. The benefits of this offering is that multiple OSs can be used on the one machine by virtualising one or more of them; this also means that a user can run applications which wouldn't normally run on the same platform.[36] In an educational environment, if a student misconfigures a machine it may be unavailable until it is fixed, which may take some time and may require some technical expertise. However, when using desktop virtualisation, if a student misconfigures or causes corruption in a VM, this will not damage the host machine.[36] There are also challenges with this method; students may not have the computing resources at home to be able to carry out such experiments. There is also the challenge of how to transport the VMs, as they are often quite large files. Distance learning students may even be required to configure their own environments and VMs with little help, which may distract from the actual learning.

The alternative would be for an institution to host the virtual laboratories on a cloud-based server. This solution provides the benefits of desktop virtualisation, but also extends these benefits away from campus. The cloud hosting will allow global access to students away from campus, which provides an opportunity for improved distance learning offerings.[36] Some cost savings can be made for the institution as resources are used more efficiently, maximising their use.[36] Using the services of a cloud service provider further cost savings can be made as they often offer an on-demand scheme where users pay only for what they use.[36] This centralisation is good for educational institutions; as work can be automatically backed up to prevent students losing work or to even prevent work being lost in case of server failure.[36] The main strength of cloud-based offerings is the simplified central management.[11]

There are some notable drawbacks to desktop virtualisation. Firstly, licencing may be an issue if institutions are issuing software to each student. It may even be the case that the institution may be required to purchase a licence for each copy that they give away.[36,37] Licencing is much simpler using cloud-based solutions, as cloud service providers often offer an "on-demand" payment model. Another particular drawback is the fact that this technology will require significant resources from the student's machine, which means that students with low powered machines may not be able to perform experiments.[36,37]

### *3.4.2. Single-VM Laboratories*

In single VM laboratories, a single VM is provided to a student to work on. A student may only need a single VM if they are auditing a machine, observing malware or configuring a device, and a single VM laboratory would suit this purpose well.[38,39] A single VM lab can still be used to protect the host machine and campus network from students' experiments, and allows other virtualisation benefits such as allowing the use of multiple OSs on the one machine.[36] It is even possible to allow remote access to VMs for distance and blended learning to allow students to experiment at home.[12] Single VM laboratories would often require less resources and configuration, which may give them a slight advantage over multi-VM labs in scenarios where access to instructors is limited and the student is required to supply all computational resources.

Single VM laboratories would not be suitable for any kind of networking. Many experiments and demonstrations in cyber security require networking, for example to demonstrate a man-in-the-middle attack would require at least three machines; two victims and an attacker. Cryptography is a core theme in many cyber security courses, to test secure communications a student may experiment by intercepting communications and then they may try to decrypt them, this would not be possible with a single machine or VM.

Overall, single VM labs can be a useful tool for teaching and learning in many topics such as malware analysis and systems auditing. As mentioned previously, students often best learn real-world skills when they are presented with realistic scenarios to experiment with. The lack of networking means that realistic scenarios are severely limited.

The University of Wisconsin aimed to give students an environment in which they could work on project work which they could access any time both on and off-campus.[40] This solution was implemented using VMware GSX Server which can be purchased and implemented by any other institution. This platform was able to provide students with remote access while maintaining the ability to isolate the VMs when required without removing the ability to remotely connect when in isolation mode. This was achieved by having three networking ports on each server, one for remote access via a web interface, the second provides Internet connection when not in isolation mode and the third to provide access to the VMs within the classroom. Virtual routing between the second and third ports is used to provide Internet access when not in isolation mode. Isolation is achieved by deactivating the second port. Students can still access their VMs remotely by using the web interface and the first port. Hardware limitations meant that a limited number of VMs were able to run simultaneously and hard drive access when running close to full capacity was a significant bottleneck.

The Xen Worlds project was developed to provide a laboratory environment for information assurance classes.[41] In this platform each student is given their own VM to minimise collusion and interference between students. This project was based on the Xen hypervisor which was found to support many VMs on a relatively small amount of resources. Xen and Xen Worlds are available for free which allows for other institutions to replicate this platform on their own hardware.

### *3.4.3. Multi-VM Laboratories*

In multi-VM laboratories, students can be provided with multiple VMs which can be networked together to create more complex experiments and realistic scenarios.

The benefits and offerings are very similar to that of single VM laboratories; except now students can be given access to entire networks of VMs. This small difference has a positive impact on the range of experiments that students are able to perform and the realism that they are able to achieve. Students are now able to experiment with full networks and may configure routing, firewalls, IDS and IPS.[23,42,43] They can be given a better practical understanding of small real-world networks. The benefits of realistic scenarios and environments has already been discussed, multi-VMs labs with virtual networks are a great way of achieving this. It is also possible to connect multiple students' VMs together to allow attack/defend type scenarios in real-time, giving students the practical experience of attacking and defending in real-time.[11]

The main advantage of multi-VM labs is their associated lower cost in terms of both money and time. Students are able to have an entire virtual network to themselves, this would be highly impractical with physical networks due to the cost, time to configure and the space requirements. Depending on the platform, there may still be heavy time costs, the virtual networks will need to be set up and configured, though some platforms automate a lot of the tasks for this. Manual configuration of virtual networks requires expertise. Having the students set up the virtual networks themselves will detract from the time available to learn the actual cyber security skills. Therefore, it is likely that an instructor or technical expert will be required to set up these scenarios and make them available to the students.

Table 2 shows that there is a lot of research output and many training platforms available which use multi-VM approaches. This increasing popularity is likely to come from the advances in virtualisation technology and the ever increasing popularity and adoption of cloud computing.

An EU-funded project has resulted in a multi-VM virtual laboratory named ReSeLa.[10] This platform aims to give students a remotely accessible lab environment to experiment with insecure protocols, malware and ethical hacking in a secure environment. This platform requires a fast broadband connection, without which the remote capabilities cannot be utilised. To combat this issue, offline versions are available; however, this will come without the benefits of centralisation.

NLS-Cloud is a cloud-based platform for network education based on Xen.[4] This platform still has many useful features and characteristics that would be useful in cyber security education. This project is particularly useful to education as it allows both structured exercises and free experimentation to be completed by the student which gives flexibility to teaching and learning.

Multi-VM labs have a massive advantage over single VM labs due to their networking capabilities. The need for realistic scenarios and environments has been echoed throughout this paper, and without the capability to create networks, this is almost impossible. Purchasing, configuring and maintaining a cloud-based laboratory and virtual networks may be costly and time consuming, however, such platforms come with increased flexibility, scalability and availability.

The SOFTICE project takes a clustering-virtualisation approach to providing a cloud-based laboratory using only open source software to minimise costs through the adaption of pre-existing tools.[44] Warewulf clustering was used to implement a load-balancing cluster consisting of many recycled desktop machines. A script based application “Manage Large Networks” (MLN) provides the ability to define networks dynamically, however, the students would have to write their own scripts. A current limitation of this project is that it supports only Linux-based operating systems, and this limits the variety of virtual network scenarios.

RULE is an established platform which provides students with networked VMs for coursework and research.[16] This platform also emulated FreeBSD hosts on a small number of physical machines. The laboratory runs on a number of mini-ITX boards on a rack to minimise the impact on the scarce laboratory space. By leveraging this relatively low-cost laboratory, the laboratory was able to provide students with some Linux experience in an otherwise windows-centric university.

The Remote Laboratory Emulation System (RLES) was originally built using VMware but was later moved to Xen due to its open source licencing model.[42] Future planned work for this project migration to a scalable blade/SAN architecture and also to implement an improved system monitoring. RLES allowed easy migration of VMs between physical hosts, this was useful as there were a limited number of VMs available. When VMs are exhausted on the server, students would be able to export a VM to a physical laboratory machine, this may cause issues for distance learning students.

VELNET is a learning environment for network education that allows students to launch their own networks via a graphical overlay thus minimising the need for configuration or scripting.[45]

V-NetLab is a cloud-based laboratory aimed at giving tutors the ability to define a virtual network once via a configuration file and easily replicate this for every student without reconfigurations.[46] This platform uses software that is readily available such as VMware and User Mode Linux (UML). There are plans for future work to create a graphical overlay to allow simplified configurations.

Drexel University have developed an online laboratory for IT education in general.[28] This laboratories novelty is that some equipment is not virtualised but instead some physical devices are accessible to the virtual networks, however, this caused some availability limitations.

Marsa-Marestre et al. stress the need for flexibility and expressiveness in the requirements for their platform “NEMESIS”, this is to allow the instantiation of realistic networks as well as giving the students the ability to practice a multitude of cyber security skills.[9] KVM was chosen for this platform due to its flexibility and adaptability to satisfy the above requirement. This platform allows the expressive definition of scenarios via the submission of an XML file. Galan et al. also propose a method of dynamically defining and creating virtual networks using Virtual Network User Mode Linux (VNUML).[47] Using VNUML imposes the limitation of only being able to include Linux-based clients.

NVLab is a cloud-based laboratory built from opens source software such as Xen and VNC to provide students with an online space to experiment with a number of different networking devices.[21] Tools are provided to allow students to define their own virtual networks using a GUI and then the network is instantiated for them.

The DETER provides the infrastructure and tools freely to verified institutions to allow them to teach practical cyber security classes.[16] The Deter test bed consists of 400 computers which are allocated depending on the needs of the experiments. Protection of outside networks is provided by the fact that only communications through the designated SSH tunnel is allowed, all other external traffic is blocked.

VLabNet is another Xen-based laboratory developed for cyber security education.[41] The authors stress a need for detailed online documentation to accompany any exercises, as opposed to others suggesting that free experimentation is important for student development.

Tele-Lab is a cloud-based laboratory available via the Internet, this platform is coupled with an E-Learning system for practical cyber security education as shown in Figure 3.[15] Security is strong in this platform as traffic can only flow through the VPN tunnel, however, this requires a lot of resources for encryption. This platform relies heavily on templates and predefined resources, when these are not available any remote connection requests are denied, limiting availability.

The V-Lab cloud-based platform is used to provide VMs for a number of different classes, and allows the flexible configuration of virtual networks.[10] This laboratory is coupled with a well-defined pedagogical module describing the delivery of the theory. The virtual networks are also strongly influenced by real-world scenarios. Pedagogic research performed using V-Lab suggested that this platform improved the final grades of students.[10]

NLS-Cloud is another Xen-based laboratory which provides virtual networks via an online management system for networking education.[4] NLS-Cloud is used to give

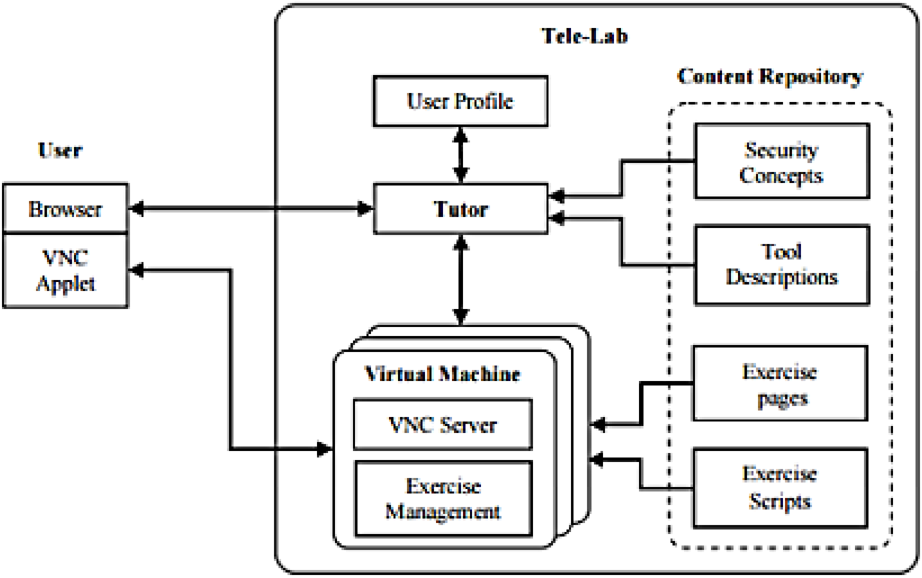

**Figure 3: Tele-Lab Architecture.[15]**

students access to specified exercises as well as their own resources to freely experiment. NLS-Cloud is made up of several components: Xen Cloud Platform (XCP), OpenXenManager (OXM) and Experiment Workflow Engine (EWE). This platform received favourable feedback however, students expressed the importance of a user-friendly GUI and future work aims to achieve this.

A number of challenges and competitions have been developed using cloud-based laboratories.[48,49] These competitions are often used to identify the best talent from the next generation of cyber security professionals.

### 3.5. Competitions

Cyber security challenges are becoming an increasingly popular way of identifying the top new talent in cyber security. Many industry sponsors and governments sponsor and support such competitions to aid recruitment.[50,51] Competitions may be delivered via a physical laboratory, a multi-user simulation or by utilising virtualised environment.

The UCSB international Capture the Flag (iCTF) is a distributed multi-user ethical hacking competition, this particular competition is highly popular and has reached more than a hundred teams and thousands of students.[52,53] These competitions is provided to users through virtualisation and available online. Scoring is calculated automatically by a "Scorebot" which checks the status of the services running on the users' VMs. A central database is used to enforce rules and host other information regarding the state of the competition. Exercises are delivered in two ways, one is an offline single-user mode and the other is a multi-user online competitive competition which proved significantly more difficult to deliver.

Some competitions such as the Air Force Association's CyberPatriot program [54] also offer significant learning resources to support cyber security training in addition to competitions.

The Cyber Security Challenge UK is supported by UK government and many industry partners.[51] This challenge is made up of a set of single-user challenges provided through a number of online video games. Scores are ranked and the top scoring users are invited to further team-based activities where they compete in front of sponsors who are looking to recruit new talent. These sponsors also donate career-enabling prizes such as funding for relevant training and certifications.[51] One complaint of this challenge is that materials are not provided to help user learn about cyber security, rather competitors are expected to already have acquired sufficient cyber security knowledge, and this limits the use of challenges as a training tool.

As mentioned previously, these competitions provide the opportunity to identify the best emerging talent in cyber security. However, such competitions have provided little opportunity to develop new talent. Training must be provided before students have the ability to be at the competitive level required by these competitions, though, some competition developers do provide learning materials. Classroom based competitions may still have merits in challenging students to apply all of the skills that they have acquired. Such competitions are often limited in scope, they often teach only one aspect of cyber security, mostly commonly ethical hacking.

## 4. Comparison of Laboratory Approaches

Table 1 summarises the strengths and weaknesses of the main categories of laboratories. The main problems with physical laboratories are the expense, lack of flexibility and restrictive time scheduling, these issues are remedied by simulation and virtual laboratories. However, simulation laboratories are limited in their realism and flexibility in terms of creating custom exercises and challenges, there is a reliance on the original developers to keep developing new exercises, which may not be bespoke. This is not the case in virtual laboratories as these use the genuine software instead of simulations. Cloud-based virtual laboratories provide additional flexibility and scalability.[12] Cloud based platforms are inherently scalable,[4,12] therefore, such platforms can be scaled to meet changing class sizes or additional modules, this would be much more difficult and expensive in a physical laboratory.

Table 2, placed at the end of the article, summarises the laboratories that were presented in the surveyed papers. In this table there is a focus on the features that were found to be important for cyber security laboratories in an educational environment.

Cloud-based laboratories have more flexible access than physical laboratories as they can be accessed at anytime from anywhere that has an Internet connection, assuming that sufficient resources are available. This level of accessibility is invaluable for students who may prefer or require to work at times that suit them, it also increased the time that students are able to access and complete the exercises. Virtualisation allows a high level of reconfiguration allowing tutors to develop and deploy realistic scenarios and exercises.

## 5. Future Work

This section will consider the requirements and best practices for the development of future cyber security laboratories and exercises.

Laboratories must be secure so that any activities in them do not affect other networks. This isolation can be achieved logically in virtual networks or physically in a physical campus laboratory.

The laboratory environment should give a realistic and flexible environment, this can be achieved through using real hardware and software. However, it is more flexible to virtualise software which enables tutors or students to more easily configure virtual networks or VMs to meet their needs.

Providing students with remote access can greatly improve accessibility and increase the amount of time that students spend practicing. Of the students surveyed at Liverpool John Moores University, 75 % of students stated that they preferred to work from home or a combination of both home and on-campus. By providing remote access, institutions can then leverage their platforms for distance learning. If students are to be expected to work remotely then there can't be any assumptions about their equipment and therefore efforts should be taken to minimise any requirements of it.

As mentioned previously, the ability to restore machines to previous states to recover from errors or to reset exercises is important. This can be achieved in a virtual laboratory by storing snapshots of varying machine states. Using this method is quicker and simpler than restoring a full operating system on a physical machine and then redeveloping the exercise.

By dynamically generating virtual networks, possibly through the user of a user-friendly graphical user interface (GUI) a student can quickly create their own virtual networks to develop their own knowledge and skills through personal experimentation. Galan et al. propose one such solution using VNUML to instantiate virtual networks, shown in Figure 4.[47] Providing features such as this, or developing the networks on behalf of the students minimises the time that students spend configuring virtual networks and increases the time they spend actually learning the cyber security skills.

It is recommended that any virtual laboratories should be multi-VM laboratories allowing students to have access to more realistic virtual networks containing different types of VMs as well as giving them the chance to experiment with network security. These virtual networks should closely represent real-world networks to give students the most realistic experience[55]. Students often have other commitments and prefer to work when and where is best for them, and simulation and virtual laboratories provide such flexibility.

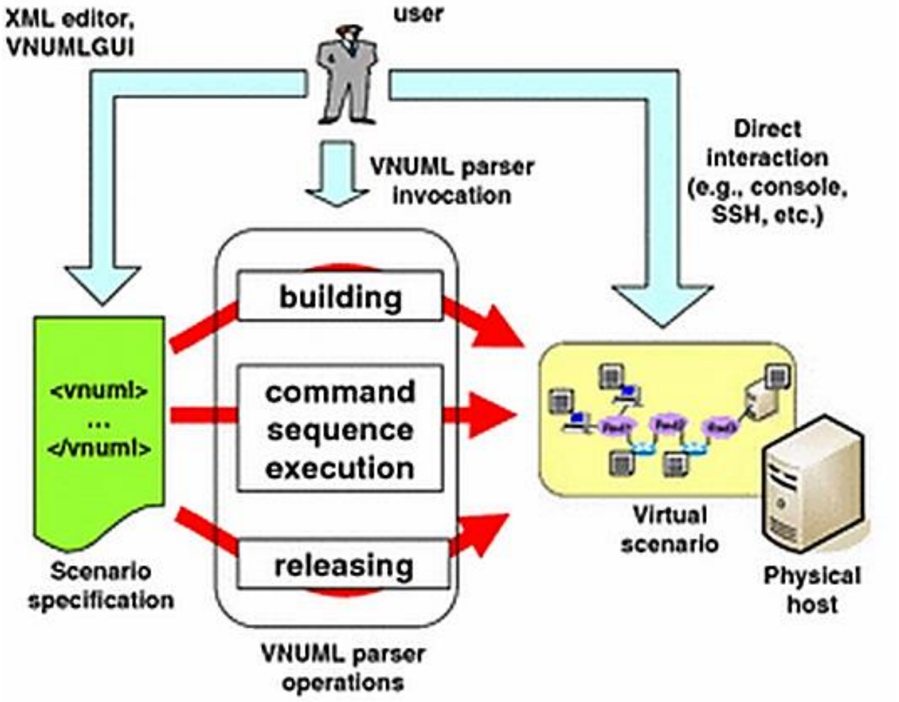

**Figure 4. VNUML Operation Workflow.**[47]

The aforementioned desirable characteristics can be achieved through the use of cloud-based virtualisation. The scalability of cloud-based solutions makes it ideal for an education environment where user numbers and storage requirements can fluctuate each year.

Cyber security is a global issue and as such any developments in such pedagogy should be disseminated to allow it to have a greater impact on global security in terms on increasing the number of cyber security professionals joining the field.[55]

## 6. Conclusion

In this paper, we presented a survey of the approaches to cyber security education. We evaluated the strengths and weaknesses in the current approaches to cyber security teaching and learning and proposed a set of requirements and recommendations to aid the development of future platforms and exercises. With the urgent need for cyber security professionals, pedagogy in this area is gaining a large amount of interest from researchers and educators.

There is a current trend of institutions adopting cloud-based virtualisation approaches to cyber security education and pedagogic research has shown that they have a positive impact on student learning.[12] Such platforms can provide the security and flexibility required to deliver realistic exercises whilst also allowing improved scalability. E-learning and distance learning is becoming common place and those who do not regularly visit the campus can be left behind with little practical exercise or little support from tutors, this can be remedied through remote access.

Some hardware may lose essential properties when it is virtualised, this can be alleviated by implementing a hybrid-laboratory which combines physical hardware with virtualisation, such as that at Georgia Tech.[30]

## Acknowledgement

The authors would like to thank the Higher Education Academy (HEA) for partly funding this research project.

## Notes

[1] Cabinet Office, *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World*, 2011, Accessed May 23, 2015.

[2] Shaw, R, S, Charlie, C Chen, Albert, L Harris, and Hui-Jou Huang, “The Impact of Information Richness on Information Security Awareness Training Effectiveness,” *Computer & Education* 52 (2009): 182-195.

[3] Reece, R, P, and B, C Stahl, “The Professionalization of Information Security: Perspectives of UK Practitioners,” *Computers & Security* 48 (2015): 182-195.

[4] Yan, Chenyang, “Build a Laboratory Cloud for Computer Network Education,” *ICCSE*, Singapore (2011), 1013-1018.

[5] Pastor, Vicente, Gabriel Diaz, and Manuel Castro, “State-of-the-art Simulation Systems for Information Security Education, Training and Awareness,” *EDUCON* (2010), 1907-1916.

[6] Shaw, R, S Charlie, C Chen, Albert, L Harris, and Hui-Jou Huang, “The Impact of Information Richness on Information Security Awareness Training Effectiveness,” *Computer & Education* 52 (2009): 182-195.

[7] Reece, R P, and B, C Stahl, “The Professionalization of Information Security: Perspectives of UK Practitioners,” *Computers & Security* 48 (2015): 182-195.

[8] Andel, Todd R, Kyle E Stewart, and Humphries W Jeffrey, “Using Virtualization for Cyber Security Education adn Experimentation,” *CISSE* (2010), 130-136.

[9] Hu, Dong, and YuYan Wang, “Teaching Computer Security using Xen in a Virtual Environment,” *ISA* (2008), 389-392.

[10] Carlsson, Anders, Rune Gustavsson, Leo Truksans, and Martens Balodis, “Remote Security labs in The Cloud ReSeLa,” *EDUCON* (2015), 199-206.

[11] Marsa-Marestre, Ivan, Enrique Hoz, Jose M Guzman, and Miguel A Lopez-Carmona, “Design and Evaluation of a Learning Environment to Effectively Provide Network Security Skills,” *Computers & Education* 69 (2013): 225-236.

[12] Xu, Le, Dijiang Huang, and Wei-Tek Tsai, “Cloud-based Virtual Laboratory for Network Security Education,” *IEEE Transactions on Education* 5 (2014): 145-150.

[13] Nagarajan, Ajay, Jan, M Allbeck, Arun Sood, and Terry, J Janssen, “Exploring Game Design for Cybersecurity Training,” *CYBER*, Bangkok, 2012.

[14] Locasto, Michael E, and Sara Sinclair, “An Experience Report on Undergraduate Cyber-Security Education and Outreach,” *ACEIS*'09, 2009.

[15] ACM, *Computer Science Curricula 2013*, 2013, Accessed November 10, 2015. http://www.acm.org/education/CS2013-final-report.pdf.

[16] Armitage, Grenville J., “Maximising Student Exposure to Unix Networking using FreeBSD Virtual Hosts,” *CAIA Technical Report 030320A* (2003), 1-6.

[17] Willems, Christian, Thomas Klingbeil, Lukas Radvilavicius, Antanas Cenys, and Christoph Meinel, “A Distributed Virtual Laboratory Architecture for Cybersecurity Training,” *ICITST* (2011), 408-415.

[18] Benzel, Terry, “The Science of Cyber Security Experimentation: The DETER Project,” *ASAC'11* (2011), 137-147.

[19] Armitage, William D, Alessio Gaspar, and Matthew Rideout, “Remotely Accessible Sandboxed Environment with Application to a laboratory Course in Networking,” *SIGITE* Florida, 2007.

[20] Abler, Randal T, Didier Contis, and Julian B Grizzard, “Georgia Tech Information Security Center Hands-on Network Security Laboratory,” *IEEE Transactions on Education* 49, no. 1 (2006): 82-87.

[21] Nance, Kara L, and Brian Hay, “Evolution of the ASSERT Computer Security Lab,” *CISSE,* Adelphi, 2006.

[22] Stockman, Mark, “Creating Remotely Accessible “Virtual Networks” on a Single PC to Teach Computer Networking and Operating Systems,” *CITC4'04* (2003): 67-71.

[23] Wannous, M, and H Nakano, “NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualisation and Virtual Network Computing Technologies,” *IEEE Transactions on learning Technologies* (2010), 129-138.

[24] Hay, Brian, and Kara L Nance, “Evolution of the ASSERT Computer Security Lab,” *CISSE* (2006), 150-156.

[25] Srinivasan, S., “Design and Development of an Information Security Laboratory,” *CISSE* Georgia (2005), 39-43.

[26] Wagner, Paul J, and Jason M Wudi, “Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course,” *SIGCSE'04* (2004), 402-406.

[27] Summers, Wayne C, Bhagyavati, and Carlos Martin, “Using a Virtual Lab to Teach an Online Information Assurance Program,” *InfoSecCD'05* (2005), 84-87.

[28] Duffy, B., “Network Defence Training through CyberOps Network Simulations,” *VMASC*, 2008.

[29] Irvine, Cynthia E, Michael Thompson, and Ken Allen, “CyberCIEGE: Gaming for Information Assurance,” *IEEE Security and Privacy* 3 (2005): 61-64.

[30] Leitner, Lee J, and John W Cane, “A Virtual Laboratory Environment for Online IT Education,” *SIGITE'05* (2005), 283-289.

[31] Caltagirone, Sergio, Paul Ortman, Sean Melton, David Manz, Kyle King, and Paul Oman, “RADICL: A Reconfigurable Attack-Defend Instructional Computing Laboratory,” *SAM'05* (2005).

[32] Liljenstam, Michael, Jason Liu, David Nicol, Yougu Yuan, Guanhua Yan, and Chris Grier, “RINSE: the Real-time Immersive Network Simulation Environment for Network Security Exercises,” *PADS'05* (2005).

[33] Tobin Jr, Donald L, and Michael S Ware, “Using A Windows Attack intRusion Emulator (AWARE) to Teach Computer Security Awareness,” *ITiCSE'05* (2005), 213-217.

[34] Ryoo, Jungwoo, Angsana Techatassanasoontorn, Dongwon Lee, and Jeremy Lothian, “Game-based InfoSec Education Using OpenSim,” *CISSE* (2011).

[35] Denning, Tamara, Adam Lerner, Adam Shostack, and Tadayoshi Kohno, “Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education,” *CCS'13* (2013).

[36] Lixandroiu, Radu, and Catain Maican, “A Model for Comparing Free Cloud Platforms,” *Informatica Economica* 18, no. 4 (2014): 40-49.

[37] Son, Joon, Chinedum Irrechukwu, and Patrick Fitzgibbons, “A Comparison of Virtual Lab Solutions for Online Cyber Security Education,” *Communiactions of the IIMA* 2, n0. 4 (2012).

[38] Lahoud, Hilmi A, and Xin Tang, “Information Security Labs in IDS/IPS for Distance Education,” *SIGITE'06* (2006), 47-52.

[39] Zenebe, Azene, and David Anyiwo, “Virtual Lab for Information Assurance Education,” *CISSE* (2010), 124-129.

[40] Villanueva, Benjamin, and Brett Cook, “Providing Students 24/7 Virtual Access and Hands-On Training Using VMWare GSX Server,” *SIGUCCS'05* (2005), 421-425.

[41] Anderson, Benjamin R, Amy K Joines, and Thomas E Daniels, “Xen Worlds: Leveraging Virtualization in Distance Education,” *ITiCSE'09* (2009), 293-297.

[42] Border, Charles, “The Development and Deployment of a Multi-User, Remote Access Virtualisation System for Networking, Security, and System Administration Classes,” *SIGCSE* (2007), 576-580.

[43] Powell, Valerie J H, Christopher T Davis, Randall S Johnson, Peter Y Wu, John C Turchek, and Ian W Parker, “VLabNet: The Integrated Design of Hands-on Learning in Information Security and Networking,” *InfoSecCD* (2007).

[44] Armitage, William D, Alessio Gaspar, and Matthew Rideout, “A UML and MLN Based Approach to Implementing a Networking Laboratory on a Scalable Linux Cluster,” *CCSC'07* (2007), 112-119.

[45] Kneale, Bruce, Ain Y De Horta, and Hona Box, “VELNET (Virtual Environment for Learning Networking),” *ACE2004* (2004).

[46] Krishna, Kumar, Weiqing Sun, Pratik Rana, Tianning Li, and R Sekar, “V-NetLab: Cost-Effective Platform to Support Course Projects in Computer Society,” *CISSE* (2008).

[47] Galan, Fermin, David Fernandez, Walter Fuertes, Miguel Gomez, and Jorge E Lopez de Vergara, “Scenario-based Virtual Network Infrastructure Management in Research and Educational Testbeds with VNUML,” *TELECOM* (2009), 305-323.

[48] *Open Cyber Challenge Platform*, 2015, Accessed May 25, 2015. http://opencyberchallenge.net.

[49] OWASP *Security Shepherd*. Accessed May 25, 2016. https://www.owasp.org/index.php/OWASP_Security_Shepherd.

[50] CESG, *Cyber Security Challenge UK*, 2015, Accessed November 11, 2015. https://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx.

[51] Cyber Security Challenge UK, *2014 Cyber Security Challenge UK*, Accessed November 11, 2015. http://cybersecuritychallenge.org.uk/.

[52] UCSB, *The UCSB iCTF Competition*, 2015, Accessed November 11, 2015. http://ictf.cs.ucsb.edu/.

[53] Vigna, Giovanni, Kevin Borgolte, Jacopo Corbetta, Adam Doupe, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, and Yan Shoshitaishvili, "The Years of iCTF: The Good, The Bad, and The Ugly," *3GSE* ( 2014).

[54] Air Force Association, *CyberPatriot*, 2013, Accessed November 12, 2015. https://www.uscyberpatriot.org/competition/Competition-Overview.

[55] Fuertes, W, J E Lopez de Vergara, and F Meneses, "Educational Platform using Virtualization Technologies: Teaching-Learning Applications and Research Use Cases," *ACE II* (2006).

## About the Authors

LUKE TOPHAM is currently a Research Assistant at Liverpool John Moores in cyber security teaching and learning with a particular interest in the application of cloud computing environments. He received his MSc in Computer Science from Liverpool John Moores University in 2015 and his BSc in Computer Science from the University of Chester in 2014.

Dr KASHIF KIFAYAT is a Senior Lecturer and Programme Leader for the Cyber Security programme at LJMU. Kashif completed his PhD at Liverpool John Moores University in 2008 on the topic of key management in wireless sensor networks. He subsequently joined the School as a lecture and has been involved in numerous security and system-of-systems related projects, including work with Thales UK and Xyone Security. Kashif is the Principal Investigator on the recent UK Higher Education Academy funded VIBRANT project to develop an educational platform for hands-on lab-based security training. Kashif's other research interests include mobile ad-hoc networks and cloud computing systems.

YOUNIS A. YOUNIS received his BSc (2003) and MSc (2010) degrees in computer sciences and computer network security from Garyounis University (Libya) and Liverpool John Moores University respectively and is currently nearing the completion of his PhD. He is a research assistant at Liverpool John Moores University. His research interests include computer security, network security, cloud computing, access control and cache side-channel attacks.

Professor QI SHI is a Professor in Computer Security in the Department of Computer Science at Liverpool John Moores University in the UK. He received his PhD in Computing from the Dalian University of Technology, P.R. China. Prior to joining Liverpool John Moores University, he worked as a Research Associate for the Department of Computer Science at the University of York in the UK. His research interests include security protocol deign, ubiquitous computing security, formal models, sensor network security, computer forensics and intrusion detection.

Dr BOB ASKWITH is a Principal Lecturer in the Department of Computer Science at Liverpool John Moores University. He received a BSc in Software Engineering in 1996 and a PhD in Network Security in 2000, both from LJMU. He leads the development and delivery of Cyber Security programmes within the department. His research interests are focussed on the security of computer networks, especially mobile, wireless, and ad hoc. He has been involved in security projects funded by UK Government and EU.

Table 2. Summary of Existing Laboratories.

| Paper Name | Laboratory Type | Virtualisation Type | Remote Access | Lab Scheduling | Persistent Storage | Reconfiguration Level |
|---|---|---|---|---|---|---|
| Exploring Game Design for Cybersecurity Training (Nagarajan, et al. 2012) | Simulation (Videogame) | None | No | Restricted to tournaments / Challenges | None | None (Dependent on Developers) |
| A Distributed Virtual Laboratory Architecture for Cybersecurity Training (Willems, et al. 2011) | Virtual | Multi-VM | Yes | Unrestricted | Yes, plus progressive e-learning | VM-level |
| Cloud-Based Virtual Laboratory for Network Security Education (Xu, Huang and Tsai 2014) | Virtual | Multi-VM | Yes | Unrestricted | Yes, access for tutors to grade | VM-level |
| ENGENSEC – Remote Security Labs in the Cloud (ReSeLa) (Carlsson, et al. 2015) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |
| Scenario-based Virtual Network Infrastructure Management in Research and Educational Testbeds with VNUML (Galan, et al. 2009) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |
| Build a Laboratory Cloud for Computer Network Education (Yan 2011) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |
| VLabNet: The Integrated Design of Hands-on Learning in Information Security and Networking (Powell, et al. 2007) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |

| | | | | | | |
|---|---|---|---|---|---|---|
| Virtual Lab for Information Assurance Education (Zenebe and Anyiwo 2010) | Virtual | Single-VM | Yes | Unrestricted | Yes | VM-level |
| Evolution of the Assert Computer Security Lab (Hay and Nance 2006) | Shared Host Virtual lab | Single-VM | Yes | Unrestricted | Yes, VM image database | Limited by hardware VM-level |
| NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualisation and Virtual Network Computing Technologies (Wannous and Nakano 2010) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |
| The Development and Deployment of a Multi-User, Remote Access Virtualisation System for Networking, Security and System Administration Classes (Border 2007) | Virtual | Multi-VM | Yes | Unrestricted (limited by resources, ability for users to view usage and decide whether to join or not) | Yes, image store for different OS updates | VM-level |
| Creating Remotely Accessible “Virtual Networks” on a Single PC to Teach Computer Networking and Operating Systems (Stockman 2003) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |
| Maximising Student Exposure to Unix Networking using FreeBSD Virtual Hosts (G. J. Armitage 2003) | Virtual | Multi-VM | Yes | Unrestricted | Yes | VM-level |

| | | | | | | |
|---|---|---|---|---|---|---|
| Information Security Labs in IDS/IPS for Distance Education (Lahoud and Tang 2006) | Virtual | Single-VM | Yes | Restricted time scheduled | No, setting wiped after use | VM-level |
| Using a Virtual Lab to teach an Online Information Assurance Program (Summers, Bhagyavati and Martin 2005) | Virtual | Single-VM | Yes | Unrestricted (limited by number of users) | Yes | VM-level |