CYBER-DEFENSE TRAINING IN THE REAL
Design Principles and Architecture of the VNEL Cyber-training Platform

Riccardo Bettati, Lauren Cifuentes, Willis Marti, René Mercer, Youngwoo Ahn, Gaurav Yadav
Texas A&M University, College Station, TX, U.S.A.

Omar Alvarez
Department of Computer Science, Autonomous University of Baja California, Mexico

Keywords: Case-based learning, Network engineering, Security training.

Abstract: We present the Virtual Network Engineering Laboratory, which creates a high-fidelity, multi-platform, remotely accessible environment where students obtain hands-on experience in network engineering and operation and in cyber defense and infrastructure protection. The facility focuses on access to real equipment in a realistic yet isolated setting. isolation allows for a broad variety of activities without danger to the surrounding operational networks, and it allows the students to learn from mistakes on equipment that is both real and well protected. The Laboratory supports fine-grained, detailed instrumentation of user activities and allows for experiments on a wide variety of real networking equipment. Real equipment is emphasized over simulation for the sake of (a) fidelity of both intended and non-intended modes of operation, (b) extendability to other protection domains such as cyber physical systems, and (c) instrumentability of student-system interactions to support run-time assessment and on-demand scaffolding.

1 INTRODUCTION

We are realizing that our technical infrastructure depends increasingly upon individuals and people running businesses coming to understand the cyber landscape and how to protect their investments and asses as managed on computers. Such audiences are often geographically dispersed and served by instructional institutions that often cannot afford to design or run high-value cyber security programs on their own. Any comprehensive strategy for cyber security requires training individuals and small businesses to secure their own parts of cyberspace, as gaps in the security of one group of cyber participants can be a conduit through which other participants are attacked.

The VNEL replaces the physical contacts between students and the machines with web-based access sessions. Students focus on technical solutions in network management without being distracted by less relevant steps. The VNEL is instructionally innovative in that it provides students with remote but real time access to equipment during networking exercises so that a large number of students can do their exercises simultaneously and at their convenience. The VNEL allows an instructor to choose the interplay of operating system support, exercise semantics, and network support to best meet curricular needs.

We have developed the VNEL as a case-based learning environment to instruct learners in cybersecurity. The VNEL differs from conventional teaching laboratories in that it does not require students to be physically located with the network equipment they are learning to manipulate. Instead, the VNEL offers a technologically innovative environment for computer engineering instruction in which students remotely manipulate equipment in a real network and conduct cased-based problem-solving exercises in a controlled, high-fidelity environment via the Internet using their web browsers.

VNEL enables instruction to be efficiently and effectively distributed across geographic regions, thereby reaching greater numbers of students, including traditionally underrepresented students, than would be possible through traditional face-to-face or on-site laboratory instruction. The VNEL provides for both distributed expertise and equipment needed for hands-on experience with networks.

Bettati R., Cifuentes L., Marti W., Mercer R., Ahn Y., Yadav G. and Alvarez O. (2010).
CYBER-DEFENSE TRAINING IN THE REAL - Design Principles and Architecture of the VNEL Cyber-training Platform.
In *Proceedings of the 2nd International Conference on Computer Supported Education*, pages 493-496
DOI: 10.5220/0002861604930496

2 CASE-BASED LEARNING IN VNEL

VNEL uses a case-based approach, where students are given a particular problem scenario to solve. They then work through a sequence of scenarios and exercises. Within each exercise are performance objectives, activities, and feedback. Activities typically include a small problem, a topology, tasks, deliverables, and self-assessments. Once students have completed the exercises, they should be able to perform the terminal activity: solving the case in the scenario.

Case-based learning was chosen as the instructional model because novices needed to learn how to gain and refine their expertise at solving real-world cybersecurity problems (Jonassen et al., 1999). In effective learning environments, that experience is scaffolded with expert case knowledge. A case serves as a representation of real-world phenomena and is a safe, yet meaningful environment in which students can develop understanding of the complexity of network engineering. Jonassen and Hernandez-Serrano (Jonassen and Hernandez-Serrano, 2002) describe the case-based reasoning cycle as the presentation of a new problem-case to solve. Learners apply previous experiences and general knowledge to solve the case, suggest solutions, test the solutions, revise their suggestions, and confirm solutions. During the cycle, learners retrieve, reuse, revise, and retain understanding until expertise is gained from the problem-case.

For the case of a Firewalls course unit, task analysis indicated that network engineers need to be able to align a network topology with security requirements, configure network access control, and protect information through encryption and VPNs. Once students have mastered each of the skills, they should be able to address the case in the problem scenario.

2.1 Remote Device Access in VNEL

The VNEL is *not* a simulation or an emulated environment. Rather, students remotely manipulate real networks and receive real-world feedback when the network works or does not work effectively. It is instructionally innovative in that it provides students with remote but real-time access to equipment during networking experiments so that a a large number of students can perform their experiments simultaneously and at their convenience. It also provides a complete instructional system including quizzes, automated assessment of simple student submissions, and opportunities for students to work collaboratively on larger, poorly structure or unstructured, case studies.

Figure 1 describes the architecture of the VNEL. The facility is accessed through a single publicly visible server, the *Web Access Exercise System* (WAES). Actual equipment is organized into *pools* that can be assigned to exercises on-the-fly. The VNEL provides a set of network devices (switches, routers, or firewalls) from a *device pool* and a set of hosts and servers from a *host pool*. When students start an exercise, the WAES brings in devices and hosts and configures the network infrastructure accordingly. All devices and hosts are connected through a virtual-LAN capable *switch infrastructure* that can create whatever connectivity is required by the exercises. This infrastructure cannot be seen by the students. Only the connections established for the exercises are visible. These connections are managed by the *configuration management* component of the WAES.

The WAES provides five services:

Courseware Access and Management. This component of the WAES provides access to traditional, non-exercise related, course material. It provides students with descriptions of case studies and links to reference material. It also provides the courseware framework for students to access the "hands-on" exercises. Finally, it also offers opportunities to author quizzes and other assessment mechanisms.

Resource Configuration. Exercises are associated with so-called *resource sets*, which define the network devices and hosts needed for the particular exercise, together with the interconnection topology as defined by the exercise. Devices and hosts are selected from their respective pools and are appropriately configured when the student starts the exercise.

Resource Management. Since the resource sets represent physical resources, and there are only limited numbers available thereof, students are encouraged to *reserve* the required resource sets *in advance*. Students do this by *scheduling* a particular exercise for a given time, and are therefore not aware of the detailed reservation issues. Given that the VNEL is used by multiple institutions, it is important to guarantee fair access to the available resources, both at student level and at institution level. Individual students, or groups of students at an institution, should be flexible in how much time they want to spend on some exercises. They should not be able, however, to over-reserve resource sets at the expense of other students or student groups at other institutions. We are experimenting with hierarchical *fair-share* scheduling algorithms to control over-allocation of resources. Students and institutions are allocated a *guaranteed share* of resources in number of reservation slots per time period. Whenever the number of slots in share is reached, no additional reservations are accepted until the end of the period. For example, an institution may

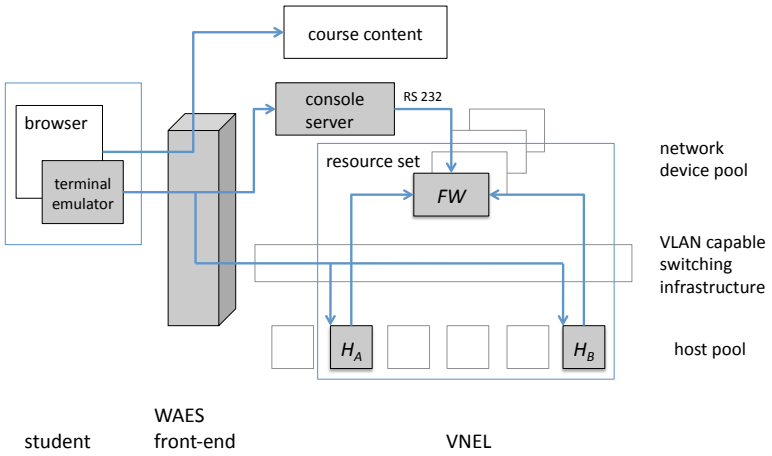

Figure 1: Architecture of the Virtual Network Engineering Laboratory.

request sixty one-hour slots of a particular resource set per day. If students reserve slots starting at some time t, and all sixty slots have been reserved by students within, say, the first three hours, no new reservations can be made until time $t+24$ if the system is highly utilized by other institutions as well. Fair-share algorithms do well in giving students or institutions more than their guaranteed share when excess capacity is available, but do not handle well situations with advance reservations. Heuristics must be studied to allow for fair allocation of spare resources in the presence of advance reservations.

Direct Device Access. Students operate on the assigned and configured devices and hosts through the devices' console or management interface, respectively. In the case of a console access, the student's browser displays a `telnet` window, and the connection traffic is routed by the WAES to a console server, which in turn is connected through an serial cable to the management console input of the device. In this way, the student establishes secure and high-fidelity console access to network devices in a customized configuration and an isolated setting using a very basic Web browser. The WAES maintains session information and monitors and logs student activity for immediate feedback and for subsequent analysis.

Functional Stress Testing. After completion of an exercise (for example after a configuration of a firewall to satisfy a given set of requirements,) the student instructs the WAES to initiate functional testing. A testing approach that is very popular with students are so-called "attack scripts", where the WAES triggers carefully authored scripts on nodes inside the configured network to simulate a red-team attack. Information about success of these scripts is forwarded to the WAES, which in turn provides a summary of the effect of the attack to the student.

Figure 1 illustrates the VNEL architecture with the simple case of a firewall exercise. The resource set in this case consists of a firewall (FW) and two hosts (H_A and H_B,) which in turn represent the internal and external portion of the internet. The VLAN capable switch infrastructure connects the Host H_A with the internal port on the firewall FW and Host H_B with the external port of FW. The student is then led through a series of scaffolded activities to configure the firewall. She manipulates the firewall through a browser-provided terminal emulator, which communicates to the WAES. The WAES in turn forwards the session through a console server to the serial console access on the device FW. The student triggers functional testing by pushing a button on the browser window, and the WAES initiates a number of scripts on both Host H_A and Host H_B to test how well the inside network is protected without cutting off critical services.

2.2 The VNEL in Practice

The VNEL facility was first used in support of an upper level undergraduate course in Networks and Distributed Processing. This course was taught with VNEL support twice a year from 2000 to 2005. Reaching over 150 students a year, the VNEL attracted significant industry support. The lab conduced several trials focused on support for professionals' continuing education. The VNEL also supported a graduate course in Advanced Network Security, taught once a year. Part of this course included a 3 month long scenario based exercise, where student groups set up their own campus or e-business and kept it in operation despite attacks by an external Red Team. Students using the VNEL formed a team that won the first Southwest Regional Collegiate Cyber Defense Competition (CCDC) (CCDC, 2009)

in 2005 and won the National CCDC in 2007.

Starting in 2007, the VNEL became a core component of our efforts to bring cost-effective and high-production-value cybersecurity training to community colleges (VTECH, 2009). We are currently collaborating with 15 community colleges across the U.S. to study the feasibility, the costs, and the effectiveness of laboratory based cybersecurity education.

3 THE CASE AGAINST VIRTUALIZATION

The benefits of the VNEL over traditional physical laboratories are evident, such as the naturally complementary nature of remote access and web-based teaching or the better isolation of sensitive cybersecurity exercises from the operational network. Recently, it *virtual platforms* have become increasingly popular for cybersecurity training. Their advantages are primarily cost effectiveness, improved scalability, and simpler management of the platforms. Non-negligible is also the interest from vendors to increase the user base for their virtualization technologies.

The VNEL largely avoids virtualization, and does so for several reasons:

Fidelity. Fidelity of both intended and non-intended modes of operation Computing and Server Nodes, such as web servers, are easy to virtualize in a high-fidelity manner with the use of virtualization veneers such as VMware Server or Xen. Other, operating system-level, virtualization technologies such as linux-VServer are less appropriate, since they do not allow for networking-level virtualization, which in turn affects fidelity. Network devices, on the other hand, cannot be virtualized using simple veneers. Instead, such devices must be *emulated*. High-fidelity emulation of network-level devices is very difficult to achieve, as both intended and non-intended modes of operation must be emulated, and network addressing mechanisms must remain transparent to the user.

Integration with Cyber-physical Environments. Increasingly, the Supervisory Control and Data Acquisition (SCADA) systems of many critical infrastructures have been moving towards open systems solutions and the Internet. This has made many of these systems highly vulnerable to security attacks. SCADA systems are characterized by the integration of traditional internetworks with physical devices, typically at the edge of the networks. The connection of such devices to the physical world makes for very different security implications, and traditional security mechanisms are not sufficient. We envision VNEL to extend into the area of training for cyberinfrastructure protection in modern SCADA systems, where a large variety of physical devices will be integrated into the platform.

Instrumentation of User-system Interaction. In its current form, the communication between the student and the exercise network is open to the WAES for inspection, monitoring, and logging. This enables the WAES to respond to student activity in real-time. We are currently developing a *Mixed-Initiative Intelligent Tutor* that develops and maintains student activity models in real-time, and that guides the students that indicate the need for help. Human instructors take over when the Intelligent Tutor indicates low confidence. The combination of human instructor and Intelligent Tutor will allow us to start experimenting in so-called *On-Demand Scaffolding*, where students are exposed to unstructured problems, and are immediately offered scaffolding on-line if needed.

Cybertraining infrastructures that rely on virtualization tend to use systems with very convenient interfaces but with proprietary communication protocols (e.g. VMware Server). This makes the monitoring of student activity very difficult. As a result, students have very little support during exercises.

ACKNOWLEDGEMENTS

This work was supported in part by the National Science Foundation under award number OCI-0753408. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of the National Science Foundation.

REFERENCES

CCDC (2009). National collegiate cyber defense competition. `www.nationalccdc.org`.

Jonassen, D. and Hernandez-Serrano, J. (2002). Case-based reasoning and instructional design: Using stories to support problem solving. *Educational Technology Research and Development*, 50(2):65–77.

Jonassen, D. H., Tessmer, M., and Hannum, W. H. (1999). *Task Analysis Methods for Instructional Design*. Lawrence Erlbaum Associates.

VTECH (2009). Virtual tools for expanding the cyber horizon (vtech). `http://vtech.tamu.edu`.