Teaching Security With Network Testbeds

Jelena Mirkovic, Mike Ryan and John Hickey (USC/ISI)
Keith Sklower (UC Berkeley)
Peter Reiher and Peter A. H. Peterson (UC Los Angeles)
B. Hoon Kang (George Mason University)
Mooi Choo Chuah (Lehigh University)
Daniel Massey (Colorado State University)
Gisele Ragusa (University of Southern California)

ABSTRACT

Network security topics are gaining importance but they are often taught using traditional, passive methods via lectures and textbooks. This paper describes our efforts to change this situation by developing teaching materials and technical support for use of network testbeds in security education. This practice cannot replace the traditional teaching approach but should complement it to better train our future security workforce. We describe our work on both the education and testbed support fronts and offer some preliminary success measures derived from observing the usage of DETER testbed and our materials in Fall 2010.

1. INTRODUCTION

This paper describes our work on using network testbeds to teach security courses. This work consists of two synergistic parts: (1) development of publicly available hands-on cyber security exercises, and (2) development of network testbed modifications to support class use.

Our hands-on exercises are linked tightly to the publicly-available, free-to-use DETER testbed [1, 2] (created by funds from the NSF and the Department of Homeland Security) at USC Information Sciences Institute and UC Berkeley, facilitating easy adoption and portability among different institutions. They are fully automated and accompanied by background reading materials and student and teacher guidelines. Exercises are hosted on our Moodle server: `http://education.deterlab.net`. Exercise development was supported by a CCLI grant from the NSF, under the award number 0920719.

Testbed modifications implemented on the DETER testbed enable automated creation, deletion and recycling of student accounts, enforce access rules to student and instructor home directories to prevent cheating, and enforce "free when idle" resource policy on class experiments. We further describe novel administrative policies that we have created on DETER to plan for class usage and to balance class and research demand on our limited machine and human resources. This work was supported by the DHS grant, under the award number N66001-07-C-2001.

1.1 Importance of Security

Computer and Network Security are topics of growing importance in everyday lives. Greater reliance on computers and the Internet in many business areas and recently in cyber-physical domain means that every security threat carries potential to inflict great damage. Perpetrators of security crimes are becoming better funded and organized. At the same time, the number of unsophisticated computer users and the number of vulnerable PCs that are always connected to the Internet grows tremendously.

Trends in job demand follow this ever-growing importance of Computer and Network Security, with openings for competent security workers in almost any US industry or government body. Staying competitive in these fields requires a lot of hands-on experience with system and network administration, and skills in diagnosing and handling operational problems. Experience and practical skills are thus the primary job requirements for security professionals and should be an essential part of security courses.

1.2 Problems in Security Education

In sharp contrast with the dynamics in security fields, and high demand for practical knowledge by employers, university courses often teach security using passive learning methods, such as textbooks, blackboard and presentation slides. Much research has shown that active learning is more engaging and motivating for students than passive learning, and results in better absorption of material and better development of critical thinking [3, 4, 5, 6].

Practical exercises that we have developed provide students with an ultimate active learning experience, enabling them to see and feel the phenomena that is

being discussed in class. Such exercises can either be used to demonstrate a threat or a defense, before covering it in lecture, or they can be used as homework assignments to let students practice the content they learned.

Additionally, many security courses fail to cover the broadness of the field, and focus either on theoretical topics, mostly cryptography, or on very narrow, practical aspects of computer security, which mostly relate to exploits. In our opinion, neither approach is strong enough to meet the needs of today's job market. Cryptography-only courses can overwhelm students with theory and mathematical formulas, without providing any hands-on experience in dealing with real world security problems. Our exercises should additionally engage students in learning about security by giving them a direct experience of the threats cryptography aims to solve. Further, while an important component of computer security, cryptography is not the only tool for handling security problems. Our exercises acquaint students with other security tools and practices.

Courses that focus on extremely practical computer security, mostly exploits and intrusion defenses, work best for students who already have extensive system design and administration skills. Increasingly, computer science students do not necessarily have such skills. Our exercises should help such students to self-learn necessary skills and will guide them gently into complexities studied in the course. For both cryptography-focused and computer-security-focused courses, our exercises should provide students with a flavor of other security problems and related solutions. Further, since we have designed the exercises so that they are easy to adopt and portable, it is our hope that they will lead to expansion of narrowly-focused courses to better cover the rich fields of Network and Computer Security.

1.3 Related Solutions to Security Education

Many security educators have concluded that practical exercises improve student learning, and have developed these targeting deployment at their universities' labs. This is an excellent first step towards improving security education, but it is not sufficient because it does not promote portability, thus failing to build on work done by others. We now contrast this approach with ours, which deploys the exercises on the public DETER testbed [1, 2].

The first problem with the lab approach is that many institutions may lack a lab facility of sufficient size and flexibility for practical exercises. Those institutions that have such a lab may be reluctant to allow security exercises because they usually involve malicious code, which may "escape" to the rest of the university's network. Even if these problems are overcome, there is a significant ongoing cost to maintaining such a lab facility, which many departments cannot afford. DETER, on the other hand, is an open testbed that any faculty member can use (and approve her students to use). Thus, faculty from under-funded institutions, minority-serving colleges, and two-year and four-year colleges has as much opportunity to benefit from our exercises as faculty from top institutions.

The second problem with individual labs is that they are usually not automated for topology and OS setup, so those actions must be done manually by the educator prior to the exercise, which requires a lot of effort. DETER, on the other hand, has fully automated topology, OS and application setup that can be archived and reused by the same or different users. Thus, not only is the setup easier and faster, but it is also easily achieved in repeat offerings of the course and is easily shared with other educators.

The third problem is that students must all be present in the lab at the same time to do an exercise, because labs are often reserved for specific classes at a specific time. With DETER, students can be given similar deadlines for exercises as for regular homeworks, and they can do the work at their own schedule, accessing DETER via the Web from their dorms, labs or homes.

The fourth problem is that exercises developed for individual labs are rarely reusable by others, because a different lab may have a different physical setup. With DETER, all setup steps are fully automated and portability is a non-issue since all the classes perform the exercises on the same testbed.

The fifth problem is that educators who adopt exercises created by others lack mechanisms to propagate any customizations or improvements back to the creator and disseminate it to a wider community. With DETER we have provided the educators with opportunity of not only using the exercises but actively contributing to the collection. Over time, this should build a community of security educators that actively exchange materials, and should lead to improved security education.

Another related effort to ours comes from the UC Berkeley security center, called TRUST – Team for Research in Ubiquitous Secure Technology. This center is heavily focused on development of security research, but it also has a strong educational agenda including workshops, curriculum development and course material exchange. Their online portal, called TAO (`https://tao.truststc.org/`), contains course materials with a security focus, mostly slideware and

Topic	Posted/planned
Intro to Linux and DETER	posted
Denial of service	1 posted, 4 planned
Buffer overflows, pathname attacks and SQL injection	posted
Man in the middle attack	posted
Firewalls and file system permissions	posted
Computer forensics	posted
NIDS	posted
OS hardening	posted
Worm modeling	1 posted, 3 planned
DNS prefix hijacking	planned

Table 1: Classes on DETER in Fall 2010

links to course Web pages. A few courses have incorporated practical exercises, performed at a university lab. We believe that our effort and TRUST's are strongly synergistic and complementary. TRUST has gathered a valuable set of course materials that can be easily reused by educators, while our practical exercises could accompany this material to enhance learning. We plan to explore this synergy in the future.

2. PRACTICAL EXERCISES

Our practical exercises were developed by Drs Reiher, Mirkovic, Kang, Chuah and Massey who are co-PIs on the NSF CCLI grant. Research interests and expertise of these instructors cover many security areas, and complement each other. Dr Reiher is expert in secure file systems and ubiquitous systems. Drs Reiher and Mirkovic have also performed extensive joint research on IP spoofing and denial of service. Dr Mirkovic additionally has developed research on worm simulation and data privacy. Dr Chuah's research focuses on denial of service and malware. Dr Kang is an expert in malware and botnets. Dr Massey is an expert in routing and DNS security.

This team has developed nine hands-on exercises so far, which are posted on the DETER's Moodle server: `http://education.deterlab.net`. Eight more are in preparation and will be posted by the end of Summer 2011. All the exercises are shown in Table 1.

Each exercise contains a student and a teacher section. Access to all exercises is protected by one password. All educators interested in using these exercises are given this password after verifying their faculty status and the password is changed each semester. The student section contains the assignment specification that can be incorporated on the class Web page or given as handout to students. It also contains links to background reading. The teacher section contains troubleshooting guidelines for exercise setup, common problems experienced by students when doing the exercise and suggested solutions, grading suggestions and a solution manual. Our goal in developing the teacher section parts of the exercises was to provide sufficient information to teachers that have little practical experience with the given security topic to competently administer the exercise in their classes and to successfully field student questions about the exercise.

3. TESTBED SUPPORT FOR EDUCATION

The DETER testbed, which is our platform for exercises, has around 400 physical machines. It is based on the Emulab technology [7]. An experimenter gains exclusive access to a set of physical machines she needs for a limited time. The machines run an operating system and applications of a user's choice and are organized into a user-specified topology. Some users that are faculty members or senior researchers are recognized as principal investigators (PIs) by DETER and have the privilege to create projects and approve other users. Each user can either create or use an existing experiment – a description of topology, operating system and applications on physical machines – when interacting with DETER. Experiments are said to be "swapped in" when physical machines are assigned to them, and "swapped out" otherwise. PIs have root access to all machines within their project, while other users approved by the PI may have the same or lower privileges, depending on the PI's decision.

Interaction with DETER occurs mostly via a Web interface, where users can use graphical tools to create and manage experiments, and via SSH once the experiment is swapped in. DETER testbed is a controlled environment in which researchers can safely test security threats and defenses. No traffic is allowed to leave DETER and all experimentation occurs over the dedicated experimental network. DETER machines can thus be safely overloaded, compromised, crashed or suffer any other consequence of a successful security attack. This poses no threat to other DETER users nor to the Internet at large.

While our current materials and testbed improvements are tied closely to the DETER testbed they should with little to no modifications be portable to other Emulab-like testbeds.

3.1 Technical Support

Because Emulab technology was developed primarily for research use it was optimized for collaborative work. When an experiment is created in a DETER research project by one member,**all** members have their home directories exported to the experiment's ma-

chines. All members can also log on to the experiment's machines. This creates problem for educational use of DETER since students can log on to experiments created by their classmates and can also access their home directories. Even if users protect their home directories, a member of the same project can access them from experimental machines because he has a sudoer privilege there and can change access rules. To address these problems we are treating class projects differently than research projects, and we have implemented the following changes to our access control mechanism.

First, if a student creates an experiment in the default group of the project, **only** this student (and no other students, TAs or instructors) gets his home directory exported to the experiment's machines. Instructors and TA's will be able to log on to the machines with root privileges. No other students will be able to log on this experiment's machines. This creates conditions for class use of DETER by individual students.

Second, if a student creates an experiment in a group other than default, **all** members of that group (and no other students, TAs or instructors) get their home directories exported to the experiment's machines, and can log on to them. Instructors and TA's will be able to log on to the machines with root privileges. This creates conditions for class use of DETER by groups of students. Content is protected between groups but collaboration is facilitated within each group.

Another feature of Emulab technology that does not work well in class setting is how user accounts are handled. The framework has no provisions for deleting a user and reclaiming their username. This works well in research setting where churn should be low but it does not work well for classes where almost all users are only active during one semester. To handle this situation we have introduced recyclable accounts for students. PIs of class projects provide us with a list of student email addresses. We automatically create accounts for that course with generic usernames derived from course name, or we reuse accounts if the course was taught before. A few weeks after the end of the class we clean up student home directories, terminate experiments created by students and change passwords on student accounts thus reclaiming them for future use.

3.2 Administrative Support

Past few semesters have brought a large increase in the number of classes that are interested in using DETER. This prompted us to implement a few administrative policies to ensure that our resources are divided fairly between classes and that class usage does not compromise our research usage. These policies were first enforced in Fall 2010.

First, we ask instructors at the start of the semester to email us a schedule of their planned DETER exercises: start time, submission deadline and the maximum number of machines the class may need assuming the worst case when all students work simultaneously. This data is input into an online document, shared via Google docs with all class instructors (with edit access) for that semester. Each week we impose a resource limit on each class according to this online schedule, which equals 2/3 of the recorded demand. This ensures to some extent that no class can starve other classes for resources. Additionally we make sure that the sum of all class limits for the week does not exceed 2/3 of all testbed resources. This ensures that some resources remain available for our research users.

Our second policy concerns budgeting of our staff time. We ask instructors and TAs to be the first point of contact for their students for all DETER related questions, and to pass on to us those questions that they cannot answer. Often student questions are quickly resolved at this level and never propagate to us. We further have an instructor-only mailing list `education@deterlab.net` that we use for announcements and general discussion related to education on DETER.

4. LESSONS LEARNED AND PLANS

In Fall 2010 there were ten courses that used DETER testbed. Table 2 lists the institutions offering these courses, the number of students in each and the number of projects done on DETER. Courses are ordered in the table by the class size from the largest to the smallest. There is a good diversity in schools offerring the courses with regard to their size, ranking and geographical location. There is also large diversity in course size and number of exercises done on the DETER testbed. Some classes used practical exercises developed under our CCLI project while others used their own materials.

Figure 1 plots number of machines used by each class, following the order from Table 2 over the course of Fall 2010 semester, and the resource limits set on the course ($2/3$ of the maximum resource demand in a given week). If the instructor provided no demand for some week (e.g., no exercise was planned then) there was no limit set. We notice two trends from these graphs. First, larger classes tend to request more resources but underutilize them frequently staying well below their set limits, while smaller classes tend to bump often against their limits. We attribute this effect to greater multiplexing in a larger class, which ensures that resources are used in a more uni-

Institution	Students	Exercises
USC	100	5
UCLA	50	5
Youngstown State Univ.	50	1
San Jose State Univ.	45	3
Santa Monica College	45	4
Colorado State Univ.	40	6
University of Portland	30	3
Vanderbilt Univ.	15	2
Johns Hopkins Univ.	13	1
Stevens Inst. of Tech.	10	14

Table 2: Classes on DETER in Fall 2010

form manner. The second effect we noticed is that classes tend to use resources outside of their planned intervals. It is possible that this is due to instructors moving exercise deadlines without updating our online schedule. Another possibility is that this is due to instructors setting up exercises prior to assigning them to students. Both these effects merit further investigation and fine-tuning of our policies to better match observed usage patterns.

Figure 2 plots number of machines used by all classes and the total number of machines used in DETER over the course of Fall 2010 semester. It also shows the aggregate resource limit of $2/3$ of DETER resources that is set over the class demand. We observe that class usage stays well below this imposed limit. We also observe that this is not due to lack of testbed resources – in all cases there were free resources in the testbed that may have been allocated to classes since total utilization stayed below 80%. This observed effect may be due to instructors overestimating their resource needs but it may also be due to us setting too strict limits on some classes (i.e. those that tend to bump against them often from Figure 1) that force them to wait for resources even when there are free machines in the testbed.

We draw three conclusions from these observations. First, $2/3$ aggregate limit on class resources can be relaxed or at least can be enforced only when testbed resources are running low instead of all the time. Second, we need a better approach to ensure fairness of resource allocation between courses since obviously some courses need more and some need less resources than their instructors originally estimate. Third, we need a better resource allocation policy that ensures that a course is only denied resources when there is real and not just possible resource shortage.

To test the impact of each of the exercises developed under our CCLI grant PIs on the grant developed brief concept inventories that are administered before and after each exercise. These assessment metrics have embedded "misnomers" in them as incorrect answers so that instructors can determine actual conceptual understanding from the hands-on exercises in which the students are engaged. Preliminary results of the inventory assessments have indicated that learners engaged in the hands-on exercises are learning relevant concepts pertinent to the DETER experiences. Across the developed exercises, total gains in conceptual understanding from the exercises range from 12- 29%.

Our future plans consist of further developing teaching materials and class support for network testbeds. First, we plan to develop more teaching materials ourselves. Second, while any educator can currently post new shared materials on our Moodle server none have done so so far. We plan to encourage those that use DETER in classes to contribute their materials to our shared repository. Third, we plan to investigate ways to support better and fair use of our resources by class and research users. One possible way to ensure this would be to develop a resource reservation system and to allow allocation of reserved resources by other users with understanding that these may be reclaimed at the time noted in the reservation.

5. REFERENCES

[1] USC/ISI and US Berkeley. DETER testbed. `http://www.isi.edu/deter`.

[2] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab. Experience with DETER: A Testbed for Security Research,. In *Proceedings of Tridentcom*, March 2006.

[3] J. R. Anderson, L. M. Reder, and H H. Simon. Radical constructivism and cognitive

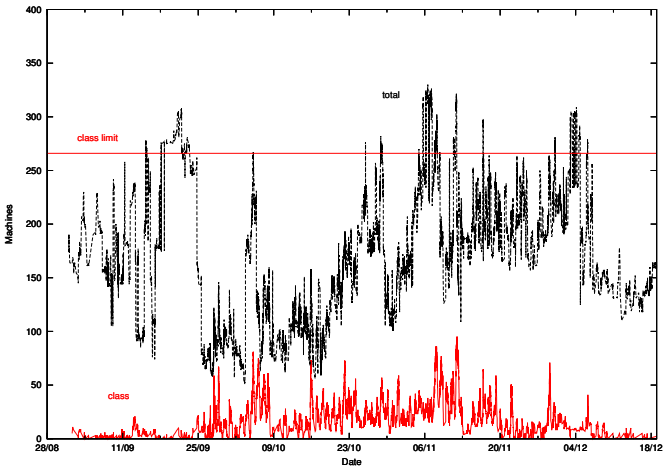

Figure 2: Total resource usage on the testbed

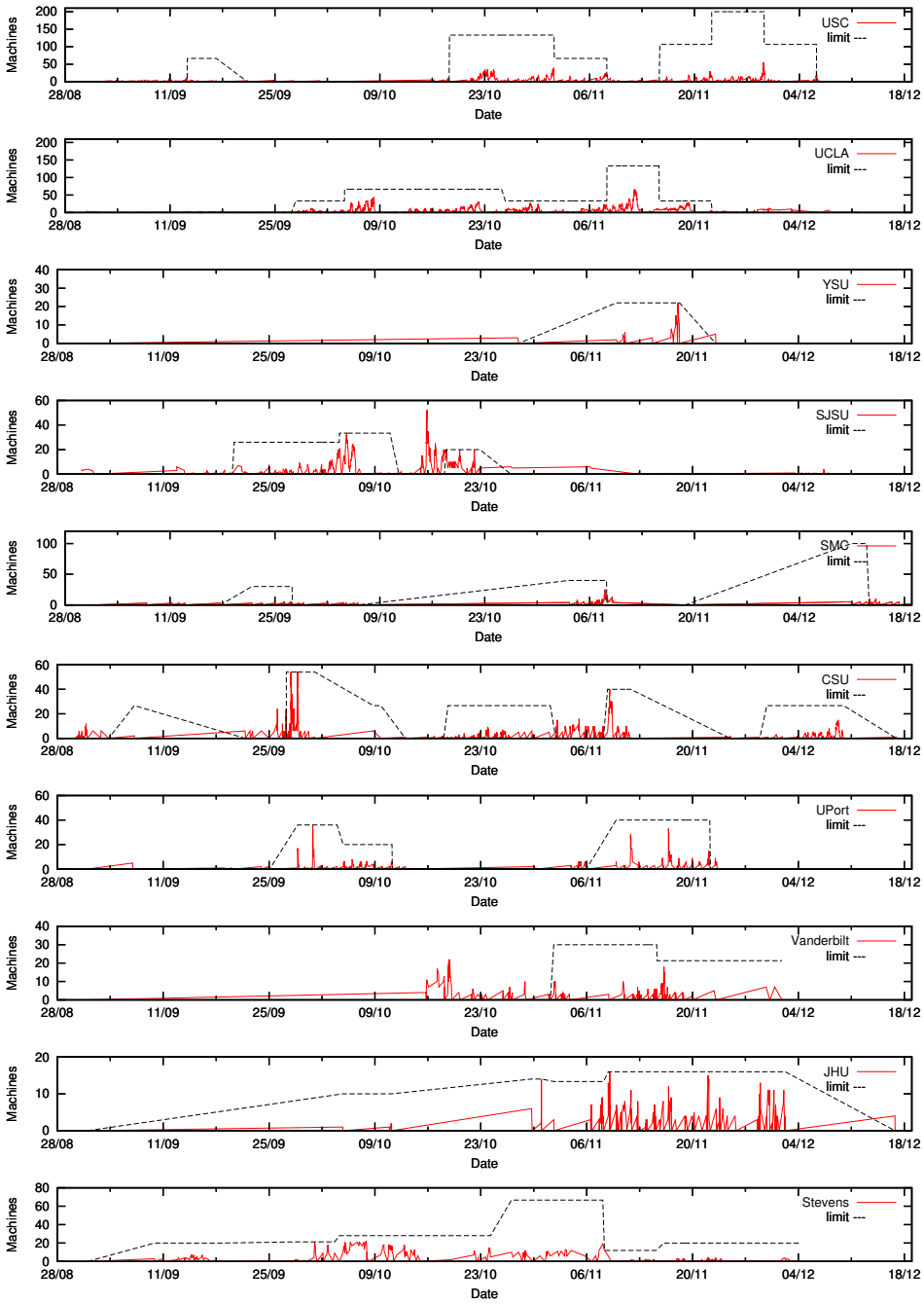

Figure 1: Resource usage per class

psychology. *D. Ravitch (Ed.) Brookings papers on education policy*, 1998.

[4] R. K. Atkinson, S. J. Derry, A. Renkl, and D. W. Wortham. Learning from examples: Instructional principles from the worked examples research. *Review of Educational Research*, 70:181–214, 2000.

[5] C. Bonwell and J. Eison. Active Learning: Creating Excitement in the Classroom . *AEHE-ERIC Higher Education Report No.1*, 1991.

[6] J. S. Bruner. The act of discovery. *Harvard Educational Review*, 31(1):21–32, 1961.

[7] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar. An integrated experimental environment for distributed systems and networks. In *Proc. of the OSDI*, pages 255–270, December 2002.