Editors: Cynthia Irvine, irvine@nps.edu | Alec Yasinsac, yasinsac@southalabama.edu

Teaching Cybersecurity with DeterLab

Jelena Mirkovic and Terry Benzel |
University of Southern California Information Sciences Institute

In 2004, the University of Southern California Information Sciences Institute (USC/ISI); University of California, Berkeley; and Sparta Inc. started the DETER project (http://deter-project.org) with the goal of advancing cybersecurity research and education. Over the past seven years, the project has focused on improving and redefining the methods, technology, and infrastructure for developing cyberdefense technology.[1] The project's research results are put into practice by DeterLab, a public, free-for-use experimental facility available to researchers and educators worldwide. Here we describe DeterLab's educational use, the support for that use, and the benefits that users experience.

What Is DeterLab?

DeterLab is an open exerimental facility funded by the US National Science Foundation and Department of Homeland Security, hosted by USC/ISI and UC Berkeley, and based on the Emulab technology.[2] It currently consists of more than 400 general-purpose computing nodes, some special hardware devices, and a set of tools for cybersecurity experimentation. DeterLab users can create and manipulate experiments using an intuitive, Web-based interface.

During each experiment, the user gains exclusive use of a set of physical machines for a limited time, which they can access via Secure Shell (SSH). The machines run the OS and applications of the user's choice and are organized into a user-specified topology. Users have privileged access to each machine allocated to their experiment and can modify its OS, install or modify applications, and modify system configurations.

DeterLab is a controlled environment in which users can safely test security threats and defenses. No traffic is allowed to leave DeterLab, and all experimentation occurs over the dedicated experimental network. DeterLab's machines can thus be safely overloaded, compromised, or crashed, or suffer any other consequence of a successful security attack. This poses no threat to other DeterLab users or the Internet at large.

DeterLab has more than 2,600 research and education users worldwide. Over 47 institutions in six countries have employed DeterLab for education, by either using it for a single assignment in a single course or using it repeatedly in multiple courses. In fall 2011, 15 courses involving approximately 400 students used DeterLab. The schools ranged from community colleges to large universities, including USC; the University of California, Los Angeles; Youngstown State University; Bowling Green State University; Santa Monica College; Colorado State University; Vanderbilt University; Johns Hopkins University; the Stevens Institute of Technology; Worcester Polytechnic Institute; George Mason University; and Lehigh University.

Using DeterLab in Education

Instructors who wish to use DeterLab apply for a DeterLab project using a short online form. Usually, instructors will create a project for each course they teach—for example, the undergraduate course CSCI 355 (Software Design for Engineers) and the graduate course CSCI 530 (Security Systems). An instructor would reuse a project for each offering of the same course; for example, he or she would use the same DeterLab project to teach CSCI 355 in fall

1540-7993/12/$31.00 © 2012 IEEE Copublished by the IEEE Computer and Reliability Societies

2011 and spring 2012. When multiple instructors rotate to teach the same course, DeterLab grants each instructor privileges to manage class accounts on DeterLab for the given school term.

Student accounts are created automatically for each class and recycled when the course ends. Instructors initiate this process by sending a list of student email addresses to DeterLab operations staff.

Usually, instructors assign simple, canned exercises to students as homework or project assignments. The DETER project team and collaborators have developed reusable, canned exercises that are hosted on DeterLab's education portal (http://education.deterlab.net). These exercises are developed specifically for easy adoption by instructors and provide sufficient background material for novice users, both instructors and students. Each exercise includes a publicly available student manual and a password-protected instructor manual. Instructors can hand the student manual to students as the assignment specification, by just changing its due date and submission instructions. Instructors can use the instructor manual to perform any necessary setup for the exercise, verify student answers against the answer sheet, and learn about common mistakes students make in the exercise. Most exercises require one to two weeks to complete.

DeterLab currently hosts exercises for the following topics:

- an introduction to Linux and DeterLab,
- buffer overflows,
- pathname attacks,
- SQL injections,
- OS hardening,
- permissions and firewalls,
- computer forensics,
- network intrusion detection,
- ARP (Address Resolution Protocol) spoofing,
- man-in-the-middle attacks,
- DNS (Domain Name System) man-in-the-middle attacks,
- TCP SYN flooding,
- worm modeling,
- worm detection, and
- peer-to-peer botnets.

For example, in the TCP SYN flooding exercise, students create a four-node star topology consisting of a client, a server, and an attacker machine, with a router in the middle. They then use a simple, Web-based tool to generate legitimate Web traffic between the client and server and generate attack traffic from the attacker machine to the server. They record the traffic trace, calculate and analyze legitimate connection durations, and explain the observed effects of the attack. They then repeat the experiment with the TCP SYN cookie defense turned on and observe how well the defense protects the server.

DeterLab exercises provide students with the ultimate active learning experience, enabling them to see and feel the phenomena taught in the classroom.

DeterLab's education portal also includes detailed guidelines for instructors about using DeterLab in class, managing their classes, adopting publicly shared education materials, and contributing to those materials. It also includes student guidelines that help them become familiar with DeterLab's experimentation model and teach them Linux and network-programming basics.

DeterLab has developed special technical and logistic support for class use. Flexible isolation protects student work from access by other students in individual exercises while supporting collaboration between students in group exercises. Instructors also have special privileges that enable them to manage their classes. They can

- access student experiments as privileged users;
- assume a student identity when accessing DeterLab or individual experimental machines to test student claims or help students with assignments;
- edit, add, or delete student accounts in their classes;
- retrieve student passwords; and
- see usage reports for their classes.

In cooperation with instructors, DeterLab limits access to its resources to achieve fair use between classes and to balance class versus research use of DeterLab.

DeterLab's Educational Benefits

In sharp contrast with the high employer demand for both foundational and practical knowledge, university courses often teach security using passive-learning methods, such as textbooks, blackboard diagrams, and PowerPoint presentations. Research has shown that active learning is more engaging and motivating for students and produces better absorption of material and better development of critical thinking.[3,4] DeterLab exercises provide students with the ultimate active learning experience, enabling them to see and feel the phenomena taught in the classroom.

Accessibility is one significant benefit of using DeterLab. University courses that focus on practical computer security (teaching mostly exploits and intrusion defenses) often work best for

students with extensive system design and system administration skills. Increasing numbers of computer science students don't have a high level of such skills. DeterLab exercises help such students learn the basic skills for a topic and then guide them gently into the topic's complexities. Furthermore, because the exercises were designed to be easy to adopt and reuse, educators can use them to expand on the topics of otherwise narrowly focused courses. This ability lets instructors better cover the rich fields of network and computer security.

Some security educators develop hands-on exercises in their own university's labs to improve learning. DeterLab has six main advantages over this approach:

- DeterLab has a large amount of hardware resources and has successfully hosted many simultaneous classes.
- It limits risk from experiments involving live malware.
- Using it is free.
- It provides automated support for topology setup, OS loading, and application installation, and experiment configurations can be archived and reused by others. Such packaging also helps instructors use DeterLab's exercises for repeat offerings of their courses.
- Students can do the lab work on their own schedule, via the Web from their dorms, labs, or homes.
- The exercises are reusable because they're all developed for the same experimental hardware and software. Instructors can use a set of shared exercises and actively contribute to them through the public portal.

Increasingly, cybersecurity professionals and students learn through games and simulations of attacks and defenses.[5,6] Such approaches complement DeterLab. They can simulate cybersecurity events on a larger scale, offering a higher-level situational awareness and highlighting the concepts the instructor wants students to learn—for example, that worm infection is preceded by scanning activity at the target. On the other hand, with DeterLab, students get practical experience with real hardware, real operating systems, and applications they can use in their future careers. For example, they can learn how to detect and filter out worm scans using the open-source Snort intrusion detection system (www.snort.org).

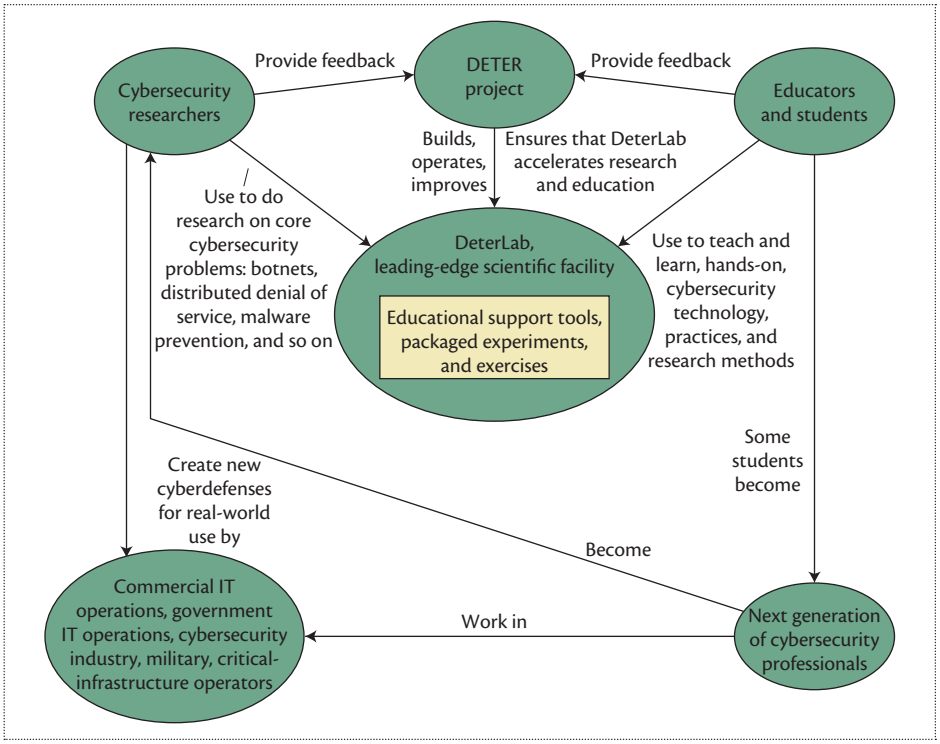

Figure 1. The synergy of research and educational use of DETER project outcomes. Educational use of DeterLab provides valuable feedback on DETER innovations and helps grow the pool of cybersecurity innovators and cyberdefenders.

The Synergy of Research and Education at DeterLab

DETER's security education mission complements its research mission to transform cybersecurity research into a rigorous experimental science.

Figure 1 shows the research and the educational uses of DETER project outcomes:

- Using the ongoing stream of DETER research results, the DETER team builds, operates, and improves DeterLab as a research and education facility, including packaged experiments that serve as exercises.
- Cybersecurity researchers use DeterLab to conduct research in core cybersecurity problems.
- Instructors use DeterLab to teach cybersecurity technology and practices. Students learn how to use DeterLab to operate experiments, thus also learning cybersecurity research practices.
- Both instructors and researchers provide direct feedback to DETER, which also independently observes their use of DeterLab.

- The DETER team uses the feedback and observation to improve DeterLab facilities and refine DETER research results. This ensures that DeterLab both meets its educational goal and accelerates cybersecurity research. This creates critical support for education by improving the infrastructure for experiment construction and reuse.

The bottom of Figure 1 shows this synergy's external benefits:

- Students gain both knowledge and practical skills in cybersecurity technology.
- Some students become cybersecurity professionals or other cyberdefenders.
- Others become cybersecurity researchers.

So, besides DeterLab's intrinsic worth, educational use of it provides valuable feedback on the DETER team's innovations and ultimately helps grow the pool of cybersecurity innovators and cyberdefenders.

In the next five years, the DETER project plans to work on the following directions for improving the science of cybersecurity experimentation:

- rigorous and modular experiment design,
- flexible experiment embedding,
- intelligent experiment interpretation and validation, and
- experiment repeatability and sharing.

We believe that advances in these directions will greatly improve not just cybersecurity research but also cybersecurity education. ■

Acknowledgments

For information on using DeterLab for teaching, visit http://deter-project.org and http://education.deterlab.net. The DeterLab exercises were developed by DETER project team members and collaborators, funded by a US National Science Foundation Course Curriculum and Laboratory Improvement grant, under award 0920719. The US Department of Homeland Security has supported recent DeterLab development under award N66001-07-C-2001.

References

1. T. Benzel et al., "The DETER Project—Advancing the Science of Cyber Security Experimentation and Test," *Proc. 2010 IEEE Int'l Conf. Technologies for Homeland Security* (HST 10), IEEE Press, 2010.
2. B. White et al., "An Integrated Experimental Environment for Distributed Systems and Networks," *ACM SIGOPS Operating Systems Rev.*, winter 2002, pp. 255–270.
3. R.K. Atkinson et al., "Learning from Examples: Instructional Principles from the Worked Examples Research," *Rev. of Educational Research*, vol. 70, no. 2, 2000, pp. 181–214.
4. C. Bonwell and J. Eison, *Active Learning: Creating Excitement in the Classroom*, Jossey-Bass, 1991.
5. V. Pastor, G. Díaz, and M. Castro, "State-of-the-Art Simulation Systems for Information Security Education, Training and Awareness," *Proc. 2010 IEEE Education Eng.* (EDUCON 10), IEEE Press, 2010, pp. 1907–1916.
6. M. Thompson and C. Irvine, "Active Learning with the CyberCiege Video Game," *Proc. 4th Conf. Cyber Security Experimentation and Test* (CSET 11), Usenix Assoc., 2011, p. 10.

Jelena Mirkovic is a computer scientist at the University of Southern California's Information Sciences Institute. Contact her at sunshine@isi.edu.

Terry Benzel is the deputy director of the Computer Networks Division at the University of Southern California's Information Sciences Institute. Contact her at tbenzel@isi.edu.