DeterLab Testbed for Cybersecurity Experimentation

Terry Benzel
tbenzel@isi.edu
USC Information Sciences Institute
Marina del Rey, California, USA

Jelena Mirkovic
mirkovic@isi.edu
USC Information Sciences Institute
Marina del Rey, California, USA

David Balenson
balenson@isi.edu
USC Information Sciences Institute
Marina del Rey, California, USA

Brian Kocoloski
bkocolos@isi.edu
USC Information Sciences Institute
Marina del Rey, California, USA

ABSTRACT

We nominate the DeterLab cybersecurity testbed for the ACSAC's 2023 Cybersecurity Artifacts Competition and Impact Award. DeterLab is an open and remotely-accessible testbed that has been continuously running since 2005, serving cybersecurity research and education community. Over the years, DeterLab has served more than 1,000 research users and more than 20,000 education users.

ACM Reference Format:
Terry Benzel, Jelena Mirkovic, David Balenson, and Brian Kocoloski. 2023. DeterLab Testbed for Cybersecurity Experimentation. In *Proceedings of Annual Computer Security Applications Conference (ACSAC'23).* ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

We nominate the DeterLab (cyber-DEfense Technology Experimental Research Laboratory, accessible at https://deterlab.net) for the ACSAC's 2023 Cybersecurity Artifacts Competition and Impact Award. DeterLab is an open testbed that can be used free of charge, and consists of an online service that is open to any cybersecurity researcher or educator. It has been running continuously for 19 years (funded by numerous NSF, DARPA and DHS grants), providing cybersecurity researchers, educators and students access to hundreds of computers and thousands of emulated networks to support their work.

DeterLab has served a broad research community, including 389 research projects, from 278 institutions, and involving 1,042 researchers, from 205 locations and 46 countries. Additionally, DeterLab has been used by teachers in cybersecurity classes to offer hands-on experiences to students. Over the years, DeterLab has been used in 237 classes, from 148 institutions, and it has helped educate 20,925 students.

In the next sections we detail what problem DeterLab solves, how to access it, how it works, and its tremendous research and educational impact.

ACSAC'23, Dec 04–08, 2023, Austin, TX

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

2 RESEARCH PROBLEM

Cybersecurity is a rich and multifaceted research field, with many complexities and interactions between applications, systems, protocols and Internet actors. Cybersecurity researchers need a safe, scalable and realistic environment to evaluate new solutions or study new threats. Students taking cybersecurity classes need experiential learning to better understand and retain complex cybersecurity concepts.

DeterLab meets these needs by offering a safe, efficient, large-scale, and versatile testbed environment that is free to all researchers, students, and educators and which is remotely accessible at https://deterlab.net. DeterLab can be used to replicate realistic cybersecurity scenarios at scale to study new threats or evaluate new solutions. DeterLab can also be used to support repeatable and reproducible experimentation – code and data shared via DeterLab can be readily reused by other DeterLab users. DeterLab can further be used to popularize cybersecurity (e.g., by demonstrations of attacks or defenses on the testbed), or to demonstrate an important concept in a cybersecurity class, to run an offense/defense exercise or as an environment where cybersecurity students can obtain practical cybersecurity skills.

3 HOW DETERLAB WORKS

DeterLab users open free accounts by visiting https://deterlab.net. A principal investigator (usually a faculty or research scientist) also creates a project on DeterLab. Graduate and undergraduate students join existing projects of their research mentors, if they are using DeterLab for research, or of their class instructors, if they are using DeterLab for a class. Within a project, a user can create one or more experiments, which exist as records in DeterLab's database. When the user is ready to interact with their experiment, they will "realize and materialize it", which leads to actual computer nodes and network links being allocated and initialized. When the user is done with the day's work, they can return the resources by "dematerializing" their experiment. Users obtain nodes on a first-come-first-served basis and can keep them as long as they are needed.

To define an experiment on DeterLab, a user specifies their desired topology using a special topology description language. The topology specification may include names of nodes, how nodes are connected together, bandwidth and delay of each link, and the operating system or hardware of each node. DeterLab has previously used Emulab technology [1] and it has recently started

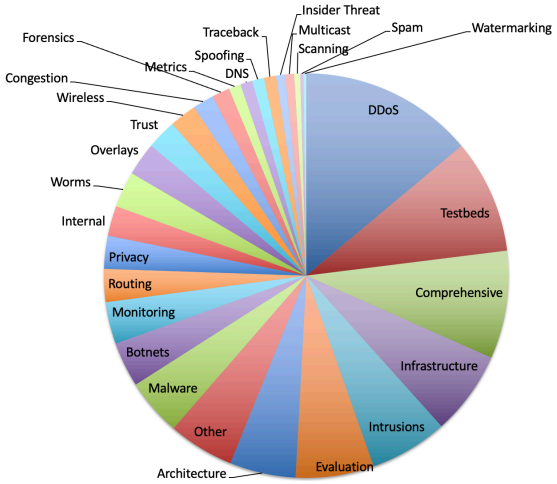

Figure 1: Projects on DeterLab, categorized per topic

using USC/ISI-developed Merge technology [2] to build the desired topology out of its compute nodes, network switches, and their connections.

When an experiment is materialized, DeterLab loads the desired operating system onto each node. The user gets superuser (root) access to all their nodes in the experiment, and can further install applications and build scripts to generate traffic, and system or network events needed for experimentation. Users can also remotely reboot their nodes.

Over the years, DeterLab has been used in numerous research projects in cybersecurity, which can be roughly categorized into 30 topics, shown in Figure 1. Around 65% of the projects were in distributed denial-of-service (DDoS), comprehensive, testbeds, evaluation, infrastructure, intrusions, and architecture had more than 20 projects each. Other research areas, such as malware, routing, botnets, worms, routing, etc., had fewer projects.

4 DETERLAB'S IMPACT

DeterLab has been continuously operated by USC/ISI (and in the past UC Berkeley), since 2005. It has played an essentia0 role in many research projects, contributing evaluation data to publications and Bachelors, Masters and PhD theses. DeterLab staff has also developed many tools that have been used for cybersecurity experimentation by DeterLab users. Finally, DeterLab has been used to provide an environment for experiential learning for cybersecurity students.

In the rest of this section we summarize DeterLab's research and educational impact.

4.1 Research Impact

DeterLab has been used by 1,042 researchers from 278 institutions, in 389 research projects. These researchers reside in 205 locations and 46 countries, on six continents (North and South America, Europe, Asia, Africa and Australia). Most of DeterLab's research users come from USA (around 800), India (34), Switzerland (32) and Germany (25).

DeterLab has also been essential in producing evaluation results for hundreds of publications and tens of bachelors, masters and PhD theses. Some of these are listed at Deter Project's Web site [3], while others can be found via Google Scholar.

In addition to hardware infrastructure, DeterLab's research and development team has produced many innovations on the testbed, to make the experimentation process more scientific, representative and reproducible. These include: realistic traffic generation tools [4–6], realistic network emulators [7], human user behavior models [8], benchmarks for DDoS defenses [9], experiment automation tools, such as MAGI [10] and DEW [11], experiment logging and monitoring tools [12, 13], flexible experiment traffic containment tools [14], etc.

USC/ISI researchers also developed and released as open source the Merge control software [2] for experimental environments, deploying it over the four years to successfully run three different research infrastructures – DCOMP, Lighthouse, and DeterLab. Merge makes running of testbeds smoother, more scalable and faster than the previously used Emulab software.

4.2 Educational Impact

DeterLab has been used extensively as a platform for experiential learning in cybersecurity and systems education. This use increased dramatically after 2010, when USC/ISI led a project funded by the NSF to produce public materials for learning cybersecurity with testbeds (award #8115780), which resulted in 25 homework assignments on various topics, such as man-in-the-middle attacks, DNS and BGP poisoning, denial-of-service attacks, intrusions, worm propagation, and password cracking. DeterLab has been used by 237 unique classes (some of them offered repeatedly), from 148 institutions. Majority of these institutions are from the US. DeterLab has helped educate over 20,000 students in the past 13 years.

In addition to homework exercises, DeterLab staff has also developed mechanisms that allow students to engage in offense/defense exercises [15], where one team protects certain resources (e.g., servers) from attack and the other team uses machines external to these resources to attack them. DeterLab team has further produced materials (setup scripts, scenarios) for four offense/defense exercises. These exercises can be used to teach students adversarial thinking and to further reinforce security concepts taught in a class.

5 CONCLUSIONS

DeterLab testbed has been instrumental in supporting cybersecurity research and education in the United States and all over the world since 2005. DeterLab continues to grow and incorporate new technologies, tools and datasets for cyberexperimentation. We nominate it for the ACSAC's 2023 Cybersecurity Artifacts Competition and Impact Award.

REFERENCES

[1] Hermenier, F. & Ricci, R. How to build a better testbed: Lessons from a decade of network experiments on emulab. In *Testbeds and Research Infrastructure. Development of Networks and Communities: 8th International ICST Conference, TridentCom 2012, Thessanoliki, Greece, June 11-13, 2012, Revised Selected Papers 8*, 287–304 (Springer, 2012).

[2] Goodfellow, R., Schwab, S., Kline, E., Thurlow, L. & Lawler, G. The DComp testbed. In *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19)* (USENIX Association, Santa Clara, CA, 2019). URL https://www.usenix.org/conference/cset19/presentation/goodfellow.

[3] project, D. DETER Publications. https://deter-project.org/deter_publications/ (2023).

[4] Genevieve Bartlett and Jelena Mirkovic. Expressing Different Traffic Models Using the LegoTG Framework. In *Workshop on Computer and Networking Experimental Research using Testbeds (CNERT)* (2015).

[5] DeAngelis, D., Hussain, A., Kocoloski, B., Ardi, C. & Schwab, S. Generating representative video teleconferencing traffic. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*, 100–104 (2022).

[6] DeterLab Team. Flooder Case Study. https://docs.deterlab.net/orchestrator/flooder/l.

[7] Kline, E., Bartlett, G., Lawler, G., Story, R. & Elkins, M. Capturing Domain Knowledge Through Extensible Components. In Gao, H., Yin, Y., Yang, X. & Miao, H. (eds.) *Testbeds and Research Infrastructures for the Development of Networks and Communities*, 141–156 (Springer International Publishing, Cham, 2019).

[8] Blythe, J. & Tregubov, A. Farm: Architecture for distributed agent-based social simulations. In *International Workshop on Massively Multiagent Systems*, 96–107 (Springer, 2018).

[9] Mirkovic, J. *et al.* DDoS benchmarks and experimenter's workbench for the DETER testbed. In *2007 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities*, 1–7 (IEEE, 2007).

[10] Hussain, A., Jaipuria, P., Lawler, G., Schwab, S. & Benzel, T. Toward orchestration of complex networking experiments. In *CSET@ USENIX Security Symposium* (2020).

[11] DeterLab Team. DEW Portal. https://dew.isi.edu (2021).

[12] Mirkovic, J. *et al.* Using terminal histories to monitor student progress on hands-on exercises. In *Proceedings of the 51st ACM technical symposium on Computer Science Education (SIGCSE)*, 866–872 (2020).

[13] Viswanathan, A., Hussain, A., Mirkovic, J., Schwab, S. & Wroclawski, J. A semantic framework for data analysis in networked systems. In *Proc. USENIX Symp. Netw. Syst. Des. Implement.(NSDI)*, 127–140 (2011).

[14] A. Alwabel and H. Shi and G. Bartlett and J. Mirkovic. Safe and Automated Live Malware Experimentation on Public Testbeds. In *Proceedings of CSET* (2014).

[15] J. Mirkovic and P. A. H. Peterson. Class Capture-the-Flag Exercises. In *USENIX Summit on Gaming, Games and Gamification in Security Education* (2014).