2024 Technology Fee Full Proposal

Title:

Enhancing Cloud and Information Security Education

Proposers:

Adam Hassan
Student, Teaching Assistant
CISE Department
E301 CSE Building,
P.O. Box 116120,
Gainesville, FL 32611
adamhassan@ufl.edu
954-696-0680

Joseph N. Wilson
Associate Professor and Graduate Program Director
CISE Department
Rm. 5400E Malachowsky
Gainesville, FL 32611
jnw@cise.ufl.edu
352-514-2191

Sponsoring Organization:

Information Security and/or Applications, Development and Integrations

Purpose and Specific Objectives:

We are requesting funding for AWS credit. These credits will be used to support the creation of modern and practical labs that will improve cybersecurity education.

The purpose of this effort is to 1) expand the CISE Department's existing capacity to build virtual networks for practical information security exercises and 2) provide the department the ability to teach students about cloud technologies and how to secure them. The proposed net funding required is $5,200 per year.

The importance of these technologies can be seen in the following two applications to curriculum.

1. Creation of practical cybersecurity labs

Using virtual machines in the cloud will let instructors quickly provision and customize lab environments for students. Crucially, current infrastructure in cybersecurity classes is supported by an NDG, VMware environment for the *Penetration Testing—Ethical Hacking* class and the remotely managed NICE (National Infrastructure for Cyber Education) environment in the *Enterprise Security* class. These lab environments are separate from each other and employ typical networks of workstations, not cloud-deployed resources. A new course to be offered in

fall 2024, *Adversarial Cyber Tradecraft*, which teaches students how to use an adversarial mindset to actively defend against modern attackers and cybercriminals will employ both these resources.

All these courses will benefit from access to cloud resources as a method of deploying new lab exercises. For one, there is a growing collection of open-source lab environments that employ cloud-deployed resources to assist in cybersecurity education (a curated list can be found at https://github.com/iknowjason/Awesome-CloudSec-Labs). In addition, technologies to develop and deploy cloud-based labs, such as Terraform, are becoming more popular and sophisticated and can support rapid development of computing infrastructure to support these courses.

Industry professionals often work as a "Blue Team" to practice defending against attackers using a "Red Team" that works to emulate potential attackers. To provide an experience like this in a safe environment because students must be able to work together against a single attacker, creating custom networks for every lab is crucial. This functionality is partly supported by NDG and NICE, but with some limitations and constraints that are not associated with cloud environments.

2. Creation of cloud environments

Despite being a critical part of industry, most CISE students are not currently exposed to cloud technologies until after graduating. Cloud environments can be much more complex than the environments a student will see with NDG or NICE. As in those environments, the cloud has concepts of machines, networks, subnets, and permissions - but also is heavily focused on access control and is significantly more complex and dynamic than traditional networks. This will play an especially important role in the *Penetration Testing—Ethical Hacking* class, providing the ability to deploy labs that cannot currently be created. This will allow students to explore cloud security and will ensure that they learn how to identify potential vulnerabilities in cloud environments and applications that they may build in the future.

Impact/Benefit:

The following use cases highlight the benefits this project will enable:

- The *Penetration Testing—Ethical Hacking* course has, in recent years, introduced a cloud security component covering the theory behind finding vulnerabilities in a cloud environment. This is one of the few topics in the class that does not have a practical lab component, as the current infrastructure does not support working in the cloud. Funding of this proposal will allow the development of labs to let students practice the theory they learn in class
  This course is offered every fall with an enrollment of about 120 students

- The UF Student Infosec Team, which has placed nationally several times in the past year in cybersecurity defense and offense competitions, has several weekly practices that involve building network infrastructure, identifying vulnerabilities on systems, actively defending against attackers, and identifying artifacts left behind by attacks. Currently, these environments are being provisioned on AWS and are supported by funding provided by students themselves. By providing funding for the construction of cloud environments, these practices can become more accessible and sustainable. In the past week, a completely custom lab environment was created on AWS for the use of the NCAE CyberGames competition[1], allowing students to practice defending against an attacker in real-time.

- The *Adversarial Cyber Tradecraft* course which will teach students how to defend against attackers will be able to present up-to-date tools and techniques. It is crucial for students to stay ahead of the curve by learning to think like an attacker and use modern tools. This course will employ group lab environments to be accessed by professors and teaching assistants to perform modern real-world attacks against

[1] NCAE CyberGames is a cyber defense competition in which students learn to set up networks and defend against professional attackers. https://www.ncaecybergames.org/

students defending computational resources. It is crucial that this be done in a virtual environment, as it will prevent malicious and/or suspicious traffic from happening on the UF wireless network. By deploying this on the cloud rather than more traditional infrastructure (eg. NDG), the professor and TAs can simulate attacks on networks that cannot be simulated in the current environment.

- While the scope of this proposal is currently only limited to cloud security education, we intend to pave the way for a higher presence of cloud technologies in the classroom. Courses like *Intro to Software Engineering* - mandatory for CISE students - can use this funding in the future to provide students with practical cloud experience before entering the workforce. Students, for example, can be assigned a project that must require serverless code and scaling using kubernetes. Indeed, many companies utilize cloud computing[2] - especially in the new age of AI. By giving students familiarity with cloud technologies early on, professors will be providing students at the University of Florida with a competitive edge when transitioning into the workforce.

- The UF Student Infosec Team, which in the last year has had meetings attended by 150+ students, will be able to give workshops on cloud security. These meetings are open to all UF students and will allow students to get informal education on important elements of cloud security. This will also promote the success of the UF SIT competitive team. Competitions like that of the Global Collegiate Penetration Testing Competition[3], the Department of Energy's CyberForce Competition[4], and the National Collegiate Cyber Defense Competition[5], all have introduced cloud security components in the past 2 years. Providing students with a way to practice cloud security will allow competitive teams to excel in a way that will bolster the University of Florida's prominence around the country.

Sustainability:

Continuing maintenance requires replenishment of funds on a recurring basis. Faculty and TAs teaching the specific courses will put in the effort necessary to configure and deploy lab environments (approximately 6 to 12 hours per environment).

Successful execution of the projects proposed herein will jump start increase in the demand for cloud resources to support both student- and faculty-driven initiatives. We expect that success of the proposal will lead cloud-based curriculum to be supported by departmental infrastructure funds and student-group based projects to be funded by recurring donations.

Timeline:

Implementation of the plan described above will take place as soon as funds are received. Cloud resources are available on-demand.

---

[2] About 69% of businesses have adopted cloud-computing technology (2023) https://visionpoint.systems/statistic/about-69-of-businesses-have-adopted-cloud-computing-technology/

[3] The Collegiate Penetration Testing Competition (CPTC) Is a competition that involves students performing a simulated penetration test on a network that prioritizes professionalism and effective documentation. https://cp.tc/

[4] The Department of Energy's CyberForce competition is a competition that involves students defending a network against attackers that also prioritizes communication and reporting skills. https://cyberforce.energy.gov/

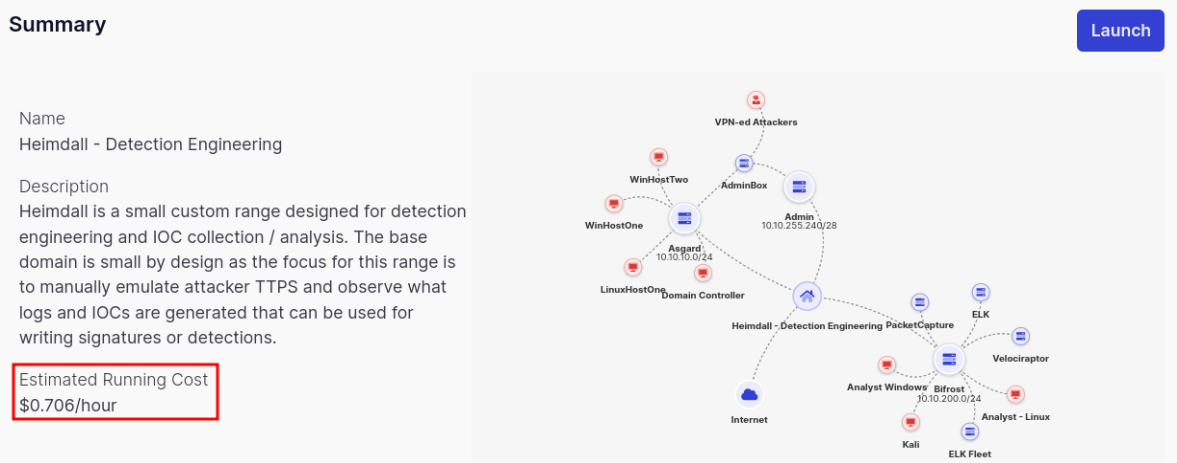
[5] The Collegiate Cyber Defense Competition (CCDC) is a competition that involves students maintaining network infrastructure by defending against professional attackers from the likes of the NSA and FBI https://www.nccdc.org/

During the months of June and July, Adam Hassan will study Terraform[6] documentation to learn how to effectively design and deploy environments that can be used by students. These networks will be used in the Fall for the *Adversarial Tradecraft* course and the *Penetration Testing: Ethical Hacking* course. Infrastructure may also be used for workshops and practices by the Student Infosec Team.

During the fall semester of 2024, lab environments will be designed for archival and reuse for ongoing and future semesters.

Budget:

Incurred costs are entirely based on labs built on AWS. Below is the hourly cost of one instance of an example lab that may be used in a classroom setting:



The calculation for the below estimate is as follows:

Active lab time in the classroom:
- $0.706/hour/environment
- 24 hour/environment
- 20 environment/lab
- 20 lab/semester
- ~= $5083.20

Lab time required for creation and testing of labs
- $0.706/hour/environment
- 8 hour/environment
- 1 environment/lab
- 20 lab/semester
- ~= $112.96

Thus, the total comes to about **$5,196 (recurring every year)**

The 2-year project budget is roughly **$10,400**

[6] Terraform is a tool that allows for the automatic creation of cloud networks based on a configuration.

Technology Fee Full Proposal Template Sponsor Signature Form

Title: Enhancing Cloud and Information Security Education
Proposer's Name: Adam Hassan

Note: By signing this form the sponsor is making a commitment to support the project. This may include providing startup, recurring or equipment replacement resources as presented in the attached budget.

Signature of sponsor: College Dean, or Unit Director, or VP for Student Affairs.

Pamela Dickrell _____ 03/18/2024

Dr. Pamela Dickrell
Associate Dean for Student Affairs
Herbert Wertheim College of Engineering **Date**

Note: By signing this form the UF IT unit is making a commitment to manage the project if selected for submission of a full proposal. This may include providing startup, recurring or equipment replacement resources as presented in the attached budget.

Signature of unit UFIT Director of a core unit:

_____ _____

Name and Title **Date**