

## A Introduction: Helping Faculty Teach Analysis Skills

According to published reports by the SANS Institute and other groups [?], the US faces a major shortage of security professionals to defend our information infrastructure from attack. In recognition of this need, security has been included as a core topic in the new IEEE/ACM CS2013 Curricula [?]. Cybersecurity is also mentioned in more than half of the other knowledge areas. At educational conferences such as SIGCSE and regional CCSC conferences, we are also seeing a growing interest in cybersecurity among faculty who do not have expertise in this area. Since it is still rare for schools to offer cybersecurity as an elective because of the tight constraints of the Computer Science curriculum, most schools do not have the luxury of offering a separate class in cybersecurity. Thus, the first step is to integrate it into other classes both at the upper and lower divisional levels. We are seeing a growing consensus articulated in the CS 2013 Curricula and in the ACM report “Toward Curricular Guidelines for Cybersecurity” [?] to fully integrate cybersecurity into the Computer Science curriculum at multiple levels in multiple courses. The ACM report also highlighted some of the the obstacles, which include the lack of: standard curricula, opportunities for faculty development, and shared faculty resources.

Professors and instructors face a significant number of obstacles to providing students with realistic enough environments where students can safely develop these skills and mindset. Although a variety of curricular resources exist, most of them focus on very specific toolsets or traditional, well-understood types of vulnerabilities and exploits. Among the few “interactive” scenarios that do exist, documentation often does not adequately explain the security implications of the scenarios that students participate in. Even faculty with some experience in systems administration would need to spend a significant amount of time configuring the exercise, and it is generally not flexible enough to be adapted to their needs or wishes. In addition, we plan to offer a webinar for faculty on teaching an introductory Computer Security class. While the webinar addresses faculty with little experience in cybersecurity the EDURange framework address the needs of faculty who have significant experience as well. It will save them time in creating new exercises updating them afterwards, and sharing them with colleagues. Potentially, they could be used to create competitions for intra- and intermural competitions. This would attract mroe students.

For students, the process of analyzing the security properties of computer systems presents a variety of difficulties. Acquiring the mindset necessary to analyze and debug systems – and thereby understand how they can’t be trusted, requires a level of engagement that most typical computer science (CS) undergraduate assignments lack and most typical information security courses do not have time for. Students are typically rewarded for following a formulaic trail: a sequence of commonly used tools. In addition, assessing students’ analysis skills is difficult problem.

The **EDURange framework** for cybersecurity exercises has been successfully demonstrated in several venues: security classes at two liberal arts colleges, a graduate-level security class, and two workshops for faculty at major conferences. There has been strong interest on the part of faculty participants in using this platform in their classes. The design goals are:

1. engaging for the students
2. easy to assess by faculty
3. easy to configure
4. exciting for the faculty, so that they will be engaged and will recommend them to colleagues

However, one of the potential barriers to distributing EDURange to them is getting faculty to use the hosting environment. EDURange is currently hosted on Amazon’s AWS/EC2 virtual cloud environment. This has made it very easy for the PIs to use it in workshops anywhere without having to worry about

installing special software. There are no plugins; the participants only need an ssh client, e.g. PuTTY on Windows. One method for distributing exercises to other faculty would require that they create an Amazon account with their credit card and potentially require their students to also sign up for accounts. We propose lowering the barrier for entry in three ways:

**First**, by creating an umbrella account in which we could enroll faculty and their classes. This facilitates distribution of EDURange and the ability to provide direct technical support. We have a verbal agreement with Amazon to do this. Currently, we are using an educational grant to provide free service to our alpha-testers.

**Second**, we propose to provide a “help desk” which could guide faculty through any difficulties in setting up exercises and using the AWS interface. From one of our recent workshops, we saw that some faculty felt that they needed more than a three-hour workshop to prepare them for using this environment in their class. We may need to help faculty who are not familiar with AWS or the EDURange framework to set up exercises. Our solution to this problem is to have a team of undergraduates who would staff an online help desk and answer questions ranging from how to set up key authentication, launch VM instances, run scripts to how to modify existing exercises or use them as templates for new exercises.

**Third**, we will run an online course/webinar for faculty on how to teach an introductory cybersecurity course using EDURange and other online resources. The ACM Cybersecurity Guidelines report [?] recommended three MOOCs, but there are reasons why a webinar would be more successful in this case. We have already talked with faculty from other schools who teach cybersecurity, and they are interested in working with us to use EDURange in at least one class, share their syllabuses and help deliver this online course. We have talked with Corrinne Sande, a PI for Cyber Watch West, and we would be able to offer this webinar through their agreement with Webex. Instructors who sign up for this course would learn to use EDURange to enhance their curriculum and create new curricula for their classes, which could range from a standard introductory security class to including some security in other classes, e.g. Networking, OS, Database systems, Computer Organization and Programming Languages. We will provide access to EDURange for free to the instructors and their students. It is an open-source project.

Our vision is that EDURange would provide a vehicle for all Computer Science faculty to *address the goals of the IEEE/ACM CS2013 Curricula* report by translating the Information Assurance and Security (IAS) core concepts and outcomes into concrete examples. There are three interconnected activities of this proposal: further developing the EDURange framework to enhance its capabilities for dissemination and assessment, providing support for faculty development through webinars and a rich collection of interactive exercises, and providing a research opportunity for students to work on developing EDURange and to work with faculty who are using it in their classrooms.

**Outcomes** If funded, the outcomes of this project will be:

1. EDURange will be used in over 80 classes at two- and four-year colleges and universities.
2. Faculty at these schools will be able to assess their students on topics in the CS2013 report using EDURange and associated materials.
3. EDURange and associated activities will enhance teaching capabilities and enhance faculty expertise.
4. EDURange will produce a concrete realization of several of the CS 2013 IAS-related Knowledge Units with respect to cybersecurity concepts, skills and learning outcomes.

## A.1 Analysis and the Security Mindset

As security educators, we are motivated by the desire to teach analysis skills and concepts to our students. Analysis skills are fundamental to the security mindset. The security mindset implies the ability to understand a system both from the standpoint of a builder and an attacker. Thus, the security mindset provides the conceptual underpinnings for a student to reason in both defensive and offensive situations. One aspect is failure modes, i.e. how can systems fail and be made to fail. These are things that a defender or attacker needs to keep in mind. Another aspect is questioning and verifying assumptions. This is particularly relevant for the defender.

We want to support courses such as the CS2013 exemplar: “The goal of this course is to introduce students to the challenges, approaches, and techniques for implementing, deploying, and maintaining secure computing systems and networks. The rationale behind this course is to meet the need for information assurance content within the CS curriculum at the same time as tailoring to the diversity of potential career paths in the program’s student population.” [?]

The panel presentation by the authors of the ACM report at SIGGCSE 2014 included the fact that out of 67 Ph.D. recipients in security in 2013, only one joined the ranks of faculty who teach. In addition to providing opportunities for faculty development, we want to interest our undergraduates in becoming cybersecurity educators at the undergraduate and graduate levels.

## Related Work

EDURange provides a unique infrastructure that enables faculty to develop exercises for students, in which they interactively develop their information security analysis skills. Information security education has been a popular, well-studied topic. Preparing a large cybersecurity workforce seems to be a national priority, but emerging viewpoints [?] seem to suggest that most efforts to date have not been as effective as government and industry seems to need [?]. \*\* is this still true? \*\* GovTech.com suggests that there is a “lack of faculty at the university level who can teach cyber-security beyond its “soft side” including policy and analysis.”<sup>1</sup>

We believe that we have identified an interesting and previously underexplored approach to enabling students to understand and apply principles and patterns (particularly dealing with the composition of trust). The challenge that we are facing is how to make it more broadly available to faculty and their students.

Judging from the Birds of a Feather sessions on Security at the last two years of SIGCSE, there has been a modest increase in the number of hands-on cybersecurity exercises, not all of which address the security mindset. It is also clear from the workshops we have attended that faculty want to use them but are frustrated because of the difficulty in disseminating and setting them up. The other frameworks that we have tried have some good features that we can emulate and some limitations that we try to avoid

### 2. Frameworks for Security Labs

DETER, werewolves, RAVE These environments are fine, except that with RAVE, new scenarios and VMs need to be installed by the developers. A faculty member can work with the developers to create new configurations an exercises, they can’t just upload some VMs and try them out.

Currently there are a few frameworks for

## A.2 Comparison of EDURange with Existing Projects

As we detail in Table 1, EDURange provides several unique and distinct experiences from existing cybersecurity labs, exercises, and curricula. The PacketWars project is probably the closest existing piece of work

---

<sup>1</sup><http://www.govtech.com/security/Cyber-Challenge-Work-Force-041811.html>

to what EDURange proposes, and there has been some work on providing students with access to “live” exercises on a small scale [?].

Table 1: *A Summary Comparison of EDURange and Existing Projects.* EDURange focuses on developing analytical skills and understanding system and network failure modes. The table below is not a criticism of existing efforts, but meant to highlight the ways in which our plans for EDURange differ from the characteristics of existing projects – these projects may have been built with different criteria in mind.

Project	Primary Disadvantage	Best Feature
Cybersiege	shallow analysis	interactive training scenarios
SEED	lacks competitive interaction	comprehensive documentation
Security Injections	focus on defensive coding patterns	introduction to basic security
CCDC	requires travel; limited remote access	interactive and competitive
PacketWars	requires travel; limited availability	contains well-structured scenarios
ITSEED	minimal instructor support, distrib by flash drive	good documentation for students
Google Gruyere	narrow focus (web apps)	cloud-based; well-documented
Security Knitting Kit	not distributed	??
The RAVE	not very flexible	cloud-based; existing lab manual
Seattle Testbed	limited in scope	easy-to-use; well-documented; P2P

Some of the projects listed in Table 1 seem to have different educational goals in mind. For example, while Cybersiege from Naval Postgraduate School provides a video-game-like, interactive environment, the decisions asked of a participant are mainly requisition and provisioning decisions rather than problems requiring technical analysis skills; this difference speaks to a different training goal. Google’s Gruyere is a great example of an interactive, well-documented, scalable cybersecurity exercise, but it only covers the space of web application vulnerabilities. Towson’s “Security Injections” mainly focus on several important security programming patterns. While the SEED material from Syracuse presents a mature, well-documented set of exercises, they are not typically interactive or dynamic. Competitions like CCDC seem to be structured in such a way as to require travel to the competition; EDURange envisions a publicly-accessible platform where even remote parties can interact. The RAVE is set up for a specific set of exercises, which are not interactive according to our definition. It provides good isolation, so that it would be very difficult for a student to gain access to the Internet from the RAVE environment. On the other hand, it limits the instructors in the same way, making it impossible to modify the configuration except through a request to the RAVE developers.

### A.3 Information Security Education

Our philosophy on information security education is based on our work on understanding and teaching the hacker curriculum [?] to students. This approach is predicated on the utility of failure modes — rather than teaching students the “success” cases, we attempt to deliver a culture shock that makes them disrespect API boundaries and adopt a cross-layer view of the CS discipline [?]. We routinely encourage our students to adopt a dual frame of mind when solving problems [?] to prevent artificial abstraction layers from becoming boundaries of competence [?].

## B Qualifications and Results from Prior NSF Support

### B.1 Richard Weiss

**Intellectual Merit:** Prof Weiss had one prior NSF grant “Collaborative Research: A Five-College Partnership for Information Assurance Education.” He worked with Mark Corner and Brian Levine (University of Massachusetts, Amherst), Sami Rollins (Mount Holyoke), Scott Kaplan (Amherst College), and Nick Howe (Smith College), to develop an interdisciplinary undergraduate course at Hampshire College. He worked on integrating security and computer architecture to exploit parallelism in cryptographic algorithms on superscalar hardware such as the DEC Alpha [?].

**Broader Impact:** Prof. Weiss has contributed to computer security education as an active participant in the SISMAT program (DUE CCLI: 0941836). This program trains undergraduates from liberal arts colleges in security. He was one of the core contributors to the CPATH project NWDCSD [?].

**Ongoing Grants:** Prof. Weiss is currently funded to work on TUES type 1: EDURange: A Cybersecurity Competition Platform to Enhance Undergraduate Security Analysis Skills (Aug 15, 2012 - July 31, 2015). The goal of that project is to create cybersecurity games that could be used for learning and assessment of security skills for students and today’s security workforce. This project is in the middle of development, and our first multi-level game assesses penetration testing skills. As part of this work, Profs Weiss and Jens Mache have led tutorials in the last two years at CCSC-NW (once with Prof Vincent Nestler) in October [?, ?]. They also gave a workshop at SIGCSE 2013 “Hands-on Cybersecurity Exercises and the RAVE Virtual Environment” with Profs. Michael Locasto, Brian Hay and Vincent Nestler. Weiss, Mache, and Locasto gave another workshop at SIGCSE 2014 “Hands-on Cybersecurity Exercises in the EDURange Framework.” Weiss and Mache also presented a poster “Teaching Security with Interactive Exercises” at ACSAC[?], a paper at InfosecCD [?], and will lead a BOF “Teaching Security Using Hands-on Exercises” again at SIGCSE 2014.

### B.2 Jens Mache

**Intellectual Merit:**

#### EDURange in the Cloud

One of the ways in which EDURange is unique is that it applies Cloud technology to addressing the unmet need of supplying faculty with interactive cybersecurity exercises in a way that is both easy-to-use and flexible. EDURange allows instructors and designers to specify exercises at multiple levels of detail. Using *yaml* as an intermediate representation, one can specify the structure of an exercise. This intermediate representation is compiled into API calls to AWS to create virtual machines and Chef scripts to install software. The portability of Chef should make it possible to port EDURange to other VMMs such as OpenStack, VSphere, etc. Since *yaml* is a declarative representation, we need something procedural or object-oriented at a higher level. Bryan Fite [?] has identified six types of entities that appear in cybersecurity exercises and competitions:

1. Node, e.g. a VM with attributes which could include players with accounts on that node
2. Network, collections of nodes and the connections among them
3. Software, which is necessary for the correct functioning of the exercise with attributes including version numbers.

4. Constraint, e.g. time limit, bandwidth limit
5. Goal, i.e. learning objective. These can be specified at a low level, such as reading or creating an artifact, reporting an IP address or password.
6. Artifact, e.g. a file that is placed on a target and could be used as evidence of achieving a goal

The next lower level of description is in terms of a *yaml* file which contains: groups, users, roles (which are also attributes), and packages, which refer to Chef scripts.

With the publication of the IEEE/ACM CS 2013 Curricula and its inclusion of computer security and information assurance, we are redirecting the exercises in EDURange to address the concepts and learning outcomes described in the IAS Knowledge Area. Since those are still at a high level, we hope to contribute to the implementation of the standards by providing concrete examples of exercises and a webinar on how to use them. We recognize that there are two groups of faculty who are our targeted audience: (1) Those who “just want an exercise”/inexperienced, and (2) those who are experienced and want to create a new variation of an exercise for their classes, a competition. or training for a competition. They want access to the configuration.

One of the issues that we have dealt with is the safety of EDURange on AWS. We want to have confidence that a student would not be able to connect to the Internet either accidentally or intentionally through one of the player Nodes. We were able to find a solution to this problem, which we confirmed with Amazon’s Web security team.

## **EDURange Exercises**

There are several examples of exercises that could be implemented in EDURange, and a few of the following have been. Two methodologies have been tested: (1) Create a VM manually, and then script it in Chef, and (2) start with a Chef script that was approximately what was needed and iteratively modify it.

### **Recon I**

Recon I is a reconnaissance exercise, where students learn how to explore a network. The learning goals for this exercise are:

1. understand networking protocols (TCP, UDP, ICMP) and how they can be exploited for recon.
2. develop the security mindset
3. understand CIDR network configuration and how subdivide a network IP range.
4. use nmap to find hosts and open ports on a network.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. network security

This exercise is relevant for both defensive and offensive roles. It currently has one level of difficulty, and we have used it in several workshops.

There are a dozen hosts on a remote network, and the student tries to find all of them as quickly as possible, and discover what ports are open and what services are running. At the knowledge level, the student is learning to use nmap and what options it uses. At a higher level, the student is learning about the TCP, UDP and ICMP protocols and how they can be used in ways that may have not been intended. In more advanced versions, students look for hosts and services that should not be on the network.

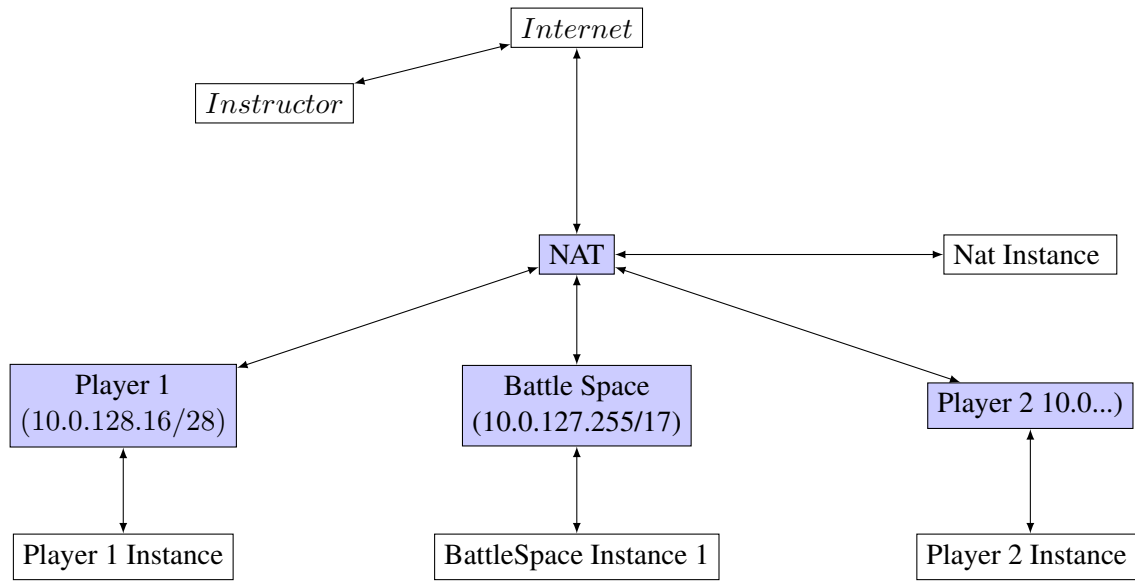


Figure 1: Conceptual diagram of the Recon I game. Note subnets are shaded (blue)

EDURange provides the capability to run the same basic scenario, changing the IP addresses and open ports of the target hosts. This allows students to repeat the exercise while trying different options of nmap to find those that meet the goals of a particular variation of the exercise. For example, the instructor might ask students to focus on speed or stealth.

### Elf Infection

Students are given a VM where one of the utilities is infected and listens on a port to open a reverse shell. They must figure out which program is infected and what it is doing. The learning goals are:

1. understand elf format
2. develop the security mindset
3. distinguish between normal and suspicious behavior of programs.
4. use nmap to find hosts and open ports on a network.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors. It shows how an attacker could maintain control of a system or exfiltrate data through infected binary files.
2. network security. The infected software will open a port and send packets to a remote server.
3. trust and trustworthiness.
4. machine-level representation of data

### strace

Students are given a trace of system calls made while a few programs are running simultaneously. The trace is cleaned up to remove the names of the executable files. Advanced versions can include malware.

The learning goals are:

1. understand how to sort through complex data
2. develop the security mindset
3. distinguish between normal and suspicious behavior.
4. use strace to characterize aspects of program behavior.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. trust and trustworthiness.
3. digital forensics

### **scapy hunt**

Students craft network packets to detect hosts that are not visible directly on the local network. They observe packets and replaying them with modifications. They gather more information by overflows the forwarding table and port knocking.

The learning goals are:

1. understand firewall rules
2. develop the security mindset
3. understand routing tables
4. understand how IP works

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. network security
3. Access control

### **Grammar Fuzzing**

This is an attack/defend exercise, where the defender implements a recognizer for a grammar, e.g. a grammar describing the input to a calculator. The attacker can look at the code and designs input that either creates false positives or false negatives.

The learning goals are:

1. perform input sanitization
2. develop the security mindset
3. understand language security (langsec) [?]

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. language translation



### B.3 Addressing CS2013

Here are the concepts and learning outcomes from CS2013 that we will address:

We will produce additional exercises that will address these goals.

Producing new knowledge about what works effectively. In addition to providing a framework for developing exercises at a high level, but we can also import VMs that collaborators produce. We are putting together this service in AWS which we make available to instructors. This doesn't use the full power of EDURange, but rather is based on the fact that we are providing a service through an AWS account where we can make The EDURange framework provides an easy way to share exercises. Every time we have run a workshop, we have given surveys and received good suggestions on ways to improve the exercises.

### Activities

The work contemplated in this proposal includes three major activities: (1) extending and enhancing the set of EDURange scenarios (e.g., with appropriate documentation and pedagogical advice), (2) supporting faculty in their transition to using the EDURange framework, and (3) designing and running an open webinar to disseminate a template outline for an introductory security course (this template also serves as a default setting for applying EDURange-based exercises).

Each activity and its supporting tasks are organized around the efforts of a specific group of personnel (students, instructors, PIs/researchers). This section of the proposal describes the primary research and training events. Activities related to assessment are described in Section ??.

### B.4 Main Goal

We stress that the main purpose of these activities is to support instructor development; many faculty are in a position of needing to develop and incorporate cybersecurity curriculum and exercises into a wide range of courses – often on relatively short notice. The audience for EDURange includes a wide variety of faculty members and instructors with varying experience and opportunities for training themselves in cybersecurity. We have actively engaged with this audience in a variety of workshops and meetings over the past five years, and despite the variety in their backgrounds, they have expressed a common need: the need for more context and expert support in bringing cybersecurity material to their classrooms, tutorials, and lab exercises. In short, they express a need for help in transitioning the wealth of available material to their specific environment and translating this material into a suitable experience for their students.

This need is difficult to address during face-to-face workshops and Birds-of-a-Feather sessions, and it is even harder to address when faculty are faced with assimilating a large amount of available cybersecurity training material unaided and unguided. Faculty are creative and talented, but they are in need of more context, timely information, and relevant advice. The activities in this proposal are focused precisely on helping faculty achieve this goal and take the final few but daunting steps between *knowing about* cybersecurity exercises and *actually using* such exercises in their classrooms.

There is a gap between the potential value of cybersecurity exercises and the actual benefit to students in practice. Closing this gap and achieving our goal through the activities outlined below can have a direct impact on the quality of student learning, but our main focus is on supporting and preparing faculty to design and deliver their own student assessment activities (primarily via EDURange), not in directly measuring student improvement.

## B.5 Activity I: Enhancing EDURange

Our first major activity seeks to enhance the capabilities of EDURange and sustain access to the infrastructure by removing barriers to adoption, including the barrier of initial cost to faculty as they first adopt it in their courses. These efforts entail monitoring and maintenance of the EDURange cloud infrastructure and various community support mechanisms (mailing lists, help resources, etc.). This activity includes two significant sub-tasks.

### Sustainable Access to EDURange Cloud Infrastructure

One major barrier to access that confronts faculty members is one of limited resources. EDURange is designed to eliminate as much of that barrier as is practical, but running in the cloud still requires some forms of delegation and management, particularly in accounting for time and elastic resources allocated to each exercise scenario. Part of this proposal seeks support to sustain EDURange as a resource *while instructors become acquainted with EDURange and transition to their own educational Amazon grants*. We have deliberately defined an “exit protocol” to bolster a realistic sustainability plan. EDURange is not meant to bear all the associated costs of a cloud platform for all users in perpetuity.

**Exit Protocol** We seek to support instructors in a way that eventually makes them independent, including the ability to run EDURange scenarios from within their own Amazon account or as funded by their own departments or institutions. Our plan stresses a significant amount of support early on and allows instructors to become comfortable with using our EDURange scenarios as delegated users within our Amazon account. As instructors gain comfort and familiarity with the technical details of the scenarios, we will work with the instructor to transition them to an independent Amazon account.

The driving factor behind this plan is a consideration of sustainability: there is an obvious need to enable faculty and instructors to operate scenarios on their own because no “free” service can support all users for an indefinite period of time. Our intent is that by the end of the period of the grant, we will have created a community of independent EDURange users with a shared experience and resources (our website, documentation, scenarios, etc.) to help train others in the larger CS education community and new faculty at their own institutions. We see this as a great example of sustainable capacity building because it is based primarily on enabling instructors to look after themselves rather than creating a perpetual dependency on the EDURange personnel.

### Module Development

The second significant enhancement to EDURange concentrates on the development and porting of cybersecurity scenarios to EDURange. This is primarily a student-driven activity.

This activity accrues two benefits. First, it augments the set of scenarios available to users of EDURange. Specifically, we will look to port some existing cybersecurity exercises to EDURange. The second benefit is in providing our students not only the opportunity to get practical hands-on experience in Computer Science topics like systems, networking, cloud, and security, but also the opportunity to develop an appreciation for cybersecurity curriculum development. This theme of benefit accruing to our students is a central consideration in the activities described in this section. We seek ways to enhance their educational experience that are not solely limited to software development or programming.

## B.6 Activity II: Direct Faculty Support

Our second major activity seeks to build our own capacity to offer faculty significant and meaningful support, advice, and documentation through mechanisms like peer instruction, debriefings, and guided setup and semi-supervised delivery of EDURange scenarios. This activity includes two significant sub-tasks. The first is a student-centric activity, and the second is a PI-centric activity.

### Semi-supervised Delivery (an EDURange “Help Desk”)

As mentioned above, faculty can be talented and motivated to learn about cybersecurity and design courses and curriculum, but even those with significant amounts of enthusiasm and awareness of cybersecurity training resources prefer to have access to an informed “second opinion”, *especially* when seeking to incorporate live exercises or demos from external organizations or other instructors. To help close that last small gap in access and give faculty members comfort and confidence in deploying and using EDURange as an instructional tool, we plan to develop a student-led “help desk” for EDURange.

This group of students, advised and supervised by the PIs, will be available to provide live support to faculty who are using EDURange scenarios for the first few times. In essence, they will provide instructors with semi-supervised delivery of lessons, tutorials, or labs based on EDURange. We know both that this model is possible and practical because we have done it ourselves several times over the past two years. We have prototyped this sort of interaction and are ready to expand it.

**Benefit to our students:** This direct support of our faculty audience has several benefits, including the ability to more closely and realistically assess how faculty are using EDURange and any difficulties or benefits they perceive. This kind of close coordination thus has benefits to the project in terms of assessment quality. However, this kind of activity tremendously benefits our students because it gives them the opportunity to practice and develop their own teaching techniques. It gives them an exposure to a variety of professors and classroom environments. They act as a valuable external resource and an expert peer to an instructor – an experience few undergraduate students ever have. This form of experiential learning should boost their own skill and confidence.

### Documentation

The second significant task under Activity II is the development of specialized documentation for each EDURange scenario. Writing this documentation is a PI-centric task because we are instructors *writing for other instructors* about our experience and expectations related to curriculum material. We can share how well each scenario worked in the classroom environment and what topics it was useful for introducing or assessing. We can point out the pitfalls inherent in some of the topics or technical details of each exercise.

In writing this documentation, we are not proposing to merely write simple step-by-step instructions for running each scenario, but also address very clearly and concisely a set of other important questions, such as: what does scoring mean? What is the best way to use this exercise in a particular class? What cybersecurity analysis skills are being taught? What are the knowledge and skill areas that can be discussed before or after the scenario? How does this map to the CS 2013 curriculum?

Furthermore, we will include in each EDURange scenario description information about what and how EDURange scores particular goals and events within the exercise. We will provide enough background information and description to calculate a basic performance score, and leave the weighting of each component to the particular instructor using it.

We will provide notes and documentation for faculty on the scenario motivation, learning objectives, keywords and topics, formative and summative assessment suggestions, descriptions of how the exercise maps to knowledge areas listed in CS2013, and suggestions for integration into non-security courses.

Faculty are likely interested in the answers to these questions because EDURange scenarios involve not only the technical details and mechanics of using the AWS infrastructure, but also the security and Computer Science curriculum issues that each scenario provokes. We plan to spend a significant amount of time documenting these relationships. An initial taste of this kind of information (necessarily brief, and far from complete) is given in Section ?? for each EDURange exercise description.

## **B.7 Activity III: Webinar and Workshops**

Our third major activity focuses on a specific set of community-building exercises that are directly linked to two components of this proposal: (1) providing an example course outline to act as a default “setting” for all the EDURange scenarios, and (2) acquiring assessment of and feedback on EDURange itself. This is a faculty-centric activity and involves the organization of both virtual meetings and face-to-face workshops. Our plans for these events are opportunistic in reducing costs in that they take advantage of our existing connections with our community and co-location at independent events.

### **A Short Course “Webinar”**

Many faculty face the challenge of formulating a course design and syllabus; it is a central part of our job. When faced with the task of creating a security course, or even of finding a set of security course modules to incorporate into a non-security course, some guidance is valuable, even if it is a rough course outline or template or categorized list of readings. Such artifacts, simple as they are, can be quite valuable because they impose a basic intellectual structure on an expansive and intricate topic. We plan to present the outline for an introductory security course to an audience of instructors. The audience can then use this outline to jumpstart their own course planning.

Many proposals for building cybersecurity capacity via the training or professional development of faculty can suffer from the practical costs and difficulties of arranging continued and costly face-to-face meetings. We recognize these challenges, and in response to the CS2013 panel findings on cybersecurity suggesting the design of a few MOOC-style courses, we have designed an online webinar, the purpose of which is to present the outline of a “typical” introductory information security course outline in a short course style.

Our intent is to conduct hour-long online video chats with the EDURange community we have identified over the past few years (attendees at our workshops and BoFs, other colleagues from cybersecurity venues and groups). We plan a total of 12..15 of these sessions, which will take place via Google Plus video Hangouts (or other suitable mechanism) and be streamed and saved to YouTube, and linked from our website [www.edurange.org](http://www.edurange.org). We plan to use the Piazza platform to continue and facilitate the discussions arising from the video chats or clarify issues raised by our presentation. The course outline itself will be available via our EDURange github account. The bulk of the effort will be concentrated in preparatory work of the design and scripting of these sessions.

Each session will present a component (i.e., topic) of a 10 week course and split time between the presentation by the lead facilitators and discussion among the attendees. We assume that each component or course topic would be addressed by two to three classroom lectures per week.

The course itself is based on a fusion of our own introductory security courses. Although we are proud of our work, we do not claim to have a monopoly on the “best” cybersecurity course. We have invited

several other facilitators to join us in designing the course outline and helping guide the discussion during the video chat sessions.

**Benefit to the community** We point out that our purpose is simply to provide a context in which EDURange exercises can be logically demonstrated; hopefully some of our audience of instructors finds the course syllabus to be useful as well, even as a place for them to start their own planning or course development. With this webinar component of the proposal, we are essentially offering an expert panel as a resource to instructors seeking to (re)develop cybersecurity topics or courses.

## **Workshops**

A vital part of this proposal is the assessment of how well these activities are supporting faculty in their vocation of delivering cybersecurity education. Our specific assessment plans are discussed in Section ??, but a critical precondition of the assessment is obtaining feedback from instructors that use EDURange. For the past several years, we have held workshops at Computer Science educational conferences where faculty can experience an EDURange scenario. We plan to continue holding such workshops.

This activity is of tremendous value because it feeds into both our assessment mechanisms and our development priorities for EDURange (both the infrastructure and the scenarios). We have found that workshop participants are a wonderful font of ideas for exercises, scoring strategies, and other improvements. Workshops serve as valuable face-to-face time with our target audience and allow us to recruit further audience members by giving them firsthand experience with us and the infrastructure.

## **B.8 Additional Value of These Activities**

The EDURange environment is meant to provide an efficient mechanism for students to immediately engage with a live exercise. EDURange minimizes and eliminates the need for both faculty and students to deal with logistics and administrative setup work for labs, tutorials, or other “hands-on” cybersecurity experiences.

This proposal brings together a wide range of experts who teach cybersecurity on a regular basis in a variety of settings. Their students are active participants in all facets of the project. One important potential contribution of EDURange is that it can offer one model of how the CS2013 principles, knowledge, and skills related to cybersecurity can be implemented in actual exercises and lessons. We plan to actively map these relationships.

## **Assessment Plan**

Answer the question: how will we demonstrate this enhanced value? Raw numbers, plus qualitative application of CS 2013. Demonstrate how much people use EDURange now that they have open access to it.

Assessment Plan – this section will have 2 sub-parts. One on raw metrics of number of users, students, profs, classes, etc. etc.

NB: any discussion of the scoring engine in EDURange probably does not belong here; that is an EDURange I concern, not for this proposal.

The second is on how well the EDURange infrastructure and scenarios map to the skills and knowledge of security throughout the CS 2013 undergrad curriculum. Assessment plan describes the assessment mechanisms, procedures, and practices

First pillar: usage stats, drawn from EDURange and Amazon infrastructure. catalogue frequency and amount of usage per prof or class. How much was EDURange used in particular kinds of classes? Is there a

difference in usage given the type of course (e.g., intro security vs. some other course vs. upper-level undergrad vs. lower-level course). For example, we can say we are all things to all audiences, SecurityInjections may be more appropriate or used more heavily

Report attendance at webinars, downloads of YouTube videos, piazza conversations, etc.

Second Pillar: (a) faculty survey (same instrument as SIGCSE...) - \* use this to drive improvement of EDURange: find dissatisfied participants in early years, revise exercises and infrastructure along the way

(b) pre/post test on a per scenario basis. Need to have identified knowledge and skills on a per-scenario basis in modules.tex

Main focus is on how well this supports faculty in their job, not necessarily a measurement (assume, that faculty, if well-supported, will do appropriate assessment of \*their\* students given educational background and institutional standards, etc.), so we will try to do pre/post test and make available, but not main focus of our internal assessment.

Third Pillar: How well/completely EDURange maps to CS 2013 infosec topics.

Timely and informed by central and guiding document of CS Ed, particularly since this document goes through great lengths to identify infosec topics throughout the curriculum.

How well does EDURange support / address the need of CS 2013 to weave CS infosec throughout the curriculum. And the faculty are best positioned to tell us this.

modules.tex is an assertion of the relationship between particular modules and particular parts of CS2013. The assessment plan here is based on how well that mapping succeeds in practice. This can be based on questions we ask in the faculty survey, but the \*analysis\* is broken out under this third pillar.

\* how often were you able to use an EDURange scenario as a launch pad to discuss curriculum topic X, Y, Z?

\* were there other curriculum topics, skills, or knowledge that it mapped to?

## Management Plan

Timeline of activities, milestones  
recruiting students

### List of Milestones

1. organize first webinar
2. run first webinar
3. followup
4. Workshops (ongoing at SIGCSE)
5. SIGCSE, CSAW (highlight cooperation with others)
6. recruit students for helpdesk
7. training first batch of students
8. Deployment of EDURange at first three..five beta users (at end of year 1, in 5 classrooms, not including our institutions)

9. Midterm Assessment report (can comment on internal assessment as well as CS 2013 “reality” in our deployed classrooms) (state of cybersecurity)...beginning of year 4
10. ??? Coordinate with Bryan Fite’s Scenario Description Language: by the end of year 3, we will due diligence on identifying other cyberscenario description languages / standards
11. end of year of year 3, we will have distributed our 6 scenarios to ENSEMBLE; the rest in year 5
12. by the end of year 2, we will have incorporated one IT-SEED external scenario into EDURange

Also include “outcomes” into this list?

## **Timeline**

## **Team Meetings, Coordination, Hackathons**

## **Dissemination**

Audiences EDURange can be useful for novice and experienced instructors in cybersecurity.

CyberwatchWest

ENSEMBLE

workshops at CCSC, SIGCSE, SISMAT, courses, CSAW

also list previous dissemination efforts to demonstrate we’ve been effective at this

## C Data Management Plan

**Data Type:** We will capture survey information using Qualtrics (which our evaluation consultant has prior experience with).

The educational modules that are created as part of this work will be disseminated through Ensemble. This resource is funded by NSF and used by instructors to find educational modules. We will also cross-post and link these modules on [www.edurange.org](http://www.edurange.org). We will publicly post all code on [github.com](https://github.com).

**Evaluator Data Access** We will share in a timely manner, all the experimental data and measures we collect with Dr. Nilsen so that he can provide help and oversight to synthesize our results into an ongoing report. Such access serves the critical purpose of keeping him current with the PI's data gathering and analysis activities so that they can continually update and improve educational modules and supporting materials. Personally identifiable information will be removed from survey data before it is stored.

**Legal and Ethical Issues:** No specific ethical or legal issues are anticipated to arise in this work.

**IRB Preparation:** Our activities in this proposal do not need any specific IRB approval. The PIs and other listed personnel have previously completed IRB and human studies ethics training.

**Access, Data Sharing, Reuse:** Any code from this project will be released under the open source MIT license. Project results will be widely disseminated to the community through project website, conference publications, journal articles, NSF annual meetings, annual reports, and similar methods. Dissemination to general public will be achieved through media outlets, magazine publication, presentation in public forums, and on [www.edurange.org](http://www.edurange.org).

**Data Standards and Capture Methods:** To collect survey data, we will use Qualtrics. The consultant has experience collecting and analyzing survey data using this platform. Data can also be exported from this platform into Excel for easy manipulation or exfiltration by other parties if desired.

We will continue to use standard development tools like Basecamp and git to manage educational modules, code, document the project, and synchronize effort across participants.

**Short-term and Long-term Data Storage and Data Management:** To date, the amount of data stored by this work can fit on a standard server. Although the anticipated data volume is hard to evaluate, we estimate that a 2TB drive will easily suffice.

No specific security measures will be needed concerning data storage.

1. System and measurement data will be stored and kept online for three years beyond the project life.
2. Source code will be stored on both local file servers and [github.com](https://github.com). These are adequate for long-term archiving.
3. Electronic copies of reports and articles will be kept on multiple devices, such as cloud document storage, laptops, desktops, and servers.

**Resources:** The PI will supervise and be responsible for implementing and maintaining this data management plan. Senior personnel, students, and contributors will be given a briefing on this plan prior to obtaining write access to [github](https://github.com) or Basecamp. This will ensure a smooth implementation of this plan.