A Helping Students Acquire Security 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. Unfortunately, most students in computer science receive very little training in security as undergraduates and lack the necessary skills for these jobs. In recognition of this need, security has been included as a core topic in the new 2013 IEEE/ACM Curricula [**?**]. At educational conferences such as SIGCSE and regional CCSC conferences, we are seeing a growing interest in cybersecurity among faculty who do not have expertise in this area. We propose to address the needs of two groups of faculty: those who have significant experience in cybersecurity and those who do not. 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 divisionial levels. It was also reported at the panel .. at SIGCSE 2014 that only one Ph.D. in Computer Security in 2012 joined the ranks of faculty who teach.

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.

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. **should we say something here about trust and trustworthiness, which is in CS2013? ** 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. One of the potential barriers to distributing EDURange to them is 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. However, the current model for distributing it to other faculty requires that they create an Amazon account 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 and providing direct technical support.

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. We may need to help faculty initially set up exercises for their classes. Our solution to this problem is to have a team of undergraduates who would staff an online help desk and answer questions about how to run scripts and

modify existing exercises or use them as templates for new exercises.

Third, we will run an online course for faculty using EDURange to teach an introductory cybersecurity course. We have already talked with other faculty who teach cybersecurity, and they are interested in working with us to share their syllabus and help deliver this online course. Instructors who sign up for this course would learn to use EDURange to create curriculum for their classes, which would range from a structured introductory security class to including some security in other classes, e.g. Networking, OS, Database systems, Programming Languages. We will provide EDURange for free to the instructors and their students over the next five years.

Our vision is that EDURange would provide a vehicle for all Computer Science faculty to address the goals of the IEEE/ACM 2013 Curricula report by translating the Information Assurance and Security (IAS) core concepts and outcomes into concrete examples. There are three interconnected components of this proposal: further developing the EDURange framework to enhance its capabilites for dissemination and assessment, provide support for faculty development through webinars, and provide a research opportunity for students to work on developing EDURange and work with faculty who are using it in their classrooms. The outcomes of this work will be:

1. EDURange will be used in 100 classes over five years at institutions other than the home institutions of the PIs.

2. Faculty will be able to assess their students on topics in the CS2013 report using EDURange and associated materials.

3. EDURange and associated activites will enhance teaching capabilites and enhance faculty expertise.

4. EDURange will produce a concrete realization of several of the IAS-related Knowledge Units with respect to cybersecurity concepts, skills and learning outcomes.

A.1 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 change how security is taught in the classroom, what is taught, improve faculty confidence to teach it, and make CS2013 a living document.

Related Work In Cybersecurity Education

Hinted at these problems in the intro, but give a more fulsome description of each, plus the specific difference / advantage of edurange. Best way to do this is emphasize different focus and outcomes? “We’re not seeking to replace, but to build/augment capacity along another direction.”

EDURange Exercises

organization and elements, learning implications With the publication of the CS2013 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 those standards.

Targeted audience is 2-fold: (1) "just want an exercise"/inexperienced (2) experienced...want configuration, etc.

A.2 EDURange infrastructure

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. There are six types of entities that we have identified as important:

- Nodes, e.g. could be a VM, attributes of the node would include players
- Networks, collections of nodes and the connections among them
- Software, which is necessary for the correct functioning of the exercise, including versions
- Constraints, e.g. time limits,
- Goals, i.e. learning objectives
- Artifact, e.g. a file that is placed on a target

Actually, the yaml file is different: groups, users, roles (an attribute), packages (Chef scripts for software)

A.3 Existing Exercises

Recon I

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

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

Concepts from CS 2013 addressed by this module:

- risk, threats, vulnerabilities, and attack vectors. This exercise shows how one might find vulnerabilities

This exercise is relevant for both defensive and offensive roles. [it currently has one level, show network diagram] 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 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. [more advanced: look for hosts and services that should not be on the network, knowing what to expect]

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 intructor might ask students to focus on speed or stealth.

Elf Infection

The learning goals are:

- understand elf format
- develop the security mindset
- distinguish between normal and suspicious behavior.
- use nmap to find hosts and open ports on a network.

Concepts from CS 2013 addressed by this module:

- risk, threats, vulnerabilities, and attack vectors. This exercise shows how how an attacker could maintain control of a system or exfiltrate data through infected binary files.
- How does this also address trust?

strace

The learning goals are:

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

scapy hunt

The learning goals are:

- understand firewall rules
- develop the security mindset
- understand routing tables
- understand how IP works

Grammar Fuzzing

The learning goals are:

- perform input sanitization
- develop the security mindset
- understand langsec

A.4 New exercises

A.5 Addressing CS2013

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

Activities

main purpose of activities is to support faculty development; they need to incorporate security development into a wide range of courses, and therefore they need more context. All activities are aimed at supporting this goal (and these outcomes).

We will bring together a wide range of experts who teach this stuff on a regular basis (plus their students) and we will put together exercises that are specifically mapped to CS 2013 and specific implimentations of their security curriculum...catar a la carte menu to fauclty that don't have that experience.

Ongoing Activities

Monitoring and maintanece of EDURange cloud infrastructure as hosted by Amazon. Support for mailing list and community building activities (twitter, etc.?)

Ongoing support for EDURange infrastructure; possibly matched by Amazon

Student-based activities * help desk: direct support our faculty audience/clients; opportunity for professional development: super TA/student aide

purpose is to twofold: close that last small gap in access (give faculty member comfort and confidence)

How do we control access? Faculty needs to commit themselves and students to participating in our assessment (see Section 5) then on FCFS basis, we will offer a student 1, 2, or 3 times? We don't have capacity to help everybody in face-to-face premium mode, they can get the mailing list asychronous support.

Platinum EDURange partners.

"1 out of 64 students went into teaching": gives student opportunity to develop teaching/education technique...apprentice model, exposure to a variety of professors and classroom environments...we don't teach grad students how to teach...this is an opportunity for practical training and course and curriculum management, development, experiential learning for our student...valuable experience for undergrads, also a variety of experience...they are not just pounding out code.. they act as a valuable external resource/expert to the faculty member they are helping.

* module development, multiple benefits to student researchers: pratical hands-on experience in systems and cloud and security, plus develop an appreciation for cybersecurity curriculum development as experssed in CS 2013.

Faculty-based activities

* design and run webinar (plan out curriculum) act as resource faculty audience; offering skeleton of an intro infosec course; cadre of instructors (panel of experts) will be given stipends to support their involvement * piazza * G+ youtube

* money for workshops at SIGCSE where we demo EDURange for attendees — this is place to get feedback; this activity feeds into our assessment and development (they give us ideas, VMs, exercises). Contact/face time target audience.

* guide students and help design scenarios; major elements, maps elements to CS2013, and we will offer documentation (we are the best people to write this b/c we are faculty members...include notes for faculty on the scenario motivation, formative and summative assessments, description of how it maps to CS 2013, how to best use it, keywords/topics, learning objectives, provides default context and possible suggestions for integration into non-security courses.

development of new scenarios and exercises. - take other people's exercises, make accesible - create new exercises of the EDURange style

Are we going to create student assessments? We will do that for a small number of exercises that we create. Our goal is to create the framework for creating assessments. we will not be the only ones creating exercises in EDURange

the webinar; the course template outline...make the point that the course is an example educational environment where EDURange can be mapped to or used.

a section on the EDURange "help desk" (another core expense item)

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. catelogue 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 ugrad 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 disastisfied 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 Piller: 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)...beginnging 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 dissmination efforts to demonstrate we've been effective at this

Data Management

Describe how we will protect PII. Describe any IRB procedures or protocols or training (for PIs and students).

Describe how we will guard and care for and dispose of our experimental data.

How will we make our data and scenarios persistent? Upload into ENSEMBLE.

Aggregate assessment and reports will be available on edurange.org