Cybersecurity Education with POGIL: Experiences with Access Control Instruction

Li Yang, Xiaohong Yuan, Wu He, Jennifer Ellis, Jonathan Land

Abstract - Given the ever-increasing realization as to how cybersecurity integrates into all aspects of daily life, cybersecurity education becomes increasingly important. While cybersecurity skillset certainly includes being equipped to safeguard businesses / organizations from cyberattacks, it also includes "professional skills" as also called "soft skills", such as teamwork, critical thinking, communications, etc. In this regard, it is important for colleges and universities to promote pedagogical frameworks that approach education in a way that does not dichotomize theory and praxis but encourages their interrelationship in terms of educating students towards these ends. In this paper, we introduced cybersecurity education materials we developed with Process-Oriented Guided Inquiry Learning (POGIL) which provides a promising educational framework for re-envisioning a holistic methodology for technical studies, specifically for the discipline of cybersecurity. As will be discussed in the findings of the student surveys below, and in the hands-on lab explaining access control, the scope of the POGIL methodology values training in the necessary content related to the specific areas of study, as well skills that complement, or work in conjunction with, the theoretical acumen gained in traditional education. Specifically, implementing POGIL within the discipline of cybersecurity assumes that technical training anticipates what students will face in real world contexts, as well as practices that will promote an integrated and holistic skillset. As a result, it is hoped that students will be prepared and empowered to succeed and to contribute as active participants within the businesses/organizations in which they fulfill their work-related responsibilities.

Keywords

POGIL, Access Control, Discretionary Access Control (DAM), Mandatory Access Control (MAC)

1 INTRODUCTION

In order to meet the demand for a workforce that can address the cybersecurity challenges confronting our society and our nation, cybersecurity programs in universities and colleges need to produce cybersecurity professionals who not only have in-depth technical knowledge in cybersecurity, but also have "soft skills" including communication, enthusiasm and attitude, team work, networking, problem solving and critical thinking, and professionalism [2]. In recent years, various student-centered, innovative pedagogies and learning environments have been explored and used in various disciplines to improve student learning and key skills, including "soft skills". In particular, one pedagogy that has been proved to be effective in various disciplines is POGIL, which stands for, Process Oriented Guided Inquiry Learning [1].

The paper is structured in the following way: First, we will give a short description of the background information regarding POGIL, as well as further describe how this approach is an effective and logical educational strategy. Second, we will present an in-class example to show how POGIL is implemented within popular topics of study in cybersecurity.

1.1 POGIL

POGIL originated in 1994 in the college chemistry education environment, and since then has been implemented in a variety of disciplines in high school and college courses, including anatomy, chemistry, physiology, biochemistry, mechanical engineering, and computer science [1]. As an instructional approach, POGIL is student-centered. As opposed to assuming the lecture is the center of the learning process, students are encouraged to learn in small self-managed groups on

specially-designed guided inquiry materials. As will be shown when we discuss access control, these materials include data or information for students to interpret, followed by guiding questions that lead students to formulate their own valid conclusions. Serving as a facilitator, the instructor observes and periodically addresses individual and classroom-wide needs. This type of inquiry-based team environment energizes students, increases student enjoyment, and provides instructors with instant and constant feedback about what their students understand and misunderstand. Moreover, it assumes that integrating multiple learning styles has a better end result than assuming that one teaching style is sufficient for all students. In this way, POGIL emphasizes that learning is an interactive process of refining one's understanding and developing one's skills [1].

POGIL differs from other student-centered instructional techniques in the following two ways: First, POGIL explicitly and consciously emphasize the development of essential process skills including teamwork, oral and written communication, management, information processing, critical thinking, problem solving and assessment. These process skills are practically the same as the "soft skills" mentioned above. Second, POGIL utilizes specially-designed, distinctive classroom materials that have the following characteristics: 1) they are designed for use by self-managed teams with the instructor being a facilitator of learning rather than the sole source of information; 2) they are designed to guide students to explore the disciplinary content: students construct, deepen, refine and/or integrate their understanding of the content; and 3) they are designed to develop at least one of the targeted process skills.

The development of a POGIL activity is based on the Guided Inquiry Learning Cycle: Exploration, Concept Invention, and Application (Figure 1). There are two categories of POGIL activities: 1) Learning Cycle Activities, which guide students to develop content knowledge through a Learning Cycle structure of exploration, concept invention, and application, and 2) Application Activities, which deepen, refine, and/or integrate the understanding of one or more concepts through application of relevant process skills.

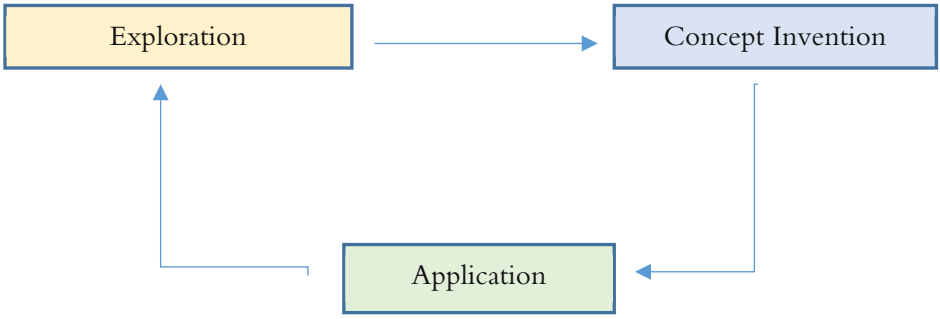


Figure 1: The Guided Inquiry Learning Cycle [1]

A POGIL activity typically includes the following components:

1. A "model." It can be various forms such as text, an equation, a diagram, a graph, a table, animation, demo, figure, etc.;
2. One to three Content Learning Objectives;
3. One to two Process Skills targeted for development;
4. A sequence of questions or actions that guide students to the targeted concept or Process Skill development; and
5. At least one application question for each concept. Further application can be within the sequence of guiding questions and/or in additional exercises/problems.

Although the POGIL instructional approach has been used in science and engineering disciplines, including computer science, use of POGIL in cybersecurity security education is lacking. While hands-on labs and case studies have been developed for cybersecurity education, a large portion of cybersecurity classroom teaching is traditional/lecture-based. To better engage and motivate students in learning cybersecurity, and develop process skills in cybersecurity students, we

propose to develop POGIL materials for teaching cybersecurity, implement the POGIL teaching pedagogy in cybersecurity courses, evaluate the teaching and learning effectiveness of the developed POGIL materials and teaching methods, and collect evidence of the effectiveness of POGIL teaching pedagogy in cybersecurity. Through assessing the developed POGIL materials and teaching pedagogy, we seek to answer the following research question: *Is using the POGIL method more effective than the traditional lecture-based teaching method in terms of learning outcomes, learning experience, attitudes and motivation?*

2 IMPLEMENTING POGIL'S INTEGRATED METHODOLOGY WITHIN STRUCTURED CYBERSECURITY

In order to better explain how POGIL operates in a classroom setting, and for the sake of time for this presentation, we have chosen to focus on one popular technical topic within cybersecurity and how POGIL helps students to learn more about it. This topic is access control. When attackers want to compromise a system, they often try to gain access in order to make unapproved modifications within the system. For these reasons, understanding access control is central to the training of cybersecurity professionals.

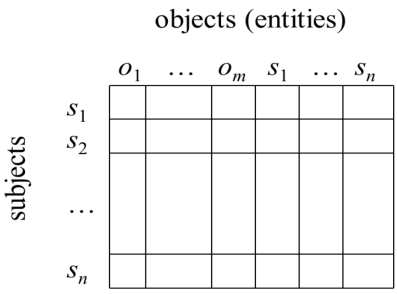
The POGIL methodology can be applied to this topic in order to help students learn more about two popular access control models: discretionary access control (DAC), and mandatory access control (MAC). After we present these models, we will discuss the ways in which POGIL fulfills specific learning objectives in a participatory way.

2.1 Cybersecurity and Discretionary Access Control (DAC)

It is well known that generally access control is understood as the collection of mechanisms that enables an authority to control access to resources in information [3]. In other words, access control specifies which (active) subject(s) have access to which (passive) object(s) with some specific access operation, as see in Figure 2.

Figure 2: Three tuples in access control

Discretionary access control (DAC) is a popular mechanism that oversees access to data objects (files, directories, etc.) and which users are permitted to resources based on the system identity. Explicit access rules are established about who can, or cannot, execute which actions on which resources. The "discretionary" part means that users can be given the ability of passing on their privileges to other users, where granting and revocation of privileges is regulated by an administrative policy. An Access control matrix is an abstract model of DAC and the state of the system is defined by a triple (S, O, A) where S means subjects, O means objects, and A means access matrix. As you can see, there are a lot of options for variation in terms of configuring system identities.



- Subjects $S = \{ s_1,\ldots,s_n \}$
- Objects $O = \{ o_1,\ldots,o_m \}$
- Rights $R = \{ r_1,\ldots,r_k \}$
- Entries $A[s_i, o_j] \subseteq R$
- $A[s_i, o_j] = \{ r_x, \ldots, r_y \}$ means subject s_i has rights $r_x, \ldots, r_y$ over object o_j

Figure 3: Access control matrix

Access control can be practically understood when considering Unix/Linux permissions. In these environments, users are allowed or denied certain access to read (r), write (w), or execute (x) a file (abbreviations may look like this on the system: **drwxr-xr-x**). Depending on who has permission to set the permissions

within a given system, these distinct permissions can be implemented in conjunction or in separation. To be allowed permission to read a file is simply to be able to view the contents of that file. To write to a file means that a user can edit or alter the contents of the file, and to execute a file means that a user can run the file if it happens to be a program or a script of some kind. The important part is that the user can decide what access privileges he or she wants other users to have. A permissions list could include the following data:

1. Ann can read File 1
2. Bob can read and write File 3
3. Carl can execute Program 1
4. Ann can write File 2
5. Carl can read File 2
6. Ann can execute Program 1

Additionally, access control is also important because it helps to classify users. For instance, users can be classified within the following three categories: owner, group, and others. The owner is the one who owns the file (i.e., usually the person who created the file). On the other hand, users can be a part of a group, in which everyone in that group has access to a file. The others are those who are neither an owner, or in a group. Typically, it is left up to the root user or system administrator to determine the kind of access/permissions and classifications that users have within a given system. Access control is vitally important to creating and maintaining secure systems for cybersecurity professionals.

2.2 Cybersecurity and Mandatory Access Control (MAC)

On the other hand, Mandatory Access Control (MAC) goes a bit further in its commitment to confidentially. Instead of users determining who has permission to what on his or her system (DAC), in MAC the system determines this. So, for example, multilevel security (MLS), which is a type of MAC, involves a database in which the data stored has an associated *classification* and consequently *constraints* for their access. MLS allows users with different classification levels to get different

views from the same data. MLS cannot allow downward leaking, meaning that a user with a lower classification views data stored with a higher classification. Consider the relation of SOD (Starship, Objective, Destination) as seen in Table 1.

Starship	Objective	Destination
Enterprise	Exploration	Talos
Voyager	Spying	Mars

Table 1: SOD table with no classification

The relation in the example has no classification associated with it in a relational model. The same example in MLS with classification will be as in Table 2.

Starship	Class.	Objective	Class.	Destination	Class.
Enterprise	U	Exploration	U	Talos	U
Voyager	U	Spying	S	Mars	S

Table 2: SOD table with classification

2.3 Applying POGIL's Methodology to DAC and MAC

Based on the aforementioned content, we can apply POGIL's instructional approach to access control in order to analyze how this encourages an interactive and integrative methodology.

First, in the discussions above, we have integrated various models for learning. By models, we are referring to graphs, charts, etc. These models are important for providing a conceptual frame of reference for students in order for them to first visualize the problem, and then think critically about how to approach solving the problem. Similar to OOP, the task is somewhat easier when you are able break the problem down into smaller parts and visualize a real-world example of what you are trying to solve in theory.

Second, the learning outcomes for access control would be for students to be able to know how various access control models work, but also be able to apply them to solve problems as a team, with each student contributing to the work as a whole. As explained above, POGIL is a very participatory and collaborative learning model. In regard to the topic at hand, before students begin asking questions about access control or looking at models, the students are divided into groups, and then each student is assigned a specific role within that group. Team roles could include a scribe (records all answers & questions and provide copies to team & facilitator (instructor)), spokesperson (Talk to facilitator and other teams), manager (keeps track of time and makes sure everyone contribute appropriately), and/or technical/reflector (considers how the team could work and learn more effectively). In this way, every student has a task and participates in the learning process.

Third, specific process skills are targeted for development. In regard to the example above about Linux/Unix permissions, a process skill could be being able identify which permissions can be categories as *subjects*, *objects* and *actions* from the following sentences.

1. Ann can read File 1
2. Bob can read and write File 3
3. Carl can execute Program 1
4. Ann can write File 2
5. Carl can read File 2
6. Ann can execute Program 1

Fourth, in order to better understand the concepts, a sequence of questions or actions are necessary to guide students to the targeted concept or Process Skill development. So, for example, if the targeted concept is file permissions and the process skill is to properly assess which users have access to what, questions may be structured in this way.

Concept: Under Discretionary Access Control the *owner* of the object directly controls the propagation of privileges and access of the object.

A DAC policy can be viewed easily as a table denoting which privileges each of the users possess.

User	object1	object2	object3
Bob	r, w	r, w	r
Alice			r, w
Eve		r, w	

- Given the policy above would the user Eve be able to gain characteristics about object1 (file size, file name, directory …)?

- Only owner of an object can grant permissions to other subjects. If Bob is not the owner of object2, but he has read and write capabilities is he able to share his access with the user Alice?
- The idea of least privilege is the policy of granting users the minimum amount of access they need to complete their job. Do you think if it can be easily implemented in the DAC Model?
- What is the important triple that is needed to create an Access Control Model?

In this section, we have considered various characteristics as to how POGIL presents a distinctive way of learning. First, we discussed how POGIL methodology could be applied to real world cybersecurity issues, such as access control. And second, we considered how POGIL helps students to cultivate the "soft skills," as mentioned above, as well as the technical knowledge, both of which will help them succeed as cybersecurity professionals.

3 EVALUATION AND ASSESSMENT

3.1 Process Based Evaluation: A Short Overview

Various educational standards exist for the purpose of evaluating whether or not colleges and universities are preparing students to succeed by training them in the necessary skillsets for future work. In particular, Process-Based Evaluation (PBE) is a methodical way to document how well a program has been implemented and is typically conducted periodically throughout the duration of the program.

The scope of PBEs is far-reaching in terms of its standards. For instance, PBE focuses on what works, what does not work, and what are the strengths and weaknesses of the resources, which are geared towards fully understanding the utility of the project deliverables. This type of evaluation investigates the process of delivering the program, including which activities were taking place, who is conducting the activities, and who is reached through the activities. Process evaluations assess the program's quality, the way the program was run, and whether the target group was reached. PBE is useful for measuring the impact of one

component of a larger program, in this case, the POGIL integration and summer workshops. In addition, the approach requires identifying the inputs (e.g., funding, staff, faculty, equipment, etc.), outputs (e.g., products or services), activities and desired outcomes with indicators (of success) prior to program implementation.

Although PBE was used to measure outcomes of a single component of the overall POGIL integration, the intent was to garner formative feedback that can be applied to future POGIL integration efforts and serve as feedback to help engage faculty and academic administrators in upcoming in-conference workshops.

3.2 Evaluation Results and Findings

The findings below are informed by a sample of undergraduate (70.83%) and graduate students (29.17%) at the University of Tennessee at Chattanooga. Some of the academic characteristics of the students surveyed include the following: The majority of students surveyed had taken a course (69.23%) for cybersecurity credit (30.77%, had not), either Introduction to Information Security, Wireless Security, Biometrics and Crytography, Database Security, or Systems Vulnerability. Some students had formal training in certain cybersecurity disciplines, while others did not. Of those who did have formal training, some of those trainings included Computer Sec+, CompTIA CSA+, Doe Training, Network+, Security+, Basic and Advance PII/RPII, and online cybersecurity fundamentals (USMC).

4 CONCLUSION

In this presentation, we have discussed how POGIL provides an instructional framework for re-envisioning technical training toward the cultivation of holistic skillsets for college and university students, specifically in the academic discipline of cybersecurity. The main question guiding our inquiry was, when compared to traditional/lecture-based learning, whether or not POGIL better comported with fulfilling the learning objectives that we hope students will internalize after their cybersecurity studies in college or university. Our analysis of this guiding question included showing the actual implementation of POGIL activities/modules within

a classroom setting, using access control as the technical topic of choice (DAC and MAC). We then went into further discussion about the logic that informed these POGIL activities; that is, the way in which the leaning took place. Last, we applied PBE as an effective educational standard for measuring how well a program is being implemented to assess whether or not POGIL meets the learning objectives for UTC cybersecurity training. Surprisingly, similar to POGIL, PBE approaches its criteria from an integrated perspective as well, not just focusing on one finding, but how the parts relate to the whole. kind of integrated approach to education is an effective framework for cultivating the holistic skillset that we hope to inculcate in the next generation of cybersecurity professionals.

REFERENCES

[1] POGIL – Process Oriented Guided Inquiry Learning, Retrieved December 10, 2015 from https://pogil.org/about

[2] United States Department of Labor, Soft Skills to Pay the Bills – Mastering Soft Skills for Workplace Success, Retrieved December 10, 2015 from http://www.dol.gov/odep/topics/youth/softskills/

[3] S. Cooper, L. Perez, and B. Oldfield, Towards Information Assurance Curricular Guidelines, in Proceedings of the 15th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE), Turkey, June, 2010.