Teaching Flooding Attack to the SDN Data Plane with POGIL

Hanan Alshaher
Computer Science
NCAT
Greensboro, NC USA
halshahr@aggies.ncat.edu

Xiaohong Yuan
Computer Science
NCAT
Greensboro, NC USA
xhyuan@ncat.edu

Sajad Khorsandroo
Computer Science
NCAT
Greensboro, NC USA
skhorsandroo@ncat.edu

ABSTRACT

Process oriented guided inquiry learning (POGIL) is a teaching technique that engages students in active learning and develops student process skills including critical thinking, problem solving, and teamwork. POGIL uses activities that are designed to guide students through questions to formulate patterns and relationships toward concept exploration. This paper describes the POGIL activities we developed for teaching Flooding Attack to the Software Defined Network (SDN) Data Plane, and our experience teaching this topic using POGIL These POGIL activities can be used by other educators in network security courses.

CCS CONCEPTS

• Security and privacy~Network security~Denial-of-service attacks • Applied computing~Education~Interactive learning environments

KEYWORDS

Process-oriented guided inquiry learning (POGIL), Software-defined networking (SDN), cybersecurity, student-centered instructional technique.

ACM Reference format:

Hanan Alshaher, Xiaohong Yuan, and Sajad Khorsandroo. 2020. POGIL for Flooding Attack to the SDN Data Plane. In *Proceedings of ACM SIGITE Annual Conference 2020 (SIGITE 2020). ACM, Omaha, NE, USA, 6 pages.* https://doi.org/ 10.1145/3368308.3415406

1 Introduction

Various teaching methods have been developed to enhance learning and engage students in active involvement instead of passive listening to improve students' learning and enthusiasm.

SIGITE'20, Oct 7–9, 2020, Omaha, NE, USA.

ACM ISBN 978-1-4503-7045-5/20/10...$15.00.
https://doi.org/10.1145/3368308.3415406

Active learning was introduced by Bonwell and Eison in 1991 [1], the purpose of which is to increase students' participation through problem solving, discussion, group work, and other methods. Another learning method named discovery learning, which means learning through self-teaching, was introduced by Baldwin in 1996 [2]. Active and collaborative learning (ACL) is another learning method that was discussed in detail by McConnell in [3]. ACL requires students to work actively in groups to develop a solution to a problem. It has been proven in several studies, such as [4], that ACL increases student motivation and confidence, increases learning skills, and decreases drop-out rates. Researchers have shown that cooperative learning activities increase students' understanding in comparison to traditional learning methods in computer science education [5][6]. Furthermore, process skills (also known as professional skills, lifelong learning skills, workplace skills, transferable skills, or soft skills) are an important aspect of learning in addition to knowledge acquisition. Thus, learning objectives should include the development of process skills, such as critical thinking, problem solving, and teamwork. In short, in addition to knowledge acquisition, effective learning engages students and emphasizes skills development.

Process-oriented guided inquiry learning (POGIL) is a teaching technique promoted by the POGIL project. The POGIL technique engages students in the classroom to work collaboratively by grouping them in teams, and at the same time, it develops students' process skills. To apply POGIL, educators create activities to meet the requirements of a typical POGIL classroom activity provided by POGIL project [7]. Each activity contains a model and sequence of questions that guide students to construct their own understanding and grasp the concept. The model can include, for example, a figure or text, and the information is not explicitly stated in the model. In a POGIL classroom, students work in teams of 4–5 on activities. Each member of the team has a distinct and well-defined role to play (e.g. manager to make sure everyone contributes and monitor time management, writer, and speaker). The instructor is an active facilitator of student learning by monitoring progress and guiding students. Because POGIL in the classroom requires students to work collaboratively on activities, it develops students' process skills, such as communication, teamwork, information processing, problem solving, and critical thinking.

Software-defined networking (SDN) is a new network platform that has a centralized control architecture, which is a suitable

environment for such attacks as distributed denial-of-service (DDoS) attacks (i.e., flooding attack), which is one of the most common threats to network security [8]. As Arash et al. stated:

> Traditionally, computer networks have been divided into three planes of functionality namely, the management plane, the control plane, and the data plane. SDN moves away from a vertical integration of network components to a horizontal one and adds distinctive separate functioning layers for policy definition, enforcement and implementation [9, pp. 1-2].

The aim in the present paper is to present how to develop activities for teaching flooding attack on the SDN data plane by using the POGIL methodology. Because POGIL is a student-centered instructional technique, students will learn by their own exploration rather than the instructor being the source of information. Furthermore, this technique emphasizes the development of process skills. Using this technique to introduce a cybersecurity topic, such as a flooding attack on the SDN data plane, helps students to understand deeply how and why it happens, encourages them to think about how to create a defense framework, and develops their problem-solving abilities.

The rest of the paper is organized as follows. First, it reviews related work on using POGIL in computer science and cybersecurity education. Then, the process of developing POGIL activity for flooding attack to the SDN data plane is given. Next, a sample POGIL activity for flooding attack to the SDN data plan is provided. Our experience with using the developed POGIL activities in class is reported. Finally, we concludes the paper and discuss future work.

2 Related Work

POGIL activities have been applied to different disciplines, and educators publicly share these POGIL activities on websites. There are several projects that develop POGIL activities and use them for teaching computer science topics.

Xiaohong et al. [10] used guided inquiry collaborative learning (GICL) to develop activities for teaching the topic of firewall and IPsec as one topic of Network Security course. The results of the survey that they conducted showed that students had increased learning outcome and participation in class. They concluded that students who learned via the GICL activities in general had positive experience compared with others who learned via the traditional lecture [10]. Since cybersecurity education has not been applied POGIL, the researchers in [11] proposed a project to do so. They developed POGIL materials for teaching cybersecurity topic which was access control. Then, for assessing learning effectiveness when POGIL was implemented, they used process-based evaluation (PBE) which was a method to evaluate how well were a program's outcomes [11].

IT3510 course was an Advanced Linux Administration class at Utah Valley University, and because of the course requirements that required students to learn and apply advanced Linux skills, up to a third of the students usually dropped the course. For that reason, the author in [12] applied POGIL activities on IT3510 class to decrease dropping out rate. Hu and Shepherd in [13] described their experience of adopting POGIL on a CS 1 class. They used six POGIL activities in three CS 1 sections. Then, they compared the results of the pass rate and retained with other sections who learned through a traditional group activity. They concluded that POGIL sections have higher pass rates and better retention than traditional sections. In [14], the author conducted a project to develop a set of POGIL activities related to computer science, including topics on data structures, algorithms, and software engineering. The author presented a sample of POGIL activities for the queues and stacks topics. In [15], the researchers conducted a survey to analyze the computer science faculty's perceptions of the benefits and obstacles of POGIL adoption in computer science classrooms. Survey respondents agreed that POGIL had a positive effect on students by keeping them engaged and active. On the other hand, one of the obstacles that was mentioned most by the respondents in the survey was a lack of availability of POGIL activities.

3 Developing POGIL Activities

The main purpose of developing POGIL activities is to guide students through exploration to construct their own knowledge about the target concepts. The authors of this paper began developing POGIL activities in Spring 2019 in one topic of Advanced Security for an Emerging Networks course. POGIL activities helped students to understand the topic in depth and to complete hands-on labs that demonstrate security issues. Developing POGIL activities for flooding attacks on the SDN data plane was based on [8]. The process of developing each activity considered two main aspects. The first aspect focused on arranging the activity to help students explore the concept and discover and formulate their own valid conclusions. The second aspect was creating an activity that develops one or more soft skills in students. For example, using a figure in the activity helps students to process information.

The first step in creating a POGIL activity identifies learning objectives. Then, a sequence of questions is created that guides students in grasping the concept. Typically, a POGIL activity document contains four to five sections. At the top of the document is a clear title followed by learning objectives. Then, prerequisite reading is featured in the following section if needed. The rest of the document contains several activities, as well as a model and series of questions that guide students through the activity. Each question has an estimated duration to help students manage time.

4 Sample Activity

This section describes a sample of POGIL activities for Flooding Attack to the SDN data plane. The full activities will be publicly available online at http://cspogil.org. The topic of Flooding

Attack to the SDN data plane covered as three activities: introduce the flooding attack to the SDN data plane, how the flooding attack to the SDN data plane happens, and how to prevent the flooding attack to the SDN data plane. Each activity should cover no more than two to three learning objectives. The following passage is a sample of the first activity (i.e. the introductory activity or introduce the flooding attack to the SDN data plane). Text from the activity is in italics.

The learning objectives for the activity includes: *students should be able to*

1. *describe how a packet is processed in OpenFlow switch and OpenFlow controller.*
2. *identify table-miss cases and explain how table-miss is handled.*
3. *compare dynamic and static (proactive and reactive) flow rule installation.*

To cover these learning objectives and complete the activity on hour and half, the time should be divided between activity's sections. The introductory activity contains five sections. The last two sections of the activity are not shown here. Each section contains model or example and sequence of questions. The information may not be explicitly stated in the model so student can explore and process the information toward concept discovery.

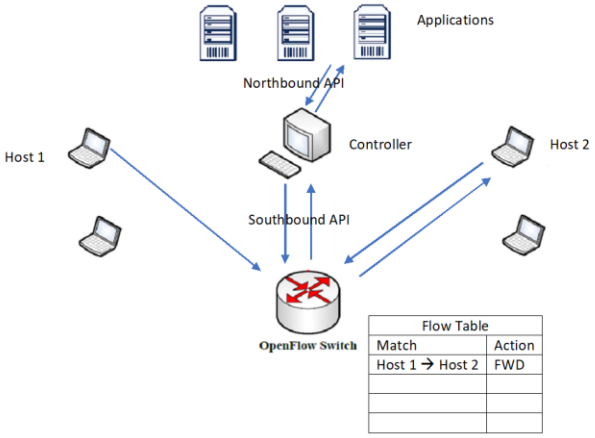

Figure 1: A SDN network with OpenFlow controller and OpenFlow switch

Figure 1 shows a SDN network with OpenFlow controller and OpenFlow switch. Current OpenFlow implementations use a "southbound" protocol. When a switch receives a new flow and there is no matching flow rules installed in its flow table, table-miss occurs. Then the data plane will ask the control plane for actions.

- *What's the different between Northbound and Southbound APIs? (2 min)*
- *When an OpenFlow switch receives a flow, what does the switch do? (2 min)*
- *What will happen if there are many table-misses? (5 min)*

The first section reviews the SDN architecture and introduces a new concept "table-miss". Then, it opens discussion on the third question which is a critical thinking question. Each question has an estimated time so students will learn how to manage their time. Since students work in group, and each member of the group has a role to play, students' soft skills such as communication and collaboration will improve.

Figure 2 shows how a packet is processed in OpenFlow switch in detail. See the interaction between the switch and the controller

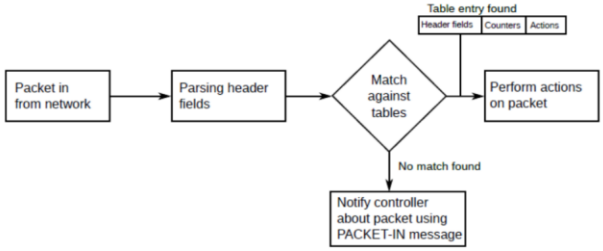

Figure 2: Packet processing in OpenFlow switch

- *Who creates PACKET-IN message? Who processes the message? (2 min)*
- *When is PACKET-IN message created? (2 min)*
- *What's the purpose of PACKET-IN message? (2 min)*
- *Based on what does the switch match a packet against in the flow table? (2 min)*

The second section illustrates how a packet is processed in OpenFlow switch. Students should be able to process the information and answer the questions.

packet_in handler function:
Figure 3 shows how packet_in handler function is processed a packet_in message in OpenFlow controller.

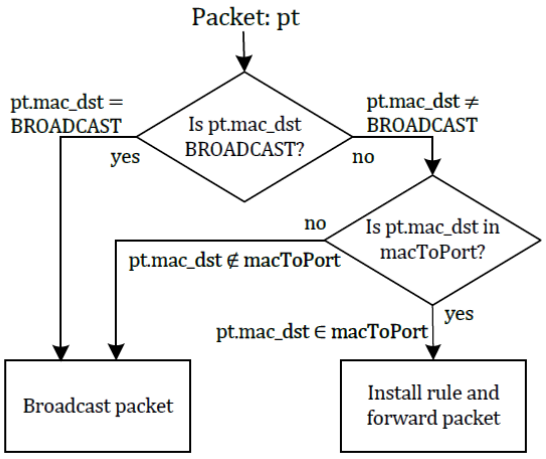

Figure 3: packet_in handler function

- *What are the input and the output of packet_in handler function? (2 min)*
- *What packet_in handler function do if the destination MAC address of the packet is a broadcast address? (2 min)*
- *What packet_in handler function do if the destination MAC address of the packet is not a broadcast address? (2 min)*

The third section demonstrates how handler function which is in the OpenFlow controller processed a packet. All the previous models help student to understand the workflow of the packet on the SDN. Thus, in the next model student will be able to describe by themselves and discover how the flooding attack to the SDN data plane happens.

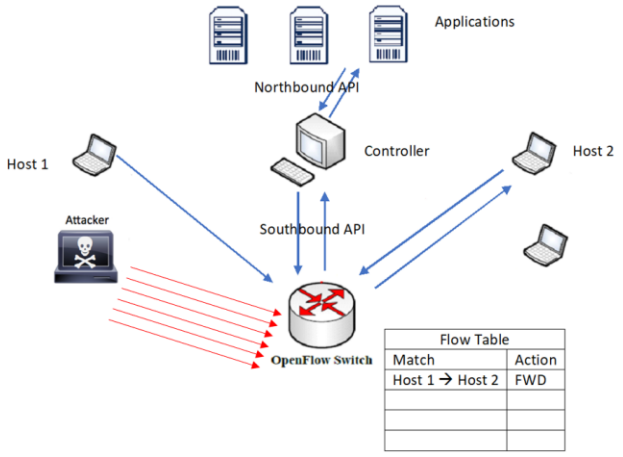

Figure 4: Adversary Model

- *How can an attacker create a table-miss? (2 min)*
- *What will happen if one host generates a flooding traffic? (3 min)*
- *What will happen if the buffer memory of switch is overloaded? (3 min)*
- *What will happen if the buffer memory of controller is overloaded? (3 min)*
- *Note: when traffic consume bandwidth and resources, it is called amplification attack.*
- *What's the relationship between denial of service attack (saturation attack) and amplification attack? (2 min)*
- *Brainstorm: How to keep the major functionalities of the SDN infrastructure working under a saturation attack in the data plane? (5 min)*

This model is the first section of the second activity (i.e. how the flooding attack to the SDN data plane happens). All questions in this model open discussion between team members to formulate a patterns and relationships toward concept exploration. Also, it motivates students to hear others' answers and ideas. At the end of this activity, students' performance on the lab assignment had significantly improved.

5 POGIL in the Classroom

The details of running a classroom using the POGIL material developed in this project are described in this section. The length of the POGIL material covers seven learning objectives, and for this reason, it is necessary to use two lectures, one and a half hours each, to cover this topic. The plan is as follows:

[1] First, the instructor announced to his class that they will have a small group discussion on the topic of SDN saturation attacks the following week. Typically, a POGIL group includes four students, each with a distinct role. In this project, the class contained eight students, so the instructor assigned them to two groups.

[2] On the day of the class, we provided the instructor with the POGIL material, which was a word document contains POGIL activity so the writer of each team can easily share his/her screen and write the team's answers, and a brief introduction to POGIL, including the roles of the members in a group. Then, the instructor posted these two files on the Blackboard 10 minutes before the class for students to download.

[3] Because of the pandemic of novel coronavirus 2019 (COVID-19), the university suspended in-person instruction and moved to online instruction. Because the classes transitioned to online, we used Zoom meetings in this project. The instructor started the Zoom session 5 minutes before the class. Then, the instructor could create two breakout rooms and assign the two groups to the two breakout rooms. The instructor has the ability to join and leave each room freely to observe the group discussion and facilitate the class.

[4] When the class started, we asked students to download the materials from the blackboard. Then, we gave a brief introduction of the class activities. The POGIL materials were divided into three sections. We asked the students to go to the breakout room to discuss the first section of the material and then asked them to leave the breakout rooms and have a whole class discussion. During the whole class discussion, the speaker of each group reported their answers. The instructor could give feedback to the students and guide the discussion.

[5] After that, students were asked to return to the breakout room to discuss section 2; thereafter, they joined the main session, then returned to the breakout room, and then returned to the main session.

[6] On the day of the next class, we provided the instructor with part II of the material before class so the instructor could post the material on the blackboard.

[7] At the end of the last class, we asked the students to fill out a survey on this learning experience.

6 Students Feedback

The POGIL activities for the topic of flooding attack on the SDN data plane were used in the Advanced Security for Emerging Networks course at North Carolina Agricultural and Technical State University (NCA&T) in the Spring 2020 semester. To determine the effectiveness of POGIL activities, a survey was created to obtain participants' feedback. Eight graduate students participated in the survey and provided feedbacks. The survey included thirty-three questions divided into four categories: student's motivation toward learning cybersecurity, student's attitude regarding POGIL learning experience and teamwork, rating student's level of knowledge for each of learning objectives, and open-ended questions to get student's opinion.

Students' responses showed that 100% agreed with the following statements:

- *Q5 - I had a positive experience working in POGIL groups in the learning of flooding attacks on the SDN data plane.*
- *Q7 - While working in POGIL groups, we were able to communicate effectively.*
- *Q10 - During the POGIL meeting discussion, the setup of various roles makes our discussion more efficient.*
- *Q14 – The POGIL method engaged me in learning about flooding attacks on the SDN data plane.*
- *Q19 - POGIL allowed me to analyze a problem and identify a solution based on the accessible information.*

Students' answers showed that 50% agreed and 50% somewhat agreed with the following statements:

- *Q6 - While working in POGIL groups, the workload and role of each member was distributed equitably.*
- *Q9 - On my POGIL team, everyone contributed to the success of the task.*

Students' answers showed that 50% strongly agreed and 50% agreed with the following statements:

- *Q12 - I think the POGIL learning experience is interesting*
- *Q13 - I'm motivated to learn about flooding attacks on the SDS data plane using POGIL.*
- *Q16 - I enjoyed the POGIL learning experience on this topic (flooding attacks to the SDN data plane).*
- *Q17 - I think the POGIL learning experience is good for me.*
- *Q20 - Education materials and practice questions in the POGIL classroom encourage me to think more actively and independently than in a traditional classroom.*
- *Q28 - After POGIL, I have more confidence in describing the concepts compared to a traditional classroom.*

Students' answers showed that 50% disagreed and 50% neither agreed nor disagreed with the following statement:

- *Q18 - It is difficult for me to learn this topic (flooding attacks to the SDN data plane) using the POGIL approach.*

Students' answers showed that 100% neither agreed nor disagreed with the following statement:

- *Q15 - I wish more cyber security topics would be taught using the POGIL method instead of the traditional lecture-based method.*

To measure students' retention and to what extent they mastered the concepts, the following reports students' responses on learning outcome related questions. The scale for the rating questions were excellent, good, average, poor, and terrible.

Students' answers were 100% good in response to the following prompts:

- *Q21 - Describe the packet processing in OpenFlow switch and OpenFlow controller.*
- *Q22 - Identify table-miss cases.*
- *Q25 - Demonstrate how a DOS attack on the data plane works.*
- *Q27 - Discuss how to prevent a flooding attack on the SDN data plane.*

Students' answers were 50% excellent and 50% good in response to the following prompts:

- *Q24 - Compare how the controller installs dynamic and static (proactive and reactive) flow rules in the switch flow table.*
- *Q26 - Define DOS attack and amplification attack.*

7 Conclusion

Teaching with POGIL is an active learning approach that has shown significant benefits, such as improving student engagement and attendance by working in groups, helping weaker students and reducing isolation by assigning roles for each member of team, and improving student performance and long-term retention. One of the challenges in developing POGIL activities is crafting a model and writing sequences of questions that guide students to construct their own valid conclusions. We have developed the POGIL activities for teaching flooding attack to the software defined network (SDN) data plane, and implemented the activities in the Advanced Security for Emerging Networks course. The feedback on these activities were very positive. During the next phase of this research, a comparison of students' grades, lab performance and retention between two sections that apply two different teaching approaches (i.e., POGIL and traditional) will be conducted. In addition, POGIL activities for the topic of flooding attack on the SDN data plane will be made available at http://cspogil.org, which is a web site for computing educators to share their POGIL activities for computer science courses.

ACKNOWLEDGMENTS

This work is partially supported by NSF under the grant DGE-1623624, DGE-1623629, DGE-1623646. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

[1] C.C. Bonwell and J.A. Eison. 1991. *Active Learning: Creating Excitement in the Classroom.* ERIC Digest.

[2] D. Baldwin. 1996. Discovery learning in computer science. In *Proceedings of the 27th SIGCSE Technical Symposium on Computer Science Education*, March 1996, Philadelphia. ACM Inc., 222-226.

[3] J.J. McConnell. 2005. Active and cooperative learning: tips and tricks (part I). *ACM SIGCSE Bulletin* 37, 2, 27-30.

[4] J.E. Miller and J.E. Groccia. 1997. Are four heads better than one? A comparison of cooperative and traditional teaching formats in an introductory biology course. *Innovative Higher Education*, 21, 4, 253-273.

[5] L.L. Beck and A.W. Chizhik. 2008. An experimental study of cooperative learning in cs1. *ACM SIGCSE Bulletin*, 40, 1, 205-209.

[6] G. Gonzalez. 2006. A systematic approach to active and cooperative learning in CS1 and its effects on CS2. In *Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education*, March 1-6, 2006, Houston, Texas. SIGCSE, 133-137.

[7] *Writing Guidelines*, 2019. Accessed 2019. [Online]. Available: https://pogil.org/authoring-materials/writing-guidelines

[8] H. Wang, L. Xu, and G. Gu. 2015. Floodguard: A DOS attack prevention extension in software-defined networks. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 239-250.

[9] Shaghaghi, A., Kaafar, M.A., Buyya, R. and Jha, S., 2020. Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions. In *Handbook of Computer Networks and Cyber Security* (pp. 341-387). Springer, Cham.

[10] Yuan, X., Zhang, T., Shama, A.A., Xu, J., Yang, L., Ellis, J., He, W. and Waters, C., 2019, October. Teaching Cybersecurity Using Guided Inquiry Collaborative Learning. In *2019 IEEE Frontiers in Education Conference (FIE)* (pp. 1-6). IEEE.

[11] Yang, L., Yuan, X., He, W., Ellis, J. and Land, J., 2019, February. Cybersecurity Education with POGIL. In *Journal of The Colloquium for Information System Security Education* (Vol. 6, No. 2, pp. 14-14).

[12] S.J. Cold. 2013. Partially flipped: experiences using POGIL. In *Proceedings of the 14th Annual ACM SIGITE Conference on Information Technology Education*, October 2013. ACM Inc., 133-134.

[13] H.H. Hu and T.D. Shepherd. 2014. Teaching CS 1 with POGIL activities and roles. In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, March 2014. ACM Inc., 127-132.

[14] C. Kussmaul. 2012. Process oriented guided inquiry learning (POGIL) for computer science. In *Proceedings of the 43rd ACM technical symposium on Computer Science Education*, February 2012. ACM Inc., 373-378.

[15] H.H. Hu, C. Kussmaul, B. Knaeble, C. Mayfield, and A. Yadav. 2016. Results from a survey of faculty adoption of process oriented guided inquiry learning (POGIL) in computer science. In *Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education*, July 2016. ACM Inc., 186-191.

[16] Hu, H.H. and Shepherd, T.D., 2013. Using POGIL to help students learn to program. *ACM Transactions on Computing Education (TOCE), 13*(3), pp.1-23.