Prospectus

How Do Students Collaborate? Analyzing Group Choice in a Collaborative Learning Environment

Analyzing Impacts of and Solutions to Cyberattack Targeting American Academic Institutions

By

Xinyue Lin

April 13, 2021

Technical Project Team Members: James Connors, Chang Lim, and John R. Hott

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____Xinyue Lin_____

Technical Advisor: _____

STS Advisor: _____

1. **Introduction**

University education has been drawing increasing attention as more students have chosen to pursue a higher degree after high school graduation. The effectiveness and information safety of university education are one of the key aspects contributing to a rewarding university experience, and therefore, I'm motivated to conduct research on these topics in an attempt to foster a better learning environment for college students (Brint & Clotfelter, 2016; Zhang-Kennedy et al., 2018).

As a student majoring in Computer Science, I am inspired to study the effectiveness of student collaboration in CS courses taught at universities. Specifically, I will conduct technical research to study whether collaboration improves grades, and if so, what is the optimal group size. In a collaborative learning environment, students are usually allowed to choose different partners for different assignments. I will analyze how collaboration groups evolve over time if students are given the choice to change collaborators. In addition, studying the factors that potentially lead to group membership changes can provide professors with insight into how to help students gain the best learning experience. Consequently, I aim to identify the key information that correlates with changes in group choices.

Universities' ability to protect student information is also crucial to ensuring safe and bright academic experiences. It is concerning to witness a growing number of malware attacks targeting academic institutions (Wood, 2020). Malware attacks are malicious software executed on electronic systems that steal personal information and conduct spying activities. In my STS paper, I aim to study the common types of malware techniques used to attack universities and the consequences of these attacks. Additionally, I will research how universities have been preventing cyberattacks and handling attack aftermaths to learn about the current situations. I

will further study the types of matured techniques utilized by large businesses to reduce potential loss due to cyberattacks in order to provide suggestions for academic institutions.

2. **Technical Topic**

Student collaboration has been widely adopted and encouraged in Computer Science Education (Slavin, 1980). Understanding how collaboration benefits students can help establish better collaboration policies in an academic setting. I aim to conduct an observational study to investigate what will happen when students are allowed to choose and change their study groups for an entire semester. Existing peer-reviewed studies have carried out experiments to control group sizes with random assignment and concluded that collaboration benefits socially, psychologically, and academically (Laal & Ghodsi, 2012). In addition, evidence from peer-reviewed literature showed that groups of size four are optimal, given an academic setting that randomly pairs up volunteers for coding assignments (Akinola & Ayinla, 2014). Yet fewer works have been done in a looser collaborative environment that gives students the freedom to choose groups. I will focus on an academic setting where students are free to make their own group choices bounded by a certain collaboration policy in order to examine the effectiveness of collaboration as well as group formation and group evolvement.

Consequently, I will observe the collaboration information from a high-level algorithm course taught at the University of Virginia, which has a collaboration policy that allows for self-selected groups with up to five members per group for each assignment. Grades and self-reported collaborators will be collected from each student for a total of nine assignments, including written and coding assignments. Additionally, the relationship between collaboration and factors such as homework release date, homework difficulty, homework type, and students' relative

performance in comparison with the class average will be analyzed to determine the key information that correlates with the change of collaborators.

3. **STS Topic**

As technology advances expeditiously, cybersecurity has gained greater importance. The number of cyberattacks has been on the rise, with a growing amount targeting academic institutions. My STS paper examines current cyberattacks aiming at universities in an attempt to study the purpose of such attacks, the resulting negative effects, and potential solutions. Existing studies mostly focus on malware attacks on business sectors and government institutions, and few have paid attention to attacks in academic settings. Consequently, university official websites and news articles will be the main sources of information.

University-wise attacks are dangerous as they can steal confidential information from the faculty and students, including telephone numbers, payment details, and social security numbers (Wood, 2020). Therefore, this topic is worth studying to call for more attention to universities as the victims. In addition, I'm interested in the strategy that universities use to prevent cyberattacks and cope with the aftermath in order to help them improve their current approaches. While a majority has already implemented security policies, these policies can be presented in more effective ways by modifying the readability and length of paragraphs (Weidman & Grossklags, 2019). Moreover, universities such as the University of Virginia have been conducting phishing simulations annually to keep students alert for phishing emails (University of Virginia, 2020). Since drills are useful, the frequency of unannounced simulations can be increased to raise effectiveness (Frost & Hamlin, 2020). I will also propose suggestions to academic institutions for better cyberattack handling based on the experiences provided by enterprises. Data leakage

resulted from malware attacks has been a persisting issue for organizations, and the strategies they have developed are also applicable in an academic setting. For instance, the Data Prevention and Detection system can be employed by universities to identify and prevent data leakage (Cheng et al., 2017).

4. **Conclusion**

Our research results have provided suggestions for professors regarding how to design classroom collaboration policies to better facilitate student learning. Since student collaboration is demonstrated to be effective, professors should promote and encourage group study, especially when completing harder assignments. In addition, professors should release grades more promptly and suggest students change groups more frequently because grade release and collaborator changes because both result in better grades.

Meanwhile, to ensure a safe learning environment, universities should define plans of response to avoid, mitigate or transfer the risk of being attacked. Faculty training and constant phishing simulations should be conducted to keep university members alert, and Data Prevention and Detection system can also be implemented as means of additional security protection. Courses of ethics can be taught so that future developers can refrain from participating in malware construction. While malware detection or prevention is still a popular topic, further research should be done to develop better techniques with a special focus on attacks targeting universities.

5. References

Akinola, O. S., & Ayinla, B. I. (2014). An Empirical Study of the Optimum Team Size Requirement in a Collaborative Computer Programming/Learning Environment. *Journal of Software Engineering and Applications*, *7*(12), 1008–1018. https://doi.org/10.4236/jsea.2014.712088

Brint, S., & Clotfelter, C. T. (2016). U.S. Higher Education Effectiveness. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, *2*(1), 2–37. https://doi.org/10.7758/rsf.2016.2.1.01

Cheng, L., Liu, F., & Yao, D. (Daphne). (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

Department of Justice Launches Global Action Against NetWalker Ransomware. (2021, January 27). https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

Frost, J., & Hamlin, A. (2020). Ransomware—A Strategic Threat to Organizations. *Mountain Plains Journal of Business and Technology*, *21*(2). https://openspaces.unk.edu/mpjbt/vol21/iss2/6

Laal, M., & Ghodsi, S. M. (2012). Benefits of collaborative learning. *Procedia - Social and Behavioral Sciences*, *31*, 486–490. https://doi.org/10.1016/j.sbspro.2011.12.091

Olsen, D. (2020). *MSU provides update on IT-based intrusion*. MSUToday | Michigan State University. Retrieved March 20, 2021, from https://msutoday.msu.edu/news/2020/msu-provides-update-on-it-based-intrusion?utm_campaign=media&utm_medium=email

Slavin, R. E. (1980). Cooperative Learning. *Review of Educational Research*, *50*(2), 315–342. https://doi.org/10.3102/00346543050002315

Sullins, J. P. (2014). A Case Study in Malware Research Ethics Education: When Teaching Bad is Good. *2014 IEEE Security and Privacy Workshops*, 1–4. https://doi.org/10.1109/SPW.2014.46

University of Virginia. (2020). *Phishing Simulation for Students—November 2020 | Information Security at UVA, U.Va.* https://security.virginia.edu/phishing-simulation-students-november-2020

Weidman, J., & Grossklags, J. (2019). Assessing the current state of information security policies in academic organizations. *Information & Computer Security*, *28*(3), 423–444. https://doi.org/10.1108/ICS-12-2018-0142

Wood, C. (2020, September 9). *9 times cyberattacks disrupted education this year*. EdScoop. https://edscoop.com/list/2020-university-k12-cyberattacks-ransomware/

Yu, B., Fang, Y., Yang, Q., Tang, Y., & Liu, L. (2018). A survey of malware behavior description and analysis. *Frontiers of Information Technology & Electronic Engineering*, *19*(5), 583–603. https://doi.org/10.1631/FITEE.1601745

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., & Chiasson, S. (2018). *The aftermath of a crypto-ransomware attack at a large academic institution*. 1061–1078. https://www.usenix.org/conference/usenixsecurity18/presentation/zhang-kennedy