secCC: Securing the Future of Cloud Computing

Special track with Cloud Computing 2020

http://www.iaria.org/conferences2020/CLOUDCOMPUTING20.html

Aspen Olmsted
Fisher College
Department of Computer Science, Boston, MA 02116
email: aolmsted@fisher.edu

***Abstract*— As cloud computing continues its evolution into one of the primary forms of application deployment, many new cybersecurity challenges are rising to visibility. These challenges include deploying legacy applications to the cloud and developing new applications for the cloud. Each model has problems ensuring the confidentiality and integrity of the data and the service level available for the applications. This special track aims to expose some of these new problems and novel approaches to solving these problems. While we want to solve issues supporting our legacy architectures and algorithms moving to the cloud, we also want to give enough energy to new and evolving architectures and algorithms to secure future applications. Both challenges with private and public cloud infrastructure are welcome**

Keywords-Business Intelligence; Cloud Computing; Heterogeneous Data

I. INTRODUCTION

Cloud Computing has evolved into the modern operating system of the early 21st century. New York University (NYU) has developed an online graduate cybersecurity program called Cyber Fellows [1]. Cyber Fellows provides a 75% scholarship towards tuition for an elite online Cybersecurity Master's Degree. Thanks to generous support, this first of its kind program is offered for the affordable price of approximately $16,000 and includes access to hands-on virtual labs, industry collaborations, and industry-reviewed curriculum, exclusive speaker events, and peer mentors.

In the Cyber Fellows program, the students are challenged to marry their life experience with the competencies they learn in the classroom to solve applied problems. The challenge not only helps to develop the next generation of cybersecurity problem solvers, it also teaches the students to differentiate between scientifically proved solutions and industry hype.

The two classes utilize a system name "peergrade" [2] to submit eight peer reviewed scaffolded submissions that lead to their final paper and presentation. TABLE I shows the scaffolded submissions along with the week they are submitted in the course. The process works by allowing the students to learn in several phases for each submission. They learn from; listening to the professors, doing the work, reviewing their peers, and reacting to the reviews.

The participants of this special track are all participants in the NYU Cyber Fellows program. The papers are the dissemination of solutions that are solved were developed and solved in the classroom. Aspen Olmsted is the professor and mentor for over one thousand students through these two classes each year. Andrew Zitek and Agam Dua are both maters candidates in the program. The professor and the students are also industry professionals. This life experience allows real work problems to be brought to the classroom for examination.

TABLE I. Research Scaffolding

Week	*Submission*
4	*Define Problem Domain and 3 Papers*
5	*Threat Model*
6	*Hypothesis and Differences from Current Solutions*
8	*Sampel Metric and Figure*
11	*Introduction Section*
12	*Related Work Section*
13	*Epirical Evidence Section*
15	*Presentation & Paper*

The organization of the paper is as follows. Section II describes the paper presented in the special session. We conclude in Section III and discuss the students' future work and how we will attempt to get more to disseminate their work at the conference.

II. SPECIAL TRACK PAPERS

There were over one thousand cybersecurity papers submitted in the past year by students in the Cyber Fellows program. Some students had terrific solutions but did not feel comfortable extending their work and submitting to the conference at this time. The first two submissions are from students in the program, and the third is from the professor.

Zitek and Olmsted [3] explore how traditional sensibility on how to assess preventative goods is underdeveloped, and consumers are left to trust suppliers who provide imperfect technology without guarantees. Typical consumers of cybersecurity tools cannot validate their expectations in terms of measurable security added, which has led to a market of tools that address only unsophisticated versions of known threats. Paying for these services may, in reality, introduce little risk and expense to an organization; however, the mental paradigm that is most advantageous is to assume they provide no protection. Classes of generic cybersecurity tools like web application firewalls will continue to be selected for the foreseeable future, where productivity-concerned

organizations are willing to buy any low-effort idea to reduce harm at an acceptable cost.

Dua and Olmsted [3] propose a model leveraging Bayesian Networks to help in the diagnostics of these systems during failures to considerably shorten the time to localize the cause of Service Level Objectives violations. As more organizations move critical infrastructure to the cloud and leverage features like auto-scaling to grow according to the customer demand, they outline the new set of challenges specific to the class of dynamic, distributed systems used to meet the demand. They develop a model that subsequently reduces the violation duration by reducing the Mean Time To Resolution.

Olmsted [5] explores how enterprise organizations have relied on correct data in business intelligence visualization and analytics for years. Before the adoption of the cloud, most data visualizations were executed and displayed inside enterprise applications. As application architectures have moved to the cloud, many cloud services now provide business intelligence functionality. The services are delivered in a more accessible way for end-users using web browsers, mobile devices, RSS feeds, and email attachments. Unfortunately, along with all the benefits of the cloud business intelligence services comes complexity. The complexity can lead to slow response times, errors, and integrity issues. An information technology department or service provider must get ahead of the problems by automating the execution of reports to know when availability or integrity issues exist and dealing with those issues before they turn into end-user trouble tickets. In this paper, we develop an Extensible Markup Language programming language that allows execution against many cloud documents and business intelligence services. The language enables issues to be proactively discovered before end-users experience the problems.

III. Conclusions and Future Work

Based on the student research's success, we demonstrate that applied Cloud cybersecurity problems can be solved by leveraging adult learners' life experience with competencies and research tools in the classroom. We plan to continue to push students to extend their work and submit to special tracks at the conference in future years.

References

[1] New York University, "NYU Cyber Fellows," [Online]. Available: https://engineering.nyu.edu/academics/programs/cybersecurity-ms-online/nyu-cyber-fellows. [Accessed 16 October 2020].

[2] peergrade ApS, [Online]. Available: https://www.peergrade.io/getting-started/. [Accessed 16 October 2020].

[3] A. Zitek and A. Olmsted, "Web Application Firewalls and Ways of Seeing Imperfect Tools," in *Proceedings of The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, Nice, France, 2020.

[4] A. Dua and A. Olmsted, "Using Bayesian Networks to Reduce SLO Violations in a Dynamic," in *Proceedings of The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, Nice, France, 2020.

[5] A. Olmsted, "Secure Business Intelligence Reporting Engine(secBIRpts)," in *Proceedings of The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*, Nice, France, 2020.