The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #43806

Increasing Faculty Cybersecurity Experience through Externship Experience

Dr. Walter W Schilling Jr., Milwaukee School of Engineering

Walter Schilling is a Professor in the Software Engineering program at the Milwaukee School of Engineering in Milwaukee, Wisconsin. He received his B.S.E.E. from Ohio Northern University and M.S. and Ph.D. from the University of Toledo. He worked for Ford Motor Company and Visteon as an Embedded Software Engineer for several years prior to returning for doctoral work. He has spent time at NASA Glenn Research Center in Cleveland, Ohio, and consulted for multiple embedded systems companies in the Midwest. In addition to one U.S. patent, Schilling has numerous publications in refereed international conferences and other journals. He received the Ohio Space Grant Consortium Doctoral Fellowship and has received awards from the IEEE Southeastern Michigan and IEEE Toledo Sections. He is a member of IEEE, IEEE Computer Society and ASEE. At MSOE, he coordinates courses in software verification, real time systems, operating systems, and cybersecurity topics.

Increasing Faculty Cybersecurity Experience through Externship Experience

Abstract

In modern world, cybersecurity has become an increasingly important field. Graduates with experience in this field are in high demand and receive a lucrative salary. However, preparing these students can be challenging. It is critical for faculty to have a deep understanding of the field. This involves not only the textbook theory, but also the workplace, work roles, and projects in which their students will be involved. Only through adequate integration of this material into the classroom can we produce graduates who are well-equipped to meet the demands of the modern workforce.

In this article, a faculty's perspective on the NCyTE externship program will be presented. The NCyTE Program supports faculty members in updating their technical skills and staying current with the latest workplace trends through a paid externship experience. The article will discuss the overall experience, the challenges in setting up the experience, and some of the outcomes from the experience.

Introduction

One of the most important things for faculty to have in the classroom is relevant experience in industry. Those starting in the engineering discipline are fresh out of university and may have had significant internship experience during their undergraduate study. As faculty advance, however, their experience in industry often ages. This is especially true in the computing field.

Graduates of academic cybersecurity programs, like many other engineering programs, are highly sought-after by industry and will be entering into applied fields. It is thus essential for faculty to have a comprehensive understanding of the current workplace, work roles, and projects. The NCyTE Externship program offers faculty an immersive experience in a real-world setting targeting the area of cybersecurity. Faculty work on-site for 80 or more hours experiencing what a student would see as an employee of the given company. They then receive a stipend for their time with the intent that the observations and learnings from the externship can be applied in the classroom.

Faculty Members Background

Having had nearly 6 years of experience in industry prior to completing my PhD., I was quite aware of industry and the need for cybersecurity expertise. This need was readily apparent as a major aspect of multimedia systems design revolved around anti-theft, a form of cybersecurity relevant to automotive systems. This background has contributed to presentations on cybersecurity, such as Big Data, Cyber Security, and the Lure of the Open Road [1] and Cybersecurity and the Lure of the Open Road [2], which looked at the past, present, future needs of the automotive industry for cybersecurity expertise through the lens of autonomous vehicles.

While these presentations and interactions have been worthwhile, what has fundamentally been missing is direct interaction in the corporate world. The needs of industry are often much different than the textbook solutions presented in class. To prepare our students to go into industry, it was important to have current, relevant domain expertise.

To obtain this background, it was important to go into the externship partially in the shoes of a new employee. While my training is more in depth than a student starting an internship or first full-time technical position, I wanted to try and identify the gaps in our outcomes that would be noticeable to a new employee by going through, as much as would be possible, the onboarding process for a new employee to the organization. This was a key goal. While our students leave from an accredited program, the program criteria leave wide latitude to individual institutions.

Beyond this introductory goal, I also wanted to find out the depth and applicability of existing certification methods in industry. As an academic advisor, students are often asking about online credentials and certifications that they can earn outside of the classroom to help their understanding of cybersecurity. I wanted to experience some of these certifications myself and evaluate how useful they are in the industrial setting.

Most importantly, I wanted to see firsthand how modern software is developed and the technical practices employed to ensure appropriate security is built into the product as it is developed and deployed. This outcome most directly relates to the DevSecOps course that is under development for the software engineering program.

My initial goal was to also try and answer these goals in the scope of more than one organization. In training prospective students, there is a danger in developing course outcomes which are overly specific to a single entity. For example, to develop cybersecurity material that is aligned with the automotive industry would easily align with my background, the material itself might lack applicability to one entering the financial services sector or healthcare sectors. As an institution, it is important to serve all our students, those going to software engineering positions with local businesses, those going to Fortune 100 leaders in the Tech sector, and also those going onto graduate school.

Identification of Corporate Externship Site

The first challenge that I faced was finding appropriate partners to work with. While our program's advisory boards have more than 30 members between the software engineering, computer science, and computer engineering programs, the summer timeframe made things quite challenging. By the time I received news of the externship, most companies had already set up their summer internships and summer programs, and many did not have the capacity to expand their programs to accommodate an extra faculty member.

A second challenge that I faced is that while the intent of the externship was to be in person in an office setting, many of the offices in the local tech sector are still predominantly remote. This is especially true of the cyber security related organizations, as the pandemic caused many companies to hire remote workers who have never set foot into local business offices. This is changing, and many software engineers are beginning to return to the office, but overall, it is not ubiquitous.

I finally ended up adjusting the scope to work with a single partner, headquartered in Chicago but with a local Milwaukee Office, that provides consulting services for companies undergoing digital transformations. I worked directly with the Vice President of DevOps and Cloud applications and was able to sit in on multiple meetings with high profile customers across the business spectrum, as well as working with other employees to observe SCRUM standups, sprint reviews, customer trainings and customer status meetings, and technical reviews. In the past, we have also had alumni either intern with the company or work full time after graduation.

Lessons Learned: Computer Organization and Infrastructure

My externship experience technically started with a tour of a super computing facility. The key takeaway from this visit was the need for students to understand supercomputing infrastructure and risk management. While our students are exposed to computer organization, and our computer engineers are exposed to computer architecture, neither program has a solid understanding of the infrastructure needs for a modern data center. While the computing resources that we teach in our program are important, the main design challenges for the site involved device cooling, auxiliary power capabilities, and data backups.

From the cooling standpoint, modern devices are changing so quickly that not all devices are able to be liquid cooled. This is especially true of GPU devices. Thus, in many cases, the challenge to deploying super computers is not computing power but keeping the computing power from overheating in a managed way. The rapid pace of change also impacts warranty issues, as it is very difficult to maintain a supercomputer that is just a few years old and quite costly to do so. Even devices as new as 3 years old may not be supported by the vendor, requiring costly upgrades just to continue routine / normal operation.

From the power resiliency standpoint, it is essential that the data center be self-sufficient from a power standpoint. This data center does not rely on solar power or any form of green energy, but rather relies on a large generator plant that is larger than many moderate sized houses. This generator plant has proven essential, as the grid supplier has needed to perform load balancing at times this summer, resulting in the need for the backup generator bank to fully power the data center through a pseudo rolling blackout.

From the data resiliency standpoint, I also observed in operation a tape backup robot. Due to the research-intensive nature of the center, data integrity and resilience is essential. To help achieve requisite goals, the center hosts two data backup robot systems, one on site and one offsite, which constantly backup the more than 14 Petabytes of file storage within the center, proving further resiliency in the case of failure.

While the material learned is not currently integrated into our programs, observing this environment does lead to the question of should our students be exposed to this material as they learn about computer organization. Traditional computer organization typically stops at the level of power utilization versus frequency and voltage – a very microscopic scale – relative to this larger scale problem. Traditional computer organization also focuses a lot on the individual processor and does not even venture into the GPU versus CPU performance differentiation problem.

While this was not the key piece of the externship and did not result in the initial planned depth, the experience was useful.

Consulting Company Experience

The bulk of the externship consisted of a two-week experience with a major consulting company in the Milwaukee area which focuses on software development and resilient deployment of software systems.   Because of the nature of the organization, the setup was hybrid in nature, with roughly 1/3 of the time being onsite and 2 / 3 being remote via Microsoft Teams.

User Security Policies

The experience began with an overview of the organization’s User Security Policies. This document, part of employee onboarding, defined the policies a new employee is to follow when working with client records. It is a general policy – not targeted to those in technology – but which must be understood by all corporate partners and be usable across domains.

The key finding from this document is that students of all disciplines need a general understanding of rudimentary cybersecurity terminology. While many of our students are exposed to VPN's through their internships, the proper usage of them and their risks is not something built into our engineering curriculum, with the exception of students who enroll in our network security elective.

There also is a strong ethical aspect of this work. As a consulting company, employees are directly connected to clients' networks, either through remote access, or preferably, client supplied devices which are maintained by the client's IT organization. This environment places employees in potentially ethically challenging environments, as it is likely they may identify potential vulnerabilities inside of a client's environment that could be exploited by an external entity. However, the company is not authorized to investigate or fix these issues. Thus, a strong culture of reporting issues that are identified through supervisors must be established. While our students do take an ethics course, the need for a deeper understanding of ethics related to cybersecurity is paramount. This concept is one that is planned to be addressed in the DevSecOps course for our Software Engineering majors but is not directly addressed within our computer science program, as the ethical component addressed focus more on big data sets and data analytics.

Certification and Training

As part of my exposure to the consulting company, I was able to sit in on training sessions and the development of training material for clients. One of the products which the company supports is a zero trust, hub and spoke architecture for constructing software intensive systems. This architecture allows organizations to slowly migrate enterprise systems from on premise to cloud-based deployments. To support their clients, however, they often were required to provide training to the organization's IT staff. As part of my tasks, I investigated the quality of some of the pre-requisite training material used to bring clients up to speed.

From a training standpoint, I completed three online certificates through Linked-In Learning. The first certificate, Azure Essential Training for Developers, provided an overview of the Azure environment, essential for anyone working in the software engineering or IT fields to support these systems. The second certificate, Learning Threat Modeling for Security Professionals, dealt with cybersecurity and threat modeling techniques used in industry. It is directly relevant to the DevSecOps course we are developing as well as to the consulting company, as the company requires a strong zero trust architecture. The last certificate, IT Security Foundations: Network Security addressed network security and mirrored, at least in concept, the course I teach in Network security.

Overall, I was extremely disappointed in the depth of material present within these certification courses. While I am certainly more knowledgeable than many, the assessment quizzes were overly simplistic, and overall, the courses lacked substantial rigor and depth. In talking with my corporate mentor, this was also a feeling he expressed, that many online certifications and courses do not provide potential employees with required skills to be productive in the engineering discipline, especially as is related to cyber security.

This also influences my advising of students and, to some extent, the evaluation of faculty candidates. As an institution, we have been trying to increase the depth in our cybersecurity faculty. While not often, we have had a few faculty list significant certifications on their Vitae in lieu of formal training. I personally have been skeptical of that without in depth research, and this experience has increased my concern in this area. I think there are certainly rigorous certifications out there and rigorous credentialing mechanisms, such as the IEEE Associate Software Developer, Professional Software Developer, and Professional Software Engineering Master certifications, but overall, many certifications lack rigor and depth.

From sitting in on some of the training and technical meetings with clients, it was clear that the clients needed this corporate training, as many of those in the IT organizations lacked formal training in the discipline. The training provided by the company to clients was high quality and clearly applicable, but also showed the extreme shortage of technical talent within the Midwest.

Student Teaching Platform

Prior to this externship, we had tentatively designed Azure DevOps as the platform to use for instruction in our DevSecOps course. This decision was made based upon several factors. In reviewing our advisory board members' responses, Azure was viewed as an important toolchain for the development of robust software solutions. In completing this assignment, it became clear that from an industry standpoint, the Azure environment made the best sense for our students, as it offers a robust, enterprise grade solution which is both intuitive and extensible, as well as being remarkable well documented and supported by the vendor.

This poses a teaching challenge from the administrative standpoint. While Google Cloud and AWS offer extensive programs for faculty members to teach the offering in the educational setting and are thus easy for a faculty member to manage, Azure with its billing model and tenant support requires much more extensive campus IT involvement. On our campus, we have fully embraced Microsoft SSO and its credential management platform, which is good. But it also now requires more support from our campus infrastructure organization to allow students to use their credentials for Azure and to have appropriate permissions to build and deploy their software. While I am currently using Azure with my senior design projects, being exposed to Azure in the corporate environment – and the strong tenant credential management capabilities built into the product – has really shown the true flexibility of the tool. While it was personally disconcerting to have access to private corporate repositories in the manner I did, it was also very promising to see what can be done with modern engineering tooling.

Future Directions

Having completed slightly more than 80 hours of externship work, I am very happy with the knowledge that I both received and reinforced through my experience. My external corporate mentor will be continuing membership on our industrial advisory board, and there is potential for future collaborations.

In the immediate timeframe, I have taught an elective version of my DevSecOps course in the spring prior to it becoming a required course in the curriculum. The experiences of the externship directly impact this. While I have always intended to discuss the security ramifications of a microservice based architecture, I can see the advantage of incorporating a hub and spoke architecture and discussion of zero trust architectures in the course. I also feel that many of these topics should be incorporated into our Architecture and Requirements course, taken by Junior students in the fall semester.

Going forward, this exposure has also made clearer the need for our institution to offer some form of a cybersecurity minor / option to engineering students. It is clear from completing the online certificates that there is a lack of rigor that can be compensated for with formal educational training, as our courses are very hands on and lab intensive. This input, and other experiences, led to the enactment of a new cybersecurity minor, which when coupled with our software engineering program, becomes very close to meeting the requirements for the COE-CD and COE-CO programs. This complements our other engineering programs and helping to further decrease the significant shortage of qualified cybersecurity talent in the Midwest.

References:

[1] W. Schilling, *Big Data, Cyber Security, and the Lure of the Open Road,* Milwaukee: Data Driven Milwaukee, 2019.

[2] W. Schilling, *Cyber Security and the Lure of the Open Road,* Milwaukee: Cyphercon, 2024.

Acknowledgements

The NCyTE Externship program, facilitated by Sinclair Community College, supported this experience.