Supervising Undergraduate Cybersecurity Projects

Prof. Aaron Carpenter, Wentworth Institute of Technology

Professor Carpenter is an Assistant Professor at the Wentworth Institute of Technology. In 2012, he completed his PhD at the University of Rochester, and now focuses his efforts to further the areas of computer architecture, digital systems, cybersecurity, and computer engineering education.

Prof. Raymond A. Hansen, Wentworth Institute of Technology
As cybersecurity grows as a specialty within electrical and computer engineering and computer science, students increasingly choose to pursue projects in the area. These projects come in the form of class projects, senior design/capstone projects, and extracurricular research of varying degrees of difficulty and sub-genres of cybersecurity. However, it is easy for these cybersecurity projects to put students in danger of violating laws or compromising equipment; thus, it is critical for faculty to properly guide and moderate these projects. While each project may be from a different subcategory of security, some general rules and tips can help maintain order for the undergraduate student teams.

In this paper, two faculty members (one in Electrical and Computer Engineering, one in Computer Science and Networking) describe their efforts to create, supervise, and guide these cybersecurity projects at Wentworth Institute of Technology. The majority of these projects have come from senior design courses and security-related final course projects. Each project was largely student-driven, inspired by the relevant course, student interests, and their level of expertise and resources. The challenge for the instructors/supervisors then was to keep the students from hurting their own systems or putting themselves in danger of breaking a law (for example, hacking into a private or government system), while also ensuring that the students are operating in a realistic and contemporary environment. This second point is especially difficult as students must see cybersecurity outside of small exercises and apply their skills in a realistic manner.

The authors will review the types of projects that students have completed in the last four years at Wentworth Institute of Technology. These descriptions will include details of the projects and the technical and ethical challenges that accompanied each. These tips and best practices are intended to provide instructors with a starting point as these types of security projects become more prevalent across undergraduate education. The descriptions will also detail the level of project that students of various backgrounds and class levels can accomplish within the cybersecurity field without monetary resources or years of experience. This work will provide new instructors and project supervisors information to guide similar projects, paving the way for much needed cybersecurity professionals to gain valuable experience during their undergraduate education.
1 Introduction

Digital components are ubiquitous and widely integrated, including smart phones, tablets, laptops, servers, smart-home devices, etc. all networked together, leaving myriad vulnerabilities within the hardware and software. Industry increasingly needs designers that can build systems with security as a first-tier design priority. Universities, meanwhile, are in the early stages of creating degree programs and other opportunities to better prepare future security engineers for the workplace. Unfortunately, providing security-centric projects in an undergraduate environment is a daunting task. Students require several key things before starting: a baseline knowledge of security and the systems and components they will be studying; the ability to identify the ethical and professional obligations of a security engineer in a given design process; hardware and software resources to execute the project goals; a safe way to test; and protection for all parties involved to ensure legal and ethical lines are not violated. Further, large-scale security projects rarely come with a tutorial process that students can follow. This makes scaffolding for security projects difficult.

At Wentworth Institute of Technology, several security classes are being taught across several departments. In this paper, faculty from the Electrical and Computer Engineering department and the Computer Science and Networking department discuss their process in supervising varied security projects, including hardware security, network and digital forensics, senior design/capstone, and research projects, all exclusively with undergraduate students. The paper will review the infrastructure provided to the students as well as describe the successes and failures of past experiences. Some of the projects will be described with sufficient enough details to allow similar projects to be repeated. An instructor in the appropriate technical fields (related to CS and/or ECE) will be able to:

- Structure student projects in a cybersecurity environment for ethical, professional, and legal guidelines;
- Choose, design, and supervise design goals for various cybersecurity projects;
- Identify possibly pitfalls for security project teams; and
- Evaluate the success of a particular project.

Overall, this paper will allow instructors across disciplines to incorporate security projects into their curricula, better providing hands-on experience to undergraduate students and preparing them to be contributing members of the cybersecurity workforce and community.

Wentworth Institute of Technology is a STEM-focused, undergraduate-centric university in Boston, Massachusetts. The student body primarily studies engineering, applied sciences, and architecture and construction fields. Class sizes are typically small, averaging around 20-25 students per class, with no teaching assistants.

The rest of this paper is as follows: Section 2 describes related work in the field of cybersecurity and security education. Section 3 describes the efforts to provide security projects through a variety of courses and extracurricular projects, including successes, failures, and recommendations for the future. Section 4 aggregates the lessons learned and recommendations for future undergraduate cybersecurity projects. Section 5 summarizes and concludes.
2 Related Work

Cybersecurity’s recent popularity in academia has created a wealth of publications, specifically regarding course and curricular designs [1, 2, 3, 4, 5, 6, 7, 8, 9], and the incorporation of ethics [10, 11], and more. Further development has been done for teaching secure computing [6, 7], embedded systems [5], or broad security curricula [3].

The work presented in this paper is not focused explicitly on curricula for security-centric classes, although some portions of curricula will be shared as needed. Instead, this work focuses on the creation, design, and execution of security-based projects for undergraduates. These types of projects have been described in previous work, most recently in [12]. The work presented here goes further than [12] in describing the details of a broad collection of projects.

Ethical and professional responsibilities are often raised as a concern. Ethical engineering and professional behavior are discussed across engineering education and are often subject to entire course curricula [10, 11]. The work described in this paper does not add to the description of ethics and hacking but does require a basic understanding of security ethics between instructor and students before the project can begin.

Project-based learning is widely considered an effective tactic for reinforcing concepts and introducing new skills to students of all levels [13, 14, 15, 16, 17, 18]. This paper relies on past understanding and acceptance of these now widespread ideas and contributes to the field, specifically in cybersecurity.

While several papers have shown at least the incorporation of project-based learning into cybersecurity or of cybersecurity into project-based courses [12, 1, 7, 5], few have described a broad approach for many students in different courses and class levels with a wider perspective [12]. The work presented here will describe how students at an undergraduate-level can obtain valuable hands-on experience in cybersecurity.

3 Projects

In order to properly contextualize the different approaches within different class or extracurricular environments, we will break the discussion into pieces. Each subsection will describe the course or research structure for which the projects were completed. Each description will be accompanied by the individual opportunities and challenges inherent to that environment, as well as example projects and recommendations for future efforts.

3.1 Electrical & Computer Engineering Senior Design

3.1.1 Course Description

Senior design or capstone projects typically involve 2-4 students working on a 2-semester-long project of their choosing. The course’s main goals are (1) to act as a culmination and application of a student’s engineering education and (2) prepare students for long-term projects more akin to a work environment. This includes project and team management, documentation, presentations,
and of course, individual and team technical work. At Wentworth, the ECE department has a 2-semester course that fits this mold. Teams of 2-4 students choose their own project with a professor’s guidance and typically their own self-provided budget. The professor’s responsibility is to keep the team on-task and on-time and contribute technical guidance.

The students have eight months split into two semesters to complete their project, and for the sake of this work, only the security-centric activities and issues will be discussed. More general senior design discussions are left for other literature sources.

### 3.1.2 Example Projects

In the last three years, there have been six projects directly exploring cybersecurity. At the time of publication, another four are in progress (but will be left out of the paper, as they are incomplete). Table 1 lists the topic, summary, and particular challenges and successes for the projects. Most of the following projects are related to the fields of electrical engineering, computer engineering, and computer science, with a few being interdisciplinary.

If the students had some background in their area or a strong technical advisor, had free or inexpensive equipment, and/or clear initial design goals, they were largely successful. In these cases, success was not necessarily a fully-tested and functional hack or secure patch. Because the goal of senior design is part project management and part technical achievement, success varies. For some teams, it was completing or surpassing their initial goals. For others, it was a more piece-wise proof-of-concept, with parts of the system working properly but possibly missing a key component or program. For all, success was forward progress towards the integration of their knowledge in engineering concepts with those of cybersecurity.

The most successful senior design projects had clear visions of how to accomplish their goals because they were similar to existing projects. The passive entry key hacking project was similar to other published work [19], as were iPhone acoustic side-channels (based on acoustic mechanical keyboard attacks [20]), and non-invasive VGA cable hacking [21]).

The on-chip network protection project was also very successful but for a different reason. In this case, the supervising professor had significant experience in on-chip interconnects and had supervised graduate students doing similar projects in the past. This meant the team had a credible source throughout the project to fill in gaps as needed.

These projects were largely successful in regards to their original goals. However, teams tended to miss their initial design goals at common points. Students that lacked the required technical expertise (e.g., wireless communication, RFID) had to learn cybersecurity and technical ECE concepts at the same time, taking more time and energy. Also, simple lab equipment sometimes fell short in the required capabilities. Student teams without credible and available resources often spent more time learning than doing (although this is not necessarily a purely negative outcome).

### 3.1.3 Challenges & Opportunities

**Challenge - Ethical discussions:** In this course, the lectures and activities revolve around broader project requirements, as there are 20-30 students working on 10 different projects. Thus,
<table>
<thead>
<tr>
<th>Project</th>
<th>Summary</th>
<th>Successes</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker Agnostic Security for On-Chip Networks</td>
<td>In a chip multiprocessor, dynamically throttle/redirect network traffic to limit the effects of a malicious program’s on-chip denial-of-service (DoS) attack</td>
<td>Created working adaptive algorithm for 16-core system; modeled attacker DoS in simulation</td>
<td>Learning entire CPU simulation tool chain in multiple languages in a timely manner</td>
</tr>
<tr>
<td>Media Automation Security using Speech Signatures</td>
<td>Create/use voice and speech recognition to identify users and securely switch user accounts with voice signatures</td>
<td>Learned speech and signal processing; able to identify keywords</td>
<td>APIs were not well-suited for this application and eventually new interfaces from commercial products were released</td>
</tr>
<tr>
<td>Voice Mimicry to Hack Voice Authentication</td>
<td>Shift one person’s voice signature to match that of another speaker, faking a person’s voice in real-time</td>
<td>Successfully mimicked voice well enough to fool Siri; students learned about acoustics, speech, signal processing</td>
<td>Difficult to scale up to many words/voices without more extensive background in speech, acoustics, and signal processing</td>
</tr>
<tr>
<td>Non-Invasive VGA Cable Hack</td>
<td>Without splicing the cable, read electromagnetic emanations from a VGA cable, interpret waves, and reconstruct original screen image at a remote location</td>
<td>Successful proof-of-concept; could read colors of large geometric areas</td>
<td>Shielding on VGA cable required more sensitive/expensive sensors or removing the shielding; needed faster sampling rate than offered by the DSP hardware provided by the lab</td>
</tr>
<tr>
<td>Passive Keyless Entry Spoofing</td>
<td>Read the signal from a passive keyless entry key-fob, record the signal, and recreate it to break into and start a car</td>
<td>Used red/blue team to create and hack various system levels, including proximity sensing; found protective solution for remote attacks</td>
<td>Difficult for undergraduates to find manufacturer specifications and to recreate signals; keys and related systems are expensive</td>
</tr>
<tr>
<td>iPhone Acoustic Side-Channel Attack</td>
<td>Use the timing and sound of “clicks” from iPhone keyboard to covertly discern what user is typing</td>
<td>Capture and analyze acoustics; use learning algorithm to train system to figure out user timing of typing (two thumbs); accurately distinguish between 2-3 predetermined phrases</td>
<td>Requires a lot of training for each user; beyond a few keywords/phrases, prohibitively difficult to analyze; must use standard grammar and sentence structure (not often true on mobile phones)</td>
</tr>
</tbody>
</table>

Table 1: Senior design projects accomplished by student teams from 2016-2018.

Lectures include how to brainstorm, how to document, conflict resolution, and engineering ethics. There is scarce time to have more targeted lecture content that would benefit just security-based projects. The ethical and professional discussions provide some foundation for all teams and thus would be applicable to the security-centric project teams. Additionally, students working on a cybersecurity project must discuss with the supervising professor all aspects of the project and sign a contract agreement (reviewed by institutional legal counsel) stipulating that the project activities will be confined to the course’s guidelines and will not be used for any nefarious or entertainment purposes. This is done to protect students, the instructor, and the university, ensuring everyone involved understands the dangers of trying to hack commercial products or build security into existing systems.
**Challenge - Cybersecurity concepts:** As previously mentioned, students in this class are not receiving technical lectures in security. Some may have taken other cybersecurity courses, as will be discussed later. But generally, students will rely on their own searches and any technical advisors (e.g., the supervising professor, outside consultant, or another professor/researcher in the school). This can be a heavy undertaking for many students. If the professor does not have a background in the field of cybersecurity or at least an expertise in the concepts required, students will need to find another source. With many senior design projects, students rely on various web sources to find tutorials on aspects of the project. For example, students often buy Arduino or Raspberry Pi devices and then find free code online. With cybersecurity, researchers are understandably hesitant to give out information that could lead to people exploiting vulnerabilities in devices. The exception is when the original hack has been patched by the manufacturer or designer of a part/system. This means that students will either have to explore the project with less guidance or rely on parts that are no longer state-of-the-art. This will require independent research on the part of the students and a commitment from the supervisor to find sources.

**Challenge - Resources:** In terms of hardware and software resources, students have two options: use what the school/department can provide or buy their own parts. This likely varies by university and department, as some lab spaces may be better equipped for security projects, and some students may be able to find funding besides themselves. For the sake of this discussion, we will assume students have access to basic ECE lab equipment (oscilloscopes, digital multimeters, function generators, breadboards and basic components, etc.) and have some student-sourced budget around $100-200. Over time, it would be useful for departments to gather more security-specific tools and equipment, if budget allows.

**Opportunity - Real-world environment:** With class projects, students sometimes struggle with placing the project within the scope of the real-world. In cybersecurity, it is often beneficial for students to understand at a deeper level how the adversarial challenges factor in; this is hard to do in short projects that focus on simpler concepts. In senior design, the time period helps students potentially go through multiple cycles of hacking and then reinforcing the system. In large enough teams, it is even possible to mimic the red/blue teams used by cybersecurity professionals. In this model, one group is attempting to hack into a device or system while another group tries to then protect the same system. This can be done in cycles to create a more secure final product. It is also more in line with how a professional cybersecurity project team may work.

**Opportunity - Unconstrained goals:** The freedom allowed by senior design also allows more curiosity-based research. Students, again with supervisor oversight, can explore a particular system, probing for vulnerabilities. Students then start with a target in mind, but they can adapt as new information and analysis become available through experimentation. For example, if a student is attempting a side-channel attack, they may find it easier or harder to accomplish. The less constrained curriculum in senior design allows them to pivot and adjust their target to account for new findings. This would be harder in shorter-term projects, as will be discussed later.
3.2 Hardware Security Course

3.2.1 Course Description

Wentworth offers a technical elective once a year called Hardware Security, which has been discussed in previous work [12]. As part of the course activities, students engage in a number of hands-on labs and a project. The labs take roughly 1-2 hours, while the project is intended to be worked on all semester and is the focus of class activity for the last 2-4 weeks.

The laboratory assignments are used for conceptual reinforcement in various cybersecurity topics, such as cryptography, side-channel attacks, and watermarking. The labs are given to students with itemized instructions and have been fully-tested prior to be given to the class. These are not projects but provide hands-on experience for the students. The main difference between these labs and the project is that labs are well-structured, while the project is open-ended.

For the project, students form teams of 2-4 people, and the team chooses a topic. In this case, unlike senior design and research, students are not pioneering new cybersecurity exploits or protections. Rather, they find a published source in the research literature and must reproduce some portion of that work. Examples are given in Table 2. Students present the source material to the class, partly to ensure they fully understand the work and the efforts and resources they will need in order to complete the project. The team also meets with the instructor for guidance and feedback.

In the three times the course has been offered, there have been 29 projects by 71 students. Listing each would be lengthy and redundant and so only particular projects were chosen, either because of their use as exemplars or as cautionary projects. Table 2 gives these examples. Most of the following projects are related to the fields of electrical engineering, computer engineering, and computer science, with a few being interdisciplinary.

3.2.2 Example Projects

Many of the described projects are actually recommended by the instructor, largely because it is possible to accomplish with simple equipment/software while still providing a challenge. The most difficult projects are typically the ones with limited resources or ones that cannot be safely or easily tested in the laboratory space.

3.2.3 Challenges & Opportunities

**Challenge - Time and Resources:** The most frequent issues that students encounter in the class project, as with senior design, tend to be time and resources. In the case of senior design projects, students have more time to find, order, and learn components. For the course projects, students are often lacking the components. Typically these include antennae and associated communication hardware, microcontrollers, and computing systems. As for time, students must be motivated to do continual work through the semester to maximize their time. Guided choice of projects from the instructor can help mitigate this issue.
Table 2: Examples of hardware security final projects completed by students from 2016-2018.

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary</th>
<th>Successes</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth Hacking</td>
<td>Attempt to take control of a remote device through its Bluetooth connection</td>
<td>Learned communication and had working Bluetooth scripts</td>
<td>Bluetooth has undergone improvements in security, so resources were outdated</td>
</tr>
<tr>
<td>Laserjet Printer Side-Channel Attack</td>
<td>Read electromagnetic emanations from laser diode in a printer to non-invasively read what is being printed</td>
<td>Student understanding of electromagnetics and EM devices</td>
<td>Lack of proper antenna, understanding of spectrum analyzer, and laser printer (suitable for disassembly) prohibited forward progress</td>
</tr>
<tr>
<td>Covert Channel in an Air-Gapped Computer</td>
<td>Using either fan speed or hard drive indicator LED, leak information from within a computer otherwise disconnected from surroundings</td>
<td>Successful manipulation of chosen covert device and leak of test key</td>
<td>Difficult to get entire integrated system, malware to vulnerable device; optical or acoustic noise reduced captured signal integrity</td>
</tr>
<tr>
<td>Acoustic Keyboard Side-Channel Attack</td>
<td>Capture sounds of mechanical typing on a keyboard; reverse engineer sounds to reveal what is typed</td>
<td>Can use existing sound software and MATLAB to do most experiments; can successfully distinguish between a small number of key presses with accuracy</td>
<td>MATLAB and signal preparation and processing may be too difficult for students earlier in their education</td>
</tr>
<tr>
<td>RFID Spoof or Jammer</td>
<td>Read, spoof, and edit content of an RFID chip/card</td>
<td>Can remotely read cards/chips and write new information</td>
<td>Students can largely follow tutorials; most RFID chips have some level of encryption, so practical application is infeasible in short time-frame</td>
</tr>
<tr>
<td>Van Eck Phreaking</td>
<td>Leak information from a system through the electromagnetic emanations from a laptop screen</td>
<td>Able to leak information and capture using simple radio</td>
<td>Students can largely follow tutorials, may be overly simplistic</td>
</tr>
</tbody>
</table>

Opportunity - Application of course material:  Most students choose to directly apply the concepts and skills acquired in the class. This presents them with the confidence to enter into future projects or jobs that involve cybersecurity.

Opportunity - Explore new material with minimal risk:  If the students decide to do a project outside the material covered in class, the project provides them with that platform. The activities for the project mimic those of past researchers, so the knowledge already exists, thus provide students with the opportunity to explore beyond class material.

Opportunity - Ethics:  Because the entire class is devoted to cybersecurity, several lectures were focused on the ethics of hacking and security. This ensures that students understand the spectrum of legal and ethical problems that arise in the field of security and force the discussion of white-hat hacking. This provides students with a stronger foundation of professional and ethical responsibilities, both in and out of the security field.

The most successful projects typically fell into two categories: projects that the instructor recommended based on prior experience and known available resources; and projects that
students found and put a lot of time and effort into exploring independently. In both cases, the students began the project with a level of confidence and knowledge, and they did not reach too far beyond their grasp in terms of knowledge, skills, and resources.

3.3 Undergraduate Research

There are myriad sources discussing the world of undergraduate research, so this work will focus instead on cybersecurity-specific undergraduate research.

3.3.1 Description

At Wentworth, there are no on-campus graduate students and instructors typically focus on teaching, with scholarly activity being a smaller, but still significant, component of their effort and time. Thus, undergraduate research is typically done by a few junior/senior students as a co-op or as extracurricular during a semester. In the three years of this paper’s scope, one instructor has run two significant research projects with three students, both related to the same topic. (At the time of submission, another project has been undertaken).

In general, students spend their time doing simulations, literature research, data gathering, and analysis along with the supervising professor. This includes meetings at least a few times a week and frequent communication. Lab resources vary based on project, but in this case, the students only required a laptop and access to the university’s server resources.

3.3.2 Projects

Three students participated in two closely related projects. The first was an exploration and comparison of physical unclonable functions (PUFs) and their potential use in a microprocessor. Some of this work was done at Binghamton University under the supervision of the author, with the completed project being presented as a poster at a conference[22, 23].

Physical unclonable functions are circuits on a chip that produce inherently random numbers based on unpredictable variations in the devices. The research done here was to explore their potential use in dark silicon chips, where large percentages of the chip are powered-off. These PUFs would then take up some portion of the “dark” chip, providing unique random numbers for possible cryptographic functions or authentication. Much of the research for the project done by the undergraduate at Wentworth required reading, organizing, and understanding previous work, as well as doing independent calculations and analysis.

The second phase of this project involved the use of on-chip caches within microprocessors as PUF devices, as the first part of the project confirmed that SRAM cells are suitable. Two students used a microprocessor architecture simulator to investigate the performance impact on the processor. This project resulted in a technical report prepared by the students and supervising professor.
3.3.3 Challenges & Opportunities

**General research issues:** As with most undergraduate research, the projects hinge mostly on time and effort, as well as not repeating other researchers’ work. Additionally, teaching students gaps in their existing knowledge takes time and delays research. These are challenges for all research, not just cybersecurity projects. Similarly, opportunities for cybersecurity projects are the same as for general research, with students doing high-level work and contributing to the research community.

**Challenge - Suitable testing platforms:** In these projects, finding a reliable, research-level testing platform was a challenge. Cybersecurity is a newer paradigm in many facets of electrical and computer engineering, particularly within computer architecture; thus, the tools to do evaluative and exploratory research requires retooling existing simulators. The dearth of credible, widely-distributed and widely-used research tools is an issue in many fields, and thus needs to be thoroughly vetted before students are brought into the research project; otherwise, the students are at risk of accomplishing little in a short time-frame. A possible suggestion is to do the project in phases, with the first phase being students finding or developing a verifiable testing infrastructure which can then be used repeatedly for projects. Similarly, pairing with a graduate or industry research partner with an existing infrastructure would expedite this portion of the research.

**Opportunity - Cutting-edge hands-on experience:** Research in any field has the potential to have a significant impact on the community and on the researchers. In this case, as cybersecurity is a relatively new design track, students have a distinct opportunity to have an impact in a novel field.

Overall, if the research infrastructure can be in place before students join the research group, the opportunities will outweigh the challenges.

3.4 Network Security Course

3.4.1 Course Description

Wentworth’s Department of Computer Science and Networking offers a required course once per year called Network Security. As part of the required course activities, students engage in a number of hands-on laboratory and an individual final project. Each of the laboratory projects is expected to require 10-12 hours over two or three weeks, while the final project is intended to require 20 hours over the second half of the semester. This project has incremental deliverables beginning 5 weeks prior to the final deadline.

The laboratory assignments are used for practical and hands-on reinforcement in various cybersecurity topics that were presented in lecture. The typical set of laboratory projects involve firewall rules and architectures, intrusion detection and prevention systems, virtual private networks, proxies, and SIEM (security information and event management) systems. Examples are shown in Table 3. These projects are given to students with a business case of a fictitious organization and their requirements. Any significant operational considerations are detailed, such
as specific tools or applications. The solution set for each deliverable is fully-vetted prior to being issued to the students to ensure the proper desired outcomes are possible. These laboratory projects are not guided tutorials, forcing students to use the information that was presented during lectures and in the project description to identify and implement the project solution(s). This is designed specifically to reinforce the theory and practice described in the lecture component of the course.

For the semester project, each student is expected to undertake an investigation of a topic that has piqued their interest. Occasionally, students are allowed to work in pairs if they have a compelling case for doing so. It is not the intent that students are identifying new cybersecurity vulnerabilities, exploits, or even developing novel defensive approaches. Rather, they examine sufficient materials in published literature to be able to fully describe a specific problem. Based on that documented issues, students then attempt to recreate part, or all, of that scenario, depending on the scope of the project. Examples of these projects are shown in Table 4. Most projects are within computer science and networking and use limited interdisciplinary concepts. Upon completion of the project, each student records a 10-12 minute presentation that includes all necessary background information, a demonstration of their project, and a lessons learned statement. This presentation is to ensure they fully understand the work, are able to communicate effectively on a technical topic, and are able to clearly articulate the challenges and pitfalls that they experienced.

3.4.2 Example Projects

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary</th>
<th>Successes</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Architecture and Rules</td>
<td>Deploy foundational FW architecture and rules on proper interfaces using OPNsense</td>
<td>Understand proper packer flow and filtering techniques</td>
<td>Use of virtualized environment and interface definitions is perplexing to some students</td>
</tr>
<tr>
<td>IDS/IPS Deployments</td>
<td>Implement intrusion detection and prevention system (Suricata) to filter specific types of traffic</td>
<td>Able to monitor specific events occurring within the network</td>
<td>Use of integrated IDS in OPNsense lacks clarity of IDS vs. IPS mode</td>
</tr>
<tr>
<td>IPSec VPNs</td>
<td>Deploy both site-to-site and remote access IPSec VPNs</td>
<td>Provide secure, encrypted tunnels for different business needs</td>
<td>The web interface for the VPN solutions oversimplifies the requirements of the tunnel for students not focusing on the requirements</td>
</tr>
<tr>
<td>Proxies for Network Traffic</td>
<td>Invoke appropriate traffic proxying, filtering, and redirection according to use cases</td>
<td>Identify legitimate vs. illegitimate traffic for a network based on specified types of traffic, sources/destinations, and times</td>
<td>Misunderstanding of traffic redirection requirements causes some students to assume either everything fully works, or “everything is broken”</td>
</tr>
<tr>
<td>SIEMs</td>
<td>Evaluate log analysis and correlation capabilities of SIEMs for security monitoring</td>
<td>Correlate basic network events between firewall, IDS, and network service, such as HTTP</td>
<td>The ELK stack has a not-inconsequential learning curve</td>
</tr>
</tbody>
</table>

Table 3: Examples of Network Security laboratory projects from 2017-2018.
The basic approach for each of the laboratory projects is the same: provide students with a defined problem as well as a framework for a clear and complete solution. Students are expected to spend the scheduled laboratory meeting times working on the project and bringing questions to the faculty member. Additional office hours are provided for out-of-class questions and answers. Students are expected to spend 2-3 hours per week outside of scheduled laboratory time working to successfully complete each project.

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary</th>
<th>Successes</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeypot/ Honeynet</td>
<td>Build a honeypot/honeynet to host web services to attack in order to monitor attack indicators</td>
<td>Gained an understanding of honeynet operations, monitoring strategies, and how to attack web services</td>
<td>Identifying legitimate traffic indicators vs. attack traffic indicators</td>
</tr>
<tr>
<td>Ethical Hacking</td>
<td>Use legitimate offensive security/ethical hacking systems to gain red team skills</td>
<td>Gained badges and achievements on several different platforms, such as CryptoPals.com or HackTheBox.eu</td>
<td>Actual student participation and competency was difficult to evaluate due to perception of team performing the successful breaches</td>
</tr>
<tr>
<td>Hacking WiFi</td>
<td>Brute force WPA2-PSK attacks, Deauth attacks, and KRACK attack</td>
<td>Most of the learning occurred from the required troubleshooting</td>
<td>Students assumed generic WiFi NICs would be able to be used to run aircrack or airodump, which resulted in many failed attempts</td>
</tr>
<tr>
<td>Multisite VPNs with Raspberry Pi</td>
<td>Construct enterprise-like multi-site VPNs using Raspberry Pis as the VPN endpoints</td>
<td>Evaluate multiple VPN approaches and routing requirements for full network-to-network connectivity over the Internet.</td>
<td>Inability to have more than a few active locations simultaneously due to choosing public WiFi hotspots for test points.</td>
</tr>
<tr>
<td>Malware Detection in IDS/IPS</td>
<td>Detonate known malware onto network host in order to develop IPS rules based on indicators of infection and CC activities</td>
<td>Identified functions of known malware and created IPS rules to prevent CC communication post-infection</td>
<td>Properly quarantining of infected VM was always a concern</td>
</tr>
</tbody>
</table>

Table 4: Examples of Network Security final projects completed by students from 2017-2018.

Each of these final semester projects were performed by the students that were interested in these specific topics. Many other topics were also investigated, as approximately 60 students enrolled in the course over the past two offerings. Most of these projects were completed using virtual machines with either VirtualBox or VMWare hypervisors.

### 3.4.3 Challenges & Opportunities

**General Laboratory Setting:** It is an ongoing challenge to find physical space for students to complete their laboratory projects in a room that is used by 8-10 sections of this and other laboratory courses. In general, the 8:00AM - 5:00PM window of time is scheduled for course meetings. Meaning, students only have access to the physical space after business hours. This has been a major driver towards the use of virtualization with occasional integration of physical hardware, such as firewalls. This also provides opportunities, as students are able to take their projects with them, as the VM reside on their own laptops.
Challenge - Virtualized Environments: Since much of the students’ work is completed on virtual machines, they are limited by the power of their own laptops. This usually results in no more than three virtual machines being able to run within their environment at any one time due to resource constraints of their laptops. This is almost always due to the 16GB RAM limit of most laptops available on campus. This could be resolved with dedicated desktop systems, where 64GB RAM or more are available. However, as mentioned above, there is a space limitation as well as accessibility limitation that renders this moot.

Opportunity - Robust Server Environment: The lack of laboratory space and accessibility issue has spurred discussions to host a limited number of high-powered rack-mount servers within the department’s server room. The opportunity would be recognized through the use of a virtualization cluster that would allow students to run upwards of 10 virtual machines within their own environment, which could also integrate physical devices such as firewalls, routers, switches, etc. for a more robust and comprehensive experience.

Challenge - Project Security: As students choose projects that are more dangerous (e.g. active attacks/hacking, malware analysis), the need to protect the rest of the devices on the network becomes more challenging. Because there is no single point of network access within the laboratory, simply quarantining a malware-infected system at the production network is not feasible. This requires direct supervision from the faculty member to ensure that network interfaces on the virtual machine and hypervisor system are correctly configured to limit all network communications. This also requires an effective means of isolating the infected VM from other virtual hosts, and host OS, on the student’s laptops.

Challenge - Project Ethics: As students are expected to spend a substantial amount of time working on laboratory projects and their semester project, there is sometimes an issue with getting more than an appropriate level of help from their peers. This is apparent in the documentation required of each laboratory objective, as it would be trivial to share screenshots or configurations of completed work. This necessitates a sufficiently pointed discussion of ethics within cybersecurity that spans more than just an assignment or course.

Generally, students do reasonably well on the mandatory laboratory projects. There are weekly meetings where there status is obtusely monitored. These hands-on assignments drive capability and competency in the tools and technologies for the students to be able to complete their own semester projects. Anecdotally, those students that have a clear vision for the type of project that they wish to investigate tend to perform better on the project, as well as gain more from the project, as indicated in their lessons learned analysis of their final presentations.

4 Recommendations

There are common themes for the projects and their successes and failures. Below is a compiled list of suggestions and lessons learned.
**General project recommendations:** The same recommendations that apply to non-cybersecurity projects of course apply here as well. This includes proper time management, organization, and effort on the part of the students and the instructor. These recommendations are by no means novel but are applicable.

**Set achievable, knowable goals:** As with many types of challenging projects, students need to set goals that are challenging, but achievable. This requires instructor oversight and testing of components of the projects. Mimicking work that has already been done within cybersecurity and adding to or changing some aspect of it can give students momentum towards completion. For example, all the keyboard acoustic side-channel attacks in senior design and Hardware Security were based on existing published work. The course projects set lower expectations, but closely followed the previous work to get hands-on project experience. The senior design project applied similar side-channel analysis techniques to a new environment with significant success, mainly based on analogous milestones from other projects. With cybersecurity, as people are predictably hesitant to release exact instructions, setting goals based on this previous work can help to scaffold the students for independent success.

**Scale and iterate, if appropriate:** As described earlier, many projects may not be achievable in a given time frame, so identifying milestones is a helpful way to mark success in the projects. Unfortunately, unit testing in cybersecurity projects can easily become either too trivial to be significant or too difficult to achieve. Thus students and instructors must scale appropriately, possibly starting with trivial tests and iterating towards a more complex and complete system. For example, for acoustic side-channel analysis, students were told to focus on a few key presses or simple phrases, rather than the entire keyboard and dictionary. Then as the team had success, more phrases and variability was added into the testing structure. For VGA side-channel analysis, first, the students needed to distinguish black and white on the screen (first invasively, then non-invasively). Then they moved onto a single color on the whole screen, then a screen of half one color and half another. These stepping stones each gave insights that could be used to further refine the approach. For any security project, these milestones will provide such insight, mark forward progress, and protect the students and instructor from straying into potentially dangerous testing (where laws are potentially broken or equipment broken).

**Resources:** All projects require hardware and software resources. The particular issue with cybersecurity projects is that security vulnerabilities are typically found in specific devices or systems under specific circumstances. This necessitates the use of the correct components, which are sometimes unclear, expensive, or unavailable. If possible, create a pool of resources that the students can borrow for the length of the project, including antenna of various wavelengths, microcontrollers, RF systems, microphones, and associated software. If the parts are not already available on campus, instructors should work with the students to research what parts need to be purchased and with what accessories/settings, ensuring that they purchase the right pieces. If possible, it is also helpful to provide noiseless environments and air-gapped rooms. This may include the design of small Faraday cages or isolated rooms to help with noise or to protect components not involved with the project.
Hacking ethics and oversight: Because cybersecurity has legal, ethical, and professional standards, it is crucial that students have the seriousness of their project impressed upon them early. In each of the projects in the paper, ethics is described either in lectures or in face-to-face conversations, and all students working on real-world, practical projects must sign an agreement that explicitly describes the parameters of their project design, testing, and use. For example, teams working on side-channel attacks are told what and whose systems they are allowed to analyze and any variance from the plan must be approved by the instructor. This protects the students from possibly straying into ethical or legal gray areas and allows the instructor to ensure no violations are happening.

Technical advising: Cybersecurity projects require a deep understanding of both the cybersecurity principles and the technical area of the project itself. For example, a project exploring electromagnetic emanations may require the use of electromagnetic waves, sensors, and side-channel analysis techniques. It is therefore critical to have consultants or other technical content at the students’ disposal. This could be the course instructor or project supervisor but may be experts outside the class or even from outside the institution. In particular, guidance on the cybersecurity principles is paramount, and if the project is being done outside of a security-related course, then this guidance may be more difficult to provide.

Reuse skills: Similar to above, it is beneficial for students to explore the cybersecurity landscape from within the confines of the skills and knowledge with which they are already comfortable. If the students are confident in programming, encourage students to do a security project using their programming skills. If they are comfortable with microcontrollers, encourage the use of those. By removing the more technical aspects as an obstacle, students can better focus on the cybersecurity tasks in the project, especially as hacking and protecting a system require deep understanding of that system. The most successful projects described here were often ones that relied on students’ skills and knowledge from previous courses and work.

Real-world scenarios: Cybersecurity is an adversarial design environment. As products are created, hackers (white hat or black hat) exploit vulnerabilities, then products are patched and vulnerabilities are removed, and then hacked again. This adversarial cycle is inherent in cybersecurity work, and thus if it can be part of the project, it will benefit not only the project success but will help students as they go into the cybersecurity workforce. If teams are large enough, split them into subteams with one subteam acting as the “hackers” and another as the “protectors.” If the teams are not large enough, having the teams do brainstorming exercises where they act as both sides can help them to develop better products and solutions and improve their own skills.

Several strategies have been used to attempt to provide as much realism into the projects as possible to give students necessary current knowledge and skills. First, there is a baseline of generalities that are timeless (within reason): filtering traffic at network perimeters (firewalls, proxies, IDS/IPS), connections between sites and users (VPNs), and ongoing monitoring of network (logging and SIEMs). The second, and more challenging approach, requires analysis of current events, discussion with industry partners, and hands-on effort. This approach takes current events, such as the Equifax breach in 2017, and applies them into the business scenario(s) and
background provided to the students. This provides the platform for the cybersecurity concepts to be integrated into the topics that students are reading about in the news, social media, etc. On occasion, industry partners will suggest topics and solutions based on experiences they’ve seen in their own organizations.

5 Conclusions

Cybersecurity is a more central part of computer-related majors as security becomes a first-tier design constraint. In computer engineering and related fields, the ability to give students opportunities for hands-on project-based experiences will make them more marketable to employers. This is a challenge, as cybersecurity projects include issues of ethics, technical concepts, available resources, and more. However, the opportunities largely outweigh the challenges, making it worthwhile to increase the availability of such projects. The work presented here describes various avenues for availing students of cybersecurity projects, including in security-specific classes, senior design projects, and extracurricular research. Challenges, opportunities, and lessons learned are provided along with example projects, in order to facilitate the spread of similar projects to other academic departments and institutions.

References


