Work-in-Progress: A Case Study in an Undergraduate Security Project

Mr. Garry Ingles
Prof. Aaron Carpenter, Wentworth Institute of Technology

Professor Carpenter is an Associate 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.

Work-in-Progress: A Case Study in an Undergraduate Security Project

Garry Ingles and Aaron Carpenter
{inglesg, carpentera1}@wit.edu
Dept. of Electrical and Computer Engineering
Wentworth Institute of Technology

Recent studies have shown new opportunities for the integration of cybersecurity courses and projects into Electrical and Computer Engineering (and related) departments. This is following the growth of the field in both industry and research. While past research discusses what does and doesn't work, from the perspective of faculty and the department, they leave out an important viewpoint by not including the perspective of the student researcher.

In this work, the authors fill that knowledge gap. This work-in-progress tells the details of an undergraduate security project from the perspective of the student, a rising junior at Wentworth Institute of Technology, an undergraduate-centric institution. The presented case study will show insight into the mind of an undergraduate as they approach and explore a new field through extracurricular research with a supervising professor. Before beginning the project, the undergraduate researcher had experience in digital logic and programming, but little experience in more advanced topics. While working closely with the academic supervisor, the student spent significant amounts of time learning the necessary technical skills. Specifically, the student worked towards recreating a FPGA security technique called "Moats and Bridges" from published research in the computer architecture security community [1].

FPGA logic blocks are capable of attacking co-resident logic blocks via side-channel attacks to reveal the inner-workings of the victim logic, as demonstrated in existing research in the community. The "Moats and Bridges" technique changes the synthesis process and provides isolation to logic modules. The synthesis process could otherwise lead to placement of logic blocks that breeds vulnerabilities and back channels. The work-in-progress discussed here will primarily focus on understanding and implementing the Moats and Bridges techniques and technology. Through the research, the activities provided insight towards the more fundamental principle of FPGA security and provided technical tasks for the undergraduate.

The goal of the work is to inform undergraduate students of difficulties that may be faced when researching material beyond the scope of their knowledge. A secondary goal is to present techniques to increase fluency with resources and results of the research conducted. Lastly, supervisors can gain insight into how best to prepare and support their researchers, particularly outside of a class or graduate environment.

1 Introduction

Cybersecurity projects are a growing topic within undergraduate and graduate education. This should be expected as the focus of security increases in necessity across engineering fields. Previous work has explored new security courses, project supervision, and more [2, 3, 4, 5, 6, 7]. While some of these touched on the student perspective, none are told from the narrative viewpoint of a student. Much previous work focuses on undergraduate research experiences [8, 9, 10, 11, 12, 13], but security, as a specialized topic within the field, has particular obstacles and opportunities, including ethics, legality, and sparsity of reliable and widely-accepted platforms and design detail.

As such, this work presents a case study of an undergraduate, extracurricular security-related project. In the summer of 2019, the student asked to do research with the professor as an unpaid co-op. The decided upon research project is described more in Section 2. As a brief description, the student set out to research and recreate a previously published project within FPGA security, creating isolated islands of computation and memory, disconnected to or connected from neighboring blocks by "moats" and "drawbridges," respectively [1].

The undergraduate was tasked with understanding and recreating portions of this research in between their sophomore and junior years. At the outset of the project, the student had completed courses in digital logic (which had minimal HDL exploration), programming with C, microcontrollers, and circuits. Admittedly, the student's lack of HDL experience played a significant role in the overall timeline of the project. The overall undertaking was daunting because of the combination of inexperience, part-time dedication, lack of a research platform and design details, and the highly-technical and involved activities.

This work describes the initial goals, adjustments, and outcomes for the student's education and growth, the professor's expectations, and the technical goals of the project. The case study concludes with recommendations for other students and professors to use in approaches to similar projects. The recommendations focus on an underclass undergraduate engineering student doing extracurricular research with a faculty supervisor but could be applied to a broader context, especially in regards to the cooperative dynamic between the supervisor and student.

The research took place at Wentworth Institute of Technology, 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. Students are required to take two co-ops, one each during their junior and senior years, with an optional co-op during the sophomore year. Co-ops can be paid and off-campus with industry and academic partners, or the students can do on-campus research and work with faculty/staff (paid or unpaid).

The rest of the paper is as follows: Section 2 describes the project from a technical perspective; Section 3 describes the planned student and technical outcomes; Section 4 details the results of the project, with Section 5 providing lessons learned and recommendations; Section 6 concludes.

2 Research Project Technical Details

The primary goals of the research experience were to gain a better understanding of the entire research process, learn and implement fundamental concepts of hardware security, and to determine viable next steps and directions for future research.

In order to put the summer's work into context, it was necessary to understand security principles such as the CIA triad (confidentiality, integrity, and availability) and find examples of pertinent materials from a list of sources provided by the professor (*e.g.*, papers, books, lecture slides). This understanding was reinforced by weekly or biweekly meetings with the professor where the student could address lingering questions and discuss next steps (email communication was used between these meetings for less formal discussions).

After initial discussions between student and supervisor, the student showed interest in FPGA design and security, and so it was agreed that the research project would involve FPGA security, including reading of relevant subject matter [14, 15, 16, 17, 18, 16] and using that information to achieve technical goals in the area. In the end, the student chose to study, "Moats and Drawbridges: An Isolation Primitive for Reconfigurable Hardware Based Systems [1]." The next step was to look at moats and drawbridges specifically and to fully comprehend their use and their implementation. Additional papers of the synthesis process and general FPGA architecture were analyzed to determine the viable steps to continue the research project [15, 14, 16].

In the "Moats and Bridges" paper, the authors describe an FPGA implementation of isolable logic blocks or modules for decreased access between these blocks, to provide better confidentiality between the block and reduce possible information leakage. To combat this, the authors used FPGA placement and routing algorithms to create "moats" around the modules, which were essentially empty logic with no connections. Then, when the modules needed to communicate out of their own block, a "drawbridge" would be created to allow on-demand communication channels. These drawbridges would only exist when required by the run-time computational needs. The creation of drawbridges relied on placement and routing but also required on-demand logic use and on-chip network primitives to complete communications.

Because an original intention was to be able to implement Moats and Drawbridges on a FPGA by the end of the co-op period, the professor also provided supplemental material to aid the learning and use of Verilog HDL.

As comprehension increased, viability to fully meet the goals faded, largely due to the complexities of the placement/routing procedures and a lack of sufficient time. However, a general algorithm was developed to place moats and drawbridges around modules in an attempt to create a version of the security primitive. The remaining sections of this paper will discuss the project's activities, goals, and outcomes.

3 Pedagogical Goals and Procedures

3.1 Student Perspective

When the student approached the professor, the primary goals they had in mind was to understand first-hand the research process and to work in the realm of cybersecurity, with particular attention

to hardware. Having previously met with the professor to discuss project options, it was agreed upon to look at recreating the "Moats and Bridges" project at a small scale. The student goals were to (1) learn how academic and scientific research is conducted, (2) to learn aspects of cybersecurity, and (3) to gain experience in hardware design and testing.

As the research began, the professor provided numerous documents relevant to hardware security and tasked the student with identifying the ones that were most relevant. Reading documents and papers is an important skill, as any researcher could share. As a rising junior, it also presented a particular challenge, as few students at that level have extensive experience in reading these types of papers. The student was fortunate to have, in addition to a professor/supervisor, a close relative with a passion and understanding of research. Throughout the initial phases of research, the student reached out to both the professor and relative with directions on how to aggregate information gathered and how to effectively organize papers by their content or relevance. After the first few weeks, techniques for reading, note-taking, and classification were developed and the student felt that they had accomplished the task of learning the contents of the research papers. This was a significant hurdle and took longer than expected. In particular, since the technical goal was a recreation of some portion of the research papers' activities, the student needed to find details on how the research was done. This is especially true as the goals of the summer co-op were to recreate at least portions of the research and to do so without an available research infrastructure.

Integral to the first part of research was of course the comprehension of security. Accordingly, the professor tasked the student to first gain understanding of the CIA triad (confidentiality, integrity, availability). Notions of the Parkerian hexad were also explored but held lesser significance than the original three pillars. The student saw application of these concepts by also learning the operation of a FPGA with various blocks and necessary communication. For example, a memory block, an adder block, and an encryption-decryption block, and their interconnection were an instructive visual to assist understanding of concepts of security and eventually of moats and bridges in particular.

In the weekly meetings, the student was able to demonstrate to the professor and, to himself, an appropriate level of comprehension. The recounting of the concepts was helpful, but this led to a hurdle for the student in terms of direction. While the professor was able to articulate expectations for every meeting, there was a disconnect between what was trying to be accomplished and how to actually do it, from the student's perspective. In particular, before building the infrastructure, it was necessary to describe the full algorithm and procedure. This required the student to revisit the source materials and solidify his understanding of the details, taking more time and energy away from future implementation.

As such, the research project can be divided into three main parts: reading and research, generation of the algorithm and procedure, and implementation. These parts highlight the goals set throughout the research process. The professor gave the student the option to present a flowchart or pseudo-code to represent the algorithm, but the difficulty was understanding where to begin and how to detail the steps. It was in this task, though, that the student gained better comprehension of the materials and went from a disorganized overall idea of the algorithm to a specific implementation of each block, moat, and drawbridge. The development of this visual representation of the system became a crucial step. The final flowchart is shown in Figure 1 and

served as the blueprint for the next phase.

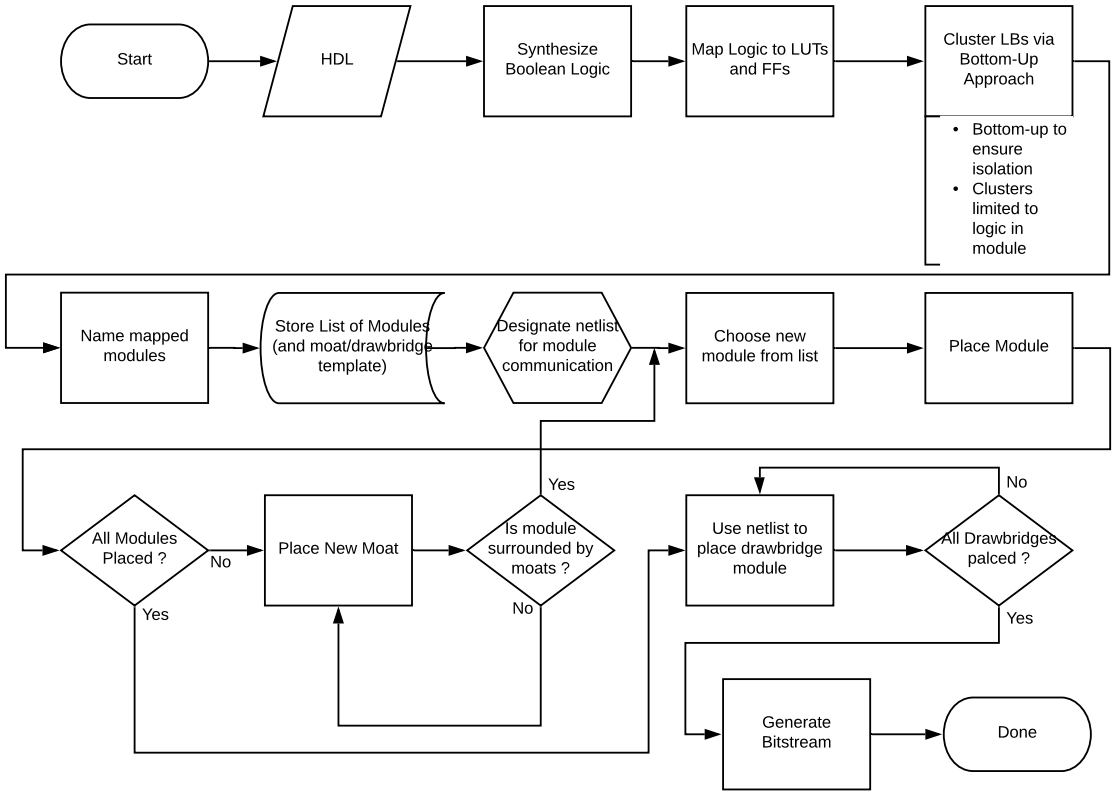

Figure 1: Student-created flowchart of FPGA place and route for Moats and Drawbridges. This was used to demonstrate understanding and would be used for actual implementation if time allowed.

In the final phase, the student had to identify some proof of concept within the algorithm in order to implement the isolation between blocks and the ability for controlled communication. While the student spent time reading and analyzing papers specific to how resources are allocated on FPGAs, they established that the required technologies were beyond short-term capabilities for the research term. The student was instructed to focus on the overall bigger picture of the algorithm and as a result the algorithm does not reveal details of a full implementations. Blocks are created from the smallest bit of logic to take advantage of re-usability and ensure isolation. As every block is mapped to logic separately, any equivalent logic, which could result shared resources and a back channel, would be mapped to separate clusters. Through this the student also gained insight into the trade-offs that are associated with how blocks are isolated. The drawbridges were then to be laid down by using additional software/technology to track the necessary connections in the synthesis process to complete the logic. While the algorithm itself is representative of the full synthesis process, the details of mapping and routing were difficult to fully illustrate in the scope of the research.

In the final stage of implementation, Verilog was to be used for some proof-of-concepts experiments. The student was given online materials (including lectures from the professor) to learn the basics of Verilog coding. Given the students prior experience coding in programming

languages, they had to understand the difference between the procedural execution of programming languages, and the physical transformation of Hardware Description Languages. Although Verilog differed from traditional coding, the student learned it incrementally and without significant difficulty, and a pseudo-implementation of the final algorithm devised.

3.2 Supervisor Perspective

The faculty member had done several course-related, co-op, and extracurricular projects with undergraduates, including security [2, 3] and digital/computer hardware projects. In each project, the pedagogical outcomes are similar:

1. The student should learn a new technical concept or skill outside of their typical courses.
2. The student should practice independent research techniques, including task management, reading/writing academic papers, and self-guiding exploratory tasks.
3. The student should gain insight into graduate-level research and/or industry laboratories.
4. The student should advance their own (self-defined) career and educational goals.

The past experiences of undergraduate research gave the faculty member a default structure to guide the student project. First, the student was asked to choose their own project direction. In the supervisor's experience, this self-direction is beneficial for motivation and for helping students in their career choices. The student was most interested in security and digital hardware, hence the FPGA security project.

Next, the student was given several academic papers from IEEE and ACM on related projects. The student was then asked to independently find and read more papers, keeping notes and asking questions as needed. The skill of finding, reading, and understanding research papers is paramount to success in engineering research. In the meetings early in the semester, the student could discuss any findings and ask any questions, and the supervising professor could give guidance and tips. These conversations also let the supervisor know the current state and plan for future tasks.

The student and faculty together identified technical tasks. In this case, the student was asked to create (or recreate) a placement and routing algorithm for FPGA mapping with the goal of potentially implementing it. This was a necessary step for two reasons: (1) to give the student insight into the base algorithm, and (2) because the Moats and Bridges research requires a change in the placement (we did not implement the change, but needed to understand its role).

Finally, the student was tasked with creating a proof-of-concept for the implementation, as full-scale implementation was too complex given the time and resources. All of these tasks were done together as student and faculty, with the faculty member helping to shape the deliverables. The goal was to let the student do exploratory, but still tangible, research tasks. These explorations were also guided by agreed upon weekly goals that directed the student's focus in a given week.

4 Results & Outcomes

4.1 Student Perspective

After 14 weeks, the student felt that even though he could not test or code a working a rendition of the fully devised algorithm, the research project was successful in terms of the original goals. Retrospectively, the student felt that creating an algorithm was the key limiting factor for making progress in the technical goals. This is largely due to the complexity of the algorithm and the lack of any immediately usable infrastructure for the implementation. There was some dissatisfaction with this shortcoming, but it taught the student that undergraduate research is not always meant to solve problems; rather, it can be a tool to increase understanding, expanding one's learning and perspective, and introduce the graduate-level experience and expectation.

Focusing on the implementation of moats and drawbridges on an FPGA, the student felt that it was a gateway into a future career field. The student wants to eventually be able to recreate moats and drawbridges on his own. As such, this semester's work was the next necessary steps to furthering understanding on FPGA architecture. The student learned the significance and applicability of embedded systems and FPGAs in today's industry, and accordingly, where innovation is necessary.

For students undertaking a similar undergraduate research project, the best way to prepare for reading and extracting information is to create a regulated schedule to prepare for the amounts of reading necessary, as well as familiarize themselves with efficient note-taking mechanisms and software. This also will have a beneficial effect of easily referring back to literature when encountering a roadblock. Thinking about application, the student should spend time practicing algorithm fabrication and visualizing how to map processes in flowcharts and pseudo-code. In this work, a large challenge was the comprehension of the design process for the algorithm, more specifically understanding how and where to start, and segmenting steps to include the proper details. Overall, the student concluded that repetition is necessary and should be advised for all aspects of research, the gathering of information ,and the implementation of it.

Finally, it was a great chance to create a connection with a professor in the student's field of the study, which will benefit the student in future endeavors. Along with a chance to create insight into the process of student driven, undergraduate research and the chance to help others facing the same or similar struggles. The student is more driven to conduct further research in other areas and hopes to become a better researcher in the process.

4.2 Supervisor Perspective

The faculty member had straight-forward goals, centered around the student learning skills and concepts, both soft and technical, that are seldom fully developed in a typical engineering course. The overall goal, in the mind of the faculty member, was not to entirely recreate an existing security design but rather to give foundational understanding to the student and allow the student to grow as an engineer. The student grew in their understanding of cybersecurity, digital hardware engineering, research methods, and more. As such, the project was a success. As with many projects, time and resources were limited, but despite that, the results, from the supervisor's view, were positive.

5 Recommendations from the Student

5.1 Recommendations for Students

As a student, the most important thing to do, is to manage your time. Set a goal time-frame for how much time is to be spent on a certain facet of the research. Understand that while it may take a while to understand the materials, gathering information is the smallest portion of research. It does, however, maintain an equal level of importance and should therefore not be rushed. Take good notes, as it will prevent the hassle of going back and reading the paper again, and organize notes in a way that, should it be necessary, the desired information can be found quickly.

Along with time management comes communication with the professor. Student-led research should have its pace driven at least partly by the student, but the professor, who has a much better understanding, is familiar with the kind of goals the student should set to accomplish their goal accordingly. Moreover, communication is an essential part to affirming information to decide next steps. Regularly scheduled meetings are a given, but the student should put forth the effort to reach out between meetings, and should remember that no question or concern is too small. It is student-led research, but it also an introduction to the field and a chance to learn to how take advantage of available resources.

Goal setting is an important factor as well. Choosing challenging, but achievable, short-term and long-term goals has a significant impact on the overall success. While the student should guide these goals, the supervisor must help choose the appropriate level of challenge.

A student must have work ethic and due diligence. Research is not always enticing or groundbreaking and it can be very taxing and difficult, but having the incentive and enthusiasm to go the extra mile will make a great researcher. Do the extra research to answer question and become comfortable with tasks that need to be done, these things are crucial to the success of the student and researcher. Application of knowledge is the largest portion of research, it requires the most time and is met with the most difficulty. It should the student's imperative to stay ahead of the game and maximize what they can achieve or attain through the experience.

5.2 Recommendations for Supervisors

The professor that has undertaken the task of mentoring and overseeing a student's research should in many ways follow the same advice as the student. Communicate with the student the expectations in terms of time frames, difficulties, and personal availability. To be able to do these things to the best of the ability, it must be ensured that some fluency with the research topics is present. This will guarantee the facilitation of accurate time tables and tangible goals for the research project.

The professor should clearly communicate when they are available to assist the student. It is student-driven research, but the professor's responsibilities lay in fostering a developmental environment to best assist the student, as best as their schedule allows, to guide the direction of student learning. It should not be the primary goal of the professor to make the student reach their goal, but rather to ensure the student maintains a good oversight of their project and they understands the process, and to act as a strong resource to the student.

6 Conclusions

This paper provides a case study of an undergraduate research project in the area of hardware security. From the student perspective, the goal of the research project was to learn the research process, learn about cybersecurity, gain a strong understating of the security primitive, and to practice implementing it on an FPGA board. The student started by understanding basic security tenets and moved on to understanding concepts of moats and drawbridges, an existing security technique in literature. The comprehension of the CIA triad and its application in the primitive moved to a focused effort looking at the synthesis process to understand how to implement the primitive. Implementation was to be achieved through coding in Verilog, and the student demonstrated strong understanding with its use. The student did not completely transfer their understanding into practice as the methodology was beyond the available time and the student's ability. By the end of the research period the student established an algorithm and brief proof-of-concept, completing the goals of learning cybersecurity concepts. This paper gives a narrative and advice for others pursuing similar exercises.

References

[1] T. Huffmire, B. Brotherton, G. Wang, T. Sherwood, R. Kastner, T. Levin, T. Nguyen, and C. Irvine, "Moats and drawbridges: An isolation primitive for reconfigurable hardware based systems," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, May 2007.

[2] A. Carpenter, "A hardware security curriculum and its use for evaluation of student understanding of ece concepts," in *2018 ASEE Annual Conference & Exposition*, 2018.

[3] A. Carpenter and R. Hansen, "Supervising undergraduate cybersecurity projects," in *2019 ASEE Annual Conference & Exposition*, 2019.

[4] S. Bratus, A. Shubina, and M. Locasto, "Teaching the principles of the hacker curriculum to undergraduates," in *Proceedings of the 41st ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '10, 2010, pp. 122–126.

[5] N. Swain, "A multi-tier approach to cyber security education, training, and awareness in the undergraduate curriculum (CSETA)," in *2014 ASEE Annual Conference & Exposition*, June 2014.

[6] X. Meng, L. Perrone, and M. Aburdene, "Approaches to undergraduate instruction in computer security," in *2005 ASEE Annual Conference & Exposition*, June 2005.

[7] R. Smith, "Boundaries and flows: A strategy for introducing information security to undergraduates," in *2008 ASEE Annual Conference & Exposition*, June 2008.

[8] P. Blumenfeld, E. Soloway, R. Marx, J. Krajcik, M. Guzdial, and A. Palincsar, "Motivating project-based learning: Sustaining the doing, supporting the learning," *Educational Psychologist*, vol. 26, no. 3-4, pp. 369–398, 1991.

[9] J. W. Thomas, "A review of research on project-based learning," Tech. Rep., 2000.

[10] B. Barron, D. Schwartz, N. Vye, A. Moore, A. Petrosino, L. Zech, and J. Bransford, "Doing with understanding: Lessons from research on problem- and project-based learning," *Journal of the Learning Sciences*, vol. 7, no. 3-4, pp. 271–311, 1998.

[11] S. Bell, "Project-based learning for the 21st century: Skills for the future," *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, vol. 83, no. 2, pp. 39–43, 2010.

[12] M. Frank, I. Lavy, and D. Elata, "Implementing the project-based learning approach in an academic engineering course," *Int'l Journal of Technology and Design Education*, vol. 13, no. 3, pp. 273–288, 2003.

[13] J. Mills and D. Treagust, "Engineering education - is problem-based or project-based learning the answer?" *Australasian Journal of Engineering Education*, 2003.

[14] D. Gomez-prado and M. Ciesielski, "A tutorial on fpga routing."

[15] R. Tessier and S. Ward, "Fast place and route approaches for fpgas," Ph.D. dissertation, USA, 1999.

[16] S. Chen and Y. Chang, "Fpga placement and routing," in *Proceedings of the 36th International Conference on Computer-Aided Design*, 2017, p. 914–921.

[17] S. Li, J. Torresen, and O. Soraasen, "Exploiting reconfigurable hardware for network security," in *11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, April 2003, pp. 292–293.

[18] T. Huffmire, B. Brotherton, N. Callegari, J. Valamehr, J. White, R. Kastner, and T. Sherwood, "Designing secure systems on reconfigurable hardware," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 13, no. 3, July 2008.