A Hardware Security Curriculum and its Use for Evaluation of Student Understanding of ECE Concepts

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.

A Hardware Security Curriculum and its Use for Evaluation of Student Understanding of ECE Concepts

Aaron Carpenter

carpentera1@wit.edu

Department of Electrical Engineering & Technology
Wentworth Institute of Technology

Abstract

Cybersecurity's increasing relevance and applicability in the research and development community and job market make it an attractive topic for both students and faculty. Thus, it is necessary for institutions of higher learning to provide courses that prepare students for the broad security-based design space. In addition to teaching students about critical security concepts, hardware-based cybersecurity projects and courses sit at the intersection of many electrical and computer engineering concepts, providing knowledge retention evaluation and assessment opportunities to the instructors and departments. A hardware security course, with optional review-based supplemental work, functions as a culmination of past courses or as an introductory Electrical and Computer Engineering (ECE) course with security-centric applications of foundational concepts.

This paper presents the curricular details of an undergraduate hardware security course designed to be self-sufficient and free of advanced prerequisites, thus accessible to a broad student body with a variety of backgrounds. The course covers cryptology, side-channel analysis, hardware Trojan horses, and other hardware-based security exploitations and countermeasures. The course concludes with a multi-week team project where students replicate existing attacks and/or countermeasures, applying their security knowledge and demonstrating skills as ECE professionals. This paper presents the interweaving of ECE topics and evaluation of students' retention of ECE concepts and skills.

"Hardware Security" has been taught twice in the last year, each time containing around 25 undergraduate students (including electrical, computer, and electromechanical engineers in their third and fourth years). These students were surveyed and evaluated regarding their confidence with and competency of ECE and related concepts at the beginning and end of the course. The data gathered were used to evaluate two metrics: 1) how well students were prepared regarding pre-requisite knowledge; and 2) how the Hardware Security course improved their understanding and confidence of ECE concepts. Student knowledge from previous courses varied, but the post-course data show that students improved their understanding and confidence in various topics. The data also point to possible weaknesses in the students' past courses, which can be used as feedback to improve the respective department curricula. Overall, the course evaluations showed student growth in hardware security and progress in reinforcing ECE fundamental knowledge.

The work presented here will help ECE faculty and departments deploy similar curricula to prepare students for a cybersecurity career and provide an evaluation of student conceptual retention and growth within their electrical and computer engineering education.

1 Introduction

In a society where digital components are ubiquitous and people implicitly trust their devices, designers must build software and hardware systems with security as a design priority. While software is often the center of the discussion of cybersecurity, hardware plays a vital role and cannot be overlooked, and thus hardware engineers must focus more on security in classes and projects. Unfortunately, traditional courses often skip security considerations in hardware design. Electrical and computer engineering students would benefit from security-related courses that stress security as a design constraint, similar to power, energy, and performance requirements.

Hardware security exploits vulnerabilities and protects the analog and digital hardware of a system and requires an understanding and application of ECE concepts such as analog and digital circuits, electromagnetics, programming, mathematics, and statistical analysis. In order to provide students with the skills necessary to protect the next generation of systems, educators must offer courses and projects that give students hands-on experience and a background in the security landscape. Meanwhile, it is important to limit the number of advanced prerequisites for such courses to allow students of varied educational backgrounds to participate. The course described in this paper is designed to be relatively self-sufficient, relying on only some basic pre-requisite knowledge, while covering relevant and applicable concepts within hardware security. The descriptions here will provide educators with a scaffolding for creating similar courses within their own programs.

The intent of a hardware security course is to further the students' conceptual and analytical design of security systems; however, due to the course's inclusion of key electrical and computer engineering topics and students, a hardware security course is a convenient lens with which to review and evaluate students' retention of concepts. Alternatively, the course's security topics could also be used as an introduction to electrical and computer engineering topics, where topics like power, transistors, and electromagnetics are taught and then applied to security-related problems. For example, the current/voltage of a RC circuit could be applied from the perspective of a power side-channel attack.

The course can further be used to develop and evaluate soft skills and the students' ability to apply engineering knowledge to culturally relevant topics. Presentations, in-class discussions, and written reports prepare students for the workplace where both soft and technical skills are required. Additionally, as discussions of ethics are integral to a course in security, the course also involves professional and ethical responsibilities. The combination of soft skills and ethical consideration included in the course give faculty a foundation to do ABET assessment to go along with the technical concepts.

In this paper, an undergraduate hardware security course curriculum is described, including a list of topics, assignments, and projects; the descriptions and lessons learned are given to guide the creation of similar courses. The groundwork for the evaluation of fundamental computer engineering topics is also presented, including, but not limited to, analog and digital circuits, electromagnetics, and programming.

The course, *Hardware Security*, has been taught twice in the past year to 46 total students, including sophomores, juniors, and seniors majoring in electrical, computer, and electromechanical engineering. These students were evaluated in their knowledge of and

confidence in select ECE concepts. These evaluations, gathered both at the beginning and end of the course, revealed a number of interesting insights. First, students who completed the course improved their understanding of the concepts and felt more confident, having revisited and applied a number of previously learned concepts. Additionally, some skills and concepts were new to some students, allowing the instructor to teach a new non-security topic with the application of the concepts being founded in security. Once the course was complete, these students were comfortable with the more foundational topics, despite it not being the focal point of the Hardware Security course, as the concepts were reinforced in a security application space.

The course was developed and taught at Wentworth Institute of Technology, which 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 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, security education, and evaluative efforts. Section 3 characterizes the Hardware Security course, as taught at Wentworth Institute of Technology over the last year, including lecture topics and assignments. Section 4 describes the assessment and evaluation tools and methodology. Section 5 provides data and analyses regarding assessment and topic retention and growth. Section 6 recommends strategies for adaptation to other departments and schools. Section 7 concludes.

2 Related Work

Cybersecurity in all its forms is an important aspect of digital design^{1,2}. Its popularity in academia has resulted in a wealth of publications, specifically regarding new course and curricular designs^{3,4,5,6,7,8,9}, the incorporation of ethics^{10,11} and game theory concepts^{12,13,14}, and more.

The work presented in this paper is meant to add to the discussion and has some underlying similarities with these existing courses, although with important and significant distinctions. There are a variety of courses and curricula developed surrounding cybersecurity, some listed and reviewed in a unified study⁸. Further development has been done for teaching computing^{6,7}, embedded systems⁵, or broad security curricula³. The presented work here describes high-level hardware security, which could be applied to large computing systems, embedded systems, or general devices, without targeting particular topics. The topics for the hardware security course focus on digital and analog hardware and largely ignores the software and mathematics of cybersecurity beyond what is needed for the hardware topics.

Ethical engineering and professional behavior are discussed across engineering education and are often subject to entire course curricula^{10,11}. Specifically, when discussing security, the line between white hat and black hat hacking can be a dangerous one, and students must be carefully shown the “right” way to hack, to improve designs for the user rather than for fun or personal gain. This is in addition to a more generic version of engineering ethics, as students are making a conscious decision to possibly find exploits within a system. The work described in this paper does not reinvent the description of ethics and hacking but incorporates the concepts using security-centric case studies from recent news.

This course uses basic concepts from game theory to help explain adversarial thinking and iterative decision-making in the face of an opponent. These concepts are highlighted in several papers^{12,13,14}, and the presented course was inspired by the key takeaways of these previous works.

Beyond the curricular design, the work presented here describes a singular point of assessing student retention of information and growth before and after the class in key topics. This type of knowledge retention tracking is not widely reviewed outside of ABET data or within broader department goals, particularly encompassing many classes. One paper does track students longitudinally to assess student sustained involvement in cybersecurity, but does not focus on broader topics within ECE⁴.

3 Hardware Security Curriculum

The Hardware Security course, taught within the computer engineering degree program at Wentworth Institute of Technology, is intended for computer engineering students at a junior/senior level, but is open to students from computer science and electrical, electromechanical, and other engineering degree programs.

Review Topics: The Hardware Security course is intended to be accessible to a broad pool of students, regardless of their major or background. Any student with college-level mathematics (probability, exponents, modulus), basic circuits (resistors, power, voltage), and digital logic (Boolean algebra, logic gates) should have the tools necessary to succeed. The students in these Hardware Security sections did have these courses in their past. Of course, because students enter the class at different expertise levels, it is beneficial to provide support materials and subject review lectures. The course designer for Hardware Security recorded and posted a playlist of review videos including some basics (circuits, digital logic, programming in C/C++/Verilog, binary math) and some more advanced (fabrication, state machines). These videos, posted on youtube.com, were available to all students and could serve as a review or an introduction, depending on the student needs. This allowed minimal pre-requisite knowledge, thus permitting a broad student population with diverse educational backgrounds.

3.1 Hardware Security Curricular Design

Hardware Security has been a 3 and 4-credit hour course (at least 2 hours of lab and 2 hours of lecture per week). The course topics are loosely based on *Introduction to Hardware Security and Trust* by M. Tehranipoor and C. Wang¹⁵, supplemented by related papers focusing on key concepts^{16,17,18,19,20,21,22,23,24}. These topics were covered in lectures with conventional Powerpoint slides and in-class exercises and discussions, but could be done with flipped classrooms or non-traditional lectures at the instructor's discretion. Weekly quizzes were used to evaluate student understanding and progress, and a weekly lab session was used to give students hands-on experience with each topic, both with small projects and a semester-long large team project.

The course covered the following topics and sub-topics during the lectures:

- Ethics: general ethical principles, black/white/gray hat hacking, ethical case studies

- Security Basics: Parkerian hexad (confidentiality, integrity, availability, authenticity, ownership, utility), basic terminology, access control
- Game Theory and Adversarial Thinking: distribution of resources, level-K reasoning, mathematical analysis, adversarial modeling
- Cryptology: transposition, substitution, steganography, symmetric and asymmetric key encryption/decryption, hash functions, key generation
- Side-Channel Analysis: power, acoustic, electromagnetic, etc. side-channel analysis to discreetly determine internal activity of digital systems, existing side-channel attacks and countermeasures
- Physical Unclonable Functions (PUFs): circuit design of memory and delay-based PUFs and their sources of variation and randomness, evaluation of robustness and randomness
- Hardware Trojan Horses (HTHs): categorization of HTH circuits and placement, triggering mechanisms, covert channels
- Digital Circuit Watermarking: algorithmic insertion of watermarks into existing digital system, impact on area, power, speed etc. of watermarked system, evaluation of watermarks' viability
- Miscellaneous Security (covered in less detail, but could be expanded): RFID, replay attacks, hardware DoS attacks, tampering, FPGA/embedded security

To give students hands-on experience, there were weekly assignments and activities. In particular, the ones listed in Table 1 were not only used for students to design, evaluate, and analyze security topics and components but also for students to revisit topics from past classes, such as digital circuits and statistics.

The labs requiring digital logic, circuit analysis, or CMOS design used standard academic simulation tools common to undergraduate courses (*e.g.*, PartSim, LogiSim)^{25,26}. These could be done using any circuit simulator that has realistic transistor modeling. Programming-based labs could be done in any high-level language with which the students were comfortable, primarily C/C++, Java, Python, and MATLAB. This gave students of different programming expertise levels a way to focus on the algorithm and not the syntax. Most assignments were completed in teams or pairs, to help students balance their competencies and prepare them for the real-world environment of engineering teams.

In the 14-week semester, approximately 10 weeks were dedicated to lectures, assignments, quizzes, and exams. For the last month, students worked on a team project. Student teams (2-3 students) each chose a hardware security project from research literature. Some past projects are listed in Table 2 along with source literature. There are four main components to the project:

1. Students read, understand, and present the original source material to the class in a 10-15 minute presentation. This includes the theory and practicalities in the attack or countermeasure. During the presentation, the audience is encouraged to participate and ask questions. This mimics a conference or job presentation.
2. Students recreate part or all of the experiment originally presented in the source material. If the experiment is too large or cannot be directly replicated, the students work with the

Assignment/Activity	Non-Security Engineering Skills
Literature Reading and Summary: Students read 10-12 papers chosen by the instructor, spanning hardware security topics; write a summary (3-6 sentences) for each paper (assigned in week 1, due in the last week)	Technical reading; writing; individual papers require technical background and understanding
Security Case Studies: In-class discussions of modern security stories (Anonymous hacking group, Chris Roberts, Edward Snowden)	Contemporary issues; modern engineering environment; professional duties; extemporaneous speaking skills
Security News: Write a report on the details and ethical implications of a modern security breach/hack	Contemporary issues; modern engineering environment; professional duties; reading/writing
Game Theory: Play game theory “games” (prisoner’s dilemma, traveler’s dilemma, Colonel Blotto, etc.) and discuss mathematics and strategies	Mathematical and statistical analysis; speaking skills, adversarial thinking
Cryptography: Create a program that uses an input string (plaintext) and key to transpose and substitute characters to encrypt into ciphertext and decrypt to plaintext (similar to DES)	Computer programming; string manipulation, algorithmic design
Side-Channel Analysis: Create NOR/NOT gates with transistors, evaluate power draw; apply power values and patterns to determine black-box circuits made of NOR/NOT gates	Basic circuit measurement; digital circuit design; CMOS circuits; statistical analysis
Physical Unclonable Function Evaluation: Design a SRAM-based PUF circuit; analyze the timing of the oscillating signal to see impact of size on PUF settling time and value	Basic VLSI sizing and parameters; digital circuit design; CMOS circuits; timing and measurement; memory cell evaluation, statistical analysis
Hardware Trojan Horse Insertion: Reverse engineer an unidentified circuit (full adder in NOR/NOT logic); insert externally triggered HTH to cause data errors; insert internally triggered HTH to cause DoS attack	Digital logic; CMOS circuits, reverse engineering
Watermark Insertion: Insert watermark using two different algorithms into a given digital system	Digital logic, system design, Boolean analysis
Semester-Long Project: Team chooses a research paper/topic and recreates the experiment of a hardware-based security attack or protective technique; see Table 2 for examples	Technical skills vary based on project; all include reading research literature; writing and presenting of technical data and procedures

Table 1: A description of significant assignments/activities in the Hardware Security course paired with the overall engineering skills for each. Each assignment/activity also reinforces the given security topic and skills.

instructor to scale the experiment to appropriate difficulty.

3. The team submits a report summarizing their experience with the project, including procedure, data results, and analysis. Team evaluations are included as part of the report and are kept confidential between each student team member and the instructor. These evaluations help the instructor parse what work was done by whom.
4. As the final step, students demonstrate their working experiment either in person or through videos and images. Ideally, students have recreated their chosen experiment or made significant strides towards completion.

At the beginning of the semester, students must sign a contract with the instructor/university stating that they will not use the knowledge gained in Hardware Security for malicious or extracurricular purposes. This is especially relevant during the project phase, as students need to be aware of the experimental limitations on their testing to ensure no violation occur.

Project Title	Description
Recreation of Timing Analysis of Keystrokes and Timing Attacks on SSH ²⁷	Monitor timing differences between transmitted keystrokes in an SSH password; use timing to determine password characters; team analyzed/predicted pairs (HE, EL, LL, LO); Skills and concepts used: understanding of SSH and communication protocols, programming, data correlation, statistical analysis
Acoustic Side Channel Attack ²⁸	Capture sounds emanating from keyboard button pressing; amplitude and timing help indicate what keys were pressed; focused on a small set of keys rather than the entire keyboard. Skills and concepts used: digital and analog signal analysis, programming, data correlation, statistical analysis
AES Encryption Hardware Trojan Horse ²⁹	Implant a HTH in an FPGA implementation of AES encryption; cause a bit flip in the 3rd stage of the process, decreasing the number of possible bit combinations for the encryption key for easier brute force attacks on the key. Skills and concepts used: encryption, FPGA design, programming, digital arithmetic hardware, error checking/robustness
Capturing and Spoofing PKE Signals for Automotive Theft ³⁰	Capture the RFID electromagnetic emanations from a key fob and spoof the signal to allow unauthorized entry into an automobile. Skills and concepts used: digital signal analysis, antenna and RF design, micro-controller programming and hardware design
Hardware LED-based Covert Channels for Air-Gapped Systems ³¹	Implant malware to control hard drive LED light. The system then leaks information from the system through the LED, which is then captured by optical sensors and reconstructed outside the system. Skills and concepts used: programming, Unix/Linux OS operation, storage hardware use, sensor design and use

Table 2: Title and description of past projects completed by student teams with citation of source material.

4 Assessment Case Study

Along with the already discussed curricular activities, the project represents the application of hardware security topics with previously learned skills and concepts, each of which can be assessed by the instructor. Because students must read papers, present technical information, work in teams, and do physical experiments, the project components also allow the instructor to assess the soft skills required for engineering students. This section will discuss a case study in using the course for these types of soft and hard skills assessments for ABET and for student knowledge retention. Many technical electives could be similarly used for assessment, but hardware security's overlap into ethics and contemporary design make it particularly useful in its complete application to assessment.

4.1 ABET Assessment

At the time of this work, ABET (the Accreditation Board for Engineering and Technology), the accrediting body for engineering programs, used student outcome assessments a-k to gauge the efficacy of a program's progress and growth³². Departments often distribute these outcomes across many classes and years³³. For example, a freshmen and senior course may have the same rubric in each class, to measure growth or improvement in that skill. The same rubric may also apply to multiple courses across the same class year, allowing assessors to measure proficiency from different perspectives.

The Hardware Security course as described here can assess any (or all, if the instructor agrees) of the outcomes in a single course. Table 3 is a list of each outcome assessment along with a corresponding assessment idea. Only two outcomes were assessed for the actual course (F and J), but all could be considered. These assessment tools are representative examples, and more examples could be created. The new ABET outcomes would also be able to map similarly to the course activities.

Student Outcome	Potential Assessment Tool(s)
(A) An ability to apply knowledge of mathematics, science, and engineering	Mathematics: cryptology proof; science: electromagnetic side-channel attack recreation or simulation; engineering: any of the laboratory assignments listed in Table 1
(B) An ability to design and conduct experiments, as well as to analyze and interpret data	Any of the laboratory assignments listed in Table 1
(C) An ability to design ... within realistic constraints ...	Since security has ethical, social, political implications, the final design project or individual labs could be used
(D) An ability to function on multidisciplinary teams	All laboratory assignments, or the semester-long project
(E) An ability to identify, formulate, and solve engineering problems	Semester-long project forces students to identify, formulate, and solve engineering problems, albeit following a pre-existing guideline
* (F) An understanding of professional and ethical responsibility	Students read and analyze a security-related news story and/or case study, specifying the professional and ethical components of the story; could be done as oral or written assignment
(G) An ability to communicate effectively	Project presentations (verbal) and reports, as well as lab reports (written).
(H) The broad education necessary to understand the impact of engineering solutions...	Engineering ethics case studies discussions/reports to determine student understanding of the impact of security vulnerabilities and fixes
(I) A recognition of the needs for, and ability to engage in life-long learning	The project literature search and reading assignment described in Table 1 each require an engagement with existing literature; semester-long project typically requires an independently gained skill
* (J) A knowledge of contemporary issues	Students read and analyze a security-related news story and/or case study; could be done as oral or written assignment
(K) An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice	All laboratory assignments, or the semester-long project

Table 3: A list of ABET student outcomes³² and potential assessment tools for each. The course, having been run twice, evaluated outcomes F and J, labeled with stars here. Some outcomes are abbreviated for brevity.

Because Hardware Security is a project-based, modern, applicable course, as long as the assignments are well designed, all ABET outcomes can be assessed in a single course. In the two semesters that the course was held, the final ABET evaluation statistics were similar to other courses.

4.2 ECE Concept Assessment

While ABET accreditation assessment is significant and necessary, a potentially more significant use of Hardware Security is to do an evaluation of student knowledge within the ECE program. Prior to entering this class, most students had taken digital logic design, programming, circuit design, physics, mathematics, and introduction to engineering. Thus, there were many topics the students should have a solid understanding of, if not proficiency with. Hardware security can thus serve as a review for each of these topics, helping to reinforce the already learned concepts through application or fill in the gaps in student knowledge. These gaps may come from students taking courses out of their intended order, lacking a proficiency in the topic upon course completion, or attrition of the conceptual knowledge over time. The evaluative results can then be used by the department to strengthen the weaker points in the students' courses.

- 1) Write a function in any language that takes in a string as an argument and displays each character 1 at a time on its own row. Assume the string has a maximum of 12 characters in it.
- 2) Draw the schematic for an inverter from NMOS and PMOS transistors. Explain why the PMOS transistor is often a larger width than the NMOS.
- 3) With what input values will the function $A \cdot B + B \cdot \bar{C}$ evaluate as a 1?
- 4) Given the circuit below, calculate the total power provided by the battery. How would you verify this with an ammeter or voltmeter?

- 5) We are designing a traffic light. What digital states (for a state machine) does the traffic light need to operate? Assume just the lights (no buttons, turn arrows, etc.) What causes these traffic lights to transition between states?
- 6) Identify as many components as possible for the device below. What is the picture representing?

- 7) Below is a list of numbers. Explain the mean, median, and mode. Identify any patterns or anomalies.

Entry No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Number	5	99	1	5	2	1	5	4	3	5	4	2	5	1	3	5	6	-7	5	1

- 8) Explain the right-hand rule as it pertains to electromagnetism.

Figure 1: Concept quiz example assignment questions given before and/or after the Hardware Security course to assess conceptual understanding of ECE topics.

To evaluate the Hardware Security course's potential as a central review course for ECE degree programs, a survey and a quiz/assignment were given to each student. The survey asked students to quantify their level of confidence of a variety of topics and skills. On a scale of 0 (no competency in that area) to 10 (expert-level), students judged the following skills/concepts: programming, basic circuits, digital logic, electro-magnetics, VLSI design, digital system design, engineering ethics, technical reading, technical writing, technical presentations, engineering

design, and statistical mathematics. A comment section was also provided so students could provide additional information, if they so desired.

In addition to quantifying their confidence, a concept quiz was given to assess their understanding. Students were asked to not consult outside sources, but rely on their own memory of concepts to answer the questions in Figure 1. The questions were then graded and a score from 0 to 5 was given by the instructor, with 0 representing no reasonable answer and 5 being a fully correct answer. There were two such assignments, one given at the beginning of the semester and one at the end. A screenshot of one of the quizzes is shown in Figure 1.

Some questions were created specifically with the Hardware Security curriculum in mind, but could be created using a broader assessment tool. For example, the mathematical question is seeking averages and anomalies, which is a part of side-channel analysis, as students would need to understand the statistical relevance of patterns. Similarly, the electromagnetic question(s) were inspired by electromagnetic side-channel and RF transmission for RFID. Meanwhile, most of the remaining questions are general ECE knowledge (CMOS circuits, resistive circuit, programming, etc.). The results of the surveys and assignments, as well as analysis of the data is included in the next section.

5 Student Knowledge Assessment Data & Analysis

The course's primary objective is to teach concepts and skills directly applicable to hardware-based security. Student feedback and grades show a strong understanding for security-related topics, particularly within specialized knowledge in the field of their chosen final project. Student feedback also indicates students enjoyed and learned from the course. However, the data and accompany discussion will focus on the evaluation of the foundational ECE concepts and skills.

Through two semesters, there have been 46 students who completed the Hardware Security course, including 26 computer engineers, 9 electrical engineers, and 11 electromechanical engineers, 22 seniors, 22 juniors, and 2 sophomores. Before taking this course, all of the students had taken basic digital logic, physics, circuits, computer programming (largely in C/C++); some may have also taken more advanced programming, analog circuits, and communications, but this varied based on class year and major.

The concept quizzes and surveys given at the beginning and end of the semesters were designed to assess (a) what knowledge students had before entering the class, (b) how confident the students were with these concepts/skills, and (c) if the Hardware Security course increased the students' knowledge in fundamental topics. The data in Figure 2 show the average score for basic skills before and after completing the course. On average, students had a reasonable understanding of most concepts central to electrical and computer engineering. The students were weakest in programming and VLSI design, specifically CMOS circuits and the general principles of fabrication and transistor layout. These results were reasonable, as programming is often identified as an issue among ECE students, and VLSI design is typically a concept taught in advanced electives.

By introducing or reinforcing concepts in a new application space, it was expected students would increase their confidence and abilities in these fields and help identify possible gaps in previous

Figure 2: Average quiz question scores (0-5) on various fundamental skills and concepts, both before and after completion of the Hardware Security course.

courses. For example, in the fall 2017 section, students were weaker than students in the summer course in terms of programming (average score 2.5/5 vs. 3.7/5) and CMOS circuits (1.1/5 vs. 2.7/5). The fall section students were a year younger (juniors) and made up of more electromechanical engineers. These two populations would have less advanced digital circuits and programming courses, so these results make sense. Conversely, advanced digital topic scores were higher for the fall 2017 cohort (4.3/5 vs. 2.9/5). The fall cohort had a newer digital logic and systems curriculum stressing advanced design techniques, thus leading to a higher score. This type of analysis is possible because of the cross-disciplinary knowledge retention evaluation being done here. The department is able to gain feedback on technical expertise of the students through their respective majors and tracks, helping to strengthen the overall program.

After the Hardware Security course was completed, students showed a general increase in their abilities for each topic. The only anomaly is in statistical mathematics, which shows a slight decrease. The quiz question for that concept was multiple parts, and it was noted that a number of students skipped a part, lowering the average score. Future quizzes will more carefully test each concept in a single part or easily identifiable multiple parts. Overall, students had an increase in understanding, ranging from minimal (state machine/digital system design) to high (VLSI design). Students already had a base knowledge, but the Hardware Security course reinforced and enhanced the already existing knowledge, as proved by the survey results.

Additionally, a small group of students who had no pre-existing knowledge in a field did demonstrate at least elementary competency in each concept, giving support to the introductory version of the course, where it acts as an introduction to topics, rather than an applied reinforcement.

Figure 3 illustrates the level of confidence for each student regarding the skills and concepts. The survey asked students to quantify their comfort with each of the concepts or skills listed, each of which would be used in Hardware Security or in ECE as a whole. For example, engineering

Figure 3: Average self-scored confidence (0-10) of students for various fundamental skills and concepts, both before and after completion of the Hardware Security course.

ethics was a lecture topic for at least one full week (3 hours of lecture) and technical reading, writing, presenting, and design were stressed heavily. This made students feel more confident in their abilities with these skills or concepts. It should also be noted that the instructor witnessed a growth in these skills through assignment quality (lab reports, presentations/discussions). Similar to the skills assessment, student confidence level increased in most of the topics.

Overall, the data illustrate that students had some level of confidence and competence prior to the course, varying by topic, and the Hardware Security course helped to evaluate, reinforce, and grow the confidence and understanding through application of fundamental ECE topics. Future instructors could tailor the course to fit a specific department's goals, but use the Hardware Security curriculum and evaluation method as a scaffolding to get similar results with a different student population.

6 Recommendations

The Hardware Security course, as described in this work, has two goals: first, educate students in the field of cybersecurity, focusing on digital hardware through a mix of lectures and hands-on projects; second, to reinforce and provide an application space for knowledge within electrical and computer engineering evaluate student conceptual growth and retention across many fields.

As most electrical and computer engineering programs have similar curricula and overall structure, many of the techniques used here are applicable universally. The hardware security topics can be introduced at various points within a program, and each instructor can refocus the specific topics, but there are some recommended strategies for implementing a similar course.

Topics List: Each instructor will bring a slightly different background to their class. The instructor of the course described here was a computer architect and digital system designer, thus focused on digital systems. However, the topics list in Hardware Security is vast and could be refocused to include different foci, such as RF, communication, or analog circuits. The book used here¹⁵ has a broad list of topics that could be enhanced by other sources. The topics list should not be seen as comprehensive or final. This would allow the instructor to assess a different concept list while maintaining a cross-disciplinary security course.

Review Topics: The course described here was taught to upperclass (third and fourth year undergraduate) students, but could be adjusted to fit first or second year undergraduate students also. For juniors or seniors, who should have more base ECE knowledge, prerequisite concepts can be reviewed briefly in class or through online/recorded lectures. This allows students to review as needed without using significant blocks of instructional time to cover these foundational concepts.

If the student population of the class is first and second year students, the “review” topics are no longer purely review and should be more central to the course and covered in more detail. The hardware security concepts would then be used as the application of the newly learned ideas. For example, power side-channel analysis of CMOS circuits would focus on power/current/voltage of a circuit’s operation and then tied to the side-channel only as application. While this more introductory version was not directly implemented and discussed in this work’s analysis, a number of students had less experience with individual topics and needed the review. These students relied more on the review topics but reinforced their understanding through the security-centric applications.

Final Projects: For a month, students in the described section chose a design project and replicated some existing hardware security experiment. The juniors and seniors can handle much of this project independently, as they have likely done projects of this scale in past courses. Because of the broad view of the project, the level of difficulty and scope varied. The open-ended nature of the project lets students explore their own interests, and students appreciated that opportunity. Students often chose broad topics, and the instructor scaled the project to the appropriate size.

However, if this class were targeted at students with less experience, the project should be more constrained. Rather than give students complete freedom to search the research and design space, the instructor should choose some known, achievable projects, for example a Van Eck phreaking of a CRT or LCD monitor or an acoustic keyboard side-channel with limited number of possible keystrokes. These projects can then be shepherded by the instructor(s) to give the students a better support structure.

Evaluation and Assessment: The evaluations provided here used generic ECE-centric questions that students in many programs have at least awareness of the concepts. However, as each department is different, the concept quizzes and surveys could be adapted to fit an individual program’s perceived strengths and/or weaknesses. In the scope of the evaluation discussed here, it is worth noting that questions should be kept general as to not overly tax the memory of students

and to not allow the questions to be too closely related to direct examples used within the Hardware Security course.

It is also worth noting that, while few instructors would agree to do all ABET assessments, the Hardware Security course does fulfill many possible assessment needs. Similar to knowledge evaluation, the ABET assessments could be modified to be appropriate to that particular course. In particular, the outcomes that revolve around real-world design and ethical responsibilities are ideal for a Hardware Security course.

This type of comprehensive evaluation of a course and its place in a program could be done with other advanced technical electives outside of security. If this is done, it is recommended to follow similar patterns in terms of review topics and evaluation techniques as presented here.

Open Discussion: It is strongly recommended to first have discussions of hacking ethics and adversarial thinking. These were provided as the first lectures, and it helped to set a common language of how hacking and countermeasure creation guides security research. It also helps to ease students into the correct mindset before they learn how to actually hack.

Because of the wide variety of background knowledge students have, be prepared to review past topics in the midst of the security lectures. For example, students may need a review of transistor fabrication when discussing hardware Trojan horses or power side-channels. Thus, it is important for the instructor to be ready to give clear and concise explanations in the moment. These types of discussions may go longer than originally intended, but can help the instructor to formulate better reviews and better future security topics, as it reveals the students' understanding and interest.

Lastly, as students come in with different interests, it is the author's recommendation to encourage as much discussion and as many questions as possible from the students. During the second run of the course, the instructor modified the assignments and projects based on the feedback and guidance of the students, which helped to create a stronger overall classroom experience.

7 Conclusions

The Hardware Security course presented serves two purposes. First and foremost, it teaches students concepts in a modern, relevant, and technically advanced engineering field, one highly sought out by employers. The structure of the course is provided here to give a framework for instructors interested in creating similar course. Second, the cross-disciplinary nature of security allows faculty to reinforce and evaluate basic electrical and computer engineering topics and supplemental topics like physics, math, and engineering soft-skills. An evaluation of two semesters of the course is provided, concluding that the course helped to enhance student understanding of these foundational areas, while also identifying potential weaknesses in the prior courses.

References

- [1] M. Hentea and H. S. Dhillon. Towards changes in information security education. 5, 2006.
- [2] B. Rogers, D. Palmgren, D. Giever, and M. Garcia. Security education in the 21 st century: The role of engineering. In *2005 ASEE Annual Conference & Exposition*, June 2005.
- [3] 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.
- [4] R. Bell, E. Vasserman, and E. Sayre. A longitudinal study of students in an introductory cybersecurity course. In *2014 ASEE Annual Conference & Exposition*, June 2014.
- [5] J. Zalewski et al. Curriculum development for embedded systems security. In *2014 ASEE Annual Conference & Exposition*, June 2014.
- [6] J. Zalewski et al. Developing an applied, security-oriented computing curriculum. In *2012 ASEE Annual Conference & Exposition*, June 2012.
- [7] M. Kermani and R. Azarderakhsh. Integrating emerging cryptographic engineering research and security education. In *2015 ASEE Annual Conference & Exposition*, June 2015.
- [8] X. Meng, L. Perrone, and M. Aburdene. Approaches to undergraduate instruction in computer security. In *2005 ASEE Annual Conference & Exposition*, June 2005.
- [9] R. Smith. Boundaries and flows: A strategy for introducing information security to undergraduates. In *2008 ASEE Annual Conference & Exposition*, June 2008.
- [10] 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, SIGCSE '10*, pages 122–126, 2010.
- [11] R. Pike. The “ethics” of teaching ethical hacking. 22(4), 2013.
- [12] C. Li and R. Kulkarni. Survey of cybersecurity education through gamification. In *2016 ASEE Annual Conference & Exposition*, June 2016.
- [13] S. T. Hamman, K. M. Hopkinson, R. L. Markham, A. M. Chaplik, and G. E. Metzler. Teaching game theory to improve adversarial thinking in cybersecurity students. *IEEE Transactions on Education*, 60(3):205–211, August 2017.
- [14] X. Liang and Y. Xiao. Game theory for network security. *IEEE Communications Surveys & Tutorials*, 15(1), 2013.
- [15] M. Tehranipoor and C. Wang. *Introduction to Hardware Security and Trust*. Springer, 2012.
- [16] A. Wood and J. Stankovic. Denial of service in sensor networks. *Computer*, 35(10):54–62, Oct. 2002.
- [17] S. Bhunia, M. Hsiao, Banga, and S. Narasimhan. Hardware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, August 2014.
- [18] M. Yu and S. Devadas. Pervasive, dynamic authentication of physical items. *Communications of the ACM*, 60(4):32–39, March 2017.
- [19] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14, June 2007.
- [20] K. Tiri and I. Verbauwhede. A vlsi design flow for secure side-channel attack resistant ics. In *Design, Automation and Test in Europe*, pages 58–63, March 2005.
- [21] T. Halevi and N. Saxena. Keyboard acoustic side channel attacks: Exploring realistic and security-sensitive scenarios. *International Journal of Information Security*, 14(5):443–456, October 2015.

- [22] P. Kocher. Computer security is broken: Can better hardware help fix it? *Communications of the ACM*, 59(8): 22–25, July 2016.
- [23] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer. Physical key extraction attacks on pcs. *Communications of the ACM*, 59(6):70–79, May 2016.
- [24] N. Radziwill, J. Romano, D. Shorter, and M. Benton. The ethics of hacking: Should it be taught? *CoRR*, abs/1512.02707, 2015.
- [25] Partsim circuit simulator. URL <http://www.partsim.com/>.
- [26] C. Burch. Logisim: A graphical system for logic circuit design and simulation. *Journal on Educational Resources in Computing*, 2(1):5–16, March 2002.
- [27] D. Song, D. Wagner, and X. Tian. Timing analysis of keystrokes and timing attacks on ssh. In *Proc. of the 10th Conf. on USENIX Security Symposium*, 2001.
- [28] D. Asonov and R. Agrawal. Keyboard acoustic emanations. In *IEEE Symp. on Security and Privacy*, pages 3–11, May 2004.
- [29] D. Mukhopadhyay. An improved fault-based attack of the advanced encryption standard. In *Proc. of 2nd Int'l Conf on Cryptology in Africa*, pages 421–434, 2009.
- [30] A. Francillon, B. Danev, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *In Proceedings of the 18th Annual Network and Distributed System Security Symposium*, 2011.
- [31] M. Guri, B. Zadov, and Y. Elovici. LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive LED. 10327, 2017.
- [32] Abet general criterion 3. student outcomes. URL <http://www.abet.org/accreditation/accreditation-criteria>.
- [33] R. Felder and R. Brent. Designing and teaching courses to satisfy the ABET engineering criteria. 92(1):7–25, 2003.