Expanding the cybersecurity pipeline through early exposure in undergraduate programs

Dilma Da Silva
Department of Computer Science and Engineering
Texas A&M University
College Station, US
dilma@cse.tamu.edu

Maristela Holanda
Department of Computer Science
University of Brasilia
Brasília, Brazil
mholanda@unb.br

Nina Miner[1]
Department of Electrical Engineering and Computer Science
United States Military Academy
West Point, US
nina.w.14@gmail.com

***Abstract*—The cybersecurity field has exponentially grown in recent history, with little to no general understanding of the requirements for professionals in the area. In 2018, it was estimated that 3.5 million cybersecurity jobs would be unfilled by 2021 globally. Many students associate the cybersecurity field with computer programming and hacking, unaware of the societal importance of this career path and its connection to many majors unrelated to computer science or computer engineering. Previous work in cybersecurity education has focused on tools that aid students in understanding specific concepts. None has taken the approach of clarifying the cybersecurity profession in the form of a short-duration seminar series. With this goal, we propose an introductory seminar and a follow-on optional seminar series. The implementation of such a strategy early in undergraduate education may allow students to connect the cybersecurity career paths to one of their societal benefits. This series is designed to provide the student with direct practical examples and thought-provoking questions for the applications of security in their daily life, emphasizing multidisciplinary aspects of the field. This paper describes our experience with this seminar series at a large public university in the Fall of 2021 and Spring of 2022. We evaluate the effectiveness of the proposed approach by assessing its impact on students' perceived awareness of cybersecurity careers and their interest in cybersecurity minors. Through this study, we observe that the seminar series resulted in an increase in student confidence regarding their understanding of the cybersecurity profession. The data also revealed an increased interest in the cybersecurity minors offered in our institution. Our implementation of this new seminar-based intervention has been limited to providing it as an extracurricular activity among many, therefore reaching only a small part of the first-year engineering students at the university. Still, the data indicates that such a seminar series is a viable instrument to make students aware of the opportunities in a cybersecurity career, its significant demand for professionals, and its potential for addressing societal problems. We make the seminar materials publicly available to facilitate the adoption of the proposed intervention at other institutions.**

Keywords— cybersecurity, seminar, perception, undergraduate, first-year

I. INTRODUCTION

Cybersecurity has been a topic of increasing importance as the internet of things continues to expand, integrating technology into every facet of critical infrastructure, daily business, and lives. Recently, in May of 2021, U.S. President Joseph Biden published the "Executive Order on Improving the Nation's Cybersecurity (14028)" [1], identifying the work necessary to improve national defense. In the past decade, there has been no shortage of leaders calling for action, guidance, and mentorship. Higher education must provide students of all disciplines an opportunity to obtain a basic understanding of cybersecurity early in their academic journey, adding the security career perspective to their future learning.

Our schooling systems are not currently exposing the importance of cybersecurity to students at large, contributing to a widening workforce gap of available security professionals. The International Information System Security Certification Consortium $(ISC)^2$ projects the global security workforce shortage to reach 1.8 million between 2017 and 2022 [2]. Thus, with over 1 million workforce shortages in cybersecurity outside of the United States, cybersecurity education is a worldwide issue. Considering this need for cybersecurity education globally, the infrastructure of schools and the ability of educators to provide cybersecurity education at every level are critical.

To address the widening workforce gap, we propose an introductory seminar and follow-on optional seminar series to increase first-year undergraduate understanding of the security dilemma. These seminars are designed to directly answer questions students have about their role in security and its impacts on society. Interest in the cybersecurity field is clouded by the misconception that the price of entrance is a highly technical skill set, one which is difficult or impossible to acquire. According to the 2020 $(ISC)^2$ Cybersecurity Perception Study, 61% of respondents believed they would require additional education before applying to a cybersecurity job [21]. The proposed seminar series seeks to emphasize the interdisciplinary aspects of cybersecurity, expose students to the basic terminology of cybersecurity, and give students an

1. This work was carried out while the author was at Texas A&M University.

understanding of the many possible paths forward within the field. Overall, our goal is to address the cybersecurity workforce gap and understand how student perception of the field of cybersecurity can improve. Our research question, therefore, is to assess the potential of a seminar series tailored to students of all backgrounds beneficial for improving student perception of the cyber security profession.

This paper is organized as follows: Section 2 discusses the prior work within the cybersecurity education research area. Section 3 describes our methodology. Section 4 details the structure of the seminars and the topics discussed in each. Section 5 describes the survey method implemented in our work and the subsequent feedback and trends observed. Section 6 highlights the components essential to the effective implementation of this program and suggests improvements for future deployments.

II. Related Work

Our analysis of previous work addressing the problem of cybersecurity education uses the systematic literature review of cybersecurity education papers by Svabensky et al. [4] as a primary resource. This work reviewed 71 papers on cybersecurity education published through the ACM Special Interest Group on Computer Science Education (SIGCSE) and ACM Innovation and Technology in Computer Science Education (ITiCSE) conferences between 2010 and 2019. We include work published in other venues to achieve a more comprehensive view of the state-of-the-art. To delineate the scope of work, it is helpful to define cybersecurity. We adopt the definition by the National Institute of Standards and Technology [5]: cybersecurity is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems services, wire communication, and electronic communication … to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation". The different roles and aspects of the cybersecurity problem require specialized comprehension with a multidisciplinary approach. Previous work in cybersecurity education research can be categorized into two approaches: tools and processes. Both have the goal of making abstract topics, allowing for easier retention and comprehension.

Tools involve new software that aids student comprehension of cybersecurity abstractions or mechanisms by providing visualizations or hand-on experimentation. D. Schweitzer and J. Boleng [6] designed a simulator tool to help students understand stack frames in memory and demonstrated its effectiveness when presented to students in a single lecture and lab. Walker et al.[7] addressed the topic of integer representation through visualizations and analysis of C code security; they demonstrated the effectiveness of their tool through increased positive student perception regarding their ability to use integers in their code. Flushman et al.[8] reviewed the application of capture-the-flag challenges, puzzle-based learning, and alternate reality games in introductory computer science courses, showing that exercising key concepts in usage scenarios increases retention.

The *Process* approach in cybersecurity education refers to course implementations or course structure reviews that may improve student learning. Egelman et al.[9] derived ten privacy principles to aid in structuring the curriculum by providing easy-to-remember concepts for students. Basawapatna et al.[10] reviewed the effectiveness of a project-first approach, allowing students to learn and implement principles in parallel to their exposure to principles, demonstrating students were able to accomplish more in projects. Mack et al.[11] analyzed the student retention of programming and security topics by contrasting content delivery through powerpoint-based lectures with the usage of hands-on implementation that leads to one culminating project. They concluded that, overall, students with the powerpoint-based lessons learned how to code but could not always explain how or why their code worked. George et al. [12] proposed a shift of instruction from offense/defense to offense/defense/use, providing a third perspective of usable security in systems from a development level. Through these lenses, the authors argue the security problem is more evident. Research analyzing broader or more complex concepts (i.e., requiring multiple modules or seminars over a full semester or more) focuses on the conceptual class structure, not on course content.

Other research projects in cybersecurity education strive to address the growing lack of diversity within the cybersecurity profession. A working group of nine professionals reviewed 82 papers [13] to identify trends in cybersecurity research and recruitment of a diverse student population. Methods for equitable access for students from various levels of high school education included summer camps, pre-college activities, and introductory courses. Approaches for infusing cybersecurity education in student life included the integration of security into existing computer science curricula, offering specific courses designed for general populations, and incorporating undergraduate students in research projects. Crichigno et al.[14] develop curriculum for virtual laboratories to address the cybersecurity workforce gap. Their curriculum focuses on technical skills and teamwork to ease students' transition from academia to the workplace through the acquisition of marketable skills. They found students thoroughly enjoyed the real-time application of security topics, motivating them to continue with the program and complete the remaining curriculum requirements.

Largely, the tools and concepts evaluated through cybersecurity education research focus on the learning experience for students who have already entered the security field or taken computer-centric coursework. Our project has different motivations and goals. The gap in previous work is an optimized class structure, potentially a set of module seminars, to increase positive perceptions of cybersecurity for students with no prior exposure. Conceptual tools specifically addressing the field's interdisciplinary nature have the potential to bring more talent to the area. To effectively evolve student perception of cybersecurity, we designed a cybersecurity seminar targeting the general student population. We evaluate how the proposed intervention method impacts student perception of the field of cybersecurity.

III. Seminar Series Methodology

Our proposed seminar series applies the basic cybersecurity themes to real-world events without requiring any technical background. The seminar series' structure has one introductory seminar and three optional seminars covering five themes. The introductory seminar, titled 'The Security Dilemma', reviews the shift from a 'move fast and break things' mentality to a 'move slow and clean your code' process. The introductory seminar was designed to stand on its own; the following-on seminars are optional. The second seminar, titled 'How and why are we attacked?', is designed to present specific attack types and real-world examples of each. The third optional seminar, 'Who is regulating cyber?', discusses the current policies and legal regulations applicable to the security dilemma. The final optional seminar, titled 'What is the solution?', covers the personnel required to take on the societal security challenge, the tools necessary to secure our systems, and the mindset developers must embody in their system and software development practices. The content in each seminar is described below, highlighting their five take-away themes.

The four seminars can be offered in different configurations, providing instructors with tools for each theme without dictating structure. The seminars were designed in four parts to address each topic in detail while providing application scenarios for each. The implementation we assessed utilized three installments where the second session contains an abridged version of the last two seminars ('How and why are we attacked?' and 'Who is regulating Cyber?'). This amended implementation was chosen to minimize scheduling conflicts and voluntary student time commitment, reducing barriers to student participation in evening seminars with no academic credit, food, or monetary compensation. The abridged seminar series covers the themes of *Reconnaissance*, *Intercept*, *Invade*, *External Domino Effects*, and *Privacy is Key,* whose descriptions can be found in Sections 3.2 and 3.3. The use of these themes gives students insight into the processes implemented for threat modeling and penetration testing while providing technical details on the approaches used by attackers.

We propose a low-level exposition of cybersecurity minimizing technical details but designed to highlight its societal value and connect concepts with incidents that received extensive coverage in the media with the goal of changing student perception of cybersecurity. The development of each topic and themes therein involved a review of two cybersecurity textbooks [15, 16] utilized in undergraduate and graduate level foundations of cybersecurity courses. Topics that were highlighted frequently or referenced often became primary themes that answer in detail larger thematic questions in terms of who, what, and how. For each topic chosen from the foundational texts, we analyzed recently published cybersecurity attacks, events, or developments to find the most applicable real-world associations. This allowed for the development of a focus question that guides students to think about the theme within their lives and experience. This interactive question is then followed by the previously defined real-world scenario addressing the theme. This presentation format aims to guide the students as they formulate an understanding of the broad theme in their lives and its manifestation in real events. To reinforce the importance of each theme within the larger topic of cybersecurity, topics are re-emphasized in support of other topics; for example, there is a repetition of themes such as internet interconnectivity in two of the seminars (namely, 'everything is connected' and 'the external domino effect'.)

The appendix (Section VII) lists the main themes communicated in each seminar. The structure of theme, its personal applications, real-world scenarios, and high-level theme technical detail reinforce the societal value of understanding security to all students at any level. Student understanding of concepts' societal value has been shown to be influential in driving women and underrepresented minorities to stay within the computing field [28]. Making this seminar series available to students of every background allows students to understand the risks and responsibilities of personal and organizational decision-making regarding cybersecurity.

IV. Evaluation

The seminar series' target audience is first- or second-year students at the undergraduate level. In our deployment of the proposed seminar series, students voluntarily attended a number of the seminars. These students may or may not have decided on a field of study, major or minor. We seek to determine if students' perception of cybersecurity can be positively bettered through participation in the seminar series.

A. Recruitment

Students were recruited using email and flyers distributed to first- or second-year seminar-style courses (i.e., required courses covering a broad range of topics) within the Texas A&M University College of Engineering. We targeted these introductory seminar-style courses because they are offered to large populations of undergraduate students within their first two years of study. These courses provide students with a view of the academic unit and its activities, such as the learning and research opportunities available. Additionally, the College of Engineering class size in our university is limited to 100 students, except for seminar courses. This exemption allows us to target the largest population of students through a single seminar presentation alone. We estimated that 850 students in the College of Engineering received direct communication through email or an announcement within a seminar course. Email communication is often ignored by students [29, 30], therefore, most likely, our advertisement efforts reached considerably less than 850 students. Other forms of recruitment involving face-to-face interaction were not pursued due to Covid-19 precautions. A broader distribution of the seminar information was not made in an effort to ensure the students recruited were of the targeted student level. Participation in all three seminars of the series was rewarded with a copy of Nicole Perloth's book 'This is how they tell me the world ends'[17].

B. Survey Implementation

The introductory seminar (i.e., the first one in the cybersecurity series) begins with asking the students to fill up a survey designed to record students' initial understanding and

perception of the cybersecurity profession. These surveys captured composite trends of perception and did not preserve personally identifiable information. At the end of the final seminar within the series, all attendees are asked to complete a follow-up survey to assess the effect of the seminar on the student's perception. Participation in the pre- and post-surveys is strictly optional and not a condition of attendance of the seminar. Students access the survey using their mobile devices or computers, based on a quick response (QR) code projected on the classroom display.

The survey is implemented utilizing the Likert scale, determining a subject's agreement with the statements presented to them [31]. Likert scales are best used for determining perception regarding specific topics or opinions [32]. The structure of the survey is divided into three categories: Impression of the Cyber Security Profession (Impression), Understanding of the Impact of Cyber Security (Understanding), and Decision Regarding their Participation in a Cybersecurity Minor (Decision). These categories assist in focusing our assessment on student perception over time. Using these three categories, we can numerically gauge students' initial and follow-on perception of the profession and their potential role in it. The responses are limited to a drop-down menu with 'Strongly Agree', 'Somewhat Agree', 'Neither Agree or Disagree', 'Somewhat Disagree', and 'Strongly Disagree'. The questions are listed as follows:

1. The cyber security profession is easy to understand. (Impression)
2. Nothing can be done to protect my data from attackers. (Impression)
3. The security of programs I write is important to me. (Impression)
4. The security of applications I use is important to me. (Impression)
5. I can eliminate buffer overflows from my programs. (Understanding)
6. I understand the concept of a zero-trust architecture. (Understanding)
7. Cyber-attacks have an impact on my life. (Understanding)
8. I will be pursuing a cyber minor. (Decision)
9. The cyber minor will increase my understanding of security. (Decision)
10. I must be a CS major to be prepared to participate in the cyber minor. (Decision)

Questions 3, 5, and 6 violate the seminar's assumption of no background requirements. The questions phrased with a cybersecurity vocabulary were included in this study because the recruitment efforts were made specifically within the College of Engineering. These technical questions also seek to determine students' state of exposure before attending the seminars. These questions, when revealing a low expected perception, indicate little to no technical understanding. In addition to these ten questions, students are given the option to provide the gender they identify with via a drop-down menu of 'Male', 'Female', 'Non-Binary', and 'Prefer not to say'. This allows for an understanding of perception based on gender and the potential impact of the seminar series on each identified gender.

V. Survey Results

To establish a control group of expected first- and second-year student understanding, the introductory seminar ('The Security Dilemma') was presented to the seminar-style course *Introduction to Computing* (CSCE 1X) offered in the Fall 2021 term. Three majors require this course: Bachelors of Science in Computer Science, Bachelors of Science in Computer Engineering, and Bachelors of Arts in Computing. Most students take the course in their second year, immediately following acceptance into one of the three specified majors. By capturing the views of students in this course, we created a picture of second-year student impressions. This cohort was used as the control group because these students had previous exposure to coding but not to cybersecurity. The participation in the optional survey was high, with 279 student responses. The demographics captured through the survey revealed 81% male, 16% female, 2% non-binary, and 1% preferred not to say.

The baseline impression in 'Impression of the Cyber Security Profession' showed that students largely had a negative perception of technical questions such as zero-trust architectures or buffer overflows, as can be expected given their little or no technical understanding of cybersecurity. They also believe the cyber security profession is difficult to understand. However, students did understand that actions can be taken to protect their data. In the category of 'Understanding of the Impact of Cyber Security', students understood that cyber-attacks play a role in their lives and value the security of the applications they use and build. In the category of 'Decision Regarding their Participation in a Cyber Minor', students understood the minor would increase their understanding. Most students at the time of the seminar were undecided on whether to pursue a minor; 42% of students were unsure if the cyber minor was restricted to computer science majors.

Two separate iterations of the abridged (i.e., three seminars format) cybersecurity series were performed for evaluation of the proposed seminar intervention. Iteration one took place following the introductory seminar delivered to the students registered in the CSCE 1X course. The two follow-on seminars were scheduled over the course of five weeks, one every other week within the fall of 2021: 28 September, 12 October, and 26 October. The second iteration was offered under a condensed timeline of two weeks within the spring of 2022: 8 February, 10 February, and 15 February. We chose this shorter timeline to leverage the period in the semester before students prioritize midterms or exams.

The attendance maintained a population of 6-10 students in iteration one (Fall 2021) and 9-11 students in iteration two (Spring 2022). In iteration one of our interventions, we had six voluntary participants in the primary introductory seminar, six participants in the second seminar, and 10 participants in the third seminar. This level of participation, although small in relation to the number of students recruited, is at the expected level of participation for an evening extra-curricular activity

due to student perceived barriers to participation. Barriers to participation in these seminars included its voluntary status, no academic incentives, occurrence during the evening, and the location (at the computer science department building) far from the primary undergraduate engineering building.

Student impression from the introductory seminar in the three-seminar series is consistent with that of the baseline impressions from CSCE 1X. Upon conclusion, ten students completed the closing survey we used to evaluate final impressions of cybersecurity and specifically their interest in the cybersecurity minor. Within these populations, we were able to analyze the change in student perception through the seminars utilizing student interest in the cyber minor. Figure 1 shows the degree of influence on student attendees, looking specifically at the question "I will be pursuing a cyber minor", based on the percentage of student respondents per level of agreement. Within this small population, we observed a strong increase in interest in the minor through a higher percentage of 'Strongly Agree' responses in the final seminar post-survey.

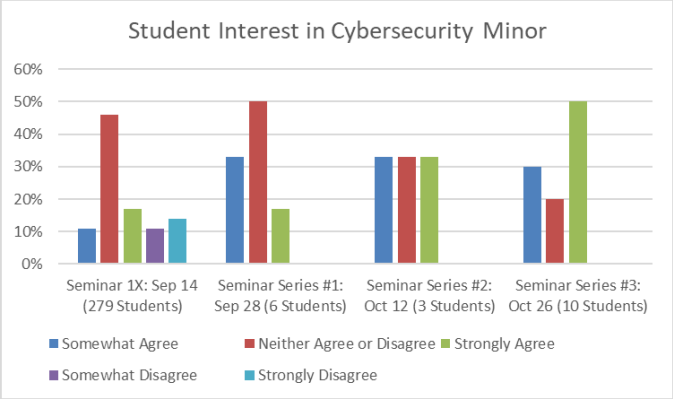

Figure 1. Analysis of student interest in the cybersecurity minor following the baseline and each seminar in Iteration One of the proposed seminar series.

Our assessment indicates that through the first iteration, seminar attendance changed student impression in the category of 'Impression of the Cyber Security Profession' to one of more confidence in their understanding of zero-trust architectures. In the category of 'Decision Regarding their Participation in a Cyber Minor', students understood the minor would increase their understanding, and it was not restricted to computer science majors. Furthermore, 80% decided on actively pursuing a minor in comparison to 28% in the baseline (i.e., the introductory seminar delivered in CSCE 1X) and 50% from the introductory seminar in iteration one. Due to the anonymity of our survey, it is not possible to determine if the students registered for the Cyber Minor.

Our second iteration of the seminar series had a population of nine students from more diverse year groups. Our audience in the introductory seminar had 2 first-year, 2 second-year, 3 third-year, 1 fourth-year, and 1 fifth-year student. The audience composition in the third (final) seminar had 2 first-year, 1 second-year, 2 third-year, 2 fourth-year, and 2 fifth-year students. However, upon the conclusion of the seminar series, only four students provided final surveys. All four students were fourth- or fifth-year students. The first- through third-year students opted out of completing the last survey. Given the scarcity of data, we cannot accurately assess how the second iteration impacted students' perceptions. Similarly, the information regarding their interest in the minor, as the respondents can no longer be influenced to participate in the cybersecurity minor: either they were already in the minor or they were too close to graduation to make it viable. The category 'Impression of the Cyber Security Profession' reflected that of the baseline group: they believe the profession is unclear and understand they can take actions to protect their data. Their 'Understanding of the Impact of Cyber Security' reflected that of the baseline as they believed cyber-attacks play a role in their lives and value the security of the applications they use and build.

The participation in the seminar series of students who were past their first and second years was unexpected. It was also surprising that, although half of these students were already being educated through the cybersecurity minor, all four survey participants reported an increased understanding of zero-trust networks.

Multiple students gave verbal feedback following the seminar, all thanking the instructor for the opportunity. Previously unanswered open-ended comment boxes were utilized in student responses to this mixed-method survey. The two student opinions quoted below indicate that the material covered in the seminar series was informative even for students with a high level of exposure to cybersecurity:

- "I believe the topics covered gave a better understanding of cybersecurity. I have read books in the field for about two years and still learned some new things in this seminar series."
- "I have really enjoyed the series so far and learning about cyber security this past week has really motivated me to spend more time being up to date on cyber security standards both in my personal life and in my career moving forward. Thank you so much for your time."

Overall, the effect of the seminar was one of increased perception of cybersecurity through student reports of a desire to learn more about cybersecurity and potentially join the cybersecurity minor. Students felt more confident in basic terminology and, where applicable, reported interest in pursuing the cybersecurity minor. The second iteration, specifically, revealed that students of more advanced year groups reported increased perception of cybersecurity from the structure and representation of cybersecurity themes taught in the provided manner.

VI. Conclusion and Future Work

The implementation of the proposed intervention (namely, a seminar series with the content described in the Appendix) only reached a small participant population of students. But there are promising signs that this simple intervention can be fruitful. Undergraduate first-year students demonstrated a

positive transformation of their perceptions of cybersecurity. Students who participated in the seminar series increased their overall interest and established a positive perception of the cyber security field.

This implementation was limited by fewer advertising and outreach capabilities available as our students came back to campus after the prolonged period of online learning and with new COVID-19 precautions such as social distancing practices. As a result, the assessment involved only a small cohort of students with an assumed lack of exposure to cyber security. The population of our seminar series participants restricted the scope and strength of statistical analyses of our survey results. Another limitation of our research is that our analysis and processes could only capture immediate changes in student perception of the cybersecurity field. Our research question attempts to analyze this but cannot capture the change in student perception over time or future increases in interest in cybersecurity following the seminar series. Lastly, our survey included technical questions whose interpretations could be affected by a student's understanding (or lack thereof) of the question. These technical questions may confuse survey results and therefore were not included in our analysis.

However, there is potential for broader impact if reaching populations from outside the College of Engineering. The content of the seminar series can still be useful for instructors in cybersecurity courses, as the material can provide clarity and application to classroom learning of cybersecurity. The use of current events and thought-provoking questions and discussion reiterate the concepts and the importance of the security themes. Our second cohort demonstrated the impact of such a structure through their appreciation of the seminar and their self-reported increased understanding, even for students who already had significant knowledge in the area.

Future implementations of this seminar series could be completed as a reception process for new first-year students. Introducing incoming freshmen of all departments to basic cybersecurity topics allows the student to understand their role as a user and exposes the interdisciplinary nature of the field. To achieve large participation, scheduling times should be prior to heavy course loads, allowing students to learn about the field. This would provide all students with exposure to the basic themes of cybersecurity defined in the introductory seminar. Students of all majors should be afforded the opportunity to learn more about cybersecurity in their daily lives and its interdisciplinary nature.

Future implementations with a focus on engineering students should extend the length of the seminar and incorporate introductory capture the flag activities which match the themes discussed. To measure the change in student perception regarding the cyber security minor, registration numbers for the minor should be monitored following the implementation of the series to maintain anonymity and student questions, comments and in-seminar interactions should be recorded. Recording all interactions resulting from the seminar series can help analyze how the student perception is truly changed. This would reveal if the use of thought-provoking questions, current events, or the discussion of the two in relation to technical terms assisted in positively changing student perception of cybersecurity. In parallel to this work, a map for introductory exposure and measurement tools for technical skillsets can greatly assist instructors in clarifying the field of cybersecurity. Additionally, this seminar series could be tested as a reinforcing tool for topics covered in security-centric coursework. The second cohort in this study demonstrated that regardless of year group, all security students could benefit from exposure to a real-world and application-based seminar series.

To aid in future implementations of the proposed approach in other institutions, the materials developed for the seminar series and supporting discussion guides have been made available for public use at https://sites.google.com/view/cyberexplained/home. We will also release lesson plans on the website.

VII. ACKNOWLEDGMENTS

The study was reviewed by the Institutional Review Board at Texas A&M University (IRB2021-0937) with a reference number of 131805.

VIII. APPENDIX – SEMINAR CONTENT

The following subsections summarize the main themes communicated in each seminar. For conciseness, the vocabulary in the descriptions below assumes cybersecurity expertise. The delivery of the material does not presuppose previous students' cybersecurity knowledge.

A. Introductory Seminar: The Security Dilemma

1. Everything is Connected
   The internet was designed to bring connections across the world [16]. However, the connection the internet now provides was not created to be isolated from bad actors, secure against bad actors, or disrupted by bad actors. The fundamental connection of the internet architecture highlights the need for specialized network management and construction to maintain the cybersecurity tenets of confidentiality, availability, and integrity.
2. Users are Essential
   Given the nature of internet connectivity, users must understand their role in security. Users are often the weakest link in cybersecurity efforts, making the strength of the cybersecurity infrastructure reliant on user behavior and understanding. User security requires regular software updates, monitoring of suspicious connections or communications, maintaining system access as necessary, and timely reporting of abnormal events. Social engineering is the most common tool for attackers to entry into systems, making it essential for users to understand how they are targeted.
3. Nothing is 100%
   High-profile equipment, software, and personnel have gained the trust of users over time, decreasing the socially perceived impact of user diligence in security. However, recent attacks show that the user must maintain attentiveness in their communications, understanding the possibility of a data leak or hack. Nothing is 100% secure,

therefore our actions in systems should not rely on them being 100% secure.

4. Slow and Secure Coding
   In contradiction to Facebook's original motto of "Move fast and break things" [18], this theme highlights that security begins at the design desk. Poorly designed code rushed to completion without testing is often riddled with exploitable vulnerabilities, such as buffer overflows, logical errors, and unchecked variables. Students must understand that their role as software development team members requires that their design, code, and operations be logically secure against simple vulnerabilities. When software is rushed to completion, external actors have a higher chance of finding vulnerabilities. This gives way to threats such as 'zero day' exploits, which can alter the intent of developed code in drastic ways.
5. Use your Tools
   The National Institute of Standards and Technology (NIST) has provided guidelines and templates that promote security at the organization level. Secure coding practices are necessary to minimize the power of exploits at the architectural and implementation levels. Proper use of encryption tools, dual-factor authentication, and frequent updates by the user or through security as a service (SaaS) are necessary to limit the power of cyber-attacks in our society. A combination of user security, organizational security, and network security are required to implement a tiered structure that can prevent, detect, and respond to attacks appropriately.

B. Seminar 2: How and why are we attacked?

1. Reconnaissance
   Observing the attacker kill chain, we highlight specific components to describe how attackers complete their exploits. Reconnaissance is the collection of data enabling attackers to prepare for or complete [external] subsequent attacks. Reconnaissance provides essential information needed to carry out ransomware attacks, data breaches, or manipulation of the data itself to portray an altered reality. The completion of reconnaissance gives information that is ultimately used in pursuit of final attack objectives: destruction, ransom, or espionage.
2. Intercept
   Cyber-attacks, such as man-in-the-middle, eavesdropping, phishing, and denial-of-service, can be visualized as a communication line that has been intercepted, corrupted, or spoofed. Communication is fundamental to the operation of the internet but requires connections that can, by failure to design with security in mind, be overwhelmed, disrupted, impersonated, and monitored. To prevent these attacks, users must understand the differences between legitimate and illegitimate communications in the form of emails, links, or webpages.
3. Invade
   The invasion of our systems is typically carried out with a form of malware such as a virus, worm, or trojan horse [19]. These invasion attacks target networks, databases, or programs following the interception, corruption, or spoof of the communication line. Defense against the invasion of interconnected systems requires continuous monitoring to determine when misuse or malware has been executed and limit its damage.
4. External Domino Effect
   Cyber-attacks have grown from isolated events on small network shared systems to nation-state manipulation of critical infrastructure and public opinions [17]. The use of networked devices within the United States has exponentially increased per capita, subsequently increasing the attack surface of the country [20]. Almost every component of our daily lives is connected to the internet, databases, or technology vulnerable to adversaries who can cause delays in communication, falsifying of information, or destruction of data and infrastructure. Ultimately, the tools we utilize can be easily manipulated to disrupt many services which support society, causing extensive damage at a high economic cost.
5. Mutually Assured Destruction
   The lethality and effectiveness of cyber weapons have grown as leaders around the world work to improve their cyber capabilities. Nation-state development of cyber offensive tools has demonstrated the willingness of government actors to utilize the weaknesses of civilian and military organizations within opposing countries. An example is the NotPetya attack, in which Russian cyber offensive actions shut down major infrastructure operations in Ukraine in 2017 [21]. If the same tools used against Ukraine were utilized against a country with similar cyber capabilities, this would lead to the destruction of both countries' digital capabilities. These tools have been generated as the next generation of critical weapons, as each country develops its capabilities and warns others of their potential power if provoked.

C . Seminar 3: Who is regulating cyber?

1. Privacy is Key
   User trust is at the heart of all security requirements and is essential to understand as a responsible digital citizen. Trust is built between providers and users as their information must be maintained with privacy in mind, and users must abide by provider security standards. Privacy of user personal information must be prioritized by businesses and organizations that handle transactions. Transactions are the essence of the internet, allowing people to exchange goods, money, ideas, and health information in real-time. However, these transactions must be regulated to ensure they are not fraudulent and protected against unauthorized disclosure. Legal policies such as Gramm-Leach- Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) ensure our monetary information and medical information are protected within databases to ensure our privacy as individuals in specific transactions [22, 23]. However, regulation with a wider reach of protection in the realm of digital security must be tackled.
2. Reasonable and Necessary
   U.S. cybersecurity policy foundationally utilizes freedom of personal risk. Organizations can determine the structure

and implementation of their cyber security infrastructure as long as they provide the reasonable and necessary measures that ensure the security of personal data within their systems. This theme is the primary element of the Federal Trade Commission (FTC) Act Section 5, which utilizes general language to provide security and privacy expectations for business and internet transactions [24]. This law ensures organizations take steps to secure customers' privacy and minimize identity theft through the 'red flags rule' to guide those decisions. However, it also leaves the determination of reasonable protection open to interpretation. Ambiguity and vagueness cause organizations and customers to accept risk where it may not be reasonable, leading to large organizational security gaps.

3. Level up
   As digital information is created, it is classified into different tiers for security protection. Low classifications typically have lower security requirements. Level up requires that we fully understand what the data contained in our systems can identify or track in terms of people, money, and private information. As more data is contained within the system, the classification and security of the system must be increased.
4. Healthcare and Trade
   Medical privacy is a significant driver for the security industry due to the high volume of personally identifiable information stored in medical systems. However, cybersecurity in hospitals is often outsourced, with few hospitals employing in-house security personnel [25]. The Health Insurance Portability and Accountability Act (HIPAA) specifically regulates the requirements of medical data managed regardless of organizational structure [26]. International trade is another main driver in cybersecurity regulation as communications, knowledge transfer, and monetary exchange all require high levels of security. The FTC bears responsibility for the regulation and verification of the authenticity of electronic transactions by consumer companies, utilizing criminal punishments as their leverage on cybercriminals [27].
5. Trust
   Trust in new systems relies on the personal integrity and understood boundaries of the designers regarding the data manipulated and collected within their systems. Developers must realize that security begins with a security-focused design that agrees upon trust boundaries and minimizes trust granted to shared external parties. The user can then trust their information is not shared with untrusting sites. User integrity and proper system use are then required for daily transactions to maintain security. Trust relationships are prominent targets for adversarial actions, maintaining cultures of 'reluctance to trust' is essential to decrease the trust-based attack surface [19].

C. Seminar 4: What is the solution?

1. Protect the Castle
   This theme can be explored through firewalls, zero-trust networks, anti-virus software, frequent software updates, measurable audits, and regular user training to ensure organization security policies are followed. Audits provide feedback to the organization and employees regarding areas requiring emphasis or further user training for proper security maintenance and stronger security postures.
2. Demand the Standard
   The highest security standard should be expected and requested of the organizations we trust. Reading and understanding user agreements and default settings of applications and networks are essential to understanding the level of trust organizations are willing and able to provide. If the highest standard is not being met within these agreements, members should feel comfortable requesting additional protection for their data, intellectual property, and personally identifiable information.
3. Govern the Hack
   Governing the hack seeks to highlight the need for the government to hold businesses accountable for cyber defense. Citizens need to advocate for and push their representatives to vote for the protection of critical infrastructure. Cybersecurity journalist Nicole Perlroth highlights the idea that cyber weapons stockpiled by government organizations leave the users of exploitable systems vulnerable until they are patched by owning businesses. These patches can only be created when discovered by the owning business or released by the government to the owning business [17]. Vulnerabilities stockpiled by governments do not last forever and must be reviewed periodically to ensure the security of consumer products is not diminished by government stockpiles. Thus, the government must hold itself and the businesses that provide technology products accountable regarding cyber defense.
4. Continue Learning
   Technology is one of the fastest-growing and changing fields. Within this industry, individual dedication to learning new approaches to risk management, software development techniques, networking skills, cybersecurity compliance regulations, and design processes is key to the comprehension of the field.
5. Find YOUR Path
   Utilizing tools such as the NIST NICE framework, students can understand how to plan and progress within the field of cybersecurity. The growth and interdisciplinary nature of the area have naturally built new positions at various levels of technical application. This theme utilizes the www.cyberseek.org tool to discuss the wide array of positions and requirements of different pathways within the cybersecurity field.

REFERENCES

[1] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed Jun. 23, 2021).

[2] L. Tsado, "Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach," Journal of Cybersecurity Education, Research and Practice, 2019(1),4.

[3] "2020 (ISC)2 Cybersecurity Perception Study." https://www.isc2.org:443/Research/Perception-Study (accessed Feb. 18, 2022).

[4] V. Švábenský, J. Vykopal, and P. Čeleda, "What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences," in Proceedings of the 51st ACM Technical Symposium on Computer Science Education, New York, NY, USA, Feb. 2020, pp. 2–8. doi: 10.1145/3328778.3366816.

[5] C. C. Editor, "cybersecurity - Glossary | CSRC." https://csrc.nist.gov/glossary/term/cybersecurity (accessed Jul. 26, 2021).

[6] D. Schweitzer and J. Boleng, "A simple machine simulator for teaching stack frames," in Proceedings of the 41st ACM technical symposium on Computer science education - SIGCSE '10, Milwaukee, Wisconsin, USA, 2010, p. 361. doi: 10.1145/1734263.1734387.

[7] J. Walker, M. Wang, S. Carr, J. Mayo, and C.-K. Shene, "Teaching Integer Security Using Simple Visualizations," in Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education, Aberdeen Scotland Uk, Jul. 2019, pp. 513–519. doi: 10.1145/3304221.3319760.

[8] T. R. Flushman, M. Gondree, and Z. N. J. Peterson, "This is Not a Game: Early Observations on Using Alternate Reality Games for Teaching Security Concepts to First-Year Undergraduates," 8th Workshop on Cyber Security Experimentation and Test (CSET 15), Washington, DC, Aug 2015, p. 8, https://www.usenix.org/biblio/not-game-early-observations-using-alternate-reality-games-teaching-security-concepts-first.

[9] S. Egelman, J. Bernd, G. Friedland, and D. Garcia, "The Teaching Privacy Curriculum," in Proceedings of the 47th ACM Technical Symposium on Computing Science Education, Memphis Tennessee USA, Feb. 2016, pp. 591–596. doi: 10.1145/2839509.2844619.

[10] A. R. Basawapatna, A. Repenning, K. H. Koh, and H. Nickerson, "The zones of proximal flow: guiding students through a space of computational thinking skills and challenges," in Proceedings of the ninth annual international ACM conference on International computing education research, San Diego San California USA, Aug. 2013, pp. 67–74. doi: 10.1145/2493394.2493404.

[11] N. A. Mack, K. Womack, E. W. Huff Jr., R. Cummings, N. Dowling, and K. Gosha, "From Midshipmen to Cyber Pros: Training Minority Naval Reserve Officer Training Corp Students for Cybersecurity," in Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis MN USA, Feb. 2019, pp. 726–730. doi: 10.1145/3287324.3287500.

[12] B. George, M. Klems, and A. Valeva, "A method for incorporating usable security into computer security courses," in Proceeding of the 44th ACM technical symposium on Computer science education - SIGCSE '13, Denver, Colorado, USA, 2013, p. 681. doi: 10.1145/2445196.2445395.

[13] X. Mountrouidou et al., "Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education," in Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, Aberdeen Scotland Uk, Dec. 2019, pp. 157–176. doi: 10.1145/3344429.3372507.

[14] J. Crichigno, S. Ahmed, J. Gerdes, and R. Brookshire, "Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances," in 2019 ASEE Annual Conference & Exposition Proceedings, Tampa, Florida, Jun. 2019, p. 32481. doi: 10.18260/1-2--32481.

[15] M. T. Goodrich and R. Tamassia, Introduction to computer security. Boston: Addison-Wesley, 2011.

[16] W. A. Conklin, G. B. White, C. Cothren, R. Davis, and D. Williams, "Principles of computer security: CompTIA security+ and beyond", (exam SY0-501), Fifth edition. New York: McGraw-Hill Education, 2018.

[17] N. Perlroth, "This Is How They Tell Me The World Ends: The Cyber-Weapons Arms Race". New York, NY, USA: Bloomsbury Publishing, 2020.

[18] H. Taneja, "The Era of 'Move Fast and Break Things' Is Over," Harvard Business Review, Jan. 22, 2019. https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over (accessed Mar. 21, 2022).

[19] WM. A. Conklin and G. White, "Chapter 15: Types of Attacks and Malicious Software" in Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition, USA: McGraw-Hill Education, 2018.

[20] L. Constantin, "Enterprise internet attack surface is growing, report shows," CSO Online, Jun. 11, 2020. https://www.csoonline.com/article/3562329/enterprise-internet-attack-surface-is-growing-report-shows.html (accessed Jan. 19, 2022).

[21] J. O'Donnell and H. Jones, "European, U.S. regulators tell banks to prepare for Russian cyberattack threat," Reuters, Feb. 09, 2022. https://www.reuters.com/markets/europe/european-us-regulators-tell-banks-prepare-russian-cyberattack-threat-2022-02-09/ (accessed Mar. 21, 2022).

[22] M. G. Oxley, "H.R.3763 - 107th Congress (2001-2002): Sarbanes-Oxley Act of 2002," Jul. 30, 2002. https://www.congress.gov/bill/107th-congress/house-bill/3763 (accessed Mar. 21, 2022).

[23] P. Gramm, "S.900 - 106th Congress (1999-2000): Gramm-Leach-Bliley Act," Nov. 12, 1999. https://www.congress.gov/bill/106th-congress/senate-bill/900 (accessed Mar. 21, 2022).

[24] "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," Federal Trade Commission, Jun. 07, 2013. http://www.ftc.gov/about-ftc/mission/enforcement-authority (accessed Mar. 21, 2022).

[25] S. T. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," BMC Medical Informatics and Decision Making, vol. 20, no. 1, p. 146, Jul. 2020, doi: 10.1186/s12911-020-01161-7.

[26] "Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC," Feb. 21, 2019. https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed Mar. 21, 2022).

[27] "Privacy and Security Enforcement," Federal Trade Commission, Oct. 31, 2018. http://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (accessed Mar. 21, 2022).

[28] R. Su and J. Rounds, "All STEM fields are not created equal: People and things interests explain gender disparities across STEM fields," Frontiers in Psychology, vol. 6, 2015, https://www.frontiersin.org/article/10.3389/fpsyg.2015.00189 (accessed Feb. 21, 2022).

[29] Carnevale, Dan. "E-mail is for old people." The Chronicle of Higher Education 53, no. 7 (2006): A27. https://www.chronicle.com/article/e-mail-is-for-old-people/ (accessed Feb. 21, 2022).

[30] EAB.com, "Which emails students read—and which ones they ignore", 2016, https://eab.com/insights/daily-briefing/student-success/which-emails-students-read-and-which-ones-they-ignore/ (accessed Feb. 21, 2022).

[31] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert Scale: Explored and Explained," BJAST, vol. 7, no. 4, pp. 396–403, Jan. 2015, doi: 10.9734/BJAST/2015/14975.

[32] "Three Tips for Effectively Designing Rating Scales," Qualtrics, Jan. 15, 2021. https://www.qualtrics.com/blog/three-tips-for-effectively-using-scale-point-questions/ (accessed Jan. 19, 2022).