

CREATING AN EFFECTIVE SECURITY STREAM IN A UNIVERSITY COMPUTER SCIENCE DEGREE

Calin Anton

Department of Computer Science, MacEwan University (Canada)

Abstract

This paper presents a cybersecurity stream within a post-secondary institution's Computer Science program to meet the workforce demands for skilled security professionals. The proposed stream integrates core systems courses with specialized modules in system and network security, aligning with the ACM CS curriculum and CSEC 2017 guidelines. It emphasizes experiential learning through hands-on labs, Capture the Flag competitions, and community-based projects. Results indicate high rankings in competitions, positive feedback from community partners, job offers, and alumni success in security roles. Although current evidence is mostly anecdotal and scalability remains a challenge, the model offers a replicable framework for integrating cybersecurity education into Computer Science programs, thereby helping bridge the gap between theory and practice.

Keywords: *Cybersecurity education, experiential learning, cybersecurity stream in computer science.*

1. Introduction

Cybersecurity has become a cornerstone of modern computing, driven by the rapid expansion of digital infrastructures and the escalating frequency of cyber threats. While Computer Science (CS) programs traditionally emphasize programming, algorithms, and software engineering, they often lack structured pathways that prepare students for specialized roles in cybersecurity. Existing offerings are frequently limited to isolated courses or elective modules, leaving graduates without the comprehensive skill set required to secure systems and networks in real-world environments.

To address this gap, we propose a dedicated cybersecurity stream embedded within a regular CS degree. Beginning in the second year, the stream integrates foundational systems courses with advanced security-focused ones, complemented by experiential learning through hands-on labs, competitive challenges, and community engaged projects. This approach ensures alignment with recognized standards, such as the ACM CS curriculum (ACM-CS, 2023) and CSEC 2017 guidelines (CSEC, 2017), and promotes the practical competencies demanded by industry.

1.1. Motivation

Despite being urgently needed, Cybersecurity education is not yet well established. A recent analysis done in Europe (Ricci et al, 2024) revealed a persistent gap between university curricula and employer needs. In the United States, a different picture emerges (Crabb, Hundhausen & Gebremedhin, 2024). Among NSA-designated Centers of Academic Excellence, programs vary widely in structure and articulated learning outcomes, and rigorous evaluation of teaching methods is scarce. Together, these findings present a common challenge: departments need flexible program skeletons that turn recognized priorities into coherent course sequences, reducing variability and accelerating implementation.

The literature also shows that educators lack a common, practical bridge between workforce frameworks and curricular building blocks. Ramezani and Niemi (2024) provide a comprehensive mapping between the NICE workforce framework (NIST, 2020) and the CSEC2017 curriculum. They identify missing units and propose roadmaps tied to job categories. A systematic review of cybersecurity-related papers between 2010 and 2019 (Švábenský, Vykopal & Čeleda, 2020) shows that topics like secure programming, network security, and offensive security are common; most studies focus on U.S. universities and rely on self-reported data, with few reusable resources and no shared datasets, thus hindering replication and future improvement.

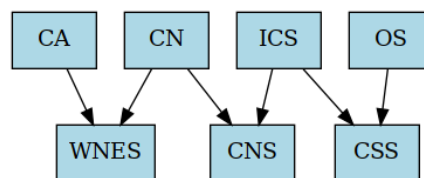
These gaps underscore the need for program proposals that align with standard frameworks and are supported by reusable resources, providing a clear blueprint for developing effective cybersecurity curricula. The proposed structure directly addresses identified gaps by integrating ACM CS curriculum

foundations and augmenting the initial two years with a systems-oriented core. It adds three security courses that focus on developing the theoretical and practical skills required by the industry. This design aligns with entry-level certifications and NICE workforce's roles, promoting employability and standardization. It also integrates experiential learning through Capture the Flag (CTF) competitions, community-engaged experiences, and a capstone project, promoting the acquisition of practical skills.

2. Structure of the proposed cybersecurity stream

The cybersecurity stream is designed to begin in the second year of a four-year CS program, building on the foundational computing sequence completed in the first year. Thus, students enter the stream with a solid experience in programming, algorithms, and data structures. The stream integrates traditional systems courses with specialized security ones, creating a consistent pathway that balances theoretical foundations with practical applications. It consists of seven courses: Computer Architecture (CA), Introduction to Computer Security (ICS), Operating Systems (OS), Computer Networks (CN), Wireless Networks and Embedded Systems (WNES), Computer Systems Security (CSS), and Computer Network Security (CNS). The prerequisite structure of these courses is presented in Figure 1.

Figure 1. Prerequisite structure.



While pursuing the cybersecurity stream, students remain aligned with the traditional CS curriculum, which includes: the introductory computing sequence (four courses covering programming, algorithms, and data structures), a software engineering course focusing on design principles and collaborative development and a capstone project, in which students work individually or in teams under faculty supervision to deliver a substantial software or systems solution. This dual-path approach ensures that students graduate with both general CS competencies and specialized cybersecurity expertise, enhancing flexibility and employability.

Courses such as OS, CA, and CN are staples of most CS programs and align closely with ACM CS curriculum recommendations. However, the stream introduces WNES, which goes beyond ACM guidelines by emphasizing embedded systems and wireless technologies, which are critical areas in modern cybersecurity due to the proliferation of IoT devices and edge computing.

2.1. Introduction to computer security (ICS)

ICS serves as the foundational course in the cybersecurity stream, introducing students to core principles and practices that underpin modern security. The theoretical component aligns with the Introduction to Computer Security course commonly found in CS programs, covering essential concepts such as the CIA triad, threat models, authentication, basic cryptographic principles as well as network and web security. These topics provide students with a conceptual framework for understanding vulnerabilities and defence mechanisms across systems and networks.

What sets ICS apart is its strong practical orientation. The course includes a comprehensive lab component delivered through a virtualized environment implemented on Microsoft Azure Lab Services. Students work within multiple virtual machines configured to simulate real-world scenarios, enabling hands-on experience with industry-standard tools.

In the labs, students explore a wide range of tools and techniques that mirror those introduced in entry-level cybersecurity certifications. These include network analyzers, firewalls, and intrusion detection/prevention systems (IDS/IPS). Students also gain exposure to basic cryptographic utilities, password crackers, network scanners, and penetration testing frameworks. Each lab emphasizes practical problem-solving, such as configuring a firewall to block unauthorized traffic or using a network scanner to identify vulnerabilities.

Beyond tool usage, ICS labs introduce students to Identity and Access Management (IAM) and fundamental networking concepts critical for security operations. Through the early introduction of these tools, the course ensures that students develop technical proficiency and an understanding of how security policies and security architecture interact. This approach bridges the gap between theory and practice, preparing students for next courses in the stream and aligning their skills with industry expectations.

2.2. Computer systems security (CSS)

CSS builds upon the foundational knowledge acquired in ICS and OS, focusing on hardening and protecting individual systems. The course assumes a secure network environment and concentrates on securing endpoints and servers that deliver critical services. The theoretical component of CSS delves deeper into cryptography, covering symmetric and asymmetric encryption algorithms, hashing techniques, and their practical applications. Students also explore the security of Windows and Linux OS, learning how to configure and maintain secure operating environments. Additional topics include Application Security and Web Security fundamentals, as well as Software Security principles, equipping students to identify and mitigate vulnerabilities in applications and services. The course also covers memory and disk forensics.

A defining feature of CSS is its intensive practical component implemented through a weekly three-hour lab session. A few lab activities use the well-established SEED labs (SEED, 2008) developed by dr. Kevin Du at Syracuse University. These activities provide guided exercises on topics such as buffer overflows, privilege escalation, cross-site scripting and secure coding practices. SEED lab activities are enhanced by incorporating current cybersecurity tools.

Most of the lab experience is organized around three components. First, students participate in National Cyber League (NCL) competitions, which simulate real-world cybersecurity scenarios and foster problem-solving under pressure. Second, they participate in community-partnered projects, applying their skills to address the actual security needs of local organizations. Third, students undertake a system setup and hardening project, where they deploy and secure popular open source applications such as DeltaChat or GitLab. This project requires students to implement best practices for securing services, managing permissions, and configuring encryption, providing a comprehensive understanding of system-level security. By combining advanced theoretical content with rigorous hands-on practice, CSS prepares students for certifications focused on Windows and Linux security, equipping them with the practical skills employers require.

2.3. Computer network security (CNS)

CNS is the advanced network security focused course in the stream, building on the foundational knowledge from CN and ICS. While CSS concentrates on securing individual systems, CNS assumes those systems are hardened and shifts the focus to protecting the network. The theoretical component of the course explores vulnerabilities and mitigation strategies for protocols operating at Layers 2, 3, and 4 of the OSI model. Students gain a deep understanding of how attacks exploit weaknesses in Ethernet, IP, and TCP/UDP, and learn defensive measures to secure these layers. The course also examines advanced topics, including firewall architectures, IDS/ISP, network access control, wireless network security, IoT device protection, cloud security, and emerging paradigms such as Zero Trust Architecture. Finally, students are introduced to network forensics, equipping them with skills to investigate and respond to breaches.

The practical component of CNS mirrors the experiential approach of CSS, with a weekly three-hour lab session dedicated to hands-on activities. Students build on the SEED labs framework by applying real-world tools and configurations to address complex network security challenges. Beyond structured labs, CNS incorporates the same experiential elements as CSS: NCL competitions and a full-term community partner project focused on designing secure network architectures or assessing network vulnerability. Therefore, this course's practical component makes it a capstone experience for the network security domain within the proposed stream.

3. Participation in national cyber league (NCL)

A distinctive feature of the cybersecurity stream is the mandatory participation in NCL competitions for students enrolled in CSS and CNS. NCL provides a realistic, gamified environment where students tackle challenges modelled on real-world cybersecurity scenarios. These competitions are structured as Jeopardy-style CTF events, covering nine major cybersecurity domains with tasks categorized as easy, medium, and hard. By engaging in NCL, students gain exposure to practical problems they are likely to encounter in professional settings, reinforcing theoretical knowledge through experiential learning.

In CSS, participation in the individual NCL game replaces the traditional final exam, emphasizing the importance of applied skills over rote memorization. CNS integrates NCL as a series of three graded assignments, corresponding to the practice, individual, and team games, respectively. Preparation for NCL is embedded into the curriculum through dedicated lab sessions, which combine theory review with hands-on exercises and practice problems. This approach enhances technical proficiency and promotes problem-solving under pressure, a critical competency in cybersecurity roles.

Beyond skill development, NCL participation has demonstrated tangible benefits for students, including increased confidence, stronger resumes, and even job offers resulting from competition performance. By making NCL a required assessment component, the stream bridges the gap between

academic learning and workforce readiness, aligning with best practices in cybersecurity education and addressing the persistent challenge of providing authentic, real-world experience within university programs.

4. Community-engaged learning projects

In addition to structured labs and competitions, the cybersecurity stream integrates community-engaged learning projects as a core experiential component in CSS and CNS. These projects connect students with real organizations, often non-profits or small businesses, allowing them to apply classroom concepts to genuine security challenges. Students collaborate with community partners to assess vulnerabilities, propose solutions, and implement proof-of-concept improvements. This approach bridges the gap between theory and practice, providing exposure to real-world constraints such as resource limitations, compliance requirements, and organizational culture. By working on real-world problems, students develop critical thinking, adaptability, and professional communication skills that traditional labs alone cannot offer.

The projects are structured to mirror professional engagements: students begin with an initial problem analysis, submit solution proposals, and deliver partial and final implementations, concluding in a formal presentation and report. Weekly meetings with community partners ensure continuous feedback and alignment with organizational needs. These experiences reinforce technical competencies and teach students how to manage client expectations, negotiate scope, and communicate effectively, skills which are essential for cybersecurity careers. Through community partnerships, the stream ensures students graduate with portfolio-ready projects and industry connections, addressing one of the most cited pitfalls in cybersecurity education: the lack of real-world experience

5. Evidence of success and limitations of this study

Several indicators demonstrate the effectiveness of the proposed cybersecurity stream. First, student performance in the NCL competitions consistently places our university among the top institutions. MacEwan consistently ranks within the top 50 schools on the NCL Power Rankings and often breaks into the top 20, competing against hundreds of universities and colleges. Individual achievements are equally impressive: most of the students finish within the top 300 out of more than 5,000 participants, while almost all of MacEwan's teams rank among the top 200 out of over 2,000 teams. These results highlight the stream's ability to develop practical, competitive skills that align with industry standards.

Second, the community-engaged learning projects integrated into CSS and CNS have received overwhelmingly positive feedback from partner organizations. All participating partners expressed satisfaction with the outcomes, and in several cases, collaborations continued beyond the initial project, demonstrating sustained value. Notably, at least two students received job offers directly from community partners, underscoring the real impact of these projects and their role in creating employment pathways. This success reflects the stream's emphasis on authentic learning experiences that bridge academic theory and professional practice.

Finally, alumni outcomes provide compelling evidence of the stream's effectiveness. A significant number of graduates have secured security-related positions in private companies and government agencies, leveraging the technical expertise and experiential learning gained through the program. These career trajectories confirm that the stream equips students with both the foundational knowledge and applied skills demanded by the cybersecurity workforce. Collectively, these achievements validate the stream as a robust, replicable model for cybersecurity education.

While the proposed cybersecurity stream shows promising outcomes, this paper acknowledges several limitations. First, the data supporting the effectiveness of the stream is sparse and largely anecdotal, drawn from competition results, partner feedback, and alumni success stories. Although these indicators are encouraging, they lack the rigour of longitudinal studies or large-scale empirical analysis. Future research should incorporate systematic data collection and quantitative metrics to validate the stream's impact on student learning and career readiness. Second, the current design assumes relatively small class sizes, capped at 40 students in our implementation. This constraint is critical because the stream relies heavily on community-engaged projects, which require intensive instructor involvement for coordination, supervision, and feedback. Scaling the model to larger cohorts could pose significant challenges, including increased workload for faculty and potential dilution of the personalized, authentic learning experience that boosts the stream's success. Addressing these scalability issues will be essential for broader adoption.

6. Practical implementation

The proposed cybersecurity stream can be adopted by CS departments without requiring a complete overhaul of faculty expertise. Instructors currently teaching OS or CN are well-positioned to specialize in cybersecurity through a structured professional development plan. In our case, the process involved three years of intensive study, culminating in a sabbatical leave dedicated to deepening knowledge and skills in cybersecurity. During this period, faculty should aim to obtain at least one entry-level cybersecurity certification, ensuring alignment with industry standards and practical competencies.

Equally important is building connections with the local cybersecurity community, such as participating in BSides conferences or joining local/regional cybersecurity groups. These networks provide opportunities for knowledge exchange, exposure to current practices, and collaboration on real-world projects. By combining formal certification with active engagement in professional communities, faculty can transition effectively into cybersecurity education roles, enabling departments to implement the stream without hiring entirely new personnel.

7. Conclusions

The cybersecurity stream presented in this paper addresses a critical gap in traditional CS curricula by offering a structured, systems focused pathway that integrates theoretical foundations with hands-on experiences. The stream combines core courses such as OS, CN and CA with specialized courses in system and network security, supported by intensive lab work and experiential components.

Evidence of success, such as strong performance in NCL competitions, positive feedback from community partners and alumni employment outcomes, demonstrates the stream's effectiveness in preparing students for real-world challenges. While limitations exist, such as reliance on anecdotal data and scalability concerns for larger cohorts, the model remains replicable and adaptable. Practical implementation strategies, including faculty specialization through professional development and engagement with local cybersecurity communities, further support its feasibility.

This paper presents a cybersecurity education approach that moves beyond isolated courses toward a cohesive, practice-oriented stream embedded within CS programs. By focusing on technical competence, problem solving ability, and industry engagement, the proposed model enhances student learning and contributes to addressing the global shortage of skilled cybersecurity professionals. Future work will focus on expanding empirical evaluation and exploring scalable solutions to ensure broader adoption across institutions.

Acknowledgments

I want to thank my current and former colleagues, Dr. Ron Meleshko, Dr. Nick Boers, Dr. Cam Macdonell, and Dr. Mohammed Elmorsy, who reviewed and helped improve the stream

References

- Computer Science Curricula 2023. ACM Press, IEEE Computer Society Press, and AAAI Press. (ACM-CS) (2023). <https://www.acm.org/media-center/2024/june/cs-2023>
- Crabb, J., Hundhausen, C., & Gebremedhin. A. (2024). A Critical Review of Cybersecurity Education in the United States. *SIGCSE 2024*, 241-247.
- CSEC. (2017). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (Report of the Joint Task Force on Cybersecurity Education). https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
- NIST. (2020). *Workforce Framework for Cybersecurity* (NICE Framework). NIST Special Publication 800-181 Revision 1. U.S. Department of Commerce, National Institute of Standards and Technology. <https://csrc.nist.gov/pubs/sp/800/181/r1/final>
- Ramezani, S. & Niemi, V. (2024) Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development, *IEEE Access*, vol. 12, PP. 61741-61766
- Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Lendak, I., & Janout, V. (2024). Understanding Cybersecurity Education Gaps in Europe. *IEEE Transactions on Education*, 67(2), 190-201.
- SEED. (2008). *SEED: A suite of instructional laboratories for computer security education*. <https://seedsecuritylabs.org>
- Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *SIGCSE 2020*, 2-8.