CyberCSP: Integrating Cybersecurity into the Computer Science Principles Course

Sumita Mishra, Rajendra K. Raj, Paul Tymann
Rochester Institute of Technology
Rochester, NY, USA
[sumita.mishra, rajendra.k.raj, paul.tymann]@rit.edu

Jamie Fagan and Sage Miller
Webster Central School District
Webster, NY, USA
[Jamie_Fagan, Sage_Miller]@websterschools.org

***Abstract*—The demand for cybersecurity professionals is projected to grow substantially, with the US Bureau of Labor Statistics reporting that employment in cybersecurity within the US will grow by 18% from 2014 to 2024, much faster than the average for all occupations. As creating a cyberspace workforce has become a matter of national security for every country, cybersecurity needs to be taught at all levels, to all students, in the educational system. The good news is that cybersecurity is also a topic that students from a wide variety of backgrounds find interesting, and as a result, it motivates them to study computing too. Over the past two decades, there has been an increased effort worldwide to incorporate computer science and computational thinking into the middle and high school curriculum. The CS10K initiative in the US has led to projects to introduce computer science at the K-12 educational level. One of these initiatives, the new Advanced Placement (AP) course in Computer Science Principles (CSP), was designed to introduce computer science in an engaging way, show students how computing is relevant in their lives, and to attract a diverse group of students to computing. The CSP Curriculum Framework allows for multiple implementations of the CSP course, permitting course designers to develop courses to engage and attract specific groups of students and that focus on specific themes in computing.**

This paper describes an approach to develop a new CSP course, CyberCSP, which integrates cybersecurity first principles throughout the course. The approach builds on an CSP course that was created from a previous collaboration between the Computer Science Department at Rochester Institute of Technology, Rochester, New York, and the Webster Central School District in Webster, New York. The paper discusses the background, details of the earlier CSP course, how relevant cybersecurity content was identified, and then integrated into the CSP course to create the CyberCSP variant of the Computer Science Principles course.

I. Introduction

Employment in cybersecurity is projected to increase substantially across the world. For example, the US Bureau of Labor Statistics reports that employment in cybersecurity is "projected to grow 18 percent from 2014 to 2024, much faster than the average for all occupations" [1]. Helping to build "the next generation's cyberspace workforce is a matter of national security, as a string of massive breaches at the federal Office of Personnel Management and private companies have highlighted" [2]. Reported hacking by Russian actors to influence the outcome of the 2016 United States election [3] is another recent example of the need for both professional cybersecurity practitioners, and computer users who understand basic cybersecurity principles and practice safe computing. Not only must cybersecurity be taught at all levels, to all students, in the educational system, but it is also a topic that students from a wide variety of backgrounds find interesting, and as a result motivates them to study computing. Introducing students to cybersecurity early in their education, in an engaging way, and showing how cybersecurity is relevant in their lives, will encourage more female and other underrepresented students to pursue careers in cybersecurity [4]–[6].

Over the past two decades, there has been an increased effort worldwide to incorporate computer science or computational thinking into the high school curriculum [7]–[9]. Within the US, the National Science Foundation started the CS10K project, which has focused on supporting projects that introduce computer science at the K-12 educational level [10]–[12]. One of these projects led to the development of the AP Computer Science Principles (CSP) course [13], which was designed to introduce computer science in an engaging way, show students how computing is relevant in their lives, and to attract a diverse group of students to computing. The CSP curriculum framework [14], allows for multiple implementations of the CSP course, permitting course designers to develop courses to engage and attract specific groups of students and that focus on specific themes in computing.

The College Board officially launched the new AP CSP course in fall 2016 and will administer the first CSP AP exam in May 2017 [14]. The AP CSP course and exam description provides a curriculum framework that details the essential information required to understand the CSP objectives and expectations. The curriculum framework allows for multiple implementations of the CSP course that enable students to develop the content knowledge and skills required to pass the AP CSP exam. These courses can be designed to engage and attract specific groups of students or can focus on specific themes in computing. Several courses to prepare students to take the AP CSP exam have been developed, and endorsed by the College Board, including following: The Beauty and Joy of Computing, an introductory computer science course developed at the University of California, Berkeley [15]; UTeach CS Principles is a complete high school curriculum, developed at the University of Texas at Austin [16]; and the course "Mobile CSP" takes the approach that developing mobile applications will motivate students to study computer science [17].

978-1-5090-5920-1/17/$31.00 ©2017 IEEE

This paper describes our approach to developing a new CSP course, CyberCSP that will integrate cybersecurity principles throughout the CSP course. The approach builds on the CSP course that was created from a previous collaboration between the Computer Science Department at Rochester Institute of Technology, Rochester, New York, and the Webster Central School District (WCSD) in Webster, New York. The next section sets the stage by presenting an overview of our existing Computer Science Principles course. Section III describes the core cybersecurity content that is needed for creating a cybersecurity-centric CSP course, and Section IV discusses our proposed CyberCSP course. Section V discusses the current status of our work, and makes a few concluding remarks.

II. Overview of our Computer Science Principles Course

Our approach is founded on long-time collaboration between RIT's Computer Science Department and WCSD, which led to the development and teaching of CSP courses during the 2011-2012 academic year at both WCSD and RIT. The WCSD/RIT partnership included an agreement to permit WCSD high school students to receive transcripted RIT credits for the CSP course taught at WCSD, perhaps the first time when college credit was granted to high school students taking CSP. The version presented here is the offering at WCSD that was taught in the 2016-2017 academic year. The RIT version was also similar.

The WCSD CSP course is designed to introduce students to the central ideas of computer science. Students engage in activities that show how computing changes the world and impacts daily lives. Students develop step-by-step written solutions to basic problems and are required to implement these solutions on a computer using a programming language. The topics of study include the history of computer development, computer hardware, networks, internets, the Internet, HTML, algorithms, programming, data representation, searching, sorting and ethical computing.

At WCSD, the CSP course can lead to AP credit through completion and submission of a portfolio and successful completion of the AP exam. The portfolio consists of two performance tasks—Explore and Create. The Explore task is an individual exploration of a significant computing innovation and involves creating a digital artifact and a written report. The Create task requires a student to develop a program on a topic that interests that interests them. A significant portion of the program must be developed independently. It is recommended that a portion of the program involve some form of collaboration with another student.

The modules delivered as part of the WCSD/RIT curriculum are shown in Table I.

TABLE I
Current CSP Outline

Module	**Title**	**Periods** (55-min)
1	Introduction	11
2	Networks, Internet and HTML	14
3	Problem Solving	10
4	Programming with Snap!	12
5	Data Representation	11
6	Sorting and Searching Algorithms	9
7	Big Data	11

III. Relevant Cybersecurity Content

To create CyberCSP from the current CSP course, it was necessary to identify appropriate security principles to incorporate into the proposed course and to identify appropriate learning outcomes. For this, we explored the K-12 cybersecurity education space, and dominant here are the NSF-NSA sponsored K-12 GenCyber summer camp program in the summers of 2014 to 2016. As Ladabouche and LaFountain point out, the GenCyber program was created to help the US deal with the shortage of cybersecurity expertise by "developing their cybersecurity awareness and stimulating their interest" in cybersecurity among K-12 students and teachers [5]. Other work shows the efficacy of the GenCyber approach in attracting teenage females to cybersecurity [2, 19]. Preliminary evaluations of the nationwide GenCyber effort shows its success in the K-12 space [5].

We reviewed the seminal work by Saltzer and Schroeder [18], the ACM/IEEE Computer Society's Computer Science Curricula [19] recommendations and the ongoing ACM Joint Task Force effort in developing curricular guidelines for cybersecurity [20] before adopting the GenCyber Cyber First Principles [28], shown in Table 3, as they seem to have become a popular choice at the K-12 level nationwide [5]].

These security principles do not conflict with the CSP courses, but serve to strengthen them in many ways, leading to the integration of traditional design practices with current security guidelines.

Learning Outcomes. Although each GenCyber camp was given great latitude in selecting their own learning outcomes, learning outcomes, such as those from RIT GenCyber camps (see Table III), were fairly typical in the camps that emphasized cybersecurity content heavily.

IV. CyberCSP Course Design

To create the CyberCSP course, we are incorporating the relevant cybersecurity content into our CSP course. To this end, we identified both a set of cybersecurity topics and associated Cyber First Principles that could be associated with each existing CSP curricular unit. In addition, based on our experiences with the GenCyber camps and the typical mindset of our middle and high school students, we realized that discussing the ethical and legal consequencies of cybersecurity attacks is crucial for this audience. Therefore, we will integrate ethics and legal issues into each of the modules we are designing.

Our approach to infusing cybersecurity into the existing curriculum permits us to essentially side-load the new materials

TABLE II
GENCYBER CYBERSECURITY FIRST PRINCIPLES

Principle	Simplified Description
Abstraction	Summarizing or explaining in a way that can be easily understood
Conceptually Simple	If something is less complicated, it is less likely to have problems and easier to troubleshoot and fix.
Data Hiding	Any attempt to prevent people from being able to see information
Domain Separation	Keep resources in separate locations so that accidents and attacks prevent multiple resources from being destroyed or made unusable at the same time.
Layering	Provide multiple layers of defense to protect system so that if one layer is defeated, the next one may catch it
Least Privilege	Limit people's access to resources and what they can do with these resources
Minimization	Simplify and decrease the number of ways the software can be exploited
Modularity	Design system in units or modules that perform a specific function, thus allowing each module to be inserted or removed from the system.
Process Isolation	Keeping processes (a process is the running of any task.) separate prevents the failure of one process from negatively impacting another process
Resource Encapsulation	Resources (hardware or software) must be separated to permit use as intended

TABLE III
GENCYBER CAMP LEARNING OUTCOMES

Students will:

1) Demonstrate basic knowledge of essential concepts of cybersecurity.
2) Describe and apply the Cyber First Principles in cybersecurity.
3) Describe common cybersecurity issues including social engineering attacks, password selection, malware and vulnerabilities, networking and firewalls, and mobile device security.
4) Apply real-world cybersecurity tools such as password cracking and website spoofing.
5) Describe ethical considerations in cybersecurity and apply them in real-world case-studies.
6) Describe why cybersecurity is a relevant discipline worthy of further study.

into existing coursework without requiring too many curricular approvals. Table IV highlights the key cybersecurity concepts infused in each of the existing CSP modules. We also provide a listing of the cybersecurity first principles covered under each module.

We are finalizing the actual cybersecurity topics and Cyber First principles, and then will define CyberCSP Module Learning Outcomes that will make most sense for each CyberCSP module. To further illustrate our approach, the section below shows how the existing CSP Networking Module can be modified to create a corresponding CyberCSP module.

CyberCSP Networking Module Enhancements. As part of the CSP networking module, students are currently introduced to the concepts related to computer networks and protocols. The module presents the TCP/IP model and the importance of following rules while creating networks. Some examples of cybersecurity concepts that can be easily integrated with the protocol discussion include denial of service attacks, spoofing attacks and man-in-the middle attacks, that result in a deviation from normal protocol behavior.

In the existing curriculum, students also learn about different types of networks, from local area networks to internetworking concepts that help create the Internet. The importance of confidentiality of data traversing these networks can be embedded in this portion of the curriculum. Simple exercises and activities demonstrating the concepts of symmetric key and asymmetric key cryptography can highlight the difference between sending information in clear text versus using encryption.

Routers and gateways play a key role in creating and protecting networks. Currently, students learn about simple routing functionalities. Some security concepts, such as the creation of access control lists and firewall rules, and their importance in the protection of networks can be embedded with the existing concepts. The appropriate mode of delivery for this new material (e.g., lecture slides, hands-on exercises, paper exercises, and video) will be determined in consultation with our high school partners.

A similar approach can be used to infuse cybersecurity concepts and principles into other CSP modules to create the corresponding CyberCSP modules, with appropriate learning outcomes.

V. CURRENT STATUS AND CONCLUDING REMARKS

We are planning to teach the CyberCSP version in one section of RIT's CSP course, which is scheduled to be taught in the fall of the 2017-2018 academic year, Given that CyberCSP will not change the learning outcomes of the current course, only the content in the course will be changed, with no additional curricular approval needed to teach the course. As the course is taught, we plan to gather assessment data and evaluate them to make appropriate adjustments. Changes are more onerous at the high school level. Given the extra material that must be developed to teach CyberCSP at WCSD, current teaching assignments, and that changes to the course will require approval, it will not be possible to have the high-school version of the course ready for use in the 2017-2018 academic year, however, we plan create and teach at least three modules at WCSD during the 2017-2018 academic year.

Successful implementation and adoption of CyberCSP will help to improve overall security awareness among average computer users, encourage students to pursue cybersecurity careers or adopt a cybersecurity-awareness, and can help to significantly increase cybersecurity capacity.

TABLE IV
SUGGESTED INFUSION OF CYBERSECURITY CONTENT INTO CSP MODULES FOR CYBERCSP MODULES

CSP Module	Current CSP Topics	Suggested Additions for CyberCSP	
		Cybersecurity Topics	**Cyber First Principles**
Introduction	History of Computers Computer Components Buying a Computer Cloud Computing Number Systems	Ethics and cyber policies. Cyber defense. Cyber attacks. *Case study: The dangers of USB sticks*	Modularity, Resource Encapsulation, Least Privilege.
Networking	Wires, Cables & WiFi IP Addresses & DNS Packets, Routing and Reliability Computer Ethics HTML, CSS Creating a Web page	Protocol security, network attacks and defense mechanisms *Case study: Rogue Hotspots*	Layering, Domain Separation
Problem Solving	Think like a Programmer Algorithms Fetch - Execute Cycle Functions Iteration Conditionals Programming Languages	Security and safety in programming Defensive programming *Case study: Think Like a Hacker*	Abstraction, Modularity, Data Hiding, Minimization.
Programming with Snap!	Software Development Decision Structures Loops Tracing Code Passwords Customized Blocks Lists	Secure software engineering Building security in *Case study: Password cracking*	Modularity, Conceptually Simple. Layering. Process Isolation
Data Representation	Text in Binary Huffman Coding Sound Images, Bitmaps, Grayscale Binary Operators	Steganography Applied Cryptography *Case study: Hiding Viruses in Plain Sight.*	Data hiding, Layering.
Sorting and Searching Algorithms	Bubble Sort Selection Sort Insertion Sort Merge Sort Linear & Binary Search Hashing Efficiency & Big–O	Exhaustive Search, Brute force attacks, Log Analysis *Case study: Guessing Passwords or Pass the Hash*	Abstraction, Conceptually Simple, Minimization, Modularity
Big Data	What is Big Data? Identifying People The Cost of "Free" Privacy Policies The Need for Encryption Password Strength Traveling Salesperson	Data privacy, access control *Case study: Think About What You Give Away for Free*	Data hiding, Least Privilege

ACKNOWLEDGMENT

We thank Trudy Howles for her insights into teaching the CS Principles course at RIT. Co-author Raj also thanks colleagues, Andy Meneely and Bo Yuan, co-directors of RIT's GenCyber summer camps in 2015 and 2016 for useful discussions about appropriate cybersecurity curriculum at the middle and high school levels, as well as RIT's CyberCorps® scholars, Joe Graham, Nick Piazza, Jesse Buonanno and Tyler Diamond, for their ideas for K-12 outreach for cybersecurity. This paper is also based upon work partly supported by the National Science Foundation under Awards DUE-1303269 and DGE-1433736.

REFERENCES

[1] U.S. Department of Labor Bureau of Labor Statistics, "Occupational Outlook Handbook: 2016-17 Edition, Information Security Analysts," 2016–17. http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm, accessed: July 06, 2017.

[2] Fandos, N, "NSA Summer Camp: More Hacking Than Hiking," Dec. 2015. http://www.nytimes.com/2015/07/18/us/nsa-summer-camp-hacking-cyber-defense.html, accessed: July 06, 2017.

[3] The Economist, "Hacked off; Hillary Clinton's Campaign," 2016. https://goo.gl/qEbexZ, accessed: July 06, 2017.

[4] L. Amo, "Addressing gender gaps in teens' cybersecurity engagement and self-efficacy," *IEEE Security & Privacy*, vol. 14, pp. 72–75, Jan. 2016.

[5] T. Ladabouche and S. LaFountain, "Gencyber: Inspiring the next generation of cyber stars," *IEEE Security & Privacy*, vol. 14, pp. 84–86, May 2016.

[6] X. Liu and D. Murphy, "Engaging females in cybersecurity: K through Gray," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, (New York, NY, USA), pp. 255–260, IEEE, 2016.

[7] T. Crick and S. Sentance, "Computing at school: Stimulating computing education in the UK," in *Proceedings of the 11th Koli Calling International Conference on Computing Education Research*, pp. 122–123, ACM, 2011.

[8] T. Bell, P. Andreae, and L. Lambert, "Computer Science in New Zealand high schools," in *Proceedings of the Twelfth Australasian Conference on Computing Education-Volume 103*, pp. 15–22, Australian Computer Society, Inc., 2010.

[9] T. Teo, "Attitudes toward computers: A study of post-secondary students in Singapore," *Interactive Learning Environments*, vol. 14, no. 1, pp. 17–24, 2006.

[10] US National Science Foundationt, "Computing Education for the 21st Century (CE21)," 2016. http://www.nsf.gov/pubs/2012/nsf12609/nsf12609.htm, accessed: July 06, 2017.

[11] J. Cuny, "Transforming k-12 computing education: Ap® computer science principles," *ACM Inroads*, vol. 6, pp. 58–59, Nov. 2015.

[12] J. R. N. Forbes, "Building a talent pool: The cs 10k project," *J. Comput. Sci. Coll.*, vol. 29, pp. 112–113, Apr. 2014.

[13] O. Astrachan and A. Briggs, "The cs principles project," *ACM Inroads*, vol. 3, pp. 38–42, June 2012.

[14] College Board, "AP Computer Science Principles, Course and Exam Description," 2016. https://secure-media.collegeboard.org/digitalServices/pdf/ap/ap-computer-science-principles-course-and-exam-description.pdf, accessed: July 06, 2017.

[15] D. D. Garcia, T. Barnes, M. Ball, E. Biga, J. Paley, M. Hill, N. Mattix, P. Safa, S. Morris, and S. Kenner, "Ap cs principles and the beauty and joy of computing curriculum (abstract only)," in *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, SIGCSE '16, (New York, NY, USA), pp. 718–718, ACM, 2016.

[16] J. Mickel and B. Beth, "K-12 Teacher Support for Computer Science Principles: An Introduction to the UTeach Course, Thriving in Our Digital World: AP (Abstract Only)," in *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, SIGCSE '16, (New York, NY, USA), pp. 717–718, ACM, 2016.

[17] R. Morelli, C. Uche, P. Lake, and L. Baldwin, "Analyzing year one of a cs principles pd project," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, SIGCSE '15, (New York, NY, USA), pp. 368–373, ACM, 2015.

[18] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, pp. 1278–1308, Sept 1975.

[19] Joint Task Force on Computing Curricula, Association for Computing Machinery (ACM) and IEEE Computer Society, *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. New York, NY, USA: ACM, 2013. 999133.

[20] D. L. Burley, M. Bishop, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, E. Hawthorne, S. Kaza, Y. Levy, H. Mattord, and A. Parrish, "Cybersecurity Curricula 2017, Version 0.5 Report," Jan 2017. https://www.csec2017.org/csec2017-v-0-5, accessed: July 06, 2017.