STEAM Powered K-12 Cybersecurity Education

Joe Chase
Dept. of Information Technology
Radford University
Radford, VA, USA
jchase@radford.edu

Prem Uppuluri
Dept. of Information Technology
Radford University
Radford, VA, USA
puppuluri@radford.edu

Ellen Denny
Radford City Public Schools
Radford, VA, USA
edenny@rcps.org

Blenna Patterson
Radford City Public Schools
Radford, VA, USA
bpatterson@rcps.org

Jennifer Eller
Bering Strait School District
Unalakleet, AK, USA
Jennifer.eller@bssd.org

Darlene Lane
Radford City Public Schools
Radford, VA, USA
dlane@rcps.org

Beverly Edwards
Radford City Public Schools
Radford, VA, USA
bedwards@rcps.org

Rebecca Onuskanich
Cyber Warrior Princess Program
Dayton, OH, USA
ronuskanich@cyberwarriorprincess.org

Abstract—The importance of incorporating cybersecurity education in K-12 to develop and strengthen the pipeline of students who pursue a cybersecurity major in college along with teaching cyber-awareness to all students cannot be overstated. Through efforts, such as the National Institute of Science and Technology (NIST) National Initiative for Cybersecurity Education (NICE) K-12 cybersecurity conferences and the NICE K-12 working groups this message is being spread to K-12 educators across the country. In Virginia, like many other states, there is a disparity among student and teacher preparation in cybersecurity between urban and rural areas. Schools lack two key resources: teachers with the required competencies and access to isolated computing networks – required for hands on exercises in security. Currently, efforts to introduce security are usually focused only at the high school level where students have already self-selected into relatively small interest groups. This paper describes the result of year-long, NSA funded project (PICSAR) designed to increase the number of teachers with competency in cybersecurity, while increasing the pipeline of students interested in cybersecurity. The project accomplished the first goal by providing graduate instruction in cybersecurity education and workshops to K-12 teachers. These same teachers then helped to accomplish the second goal through the development of age appropriate, integrated, STEAM lesson plans from Kindergarten through the 12th grade. For each topic in cybersecurity (e.g. Cryptography), a skills progression plan was developed and then lesson plans developed and piloted to appropriately introduce the topic at each grade level.

Keywords—cybersecurity; education; K-12

I. INTRODUCTION

The need for Computer Science/Information Technology (CS/IT) majors in the workforce cannot be overstated [1]. Among CS jobs, information security tends to be in high demand with a "*growth rate that is over three times faster than all Information Technology (IT) jobs*" [2]. The Bureau of Labor Statistics Occupational Outlook Handbook [3, 1] indicates that the job growth outlook for 2016-26 in security is expected to be 28.5%, faster than average. Most of these jobs (over 61%) require a Bachelor's degree or higher [2] [4], a fact that reinforces the need to increase the pipeline of students from high schools interested in a CS/IT major at the B.S level with cybersecurity as a focus.

However, as pointed out in [5] [6], the number of high schools offering such courses is very low. Current CS/IT courses are either vocational in nature (e.g., networking courses focused on CISCO certifications) or advanced such as the pre-AP, AP CS, or International Baccalaureate (IB) courses. Participation in these courses is very limited [5]. The lack of high school offerings in cybersecurity is often the result of a lack of teachers with competency to teach cybersecurity. Further, the lack of participation in the courses that are offered is at least partially the result of these courses being offered at the high school level where students have already self-selected into relatively small interest groups. Student exposure to cybersecurity topics prior to high school is very limited meaning that if there is not an influence from home, many students may never know the options available to them.

The NSA funded PICSAR project, a partnership between Radford University's Center for Information Safety and Security, Radford City Public Schools, and the Cyber Warrior Princess Program, builds upon on a strong foundation in K-12 [7] outreach in cybersecurity that the authors, along with collaborators have been developing since 2012 [8] [9] [10]. This includes:

a) A high-impact novel curriculum in introductory cybersecurity for middle/high school students and their teachers [7]. The courses, offered online, cover a vast array of foundational knowledge (networking, web technologies, Linux and Windows operating system usage) and introductory cybersecurity (hacking, cryptography, network and host hardening) using capture the flag challenges as a just-in-time and active learning strategy. To date, 107 teachers from more than 60 schools have taken the teacher preparation graduate course. Since January 2014, more than 1,000 high school and middle school students have used this curriculum either as part of a formal dual-enrollment online course in security, or as preparation for a two week long RUSecure CTF - capture the flag (CTF) contest that Radford University organizes annually for K9-12 students (ctf.radford.edu).

This work is supported by National Security Agency

The RUSecure CTF is a contest aimed at introducing cybersecurity and preparing students in the field – all packaged and delivered as an exciting online and in-person event.

b) A state-of-the-art cyber-range (security-lab.radford.edu) for use by both students and teachers.

c) Promoting teacher preparation in cybersecurity through panels, workshops, and presentations at various conferences and workshops including: panels at the Colloquium on Information Systems Security Education [7], the annual NICE (National Initiative for Cybersecurity Education) K-12 Cybersecurity in Linthicum – MD (2015) [9] and Arlington, VA (2016) [8], Making Connections at Roanoke VA and the 2018 ACM Technical Symposium on Computer Science Education (SIGCSE) in Baltimore MD [11].

The PICSAR project is strengthening and greatly expanding the curriculum to train teachers with the competencies required to teach cybersecurity courses that follow Virginia's guidelines and cover the syllabus for professional certifications including CompTIA Security+, parts of CISSP, and CIS Security controls. The need for this expansion is immediate and severe as the need for qualified teachers has only increased. The Virginia Department of Education (VDOE), like several other states, is working to incorporate cybersecurity into high school curriculum – mainly to boost the pipeline of interested students to fill industry workforce needs. In 2016-17, VDOE developed a security curriculum for K9-12. As an outcome of these panels, Virginia is adopting a model where high school students can take multiple security courses starting from cybersecurity foundations leading up to material that meets the competencies of the CompTia Security+ certification. In order to help meet these goals, the PICSAR project is (i) expanding graduate education for teachers in cybersecurity by adding advanced topics that map to elements of the NIST cybersecurity framework as well as the Security+ certification along with basics of 8 domains in CISSP, (ii) ensuring teachers can use the credentials towards their licensure re-certification/professional development, (iii) ensuring that teachers gain competency and confidence to teach security and (iv) continuing to support remote isolated networking environments (cyber-ranges) for teachers to easily provide hands-on exercises to students. The curriculum ensures a hands-on approach to security where teachers work with real-world attack and defense techniques – so that teachers can take this same approach to excite and motivate their students in high schools.

In addition, the PICSAR project is helping to build a foundation for high school study of cybersecurity by working with K-8 faculty to develop age appropriate STEAM lesson plans integrating cybersecurity topics at all grade levels. Eighteen faculty and two administrators from Radford City Public Schools in Southwest Virginia are working with the PICSAR project investigators to learn more about cybersecurity and then apply that knowledge to develop age appropriate STEAM lesson plans. To date, faculty working on the project have created more than 25 such lesson plans in Cryptography, Forensics, Reconnaissance, and Digital Ethics and Law. Faculty have also created skills progressions for these topics. These skills progressions for cybersecurity topics will allow the same topics to be revisited and reinforced at a variety of age levels with age appropriate materials allowing all students to gain a deeper and more robust understanding of cybersecurity, as well as preparing and motivating self-selected students for further study in cybersecurity. One of the outcomes of the PICSAR project will be a library of age appropriate lesson plans that can then be shared with other K-12 faculty, as well as expanded, assessed, and enhanced as the lessons are used.

II. Related Work

Numerous efforts are underway across the U.S. to excite students about CS/IT in general and cybersecurity in particular. The majority of these efforts can be divided into two different camps: *basic cyber awareness and activities requiring higher-level technical skills and multiple courses to provide pre-requisite knowledge* – both are a challenge in school districts with limited IT/security foundational knowledge among teachers. While the former efforts are not thorough enough to build any meaningful IT foundational knowledge, the latter are more in-depth multi-semester efforts that primarily draw motivated, self-selected high school students and are limited to few schools. There is a need for more opportunities that begin earlier and that bridge these two content camps, providing scaffolding for students to explore aspects of CS/IT through the vast array of foundational knowledge required for cybersecurity.

This project was greatly influenced by several related efforts in teaching cybersecurity to high school students. These efforts broadly fall into two categories:

- ***Extra-curricular programs*** *(after school, summer camps, summer workshops, informal clubs and competitions)*. By far, these programs seem to be the most popular. These include: National CyberSTEM [12], Camps and workshops by Educational Technology Research, Policy and Outreach (ETPRO) [13], the Air Force Association's CyberPatriot [14], the CSAW-Cyber high school forensics competition [15], Hacker High School [16], the National Board of Information Security Education cyber camps [17], and SANS CyberAces [18] to list a few.
- ***Formal computer-security tracks for K-12***. These include curricula developed in schools with technological and personnel resources to support such courses As there are several such schools, we list only a sample here: Shenandoah Valley Governor's School (SANS CyberAces curriculum), Rome Catholic School [19], and Los Angeles Unified School District (http://www.exploringcs.org/curriculum) that teach the basics of cybersecurity in K-12.

In addition to the various efforts to excite and engage students about CS/IT topics as well as cybersecurity, PICSAR project investigators also examined efforts into the development of frameworks to model cybersecurity knowledge and process. The most successful of these efforts appear to be the National Initiatives for Cybersecurity Careers and Studies (NICCS), NICE Cybersecurity Workforce Framework (NIST SP 800-181) [20], and the NIST Cybersecurity Framework (CSF) [21].

The National Initiatives for Cybersecurity Careers and Studies (NICCS) provides an education and training catalog in which all approved training courses are mapped to the NICE Cybersecurity Framework. The NICE Cybersecurity Framework provides a standardized way to categorize, organize, and describe cybersecurity work into categories, specialty areas, work roles tasks, and knowledge, skills and abilities (KSAs).

These KSA's are being leveraged to guide the development of the PICSAR K-12 Cybersecurity Framework and outlining what knowledge and skills should be taught at which grade level. Aligning a framework specific to cybersecurity helps to ensure that the pathways to student success are clearly defined and lead to the objectives of the Nation by ensuring that we fill the current and future cybersecurity workforce gap.

Developing curriculum for K-12 students requires a slightly unique approach than teaching adults, all the while ensuring that the end goals remain the same: promote good cyber hygiene for students, while exposing them to cybersecurity opportunities in a fun and exciting manner. With this goal in mind, the PICSAR project added the following constraints: 1) all students do not learn the same and 2) the education goals and standards need to map back to the common framework. We selected the National Initiatives for Cybersecurity Careers and Studies (NICCS), NICE Cybersecurity Workforce Framework (NIST SP 800-181) [20], along with the NIST Cybersecurity Framework (CSF) [21] as our foundation for developing our proposed K-12 Cybersecurity Framework.

A. *Maintaining the Integrity of the Specifications*

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. Building Teacher Competency in Cybersecurity

As discussed earlier, the PICSAR project is strengthening and greatly expanding the curriculum to train teachers with the competencies required to teach cybersecurity courses. This has been accomplished by:

- Continuing to refine the Cybersecurity for Educators graduate course (ITEC 545)
- Implementation of an Advanced Cybersecurity for Educators course (ITEC 546)
- Providing tuition assistance for approximately 50 K-12 teachers and administrators to take one or both of these courses
- Online and face-to-face workshops for K-12 teachers

A. *Cybersecurity for Educators Graduate Course*

The Cybersecurity for Educators graduate course (ITEC 545) was first developed under a grant from the NSA Mathematics Education Partnership Program (MEPP) program and offered for the first time in the fall of 2016. The course uses challenge-based education in the form of a Capture the Flag (CTF) contest. In this way, teachers may work at their own pace taking advantage of just-in-time and active learning.

Each challenge is constructed with the challenge itself, the required flag, and any hints or associated educational materials. The contests are built upon an open source product called Mellivora[1]. This software also provides a scoreboard feature allowing students to track their performance relative to other students. Figure 1 shows a couple of sample challenges from the course.

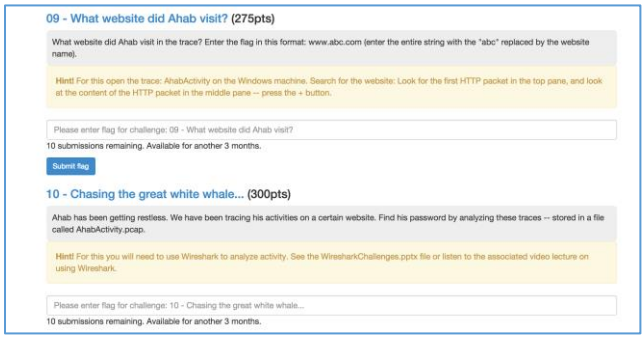

Fig. 1. Sample Challenges

In addition to the contest environment, teams are also provided access to a web-based, isolated, secure environment hosted as a cyber-range by Radford University. This environment, made possible by a partnership with CypherPath™, allows teams access to both Windows and Kali Linux virtual environments that have been preloaded with flags and software required for the given challenges. This virtual environment allows students to try a variety of cybersecurity tools and techniques in a relatively consequence free environment. Figure 2 shows an example of this virtual environment. Because both the contest environment and the cyber-range are web-based, the only computing resource required of students is a web browser.

The CTF and virtual environment are further supported with online meetings and presentations, as well as asynchronous materials. To date, approximately 95 teachers and administrators have taken advantage of this course with

[1] https://github.com/Nakiami/mellivora

approximately 30 of those receiving tuition assistance this past year from the PICSAR project.

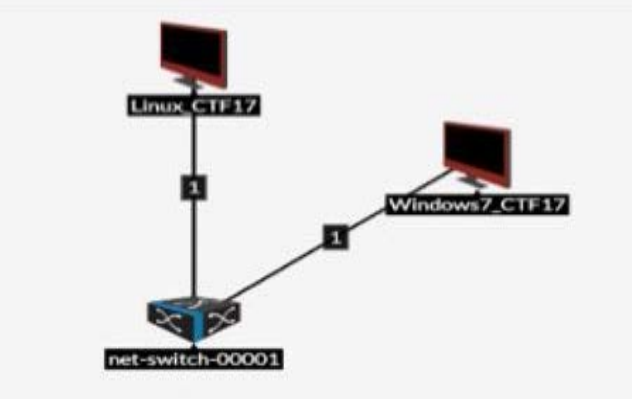

Fig. 2. Example of the Cypherpath Virtual Environment

B. *Advanced Cybersecurity for Educator*

As part of the PICSAR project, building upon the success of the ITEC 545 – Cybersecurity for Educators, and in response to demand from participating faculty that wanted to go farther and deeper into cybersecurity, we developed ITEC 546 – Advanced Cybersecurity for Educators.

This 3-credit hour graduate course was developed specifically for educators with a strong background in networking and with at least some background in cybersecurity (ITEC 545 or equivalent). The course is modelled after the CIS Security controls (www.cisecurity.org/controls). While there are several ways to introduce cybersecurity, we chose to use the CIS security control model to provide an industry perspective to educators. The course provides teachers with experience in using standard benchmarks and tools for host and network hardening. In addition, the course covers aspects of penetration testing and incident response.

C. *Online and Face-to-Face Workshops for K-12 Teachers*

While many K-12 faculty have taken advantage of the opportunities to enroll in ITEC 545 and ITEC 546, there were additional faculty from Radford City Public Schools that participated in the PICSAR project. In order to get those faculty up to speed in cybersecurity and to focus the efforts of the group on one topic at a time, multiple online and face-to-face workshops were held.

Because of the limited, one year, duration of the project, the scope of the PICSAR project was limited to four topics chosen from the field of cybersecurity: Cryptography, Forensics, Reconnaissance, and Digital Ethics and Law. Each topic was a focus of the participants for approximately two months beginning with an online overview presentation of the topic, moving on to a face-to-face, half-day workshop for each topic, and then followed by working groups organized by grade level (e.g. K-2, 3-5, 6-8, and 9-12) to develop lesson plans.

IV. Building Student Interest in Cybersecurity

A. *Creating the Context for K-12 Cybersecurity Curricula*

Developing curriculum for K-12 students requires a different approach than teaching adults, all the while ensuring that the end goals remain the same: promote good cyber hygiene for students, while exposing them to cybersecurity opportunities in a fun and exciting manner. With these goals in mind, our project has always maintained three principles:

- students do not all have the same background or learn in the same way – we need to meet them where they are
- the education goals and standards need to map back to the common framework
- the lesson plans developed must map to the Virginia Standards of Learning

The first of these, meeting students where they are, is addressed by ensuring educators in our program, from all grade levels and backgrounds, developed curriculum that works for them in their classrooms. With the assistance of Radford University professors, Radford City School administrators and cybersecurity subject matter experts, this ensures that, for example, we have 5th grade history teachers incorporating the history of cryptography in their daily courses, along with 3rd grade art teachers showing how to artistically represent binary numbers with various forms of art products such as beaded necklaces with secret messages in them. Curriculum integrated with STEAM encouraged educators to create such hands-on activities as breakout boxes and mystery games.

We chose the National Initiatives for Cybersecurity Careers and Studies (NICCS), NICE Cybersecurity Workforce Framework (NIST SP 800-181) [20], and the NIST Cybersecurity Framework (CSF) [21] to provide context for our curriculum development. Satisfying our second principle of ensuring that our K-12 Cybersecurity Framework mapped back to NICCS required that we complete a mapping of the NICE Cybersecurity Workforce Framework, along with the NIST Cybersecurity Framework (CSF) to ensure that the educators were provided a clear linear program from which to create curriculum. Developing our K-12 Cybersecurity Framework around an already approved and widely utilized existing framework will ensure that K-12 students are provided a clear path for educational and career goals. Our preliminary work included the development of an initial K-12 Cybersecurity Framework to provide educators the building blocks of concepts and practices in which we can then use to create the K-12 Cybersecurity Standards. Our initial proposed K-12 Cybersecurity Framework is outlined in Table I. We continue to expand this framework by grade level.

TABLE I. PROPOSED K-12 CYBERSECURITY FRAMEWORK

- Cyber Hygiene
  - Stay safe online
  - Protecting your devices
  - Good vs. bad hacking
- Cybersecurity Fundamentals
  - Definitions, Terminology and Acronyms
  - Introduction to Encryption Technologies
  - Risk Management
- Security Administration
  - Computer system hardening (Patching, antivirus and SPAM)
  - Access control, Identification and Authentication
  - Encryption Solutions and configurations
- Network Security
  - Perimeter defense security
  - Security Operations Center (SOC)
  - Routers, switches and network device configuration and security
- Offensive Security
  - Social Engineering
  - White-hat Hacking
- Cyber competitions

The third principle of mapping lesson plans to the Virginia Standards of Learning became a part of the standard template for lesson plans and part of the process for creating those lesson plans described below.

B. The Curriculum Development Process

As described above, four topics in cybersecurity were chosen as the focus of the PICSAR project: Cryptography, Forensics, Reconnaissance, and Digital Ethics and Law. Each topic was a focus of the participants for approximately two months beginning with an online overview presentation of the topic, moving on to a face-to-face, half-day workshop for each topic, and then followed by working groups organized by grade level (e.g. K-2, 3-5, 6-8, and 9-12) to develop lesson plans.

Eighteen faculty from Radford City Public Schools participated in the project with fairly good distribution of background and expertise from kindergarten through high school. In addition to the project principal investigators, these working groups were also assisted by Radford University students with expertise in cybersecurity. A draft lesson plan template was developed before the first half-day workshop in order to provide a starting point for the various grade-level groups.

Cryptography was the first topic addressed and as described above, this involved an online meeting and presentation followed by a half-day workshop. It became apparent after the first workshop, that an organizing group of teachers would be needed to keep such a large group working smoothly together. Thus, one teacher was selected from each grade-level group and, along with the principal investigator from Radford City Public Schools, this group became known as the Leads. They took on responsibility for finalizing the lesson plan template, helping the groups move forward as each new topic was introduced, and making sure that lesson plans were complete before being published.

Another product of this Leads group was the realization that we needed to develop skills progression plans (i.e. vertical integration charts) for each topic in order to help guide the working groups on what was appropriate at each grade level and what they could expect students to have already covered before a particular grade level. While not a part of the original NSA proposal, these skills progression plans have become a major part of the resulting product. Table II shows a partial skills progression for Cryptography. After Cryptography, the group shifted focus to Reconnaissance, then Forensics, and finally Digital Ethics and Law.

TABLE II. PARTIAL SAMPLE OF SKILLS PROGRESSION (FILLED BLACK INDICATES COVERAGE AT THAT GRADE LEVEL, FILLED GREY INDICATES ASSUMED PRIOR KNOWLEDGE)

Objective/Skill/Concept	K-2	3-5	6-8	9-12
Define Cybersecurity as related to cryptography	■			
Internet Safety	■			
Private Information	■			
Ciphers	■			
Patterns as related to ciphers	■	■		
decrypt	■	■		
encrypt	■	■		
Substitution/transposition cipher		■		
Sensitive data and confidentiality			■	

C. The Resulting K-12 Cybersecurity Curricula

While the development of lesson plans continues, to date, faculty participating in the project have published 30 lesson plans ranging from kindergarten cryptography looking at secret codes to high school reconnaissance where the students cyber-stalk Stephen Hawking. To provide a sample

of the lessons created, Table III shows the lessons created for grades K-2.

TABLE III. SAMPLE K-2 LESSON PLANS

Grade Level	Topic	Title
1st	Cryptography	Thomas Jefferson – Jefferson Disc Cipher
2nd	Cryptography	Helen Keller
K	Cryptography	Secret Codes
K	Cryptography	Viruses
K-2	Digital Ethics and Law	Cyber-Ethics Netiquette
2nd	Forensics	CSI Radford
2nd	Reconnaissance	Private Information
K-2	Reconnaissance	What Would You Do?

V. SAMPLE LESSON PLAN – CSI RADFORD

The goal of this 2nd grade, STEAM integrated lesson is for students to learn about cybersecurity through an engaging, problem-based activity. Students will become CSI Radford investigators as they work together to investigate who hacked a school computer. In small teams, students will follow the clues and eliminate possible suspects, until the true suspect is discovered at the end of the lesson. While the lesson focuses on cybersecurity, it has been created as an integrated lesson pulling in reading expectations, technology standards, math concepts and essential skills such as communication, problem solving, creative thinking and collaboration.

Fig. 3. Materials for CSI Lesson Plan

As shown in Figure 3, materials are provided for the teacher to print in preparation for the lesson including:

- ID tags/badges for students to wear
- Crime scene (digital footprints scattered in area, crime scene or caution tape around area)
- Each group's materials (Dossier Folder with 5 suspects dossiers, Evidence Folder - with clues, Spy Kit with a tape measure, a magnifying glass (optional), other spy fun item like hat, glasses, trench coat, iPad or tablet with QR code scanner, suspect check off chart)
- A lockable box or bag containing the final NMAP clue is place in the room with a 5-digit word lock set to the word "TRACE". Crime Scene Investigators will need to solve the cypher on one of the other clues to open the word lock.
- Reveal Folders - one folder for each suspect. Put "I didn't do it" in all except Mr. Black. Put the guilty printout in his folder.

The objectives include:

- The student will demonstrate their knowledge of cybersecurity by following clues to solve a mystery
- The student will identify the hacker by analyzing evidence and collecting data
- The student will assess the "crime scene" by using a variety of cybersecurity tools (nmap, cryptogram, dossier)

The lesson begins with one of the teachers reading the following to the students:

> *One of our computers has been hacked. You have been chosen to investigate the crime scene and figure out the criminal. You will need to work with your teams to study the clues. CSI Radford has narrowed it down to five suspects. Their dossiers are provided for each team. Use the information on the dossiers and compare it to the evidence found at the scene and on screenshots provided in your evidence files. Good Luck!*

The class is then divided into groups of 2-4 students each. Students work together to solve the crime. The suspect who has a check in every box is the one who did it! When time is up, all of the students are gathered in the crime scene. The reveal folder for each suspect is held up one at a time, as shown in Figure 4, and the students are asked to raise their hand if this is their prime suspect. Each folder contains a card that reveals if that suspect did it or not. Some students may be confused by the last clue (Nmap) but they should realize that just because Mrs. Ruby was the last to make an entry, making an entry is not a sign of guilt but removing information would be (i.e. Mr. Black). Lastly, students and

teachers celebrate solving the crime and have a discussion of real jobs that are similar to this simulation.

Fig. 4. Revealing the Criminal

Through the CSI experience, students will broaden their mindset in regards to cybersecurity. Integrating math and English with a cybersecurity-based quest creates a learning opportunity for young students that not only offers a real-world application, but does so in an atmosphere of mystery and light competition. The lesson showcases cybersecurity in a positive and engaging manner, inspiring children at a very young age as well as helping them become savvy cyber warriors!

VI. Future Work

The PICSAR project continues with the principal investigators continuing to work with faculty from Radford City Public Schools to:

- Implement and assess the published lesson plans
- Continue to refine and develop lesson plans that have yet to be published
- Identify topics and opportunities for lesson plans
- Disseminate the lesson plans beyond the original project participants

Many of the 30 published lesson plans have already been piloted in the classroom. Each time one of these lesson plans is implemented, we learn more about what works well, what needs to change, and opportunities to extend the lesson in perhaps unanticipated ways. This continuous evolution and improvement will continue as long as the lesson plans are in use.

In addition to the 30 lesson plans that have been completed and published, project participants have created approximately 30 additional lesson plans that are still in the process of being reviewed and edited prior to publication. We expect that most of these lesson plans will be published by the end of the 2018-19 academic year.

As the expertise in cybersecurity continues to increase among participating faculty and as they gain more experience integrating these topics into their STEAM lesson plans, more opportunities and ideas continue to emerge to create new lesson plans. In addition, it is the goal of the PICSAR investigators to continue to expand beyond the four initial cybersecurity topics.

PICSAR project results were recently shared with educators from around the Commonwealth of Virginia at the 1st Annual Virginia Cybersecurity Education Conference and at Radford University's 2019 NSA GenCyber Camp for Teachers. Project investigators and participants are also already slated to present results at upcoming teacher workshops. It is our intent to expand the project participation beyond Radford City Public Schools and into the surrounding regions this coming year.

Acknowledgment

The authors would like to thank Radford City Public Schools along with the participating teachers for their contribution to this project. In addition, the authors would like to acknowledge the assistance of the Radford University student Cyber Warriors for their help in the training sessions.

References

[1] C. Crouch, "Bankrate," 8 14 2017. [Online]. Available: www.bankrate.com/finance/person-finance/high-paying-college-majors-1.aspx.

[2] BurningGlass, "Job Market Intelligence, Cybersecurity Jobs," 2015. [Online]. Available: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf. [Accessed 1 July 2016].

[3] BLS, "Bureau of Labor Statistics," 14 8 2017. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[4] Office of Career and Technical Education, Virginia Department of Education, 2016. [Online]. Available: http://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf. [Accessed 1 July 2016].

[5] K. Wagstaff, "TIME Magazine," 16 June 2012. [Online]. Available: http://techland.time.com/2012/07/16/can-we-fix-computer-science-education-in-america/.

[6] D. Lewis, "Computer science: It's where the jobs are, but schools don't teach it," 12 9 2014. [Online]. Available: http://www.mercurynews.com/opinion/ci_26510658/computer-science-its-where-jobs-are-but-schools. [Accessed 1 7 2016].

[7] P. Uppuluri, J. Chase and J. Pittges, "Scare and Prepare: Increasing Awareness, Safety and Passion for Cybersecurity," in 45th *ACM Technical Symposium on Computer Science Education*, Atlanta, 2014.

[8] P. Uppuluri, "Training Teachers in Cybersecurity," in *National K-12 Cybersecurity Conference*, Arlington, VA, 2016.

[9] P. Uppuluri and Z. Dannelly, "Panel on Higher Materials and Resources to Support Outreach," in *National K-12 Cybersecurity Education Conference*, Linthicum, MD, 2015.

[10] P. Uppuluri, J. Chase and J. Pittges, "Scare, Prepare, and Dare: High Impact, Low Cost Incorporation of Cybersecurity in High School Curriculum," in *The Colloquium on Information Systems Security Education*, Las Vegas, NV, 2015.

[11] J. Chase and P. Uppuluri, "Workshop: Building a Virtual Challenge-Based Learning Environment," in *49th ACM Technical Symposium on Computer Science Education*, Baltimore, MD, 2018.

[12] CyberSTEM, "CyberSTEM/CyberWatch," [Online]. Available: http://www.edtechpolicy.org/cyberK-12/cyberstem_high.html. [Accessed 26 December 2012].

[13] ETPro, [Online]. Available: http://www.edtechpolicy.org/etpro/projects.html.

[14] CyperPatriot Training, "CyperPatriot Training," 1 January 2011. [Online]. Available: http://www.uscyberpatriot.org/CP5/Training.aspx. [Accessed 26 December 2012].

[15] NYC Poly University, [Online]. Available: http://www.poly.edu/csaw2012. [Accessed 26 December 2012].

[16] ISECOM Hacker High School, "ISECOM Hacker High School: Security Awareness for Teens," 1 January 2000. [Online]. Available: http://www.hackerhighschool.org. [Accessed 26 December 2012].

[17] National Board of Information Security Examiners, [Online]. Available: https://www.nbise.org/uscc/camps/. [Accessed 26 December 2012].

[18] SANS, [Online]. Available: http://www.cyberaces.org/courses/. [Accessed 5 November 2014].

[19] Rome Catholic School, "Cybersecurity K-12 curriculum," [Online]. Available: http://www.romecatholic.org/jr-sr-high/cyber-security-k-12-curriculum/. [Accessed 26 December 2012].

[20] W. Newhouse, S. Keith, B. Scribner and G. Witte, "National Initiative for Cybersecurity Education (NICE)," August 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/final. [Accessed August 2018].

[21] NIST, "NIST," 16 April 2018. [Online]. Available: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. [Accessed August 2018].

979-8-6425-4896-7/20/$26.00 ©2020 CISSE