Bulldog Bytes: Engaging Elementary Girls with Computer Science and Cybersecurity

Litany Lineberry, Sarah B. Lee, Jessica Ivy, and Heather Bostick
Mississippi State University

Abstract

Responsive to broadening participation challenges, Mississippi State University (MSU) established the Bulldog Bytes Outreach Program in 2013 with a residential summer camp for middle school girls funded through the National Center for Women in Information Technology (NCWIT). Since then the program has grown to provide co-curricular activities to K12 students throughout the state. Following a pilot offering of an elementary camp in 2016, the Bulldog Bytes program delivered two of these camps in small towns during 2017, supporting a strategy of engaging under-resourced students with computing in their home communities. This paper will detail our project-based approach to learning and share experiences from the elementary camps.

Keywords

K12, robotics, cybersecurity, education

Introduction

Ninety-two percent of teens report going online daily, with 24% who say they go online "almost constantly".[1] With even younger citizens in the United States using online computers more than ever before, and research indicating that the high school years is likely too late to influence perceptions and self-efficacy in computing as a career path, it is imperative that we engage students early in life.[2] By engaging students in computer science at an early age, we can promote the development of self-efficacy in computing before adolescent opinions are formed that may discourage girls from seeking curricular or co-curricular experiences in computing.[3] A Study done by the National Girls Collaborative Project states that although women earn 57.3% of bachelor degrees in all fields in 2013 and 50.3% of science and engineering bachelor degrees, only about 17.9% of women receive these degrees in computer science.[4]

Background

The Bulldog Bytes summer camp program at MSU is an important link in the MS Alliance for Women in Computing that places particular emphasis on increasing the number of women on computing pathways. The National Security Agency's (NSA) Inspiring the Next Generation of Cyber Stars (GenCyber) program has been a presence at MSU since 2014. GenCyber program goals are presented as follows:

> The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe on-line behavior and how

they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K-12 curricula.[5]

With the integration of GenCyber and Bulldog Bytes, the MSU team has developed an outreach program that promotes development of a diverse cyber literate workforce in MS.[6] Alumni of Bulldog Bytes programs have become NCWIT Aspirations in Computing awardees, and many have participated in other co-curricular activities that support interest in computing and cybersecurity. GenCyber alumni are among students at MSU studying cybersecurity.

In 2017, forty girls, 2nd to 6th graders, were introduced to computer programming as well as cybersecurity concepts. Two camps were held in small towns in Mississippi: one in West Point and one in Columbus. Columbus' African American population under 18 is 92%, with 79% in West Point.[7] Both communities report 87% of children qualified for free/reduced lunch.[8] Students were recruited through after school and summer programs for at-risk children, local elementary school faculty and administration, and through social media. Each camp was held from 9:00 am to 2:00 pm, Monday through Friday. A light breakfast was provided, along with lunch and a take-home snack. At the end of each camp week, participants took home a robot and a school backpack with the GenCyber logo.

Curriculum Overview

Hands-on, project-based learning strengthened teamwork and problem solving skills. Using Finch robots, girls learned to create computer programs using *Snap!*, a drag and drop programming interface. With levels of *Snap!* that increase in difficulty, participants were able to work at their own pace and use their creativity to design and implement project ideas. The camp curriculum that was implemented was heavily focused on the GenCyber First Principles, as required by the program. These principles are described in Table 1[9].

Principle	Description
Minimization	Decreasing the number of ways that software can be exploited.
Simplicity	Keeping things simple so that problems are easier to identify and fix.
Abstraction	Summarizing in a way that is easy to understand.
Information Hiding	Preventing users from seeing information that they do not need to see.
Least Privilege	Limitations on what access users have to resources and how they can use the resources.
Modularity	Each module should have its own function and be able to be inserted or removed.
Layering	Multiple layers of defense for protection.
Resource Encapsulation	Resources should be separated and used only as intended.
Process Isolation	Keeping processes separate prevents the failure of one process from negatively impacting another process.

Domain Separation	Separating areas where resources are located prevents accidents and loss of data, keeping information worlds from colliding.

Table 1. GenCyber First Principles

Active learning was encouraged through hands-on mini projects. Each day, group projects were used to teach students about the 10 GenCyber principles as well as computer programming and internet safety. The Simon Says game was used each morning as an ice breaker and to reinforce learning. On the first day of camp, the participants played a game where they tossed a beach ball that had questions written on it such as 'Do you like peanut butter and jelly sandwiches?" and "Do you have a pet?" When the recipient of the ball answered a questions, they tossed it to someone else. This was a way for students to get to know one another in a short period of time. GenCyber bucks were given throughout the week for correct responses to prompts or completion of tasks. On Wednesday and Friday, participants could use those bucks to purchase school supplies and other items in the 'store' that was provided. The curriculum modules are outlined in Table 2, and activities supporting these modules are described further below.

Module	**At the end of the module, students will be able to:**
Computer Programming	• Demonstrate knowledge of First Principles: *minimization, conceptually simple, abstraction, modularity, resource encapsulation, process isolation* • Demonstrate, through individual and pair/team project assignments, the ability to formulate project requirements and appropriate alternative solutions using a block programming language
Introduction to Cybersecurity	• Demonstrate knowledge of First Principles: *data hiding, least privilege, layering, domain separation* • Be able to list risk of online activity and steps one can take to protect personal data and identity • Demonstrate understanding of storage media vulnerabilities • Give an example of an ethical dilemma one might face in the cyber domain
Cryptography	• Demonstrate knowledge of First Principles: *data hiding, least privilege, layering, domain separation* • Describe the basic concepts of cryptography

Table 2. Curriculum Modules

In order to teach computer programming and demonstrate the First Principle modularity, students were introduced to coding using Finch robots. Students used the drag-and-drop *Snap!* interface.[10] Each student started off on the basic level and at their own pace progressed through levels 2, 3 and 4. Level 1 is the most basic programming level that *Snap!* offers; it focuses on motion and changing the LED sensors to different colors. Level 2 is similar to level one except that it focuses more on letting the user control how far the robot moves and showcases the different colors the users can implement at one time. Level 3 is an intermediate level where conditional statements are introduced. Level 4 is the most complex level where more advanced programming concepts are used such as if-then-else blocks.

To demonstrate cybercrime concepts and file recovery, students were given flash drives with documents on them and asked to delete the files. Autopsy is a software product that provides a 'File Manager' type of interface and shows details about deleted data and file system structures.[11] Students used Autopsy to see how easy it was to retrieve documents that they thought were permanently deleted. For password cracking and encryption, students used Caesar cipher and then with a partner they created their own secret messages that their partner had to crack.[13] The partner in the activity was only given the alphabet shift to use. For email phishing, fishing for real fish was discussed to establish context. Phishing was then described, and the participants were given emails to decipher and decide if the email looked valid or risky. Two video games, SpaceScams and BruteForce, were used to help students understand how to spot fake and phishing emails as well as how to test the strength of passwords. These games have been used with success in other GenCyber camps and were adopted by Bulldog Bytes. In BruteForce, students have twelve chances to create their own password or use one from a rolling list and place it in the spaces. Once placed it is either given a wall made of wood, bricks, or steel to demonstrate how easy or hard it is to break down and get through. SpaceScams was used to demonstrate phishing. Emails appeared on the screen and the game user had to shoot the ships with emails that were considered phishing. [12]

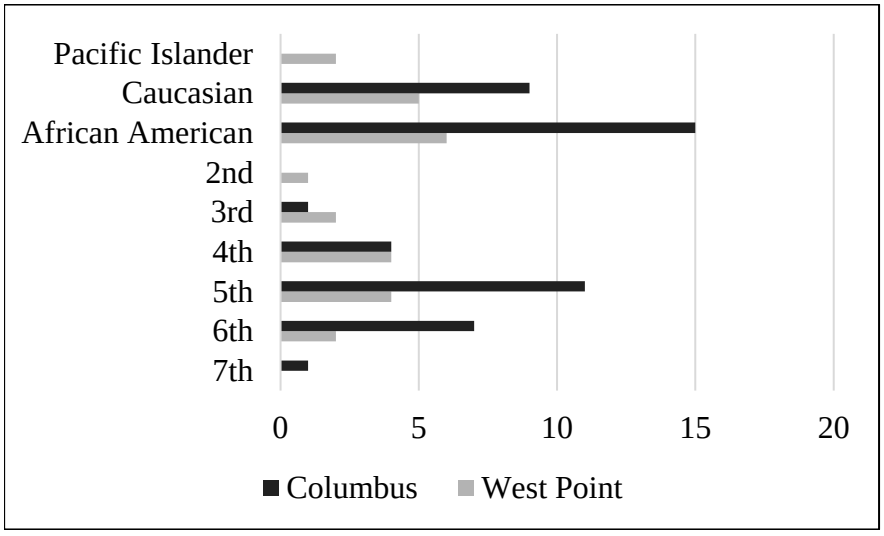
To emphasize digital citizenship, students were asked to create posters with poster paper and markers to describe how to behave safely online. Students explained internet safety, why is it important, and how they and their friends can stay safe while using the internet. Using the website "howsecureismypassword.net", students practiced creating passwords using guidelines for strong passwords. The site returns a message for each password stating an estimate of how long it would take for the password to be cracked.

At the end of the week, students used the skills they had learned to design programming projects that they could show to their friends and family on the last afternoon. Examples of projects included robot racing and having the Finch write on paper with a marker taped to the robot.

Discussion

Characteristics of the participants, by race and completed grade, are shown in Figure 1.

Figure 1. Participant characteristics.



During the camp, the mentors quickly observed that students needed "movement time", so time was set aside for outside activities that involved play and exercise. The camp mentors implemented the GenCyber bucks into these outside activities, asking questions about GenCyber principles with responses rewarded through bucks and advancement in the game as appropriate. Some students were observed gaining confidence on the first two levels of Snap and expressing hesitance to move to more advanced levels. GenCyber bucks were an effective way to motivate most of these students to move to other levels. Another observation was that some of the GenCyber principles, particularly Abstraction, were harder to comprehend. The youngest of the participants tended to struggle more with the advanced vocabulary used in explanations of all of the principles. Learning was accessed through observations of group activities and a 'think-pair-share' activity at the end of most days. GenCyber bucks were used in group sessions to reward correct responses.

Anecdotal evidence reveals that this type of camp does spark interest in computing and cybersecurity. Five of the participants had attended a similar day camp in 2016. Three attended a computing workshop that was hosted at MSU during the 2016-2017 academic year. One of the participants in the 2016 pilot camp worked as a junior mentor in Columbus camp. At least three of the participants have expressed interest in applying to a GenCyber residential camp in 2018.

Future Plans

In 2018, the elementary camps will be extended to six communities in the state. 120 elementary students rising 2rd through 5th graders, will be recruited. Data collection is required to make a determination if this co-curricular activity influences persistence on a computing or cybersecurity education pathway. Pre- and post-assessments will be implemented to inform a longitudinal study on the impact of this type of program offering on self-efficacy in computing.

Curriculum improvements underway include a focus on improving the coverage of the GenCyber principle 'abstraction' since it is fundamental to computational thinking. Proper handling of laptops and robots will be modeled on the first day and reinforced throughout the week. Exit tickets in the form of a passport-style booklet will be designed and implemented in the 2018 program that students will complete and show to camp mentors before departure each day. This will assist in measuring learning outcomes and the progression of students through programming levels and knowledge of and demonstration of cyber security concepts.

Acknowledgements

The Bulldog Bytes elementary camps in 2017 were funded through GenCyber (#H98230-17-1-0249) and supports goals of the NSF INCLUDES MSAWC (NSF # 1649312). The authors thank Doug Marchant and Emily Epps for donations supporting this work.

References

1 Lenhart, Amanda, "Teens, Social Media & Technology Overview 2015", Pew Research Center Internet & Technology, 2015, Retrieved November 8 2017 from http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/.

2 Bharti, Prasanna, "Why is Digital Citizenship Important? Even for Youngest Kids", EdTechReview, 2014, Retrieved on November 8 2017 from http://edtechreview.in/trends-insights/insights/1331-why-is-digital-citizenship-important-even-for-youngest-kids.

3 Kelly, Kimberly, David A. Dampier, Kendra Carr, "Willing, Able, and Unwanted: High School Girls' Potential Selves in Computing", Journal of Women and Minorities in Science and Engineering 19(1), 2013, 67-85.

4 National Girls Collaborative, Retrieved November 7 2017 from https://ngcproject.org/.

5 GenCyber website, Retrieved November 7 2017 from https://www.gen-cyber.com/about/.

6 Lee, Sarah, Stacy Kastner, and Rian Walker. Engineering For The Future: Mississippi State University's Cyber Summer Programs. Proceedings of the 2016 ASEE SE Annual Conference, 2016.

7 Mississippi Department of Education, data reported in 2016, Retrieved November 7 2017 from http://mdereports.mdek12.org/data/

8 datacenter.kidscount.org, data last reported in 2011, Retrieved November 7 2017.

9 Payne, Bryson R.; Abegaz, Tamirat; and Antonia, Keith (2016) "Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy," Journal of Cybersecurity Education, Research and Practice: Vol. 2016 : No. 2 , Article 3. Retrieved November 7 2017 from http://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/3

10 https://www.finchrobot.com/software/snap

11 https://www.sleuthkit.org/autopsy/v2/

12 Thornton, David (Jacksonville State University). SpaceScams and BruteForce Games (Lesson Plan). Retrieved November 7, 2017, from https://www.dropbox.com/sh/7n5fx23300uuvi4/AACEOv6rEkSqyyyjNI_9HRbAa?dl=0

13 Bryant, Lance; Caesar Ciphers: An Introduction to Cryptography, Purdue University, Portugal, 2007.

Litany Lineberry

Lineberry is currently a Ph.D. student in CS at MSU with a research focus in cybersecurity education. She received her MS in CS with a concentration in Information Assurance from North Carolina A&T University. Her BS in CS was received from Voorhees College. Previously, Lineberry was Area Coordinator and an Instructor in CS at Voorhees.

Sarah Lee

Lee received her Ph.D. in computer science from the University of Memphis. She earned her bachelor's degree in computer information systems from the Mississippi University for Women and a master's degree in CS from MSU. She spent 19 years in a variety of roles in the information technology division of FedEx Corporation. Lee is PI for NSF INCLUDES MSAWC.

Jessica Ivy

Ivy received her Ph.D. in Curriculum and Instruction from The University of MS (UM). Her BA in Education degree and Master of Education degree, both in Mathematics Education, were earned at UM. She was as a Research Fellow at the Center for Mathematics and Science Education after teaching high school math in rural MS. Her research areas include the integration of technology to enhance student learning and the exploration of rural mathematics education and teacher preparation.

Heather Bostick

Bostick is a sophomore computer science major at MSU. Before attending MSU, she participated in a residential GenCyber summer camp. A Mississippi Affiliate Aspirations in Computing award winner, Heather has worked for two summers as a camp mentor for MSU's Bulldog Bytes program.