The Adventures of ScriptKitty: Using the Raspberry Pi to Teach Adolescents about Internet Safety

Ovidiu-Gabriel Baciu-Ureche
United States Military Academy
West Point, NY
gabriel.baciuureche@gmail.com

Carlie Sleeman
United States Military Academy
West Point, NY
carlie.p.sleeman.mil@mail.mil

William C. Moody
United States Military Academy
West Point, NY
William.Moody@westpoint.edu

Suzanne J. Matthews*
United States Military Academy
West Point, NY
Suzanne.Matthews@westpoint.edu

ABSTRACT

Internet safety and privacy considerations are increasingly important topics for adolescents. While online games and other media exist to introduce middle school and high school students to security and privacy concepts, there are very few practical exercises that reinforce concepts in a hands-on manner. In this paper, we introduce *The Adventures of ScriptKitty*, a free on-line learning aid that is used in conjunction with the Raspberry Pi single board computer. We piloted *The Adventures of ScriptKitty* to 51 middle school and high school students. Our results show that students significantly improved their understanding of basic network topics and felt more confident on how to stay safe on the Internet.

CCS CONCEPTS

• **Applied computing** → **Education**; • **Security and privacy** → *Human and societal aspects of security and privacy*; • **Hardware** → *Emerging tools and methodologies*;

KEYWORDS

Raspberry Pi, Cyber Security, Internet Safety, K-12 Education

ACM Reference Format:
Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, William C. Moody, and Suzanne J. Matthews. 2019. The Adventures of ScriptKitty: Using the Raspberry Pi to Teach Adolescents about Internet Safety. In *The 20th Annual Conference on Information Technology Education (SIGITE '19), October 3–5, 2019, Tacoma, WA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3349266.3351399

1 INTRODUCTION

Cybersecurity and online safety practices are not commonly taught at the middle school and high school levels. However, Internet use is virtually ubiquitous amongst adolescents (ages 11-18). The National Center for Education Statistics suggests that 68% of 11-14 year-olds and 78% of 15-18 year-olds in the United States use the Internet at home, with 92% of U.S. teens accessing the Internet through a mobile device [20]. A 2018 study by the Pew Research Center [1] indicates that 95% of teenagers have access to smartphones and 45% of teens report themselves as being online almost constantly. However, many adolescents do not understand how their information is used online. In one recent study, 50% of surveyed teenagers either felt that the information they posted online was considered private, or had no concept of online privacy [23].

Several organizations have begun to capture which Internet safety concepts are important for students to learn and when to teach them. For example, ACM's Model Curriculum for K-12 Computer Science [32] recommends that by 9th and 10th grade, students understand the basic components of computer networks and the ethical issues that arise from their use. The CS Teachers Association (CSTA) recommends that by age 11, students learn the basics of how information is transferred across the web and how to protect personal information [27]. A 2013 survey of "stakeholders" (parents, teachers, teenagers) suggests that Internet safety should be taught as early as elementary school, but that many teachers and parents feel under-prepared to introduce the concepts [19].

In this paper, we introduce *The Adventures of ScriptKitty*, a free online story-based educational aid that aims to improve cyber awareness amongst teenagers and adolescents through practical hands-on exercises. The *ScriptKitty* materials are designed to be used in conjunction with the Raspberry Pi, a $35.00 single board computer with a System-on-Chip (SoC) processor similar to those found in mobile phones. In addition to the *ScriptKitty* online stories and tutorials, we provide a GitHub repository containing the technical materials needed for educators to set up a Raspberry Pi for home or classroom use. Our goal in developing *ScriptKitty* is to make adolescents aware of their activities online, and to educate them on how to best protect themselves.

We piloted a portion of the *ScriptKitty* materials to 51 middle school and high school students across three workshops. Specifically, we focused on the module introducing network fundamentals and packet sniffers. We measured the improvement in student performance pre- and post-workshop and asked students to self-assess their confidence on various topics. Our results show a significant improvement in student performance, and sizeable increases in student confidence. We believe *The Adventures of ScriptKitty* will be a valuable resource to help increase student awareness of their digital footprints.

*Corresponding Author

SIGITE '19, October 3–5, 2019, Tacoma, WA, USA
2019. ACM ISBN 978-1-4503-6921-3/19/10.
https://doi.org/10.1145/3349266.3351399

2 RELATED WORK

In addition to the ACM’s Model Curriculum for K-12 Education [32], both the K-12 Computer Science Framework [7] (a collaborative effort by ACM and multiple other computing organizations) and the the CSTA K-12 Computer Science Standard [27] highlight the need for a progressive understanding of networks, the Internet and the impacts of computing. The K-12 Computer Science Standard outlines detailed expectations for students. For example, middle school and high school students are expected to model network protocols and explain the trade-offs between public and private information sharing. The GenCyber program [11] seeks to develop cyber awareness in K-12 students and teachers across the United States and outlines concepts and principles for practicing and understanding cybersecurity.

Despite the recognized need, network and Internet fundamentals are not widely taught in schools [19, 32]. When Internet safety is taught, fear is often used as a key motivating factor [16, 34]. A recent study of 75 mobile online security applications shows that “safe use" by adolescents is enforced by parental controls rather than teenager self-regulation [34]. Researchers present the Teen Online Safety Strategies (TOSS) model that focuses on teen self-monitoring, impulse control, and risk-coping which are aided by understanding security threats and impact of decisions [34]. A more recent study supports the TOSS model, showing that children were more willing to accept restrictions on devices when they fully understood the threat and co-designed the monitoring interfaces [18]. An earlier study also argues that that building confidence in the skills of users is the most effective strategy for improving online safety [16].

Most practical exercises focused on network fundamentals focus more on attacking/defending systems and less on the user-level implications and impacts of those attacks. For example, capture the flag (CTF) competitions like PicoCTF [6] are increasingly popular at the high school and college levels, where teams race to solve challenges and search for “flags". CyberCIEGE [31] is an online game that creates scenarios where students have to make decisions about designing and maintaining the network security of a lab. The CyberPatriot [33] competition enables high school and middle school students to protect and defend critical information systems against an active threat.

While the aforementioned competitions and tools are excellent for students actively planning on careers pursuing cybersecurity, they are less useful for educating users on the threats they face online. Researchers have argued that cybersecurity education should focus on the most common threats and that hands-on exercises are the best way for students to learn [9]. GenCyber summer camps [8, 10, 15] offer hands-on opportunities for K-12 students to learn about cybersecurity. However, the camps are localized to particular regions in the United States and the materials are not freely available for large-scale classroom adoption.

A key novelty of *The Adventures of ScriptKitty* is its use of the Raspberry Pi, a $35.00 single board computer (SBC) that is widely used for STEM education at the K-12 level due to its low cost and strong community support [28]. The Raspberry Pi has been successfully used to introduce middle school and high school students to digital signal processing [24], engineering concepts [14], space technology [30] and computing [2, 13]. The Raspberry Pi is also used to introduce K-12 students to STEM in developing nations [35].

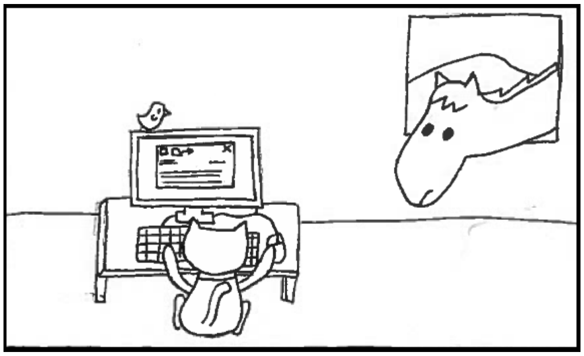


Figure 1: A sample comic from the story-line

Our work is also novel in its use of comics (see Figure 1) and a story-based approach to help make the material more attractive to a younger audience. The use of comics for teaching cyber security is a relatively new concept. CySCom [17] creates comics using the Comic-BEE [26] educational tool to create a “choose-your-own-adventure” comic targeted toward high school students. The Army Cyber Institute and Arizona State University have used graphic novels to help users visualize the future of cyberspace operations [29]. However, these projects introduce concepts in a passive manner and do not pair concepts with hands-on exercises. In contrast, *The Adventures of ScriptKitty* focuses on the “so what" factor by letting students observe how easily security compromises can occur with commonly used free tools.

Lastly, many cyber security materials are not freely available and may be expensive to deploy, limiting their effectiveness in more resource-constrained classrooms. In contrast, the *ScriptKitty* materials are free to access [3–5] and include an SD card image and GitHub repository that enable instructors to quickly setup the materials on purchased Raspberry Pis. To the best of our knowledge, *The Adventures of SciptKitty* is the first freely available project that combines comics with hands-on exercises to introduce Internet safety and network fundamentals on the Raspberry Pi.

3 OVERVIEW OF MATERIALS

Our free online materials come in several parts. First, we use GitBook [5, 12] to present the *ScriptKitty* story-line and tutorials in an easily readable web format. The story-line and tutorials are meant to be used in conjunction with the Raspberry Pi. In order to reduce setup time, we distribute a custom Raspberry Pi 3 image [3] pre-loaded with Kali linux and all the needed software. For educators using different versions of the Raspberry Pi or who want to use our materials on other computers, we make our materials available through a GitHub repository [4]. The repository contains detailed instructions and install scripts to assist users in installing all necessary packages on a Raspbian or Kali-based image.

Our story is broken into four chapters, each with new plot point and a technical component that guides students through an interactive exercise. The premise of the story is as follows: one morning, Ruby (a.k.a. “ScriptKitty") is shocked to discover her human (Gerry) looking at pictures of cats on the Internet. Hurt and confused, she enlists the help of Pixel (a canary) and Ed (a pony) to help figure out what's going on. While our story encompasses four chapters, we focus our pilot study on the first two chapters. In the paragraphs below, we provide a robust overview of chapters 1 and 2 and a summary of the last two chapters.

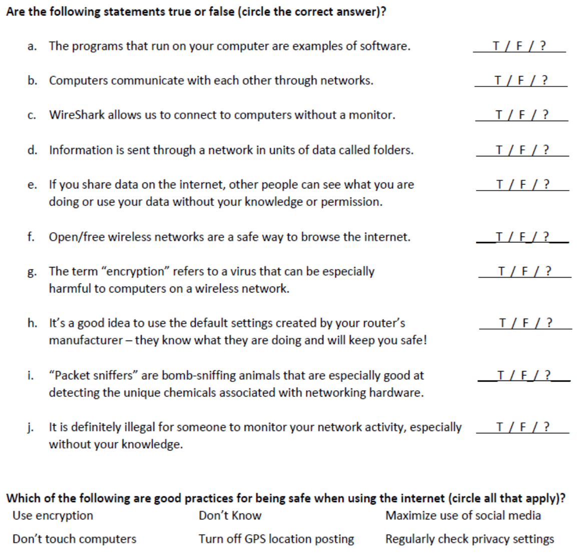
In the first chapter, students are introduced to the characters in the story and to the Raspberry Pi SBC. Students are guided through connecting the required peripherals of a display, keyboard, and mouse to boot the computer. Instructions for advanced users to access the Pi remotely from another computer using SSH are also provided. We note that this chapter supports the first two levels of the ACM Model K-12 Curriculum [32], and the CSTA K-12 Standard Level 1B Computer Systems identifier on Devices [27].

The next chapter represents the most advanced technical portion of the story, introducing students to networks, packets, and packet sniffers. We discuss packets and their composition while introducing the protocols, IP addresses, ports, and payload components. In the practical exercise, students are provided a packet capture (PCAP) file purporting to be Gerry's Internet traffic, and use Wireshark [22] to view his web searches and even read his emails. We discuss the ethical gray area of packet sniffing, and ask students if they agree with Ed's assessment that Ruby's actions amount to an invasion of privacy. We mention that it is common for organizations to run packet sniffers on their own networks, and to be aware of their existence and use. The students especially learn of the dangers of packet sniffers on unsecured wireless networks, and how hackers can use packet sniffers to snoop on people's Internet traffic in public spaces.

We close the chapter with general advice on staying safe on the Internet, including the need to use encryption whenever possible, how to identify when a network connection is secured (look for HTTPS), and how to change settings on one's phone to prevent them from auto-connecting to unsecured wireless networks. We discuss the dangers of using of social networking, and how nothing posted on the Internet is truly private.

The material in chapter 2 supports many of the foundational elements of computer security education. The materials directly address the "Networks and Internet" standards for levels 1B, and most of level 2 for the CSTA K-12 standard. The ACM K-12 curriculum strives for students to exhibit legal and ethical behaviors when using information technology and to be able to describe and discuss the impacts of those decisions. Our materials meets level II topics and goals related to "Computer Science in the Modern World" [32], including understanding the basics of computer networks, and ethical issues relating to computer networks [32]. The chapter also aligns with the "Think like an Adversary" GenCyber concept and is likely useful for GenCyber camps looking to integrate a hands-on packet sniffing component.

The final two chapters expose students to the dangers of weak passwords and closes out our story. As a practical exercise, students use Wireshark to extract a password-protected archive from the packet capture in Chapter 2, and use John the Ripper [21] to crack the password on the archive. The last chapter focuses on the dangers of password reuse and its implications. As a practical exercise, students re-use the password they discovered in Chapter 3 to "log on" to Gerry's computer. We close the chapter with a discussion of password management and a discussion of social engineering attacks. These chapters support the ACM K-12 curriculum topics for password security, and the CSTA K-12 Level 1B and 2 standards on "Networks and Security" for creating strong passwords and proper password management [27]. The final two chapters also align with the "Think like an Adversary" and "Defense in Depth" GenCyber cybersecurity concepts.



Are the following statements true or false (circle the correct answer)?

a. The programs that run on your computer are examples of software. ___T / F / ?___

b. Computers communicate with each other through networks. ___T / F / ?___

c. WireShark allows us to connect to computers without a monitor. ___T / F / ?___

d. Information is sent through a network in units of data called folders. ___T / F / ?___

e. If you share data on the internet, other people can see what you are doing or use your data without your knowledge or permission. ___T / F / ?___

f. Open/free wireless networks are a safe way to browse the internet. ___T / F / ?___

g. The term "encryption" refers to a virus that can be especially harmful to computers on a wireless network. ___T / F / ?___

h. It's a good idea to use the default settings created by your router's manufacturer – they know what they are doing and will keep you safe! ___T / F / ?___

i. "Packet sniffers" are bomb-sniffing animals that are especially good at detecting the unique chemicals associated with networking hardware. ___T / F / ?___

j. It is definitely illegal for someone to monitor your network activity, especially without your knowledge. ___T / F / ?___

Which of the following are good practices for being safe when using the internet (circle all that apply)?

Use encryption Don't Know Maximize use of social media

Don't touch computers Turn off GPS location posting Regularly check privacy settings

Figure 2: Sample quiz questions

4 ASSESSMENT

We piloted a portion of *The Adventures of Script Kitty* to three different groups of students in the form of workshops. Due to the limited time that we had with all sets of students, we only had time to introduce the Raspberry Pi and assess the packet sniffing exercise in Chapter 2. IRB restrictions also limited us to evaluating middle school and high school students.

The first workshop was given to a set of middle school students at a local middle school who were all part of their school's coding club. We label this population going forward as "Middle School". Since the coding club meets for only an hour, we were restricted to at most an hour for our workshop. While not all students provided demographic information, the data we gathered indicated that the middle school students ranged in age from 11 to 14 years old, and were mostly young white males.

The second and third workshops were given to two separate groups of minority women who attended various NYC high schools. The first group of young women attended various charter, college preparatory, and other limited admission schools. All the students attended the same charter school during middle school. This population is labeled in our study as "Charter School". Our last group of young women all attended various NYC area public schools. This last population is labeled in this paper as "Public School". Unlike the middle school workshop, the two high school workshops were 90 minutes long, allowing us extra time to discuss ethical implications.

Table 1: Middle School Results

Question	(Pre-/Post-) Population	Pre-Quiz	Post-Quiz
True/False	22/15	3.59	4.53
Best Practices	22/13	2.27	2.62
Conf./Using	17/10	4.14	4.30
Conf./Understanding	17/10	2.50	3.70

All populations were given a pre-quiz prior to the workshop and post-quiz at the end of the workshop that contained identical questions. Figure 2 shows a listing of sample questions. To discourage guessing, an “I don't know" option was added to each question. The first set of questions were a series of True/False questions designed to assess students' knowledge about networks, packets, WireShark, and implications of using a network. Since the first workshop was limited to only an hour, the quiz taken by the Middle School population contained only the first 6 questions. The 90-minute workshops given to the high school students were expanded to contain all 10 True/False questions. The next question asked students to circle good practices to stay safe on the Internet. Lastly, we asked students to rate (on a Likert scale) how confident they were about using computers vs. understanding how networks/the Internet works.

5 RESULTS

Results for the three populations are shown in Tables 1- 3. For the True/False questions, the authors gave a point to every question that was answered correct (an incorrect response or an “I don't know" response was assigned zero points). Hence, the maximum score that a student could earn on the True/False questions in the middle school and high school workshops was 6 and 10 respectively. For the Good Practices question, the authors counted the number of correct circles (“use encryption", “turn off GPS location posting" and “regularly check your privacy settings") and the maximum score was 3.

We used the R package [25] to conduct significance analysis. Due to the variations in the population sizes, R automatically selected a Welch two-sample t-test for this analysis.

5.1 Results with Middle School Students

Table 1 summarizes our results with the Middle School population. As previously mentioned, we were restricted to no more than an hour with this group of students. For the True/False component of the quiz, we saw an improvement from 3.59 (59.8%) to 4.53 (75.5%). We also noticed a reduction on the number of “I don't know" responses; 16 middle school students indicated at least one “I don't know" answer to True/False questions on the pre-quiz, compared to 3 on the post-quiz.

The students did fairly well on the Best Practices question on the pre-quiz and post-quiz. We speculate this could be due to prior exposure to computing topics. As mentioned, the Middle School population consisted of students who were part of the school's coding club. Only two students selected “I don't know" for this question on the pre-quiz (and none did on the post-quiz). While we see a rise in the average score on this question, it was slight.

Lastly, we asked the students to self assess their confidence in “using computers" vs. “understanding how computers and networks work". The middle schoolers were already very confident *using* computers prior to the workshop, and remained so afterwards. However, a different story emerges when middle schoolers were asked to self report their confidence on “how computers and networks work". The average score increased from 2.5 to 3.7 from the pre-quiz to the post-quiz, indicating that student confidence on understanding how computers and networks worked improved as a result of our workshop. Students also reported enjoying reading the comics and became invested in the story (*I wish Ruby was my cat!*, exclaimed one middle school student).

There were several threats to the validity of this initial study, several of which caused us to redesign the workshop for our high school populations. The biggest threat to validity were students failing to complete all questions on the pre-quiz and post-quiz, primarily due to students getting distracted and parents coming to pick up their children earlier than anticipated. Early departures and distracted students resulted in 7 students leaving without taking the post-quiz. Of the remaining 16 students who took the post-quiz, only 13 completed the Best Practices question, and only 10 answered the confidence questions. While we had attempted to number the quizzes to keep track of which students took what quiz, the classroom separated the area that students sat to take the quizzes from the area they completed the workshop. Students did not return to their original seats after the activity, removing our ability to correlate pre- and post-quiz scores. Thus, significance results are omitted for this workshop.

5.2 Results with High School Students

Our issues with the Middle School population forced us to re-evaluate how our assessments were conducted. Our high school workshops were located in a classroom with sufficient power supplies at each desk, so that students did not move around during the workshop. The workshops for high school students were 90-minutes each, enabling us to extend the True/False component of the quiz to 10 total questions. The confidence questions were modified specifically assess student confidence on understanding how the Internet works, and how to stay safe online.

Despite our best efforts, there were still a couple instances where students skipped questions or did not complete the post-quiz. Of the 16 students in the Charter School population, all completed the True/False questions, 15 completed the Best Practices question and 12-14 completed the confidence questions. While 14 students started the workshop in the Public School population, one student left early due to feeling unwell; data on at most 13 students were consequently collected. While 13 students completed both the True/False and Best Practices questions, only 9 students answered the confidence questions. Unlike our first workshop, we were able to correlate the scores in the high school populations, enabling us to perform a two-sample paired t-test.

Table 2 and Table 3 depict the improvements in average score for each question and the associated p-values. Despite attempting to make the True/False question component harder, we saw a statistically significant improvement in student performance in both populations. For example, the Charter School population averaged 50% on the pre-quiz compared to 63.1% on the post-quiz. The Public School population experienced a larger improvement, with a jump

Table 2: Charter School Results

Question	(Pre-/Post-) Population	Pre-Quiz	Post-Quiz	P-value
True/False	16/16	5.00	6.31	0.0239
Best Practices	15/15	1.80	2.23	0.0484
Conf./Using	14/14	3.50	3.79	0.5000
Conf./Understanding	13/13	2.92	3.62	0.0019
Conf./Safety	12/12	3.16	4.00	0.0172

Table 3: Public School Results

Group	(Pre-/Post-) Population	Pre-Quiz	Post-Quiz	P-value
True/False	13/13	3.92	6.69	0.0014
Best Practices	13/13	1.54	2.46	0.0148
Conf./Using	9/9	4.16	4.16	1.0000
Conf./Understanding	9/9	2.78	3.67	0.2249
Conf./Safety	8/8	2.94	4.13	0.0371

in average score from 39.2% to 66.9% on the True/False component. A reduction in the number of "I don't know" responses for the True/False component can also be observed for both populations. While 9 students from the Charter School population and 13 students from the Public School population indicated at least one "I don't know" answer on the pre-quiz, only 4 Charter School students and 4 Public School students indicated at least one "I don't know" response on the post-quiz.

The high school populations also experienced a statistically significant improvement in average scores for the Best Practices question. The Charter school population's average score improved from 1.68 to 2.23, while the Public School population improved from 1.54 to 2.46. Only 2 students from the Charter School populations indicated "I don't know" for the Best Practices question on the pre-quiz, compared to 3 from the Public School population. No students from either population selected this response on the post-quiz.

5.2.1 Confidence Analysis. The high school populations were also asked to self-assess their confidence levels on using a computer vs. "understanding how the Internet works" and "what you need to stay safe on the Internet". Responses from individuals who did not complete the associated question on both the pre-quiz and the post-quiz were excluded. We were able to procure 22 responses on "understanding how the Internet works" and 20 responses on staying "safe on the Internet". Like the Middle School population, the students from the high school populations were already very confident on using computers. Both high school populations showed an improvement in confidence from the pre-quiz to the post-quiz in understanding how the Internet works. While the Public School population's average confidence level increased from 2.78 to a 3.67 from the pre-quiz to the post-quiz, the result was not found to be significantly significant. Further analysis revealed that the confidence scores for three individuals in the Public School population actually went down. We speculate that the decrease may have been due to initial overconfidence, and that our workshop may have showed them how little they understood about the Internet to begin with.

However, there was a statistically significant increase in confidence in both high school populations on staying safe online. The Charter School population's average confidence rating increased from 3.16 on the pre-quiz to a 4.00 on the post-quiz. The Public School population's average confidence rating increased from a 2.94 to a 4.13. Our results suggest that our workshops significantly improved student confidence on staying safe on the Internet.

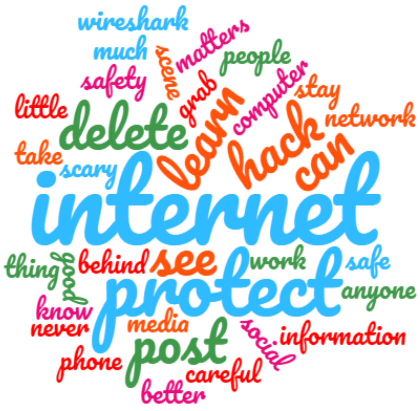


Figure 3: Big takeaway from the workshop

5.2.2 Open-Ended Responses. Our results are bolstered by the set of open-ended responses we received from our high school students. We asked students to note "what was the one thing (good or bad) that you took away from this workshop?". We received a total of 14 responses. Figure 3 shows a summary of the responses. We removed punctuation, capitalization, and stop words and applied stemming to merge similar words (e.g. "learn" and "learned"). In general, students were most impacted by the fact that others can "snoop" on their network traffic using a tool like Wireshark. *It doesn't take much to be a hacker*, noted one participant. *Internet safety matters!* exclaimed another.

6 CONCLUSIONS & FUTURE WORK

In this paper, we introduce *The Adventures of ScriptKitty*, a novel educational aid to teach adolescents about Internet safety through hands-on exercises on the Raspberry Pi. Our freely available materials makes *The Adventures of ScriptKitty* easy to deploy in a home or classroom setting. The current set of chapters match many of the CSTA K-12 objectives related to Networks, the Internet and social impacts. Lastly, the concepts covered in several chapters align with several GenCyber concepts, suggesting that the *ScriptKitty* materials can easily be integrated into existing GenCyber curricula.

We ran a pilot study on 51 middle school and high school students. Our results show that our materials were well received and had a significant impact on student learning of basic networking concepts. Student confidence on understanding how networks/the Internet works and how to stay safe online also increased considerably. While further assessment is needed to evaluate the *ScriptKitty* password security module, our preliminary results are promising and suggest that our materials are successful in educating students about key topics while building confidence in an important skillset.

There are many avenues for future work. To expand the ethical discussions of *The Adventures of ScriptKitty*, we plan to partner with Comic-BEE [26] to create interactive storylines with more decision making. We believe that having a more heavily-comic focused approach will improve student engagement, especially amongst younger audiences. While our middle school students thoroughly enjoyed reading the comics, they did not enjoy reading large blocks of text accompanying the technical components. Increasing the concentration of comics in the materials will be a primary focus going forward. We also plan to run additional workshops to generate additional feedback to continue to improve the *ScriptKitty* materials and assess the remainder of the chapters.

The use of the materials in conjunction with the Raspberry Pi was a clear success. All of our populations thoroughly enjoyed using the Raspberry Pi. Educators at other institutions have also started using the *ScriptKitty* materials with elementary school students, and reported back to us that students loved the storyline and playing with the Raspberry Pi. While formal assessment of this group is not yet available, we do want to expand the *ScriptKitty* materials to cover a greater range of Internet safety topics and complete assessment with younger populations.

7 ACKNOWLEDGEMENTS

The *Adventures of ScriptKitty* was created and drawn by the first two authors while they were undergraduates at the U.S. Military Academy. The last two authors were the faculty advisors on the project. Karlee Scott also assisted in drawing comics and survey design in the early stages of the project. We also thank Raymond Blaine and Joe Sagisi for assisting with the high school workshops. The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of the Army, Department of Defense or the U.S. Government.

REFERENCES

[1] Monica Anderson and Jingjing Jiang. 2018. Teens, Social Media & Technology 2018. https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/

[2] Crispin Andrews. 2013. Easy as Pi [Raspberry Pi]. *Engineering & Technology* 8, 3 (2013), 34–37.

[3] Ovidiu-Gabriel Baciu-Ureche. 2018. The Adventures of ScriptKitty: Raspberry Pi 3 Image. Internet Website, last accessed 29 May 2019. http://www.suzannejmatthews.com/images/aosk/aosk_v2.7z

[4] Ovidiu-Gabriel Baciu-Ureche, William C. Moody, and Suzanne J. Matthews. 2019. The Adventures of ScriptKitty: Github Materials. Internet Website, last accessed 29 May 2019. https://github.com/ogBaciu/Files-for-AOSK

[5] Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, Karlee Scott, William C. Moody, and Suzanne J. Matthews. 2018. The Adventures of ScriptKitty. Internet Website, last accessed 29 May 2019. https://suzannejmatthews.gitbooks.io/aosk/content/

[6] Peter Chapman, Jonathan Burket, and David Brumley. 2014. PicoCTF: A Game-Based Computer Security Competition for High School Students. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. USENIX Association, San Diego, CA. http://www.usenix.org/conference/3gse14/summit-program/presentation/chapman

[7] K-12 Computer Science Framework Steering Committee. 2016. *K-12 Computer Science Framework*. Technical Report. ACM, New York, NY, USA.

[8] Amber Dryer, Nicole Walia, and Ankur Chattopadhyay. 2018. A Middle-School Module for Introducing Data-Mining, Big-Data, Ethics and Privacy Using RapidMiner and a Hollywood Theme. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, New York, NY, USA, 753–758. https://doi.org/10.1145/3159450.3159553

[9] S. Dutta and R. Mathur. 2012. Cybersecurity âĂŤ An integral part of STEM. In *IEEE 2nd Integrated STEM Education Conference*. IEEE, 1–4. https://doi.org/10.1109/ISECon.2012.6204166

[10] Vitaly Ford, Ambareen Siraj, Ada Haynes, and Eric Brown. 2017. Capture the Flag Unplugged: An Offline Cyber Competition. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17)*. ACM, New York, NY, USA, 225–230. https://doi.org/10.1145/3017680.3017783

[11] GenCyber. 2014. Gen Cyber: Inspiring the next generation of cyber stars. https://www.gen-cyber.com/

[12] GitBook Inc. 2014. GitBook: Documentation Made Easy. Internet Website, last accessed 7 August 2018. https://www.gitbook.com/

[13] Vic Grout and Nigel Houlden. 2014. Taking computer science and programming into schools: The Glyndŵr/BCS Turing project. *Procedia-Social and Behavioral Sciences* 141 (2014), 680–685.

[14] L. M. Herger and M. Bodarky. 2015. Engaging students with open source technologies and Arduino. In *2015 IEEE Integrated STEM Education Conference*. IEEE, 27–32. https://doi.org/10.1109/ISECon.2015.7119938

[15] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Game Based Cybersecurity Training for High School Students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, New York, NY, USA, 68–73. https://doi.org/10.1145/3159450.3159591

[16] Robert LaRose, Nora J. Rifon, and Richard Enbody. 2008. Promoting Personal Responsibility for Internet Safety. *Commun. ACM* 51, 3 (March 2008), 71–76. https://doi.org/10.1145/1325555.1325569

[17] B. Ledbetter, Z. Wallace, A. Harms, A. Siraj, and L. Buchanan. 2016. CySCom: Cybersecurity COMics. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. 282–284. https://doi.org/10.1109/ISI.2016.7745490

[18] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 523, 9 pages. https://doi.org/10.1145/3173574.3174097

[19] Megan A Moreno, Katie G Egan, Kaitlyn Bare, Henry N Young, and Elizabeth D Cox. 2013. Internet safety education for youth: stakeholder perspectives. *BMC public health* 13, 1 (2013), 543.

[20] National Center for Education Statistics. 2019. Children's Access to and Use of the Internet. *The Condition of Education* (2019). https://nces.ed.gov/programs/coe/pdf/coe_cch.pdf.

[21] Openwall. [n. d.]. John the Ripper password cracker. Internet Website, last accessed 29 May 2019. https://www.openwall.com/john/

[22] Angela Orebaugh, Gilbert Ramirez, and Jay Beale. 2006. *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier.

[23] Jessica A. Pater, Andrew D. Miller, and Elizabeth D. Mynatt. 2015. This Digital Life: A Neighborhood-Based Study of Adolescents' Lives Online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2305–2314. https://doi.org/10.1145/2702123.2702534

[24] M. S. Pattichis, S. Celedon-Pattichis, and C. LopezLeiva. 2017. Teaching image and video processing using middle-school mathematics and the Raspberry Pi. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 6349–6353. https://doi.org/10.1109/ICASSP.2017.7953378

[25] R Core Team. 2013. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. https://www.R-project.org

[26] Secure Decisions. 2017. Comic-BEE: Comic-Based Education & Evaluation for Cyber Security. Internet Website, last accessed 27 September 2018. https://comic-bee.com/

[27] Deborah Seehorn, Stephen Carey, Brian Fuschetto, Irene Lee, Daniel Moix, Dianne O'Grady-Cunniff, Barbara Boucher Owens, Chris Stephenson, and Anita Verno. 2011. CSTA K–12 Computer Science Standards: Revised 2011. (2011). 104111.

[28] Jesse Strycker. 2015. The Raspberry Pi: Not a Poor Man's Computer, but an Interesting Possibility. *Educational Technology* (2015), 30–34.

[29] Devin L Suits. 2019. New graphic novellas to educate Soldiers, families on future cyber threats. https://www.army.mil/article/215922/new_graphic_novellas_to_educate_soldiers_families_on_future_cyber_threats

[30] J. Taylor and D. A. Nero. 2017. Project HALON: Engaging secondary students in high-altitude ballooning experiments. In *2017 IEEE International Conference on Electro Information Technology (EIT)*. 587–592. https://doi.org/10.1109/EIT.2017.8053432

[31] Michael Thompson and Cynthia Irvine. 2011. Active Learning with the CyberCIEGE Video Game. In *Proceedings of the 4th Conference on Cyber Security Experimentation and Test (CSET'11)*. USENIX Association, Berkeley, CA, USA, 10–10. http://dl.acm.org/citation.cfm?id=2027999.2028009

[32] Allen Tucker, Fadi Deek, Jill Jones, Dennis McCowan, Chris Stephenson, and Anita Verno. 2003. *A Model Curriculum for K–12 Computer Science: Final Report of the ACM K–12 Task Force Curriculum Committee*. Technical Report. New York, NY, USA. ACM Order No.: 104043.

[33] G. B. White, D. Williams, and K. Harrison. 2010. The CyberPatriot National High School Cyber Defense Competition. *IEEE Security Privacy* 8, 5 (Sep. 2010), 59–61. https://doi.org/10.1109/MSP.2010.166

[34] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 51–69. https://doi.org/10.1145/2998181.2998352

[35] N. S. Yamanoor and S. Yamanoor. 2017. High quality, low cost education with the Raspberry Pi. In *2017 IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE, 1–5. https://doi.org/10.1109/GHTC.2017.8239274