High School Cybersecurity? Challenge Accepted – Radford University's RUSecure CTF Contest for High School Students

J. D. Chase
School of Computing and Information Sciences
Radford University
Radford VA, USA
jchase@radford.edu

Prem Uppuluri
School of Computing and Information Sciences
Radford University
Radford VA, USA
puppuluri@radford.edu

Abstract—Given the demand for Cybersecurity workforce, the goal of the RUSecure project at Radford University is to increase the pipeline of students who plan to pursue Computer Science/IT as a major with Cybersecurity as their focus. We identified a variety of challenges to the introduction of Cybersecurity topics in high school including lack of qualified teachers, limited number of students motivated to study IT topics, large number of prerequisite topics and scarcity of computing resources required for such topics. Even an introductory Cybersecurity course requires students to have a wide array of foundational knowledge in topics such as networks. Hence, Cybersecurity programs in schools/colleges are multi-semester efforts where the first couple of semesters focus on the foundations – thus only drawing motivated students as it takes multiple semesters before students work on security problems. In response to these challenges, we developed a strategy that is exciting, rigorous and easy to adapt for high school students. This strategy employs active learning in the form of capture-the-flag (CTF) contests to drive learning. Teams of three to five students work on security challenges while competing with teams from around the state, region, and Nation. Foundational knowledge is introduced on a just-in-time basis. This paper describes these contests and their effectiveness.

Keywords—Cybersecurity, High School, Education, Active Learning, Just in Time Learning

I. INTRODUCTION

The need for CS/IT majors in the workforce cannot be overstated. 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"* [1]. The Bureau of Labor Statistics Occupational Outlook Handbook indicates that the outlook for 2019-29 in Cybersecurity is expected to be very strong with approximately 31% growth. Most of these jobs require a Bachelor's degree or higher [1] [2]. Thus, there is a 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 [3] [4], 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 or AP CSP courses such as the AP CSP: Cybersecurity (National Cybersecurity Training & Education (NCyTE) Center, 2021). Participation in these courses is very limited [3]. Through the RUSecure project, our goals for these contests are to:

- Eliminate the barrier of teacher preparation by providing easily accessible, short, high impact materials associated with each challenge.
- Increase the number of students motivated to pursue further study in CS/IT and more specifically Cybersecurity by introducing the topics in a fun and competitive environment.
- Eliminate the need for long prerequisite chains by providing prerequisite knowledge in a just-in-time manner associated with each challenge.
- Eliminate the barrier of lack of computing resources by providing student teams access to a secure, isolated cyber-range hosted by Radford University.

The challenge in introducing Cybersecurity topics in high school is the wide array of pre-requisite topics needed for a thorough introduction to Cybersecurity including: *networking*, *fundamentals of the web* (e.g., client side scripts, web servers, database management systems), *advanced usage of Linux and Windows™ operating systems*, and other topics of CS/IT (e.g., regular expression, discrete math). Further, to attract more students into the pipeline, any such introduction has to keep students motivated – a difficult task if they are forced to take several pre-requisites before they get to the actual topics of Cybersecurity. We developed the RUSecure CTF Contests to adapt the strategies of *just-in-time* and *active learning* to Cybersecurity [5] [6] [7]. Topics are introduced through capture-the-flag (CTF) contests, where teams of students are provided challenges that start from very basic and progress to quite advanced. The solution for each challenge is a flag, for example, a string created

This research was funded in part by NSA, NSF, and Cypherpath.

using a secure hash function such as MD5. To obtain the flag, students must solve the challenge and if they do not have the required background knowledge for the challenge, they can refer to short (less than 10-minute) multi-media lectures or notes.

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* – 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 students and are limited to few schools. There is a need for more programs 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:, the Air Force Association's CyberPatriot [7], the CSAW-Cyber high school forensics competition [8], Hacker High School [9], the National Board of Information Security Education cyber camps [10], and SANS CyberAces [11] to list a few.
- ***Formal computer-security curriculum for K-12***. These include curricula developed in schools with technological and personnel resources to support such courses as well as comprehensive courses such as those from Teach Cyber [12] – from DARK enterprises, Hacker High School that teach the basics of Cybersecurity in K-12.

High school CTF contests are not unique and there are several of them including the ones discussed in the NICE K12 Working group one pager [13]. The contribution of this article is to describe our effort in teaching cybersecurity using a CTF contest.

III. The RUSecure Contest

A. RUSecure Contest History

The RUSecure CTF Contest began in 2014 as part of an NSA MEPP Grant and with support from Cypherpath. The original goal of the Contest was to explore applying the just-in-time learning strategies developed for Radford University's on-campus cybersecurity programs to the introduction of cybersecurity topics in high schools and community colleges. Participation in the RUSecure CTF Contests has grown at a remarkable rate since 2014. Table I shows the growth of the Contest since inception.

TABLE I. Participation in the RUSecure CTF Contests

Year	Number of Teams	Number of Students	Number of Schools
2014	9	36	4
2015	13	56	7
2016	18	81	9
2016-2017	70	303	32
2017-2018	130	546	58
2018-2019	345	1449	106
2019-2020	505	2057	123
2020-2021	302	1233	70

It is interesting to note that the numbers dramatically changed in 2016-2017 when the Contest was expanded from one round to three rounds:

- Preliminary Round - open to all participants; includes hints and educational materials (motivation and education – Scare and Prepare)
- Qualifying Round - open to all participants but without the hints and educational materials (motivation and assessment – Dare)
- Final Round which is open to the top teams from the Qualifying Round (motivation and assessment – Dare and Celebrate).

The 2019-2020 RUSecure CTF Contest successfully completed the Preliminary Round and the Qualifying Round before shutting down due to the pandemic. However, the 2020 Final Round was cancelled. We were able to complete all three rounds of the 2020-2021 RUSecure CTF Contest, with greatly reduced participation as schools dealt with the complications of the pandemic.

Participation in the RUSecure Contests is free. Through the years, the Contest has been supported by multiple grants from the NSA, in kind support from Cypherpath and through internal funding from the Radford University (RU) School of Computing and Information Sciences (RU-SCIS) and the RU Artis College of Science and Technology.

B. RUSecure CTF Contest Organization

The RUSecure CTF Contests challenge students in a wide variety of topic areas including anatomy of an attack, networking, cryptography, hashing, forensics, web security, Windows/Linux security, and reverse engineering. Contests

have also included challenges involving hacking of IOT devices as well as securing systems and devices from attack.

The Preliminary Round, which is several weeks in duration, provides an opportunity for students to learn a great deal of material in a short period of time, motivated by challenges and supported by hints, videos, and other educational materials. Beginning in the fall of 2019, the Preliminary Round was expanded to 12 weeks in order to give teachers maximum flexibility on how to integrate the Contest into their classroom.

The Qualifying Round, generally limited to two weeks, provides an opportunity for students to test their mettle against their peers and continue to hone their skills while competing for an invitation to the Final Round. When the Final Round was introduced in 2017, only the top 7 teams from the Qualifying Round were invited to the Finals. Beginning in 2019, in order to make sure that all areas of the Commonwealth of Virginia had the opportunity to participate, we began inviting the top placing team from each of Virginia's eight VDOE Regions, as well as the top 7 remaining teams, regardless of location.

The Final Round is a 1-day, typically on-campus event, where the top-placing teams from the Qualifying Round compete for prizes and scholarships. The 2019 Final Round was live-streamed on the front page of Twitch.tv. More information is available about the RUSecure CTF Contest at https://www.twitch.tv/rucsat/video/406645013. The 2021 Final Round was a virtual event.

The RUSecure Contests are open to currently enrolled high school, home school, or community college students. Teams registering for the Contest must include at least three team members but no more than five including the captain and must include a faculty member as a coach. We do limit participation to U.S. students only to avoid entanglement in any international laws regarding Cybersecurity.

C. The Challenges

The RUSecure CTF Contest is made up of a variety of challenges. 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 CTFd [14]. Fig. 1 shows a sample challenge from a recent contest. CTFd also provides back-end features allowing administrators to monitor the contest in real-time, analyze how teams are performing on each challenge, look at submissions including incorrect answers, and adjust on the fly. The CTFd environment also includes a Scoreboard as shown in Fig. 2 to allow teams to keep track of their relative performance in the contest.

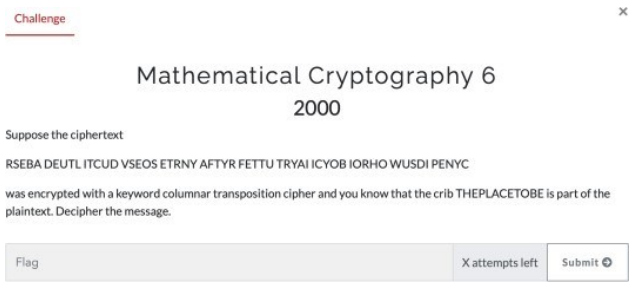

Fig. 1. Sample Challenge from RUSecure CTF Contest

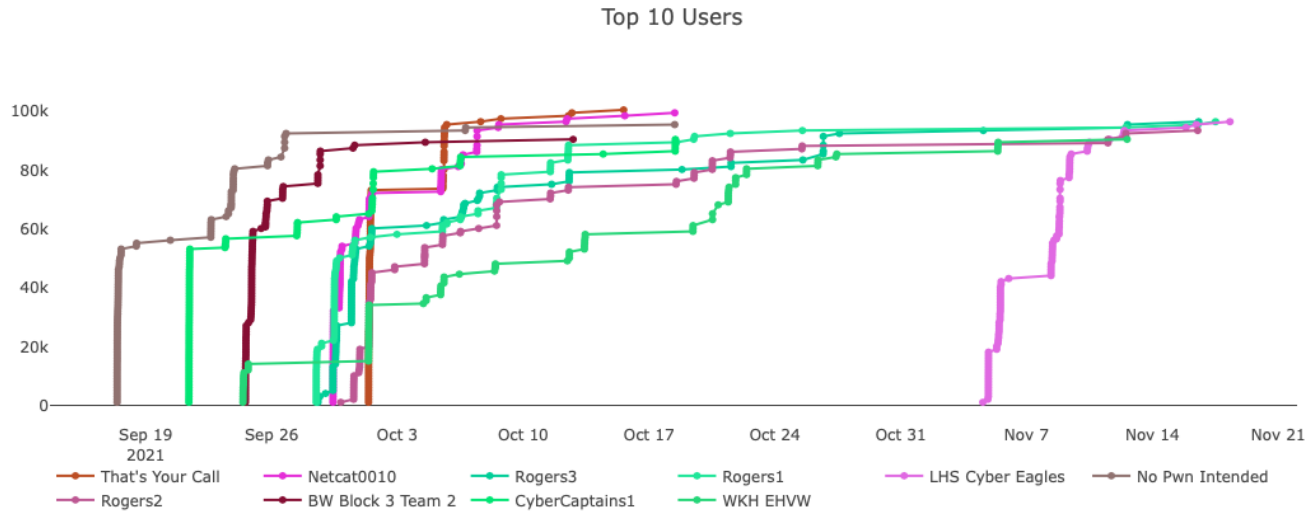

Fig. 2. Sample Partial Scoreboard from RUSecure CTF Contest

Many of the challenges for the contests are created by Cybersecurity students at Radford University, providing the further benefit of allowing these students to expand their own knowledge and skill.

D. The Environment

In addition to the contest environment, CTFd, teams are also provided access to a web-based, isolated, secure environment hosted as a cyber-range by Radford University. For the first several years of the Contest, this environment was hosted in the Cypherpath environment. However, we are now making use of VMWare™ technology. This environment allows teams access to both Windows and Linux virtual environments that have been preloaded with flags and software required for the given challenges. Because both the contest environment and the cyber-range are web-based, the only computing resource required for teams to compete in the contest is a web browser.

E. Using CTF Contests to Direct Learning

To apply active learning strategies, each topic is covered in one or more CTF challenges. As student teams attempt the challenges in the Preliminary Round, they can refer to short multi-media lectures or notes to help with the topic. The lectures are kept short based on lessons from efforts such as the Khan academy [15] on how to hold student attention. In keeping with the goal of limiting the need for computing resources, these lectures are hosted on Vimeo™ so as to be accessible from multiple devices.

To make CTFs exciting, the challenges need to be hands-on. To accomplish this, we modeled the challenges loosely around the anatomy of a computer hack. Specifically, the steps that a hacker takes to identify vulnerabilities in a computing infrastructure and exploit them lend themselves to introduce various foundational topics and teach cyber defense as well in the process. As an example, one of the first steps a hacker takes is to gather as much information as possible about the victim machine. This topic allows us to introduce the basics of networking: how victim machines are identified and addressed and how routing in networking works.

Hacking isn't malicious. In fact, as ISECOM [9] puts it "hacking is a method of problem solving that combines resourcefulness, logic, creativity and study." The ability for students to hack will provide them with in-depth knowledge of how attackers attack and how they can be countered. Most efforts to teach cyber security to high school and community college students emphasize hacking through CTF and other cyber defense contests such as the US Cyber Patriot [8] and SANS CyberAces [11].

Beginning with the 2019-2020 Contests, students were also challenged to harden Windows and Linux environments against attack. In these cases, the flags were actually reversed. For example, if the Red Team can access the flag on the team's system, then they may lose points for that challenge.

IV. Market Penetration, Utilization,and Effectiveness of the CTF Strategy

While it is difficult to directly measure the effectiveness of the CTF strategy separate from coursework and other preparation, we have collected a great deal of evidence of the impact of the RUSecure strategy through surveys of coaches and students, direct discussions with coaches and students, and observing the choices and success of some of the RUSecure CTF contestants. Over the eight years since its inception, the RUSecure CTF Contest has grown from a small handful of teams representing mostly local schools to more than 2000 students from more than 75 schools across the entire Nation. However, we measure our success through the following questions:

- Market Penetration – What is the reach of the Contest within the Commonwealth of Virginia?
- Utilization – How are high school and community college instructors making use of the Contest to support their classrooms?
- Effectiveness – What is the impact of the Contest for those that participate?

A. Market Penetration

Our goal is to ensure that a student's zip code should not determine their opportunities in Cybersecurity. However, early on in the development of the RUSecure Contest, it became apparent that there is a large disparity in the opportunities available to high school students. Simply put, the large suburban school districts have more resources available in the area of Cybersecurity. This has been demonstrated repeatedly by both the participation in the Contest and the success in the Contest (i.e. making it to the Final Round). Fig. 3 provides a map of teams participating in the 2018 Preliminary Round. Keep in mind that in this figure, one pin may represent multiple teams. As you can see, the vast majority of the teams are from the suburban population centers in Virginia or in areas surrounding universities. Fig. 4 shows the participants in the Final Round of the same 2018-19 Contest. The one outlier in Fig. 4 is a Community College team from Danville VA.

To improve the market penetration of the contest, we decided not only to invite the top 7 teams in the qualifying round but also 1 team from each of the 8 Virginia Department of Education designated regions.

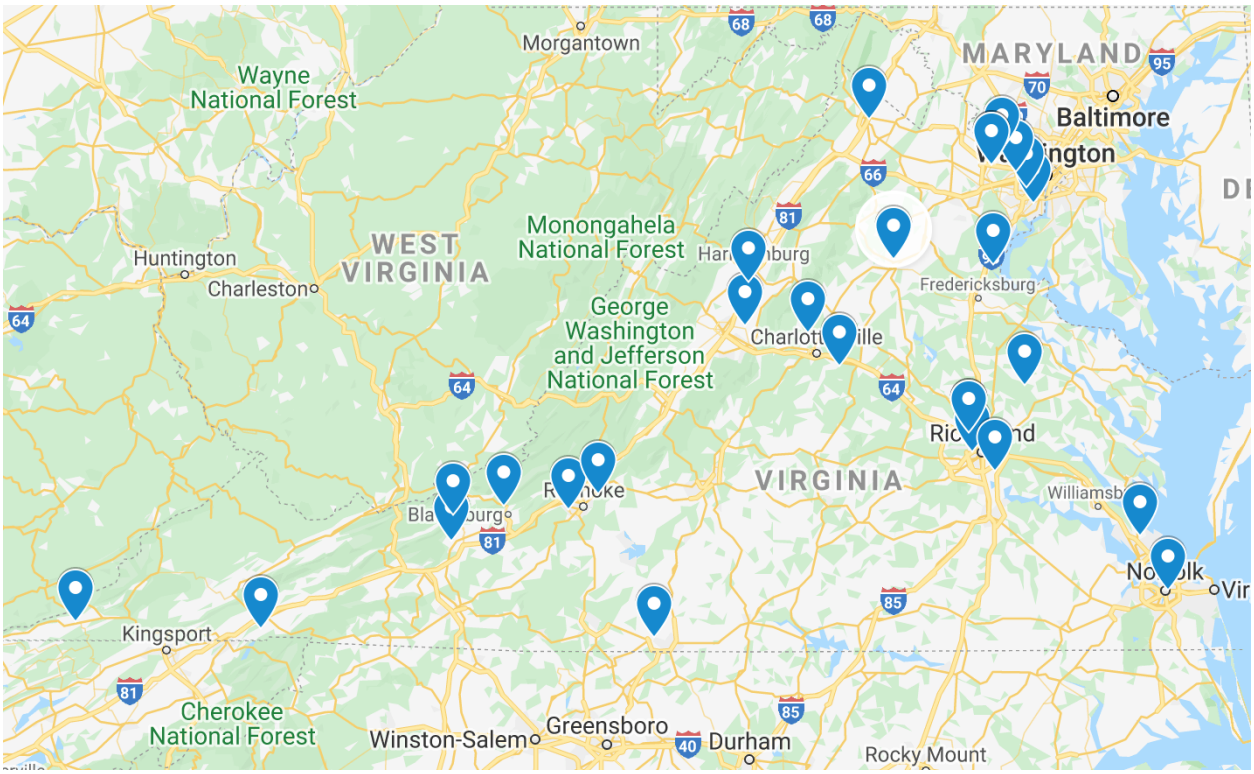

Fig. 3. Locations of teams competing in the 2018 RUSecure Preliminary Round [16]

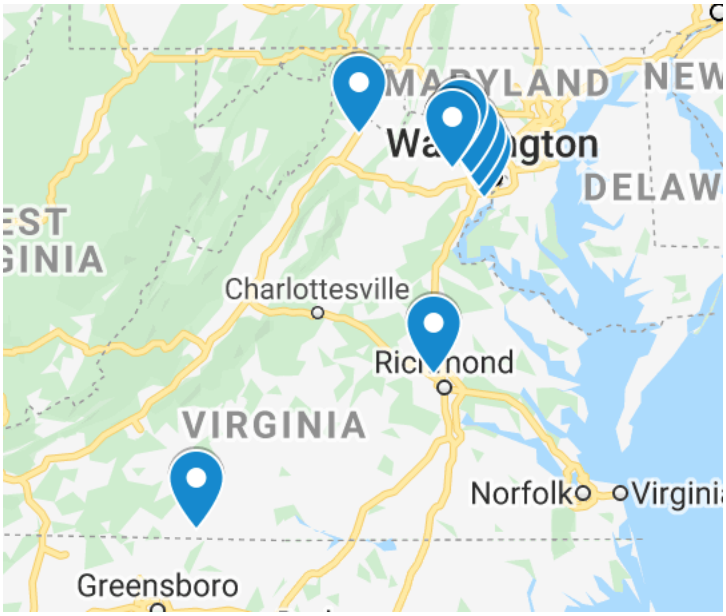

Fig. 4. Locations of teams invited to the 2019 RUSecure Final Round [17]

B. *Utilization*

We intentionally redesigned the Preliminary Round starting in the fall of 2019 to expand it to three full months to allow teachers more freedom to incorporate the Contest into their classroom more effectively. As a result, multiple schools began enrolling all of their Cybersecurity students making the Contest a required part of their classroom experience.

Multi-year survey results tell us that teachers have used the Contest as both graded and ungraded work, both inside and outside of the classroom, and as part of Cybersecurity club activities.

We have also seen an expansion of the utilization of the Contests by grade level. In the initial contest, virtually all of the participants were high school seniors or community college students. However, we are now seeing teachers register students as young as the 8th grade meaning that the same students are participating year over year. This has interesting consequences for Contest planning and design as we may now have the same student participating for as many as four years.

C. *Effectiveness*

In their comments about the contest both in formal surveys and informal conversations, teachers/coaches rave about the motivation, engagement, and time on task for their students participating in the contests. The effectiveness of the contest is also demonstrated by how teachers are now making use of the contest, as described above. The fact that many students now have the opportunity to participate multiple times across multiple years creates a deeper level of understanding.

That deeper level of understanding is also reflected in the scores. In the 2018 Preliminary Round, two teams cleared the board (i.e. solved every challenge) and several more teams were very close. This had not happened in any of the prior contests. So much improved is the level of understanding among the participating teams that we had to create challenges that were more intricate and more difficult.

While direct measure of the effectiveness of the contests themselves remains challenging, we have been able to measure the CTF strategy in other ways. For example, the same strategy was applied to a graduate course to prepare K-12 teachers to teach Cybersecurity. 92% of the educators who participated in the CTFs among those who responded to the survey indicated that *the CTFs helped them to understand the material faster than a traditional lecture*.

V. Conclusion

The CTF approach which implements the just-in-time strategy of teaching is highly effective in keeping students motivated and helps in covering a vast array of topics without requiring extensive pre-requisites. Our efforts indicate that not only is it possible to provide an introduction to Cybersecurity to students with a very limited IT/CS background, but it is possible to do so in a highly engaging manner.

References

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

[2] 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].

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

[4] 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/comp science-its-where-jobs-are-but-schools. [Accessed 1 7 2021]

[5] CyberSTEM, "CyberSTEM/CyberWatch," [Online]. Available http://www.edtechpolicy.org/cyberk12ARCHIVE/c3K12.html. [Accessed January 2021].

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

[7] CyperPatriot Training, "CyperPatriot Training," 1 January [Online]. Available: https://www.uscyberpatriot.org/competition/training-materials. [Accessed December 2012].

[8] NYC Poly University, [Online]. Available: http://www.poly.edu/csaw2012. [Accessed 26 December 2]

[9] ISECOM Hacker High School, "ISECOM Hacker High Sc Security Awareness for Teens," 1 January 2000. [Online]. Available: http://www.hackerhighschool.org. [Accessed 2 December 2012].

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

[11] SANS, [Online]. Available: https://www.cyberaces.org/courses.html. [Accessed 5 November 2014].

[12] Dark Enterprises, [Online]. Available: https://teachcyber.org/about/. [Accessed September 2020]

[13] NICE K-12 Working Group, [Online]. Available: https://www.nist.gov/system/files/documents/2020/05/06/nice_k12_subgroup_competitions_onepager.pdf. [Accessed September 2018]

[14] CTFD, [Online]. Available: https://ctfd.io/. [Accessed May 2017]

[15] Kahn Academy, [Online]. Available: https://www.khanacademy.org. [Accessed June 2014

[16] Google Maps: Locations of teams competing in the 2018 RUSecure Preliminary Round, *Google Maps* 2021, https://goo.gl/maps/

[17] Google Maps: Locations of teams invited to the 2019 RUSecure Final Round, *Google Maps* 2021, https://goo.gl/maps/