picoCTF: Teaching 10,000 High School Students to Hack

Preliminary Report

Peter Chapman David Brumley
peter@cmu.edu dbrumley@cmu.edu

June 21, 2013

Abstract

In the spring of 2013, two student-lead organizations, the Plaid Parliament of Pwning and Team Osiris, designed and hosted a computer security competition for high school students called picoCTF. Unlike existing competitions, picoCTF focuses primarily on offensive hacking skills presented in the form of a web-based video game to better excite students about computer science and computer security. Over the 10-day competition nearly 10,000 middle and high school students participated across almost 2,000 teams vying for $25,000 in prizes, making picoCTF, to the best of our knowledge, the largest hacking competition ever held. The competition introduced thousands of high school students to advanced topics such as the command-line interface, cryptographic ciphers, the client-server paradigm of the web, file system forensics, command injection, data representation, and program representation. picoCTF sets a new standard in scale and educational impact in pre-collegiate computer science.

1 Introduction

The Plaid Parliament of Pwning (PPP) [10] is a computer security research group at Carnegie Mellon University, composed of undergraduates, graduate students, and university staff. In addition to hosting study sessions and student-lead courses, the primarily role of PPP is to compete in computer security competitions called **CTFs**. In a standard-format CTF (capture-the-flag), teams of students and professionals race to answer computer security challenges, often searching for digital "flags" hidden on servers, in encrypted text, or obfuscated in binary programs. Challenges are open-ended and require expertise in computer forensics, cryptography, reverse engineering, binary exploitation, and web security. When a team submits a flag, they receive points for solving the challenge. The team with the highest score at the end of the competition wins. CTFs are set up as a fun, legal way for students and professionals to practice and demonstrate their skill.

The Plaid Parliament of Pwning is one of the top CTF teams in the world, consistently ranking in the top two positions worldwide [5]. As is customary, PPP hosts an annual CTF for hundreds of students and professionals called plaidCTF.

In the summer of 2012, researchers from the National Security Agency (NSA) visited Carnegie Mellon University to meet with professors on the latest developments in computer security. Completely unaffiliated with recruitment, the government officials informally met with members of PPP.

Sharing a common interest in CTFs and high school education, PPP offered to host a CTF for high school students with seed funding provided by the NSA[1].

1.1 Sponsors

We would like to thank our sponsors:

Gold Sponsors Symantec and CMU ETC donated $10,000.

Silver Sponsors Intel and Microsoft donated $5,000.

Other Sponsors

- Amazon Web Services provided $2750 of credit to winning teams and schools.
- The Information Networking Institute donated $2,500 for prizes and scholarships.
- Cloudshark provided their web-based network protocol analyzer suite for picoCTF participants.
- Pearson donated Chapter 3 of *Computer Systems: A Programmers Perspective*.
- Wiley donated 30 textbooks to the winning teams.
- The National Security Agency provided the initial funding for picoCTF.
- SEI worked with picoCTF during project conception and funding management.

1.2 Goals

Initial planning for picoCTF began in the fall of 2012. We outlined three goals:

1. Provide an authentic, fun, interactive introduction to computer security.

2. Encourage students to pursue degrees in computer science or related disciplines, regardless of incoming background.

3. Nationally recognize and inspire top competitors to become industry leaders.

To assist in building an effective interactive experience we recruited game design experts, Team Osiris [8], from the Entertainment Technology Center [6]. In conjunction with Team Osiris we built the challenges in picoCTF around a web-based story-driven game, featuring multiple levels, cutscenes, character interaction, and sound effects (Figure 1 shows a scene from the finished game). Over the course of four months, a team of 13 students from PPP and Team Osiris led by David Brumley built picoCTF[2]. From April 26th to May 6th 2013, nearly 10,000 middle and high school students competed in picoCTF 2013. To the best of our knowledge picoCTF 2013 was the largest computer security competition ever held. We view picoCTF to be an outstanding success as we introduced advanced technical topics to thousands of students in a hands-on fashion.

---

[1]The National Security Agency does not endorse picoCTF or PPP in any way. The NSA had no involvement in the production or management of picoCTF. No correspondence regarding the competition should be addressed to the NSA. Instead, please contact the authors directly.
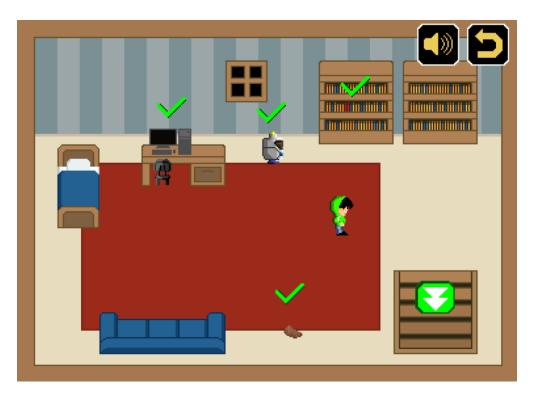
[2]`https://picoctf.com`

Figure 1: The world-view of the first level

In the following we will discuss related initiatives (§2), the competition format and content (§3), our methodology and lessons learned in building picoCTF (§4), the impact of the competition (§5), and our plans for expanding on our success (§6).

Ethics Hacking tends to be misrepresented as a malicious activity. Done legally, hacking is not only a creative way to garner interest in computer science, but perhaps the best possible way to learn about how computer systems work – similar to taking apart and reassembling a car as an educational exercise. However, as with most technical skills, there are malicious applications and we felt it paramount to stress wherever possible that we do not condone and actively discourage illegally breaking into systems, stealing personal information, or disrupting computing services.

2   Related Efforts

picoCTF is neither the first nor only computer security competition for high school students. The High School Cyber Forensics Challenge [7] focuses on computer forensics. The preliminary round is held online, but the finals are hosted in conjunction with the Polytechnic Institute of New York University's CSAW CTF. The CyberPatriot National High School Cyber Defense Competition [12] is an annual defensive competition. Both events have underlying stories to motivate challenges. In contrast to the skills emphasized in the Cyber Forensics Challenge and Cyberpatriot, picoCTF places a strong emphasis on offensive techniques to encourage students to creatively explore and experiment with computer systems.

More closely related, the US Cyber Challenge periodically hosts a Cyber Quest [3] to test skills ranging from vulnerability analysis to cryptography. The format of Cyber Quest is significantly different than the game presentation and quantity of challenges in picoCTF.

In the classroom, computer security is rarely taught. Both the College Board's Advanced Placement Computer Science examination [9] and the ACM Model K-12 Curriculum [11] only discuss computer security and privacy in a social context.

3   Competition Overview

picoCTF is a series of 57 independent challenges in forensics, cryptography, reverse engineering, web and script exploitation, and binary exploitation. Students in grades 6-12 were eligible to compete on teams of five or fewer over a ten day period in the spring of 2013.

Organization   Though CTF problems are traditionally presented in a text-based manner, we followed the trend set by PlaidCTF and opted to build picoCTF around a game experience. The game is divided into four levels each advancing the story and increasing in difficulty. Level 1 begins as the player discovers a crashed robot in their backyard. Aimed at students with no programming experience, the first level unfolds as the player repairs the robot. The criteria for advancing is level specific; for example, level 1 is completed after solving 3 out of the 5 available problems, at which point the player can continue to solve the remaining level 1 challenges or start level 2.

In levels 2 and 3, the player recovers the robot's lost ship at a nearby spaceport and then returns to space to participate in an intergalactic hacking contest in level 4. Level 2 is designed for students with introductory programming experience in languages such as Visual Basic or Alice. Level 3 is targeted at AP Computer Science students with a stronger background in programming. Lastly, level 4 is a diverse set ranging from difficult to professional-CTF difficult challenges across all categories. We opted to divide the competition into levels to better account for the vastly different backgrounds of participating students. We want each student to leave picoCTF satisfied with accomplishment, from the 6th grade student with no programming experience to the exceptional hacking senior.

Rules and Scoring   We assigned each challenge a point value corresponding to the predicted difficulty. Upon solving a challenge, the point value is added to the team's score. The winner of the competition was the team with the most points (last problem solved was used as a tiebreaker). Teams were encouraged to use all available resources but were forbidden to receive direct assistance from persons outside the team.

Gameplay   picoCTF supports two challenge viewers: the Game Problem Viewer and the Basic Problem Viewer. The Game Problem Viewer is an HTML5 game where the player can explore and interact with the world (Figure 1) selecting on objects to view challenges (Figure 2). The Basic Problem Viewer simply displays the description for each challenge, ideal for older browsers and serious competitors. Many problems ask the student to perform a privilege escalation attack on a vulnerable executable. We host these problems on a Linux server for students to SSH directly or through a web client [2]. Additionally we provide an IRC-based chat room for students to discuss
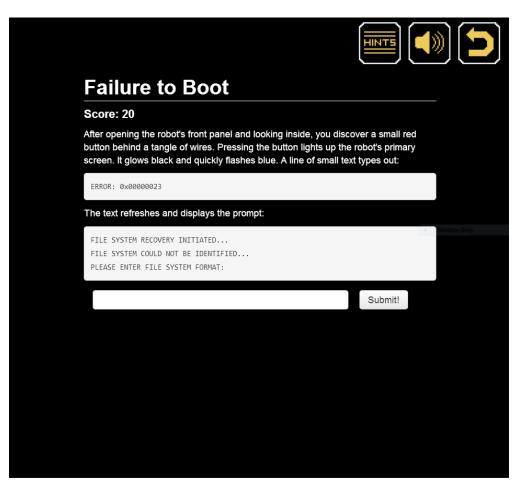
Figure 2: A challenge displayed in the picoCTF game

challenges with competition organizers. Lastly, we created a series of 7 lectures on select topics to provide background for some of the difficult challenges.

Awards and Sponsors Primarily to support awards, picoCTF 2013 was generously sponsored by 11 different organizations[3]. picoCTF 2013 had 3 winning teams and 3 winning schools. A team was eligible if each individual on the team was a 6th-12th grade student in the United States. The school affiliated with a team was eligible if each member attended that school. A school could field an unlimited number of teams and multiple winning teams could attend the same school. Winning teams and schools received cash awards ($1000-$8000), credit to Amazon Web Services ($250-$1000), a selection of books from Wiley publishing, trophies, printed and signed certificates, and t-shirts.

4 Building picoCTF

picoCTF is the result of a joint-effort between two student organizations, PPP [10] of Carnegie Mellon University's CyLab and Team Osiris [8] of the Entertainment Technology Center. Eight
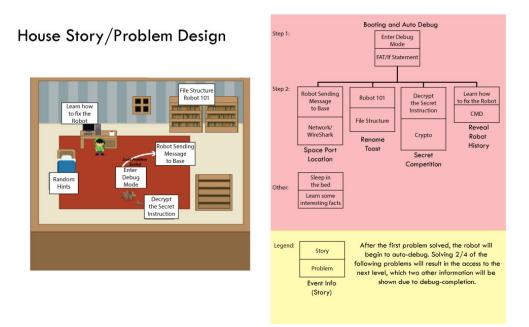
---

[3]https://picoctf.com/sponsors

Figure 3: Early storyboard for the first level of picoCTF

students from PPP and five from Team Osiris worked on the project 10-40 hours a week on top of other student commitments. We met twice weekly, once in a design meeting and also a Sunday work session.

Accommodating Schools A guiding principle in the design of the competition was to accommodate the busy schedules of students and teachers in a school environment. To that end picoCTF 2013 covered two weekends and an entire work-week, giving students the freedom to find an available weekend and teachers the ability to integrate the competition into class time. Further, we ensured that a modern web browser is sufficient to complete all of picoCTF, since many school have restrictions on installing software. Unfortunately, many students found the picoCTF 2013 timing to be difficult as it occurred immediately before the two-week period of Advanced Placement exams. For that reason, some instructors did not notify their students of the competition.

Challenge and Game Design We designed competition challenges and gameplay simultaneously, each contributing to the other. In a series of brainstorming sessions we enumerated a set of challenges generally appropriate for our target audience. Inspired by common game design principles we settled on a four level game to clearly separate challenges by difficulty in an effort to account for the diversity of student backgrounds. Early in development we formulated the basic story around the player repairing a fallen robot from space. Team Osiris expanded on the concept, creating storyboards for each level. Figure 3 shows an early storyboard for the first level detailing individual challenges and their effect on the game world.

User Testing We worked with two local Pittsburgh high schools to understand the skills and resources available to students. The staff at both schools was incredibly helpful in both giving feedback and granting access to students. We ultimately held two testing sessions with local Pittsburgh high schools on the first level of the competition. From that session we found that students

enjoyed the competition but needed a place to go for help when stuck. Based on that feedback we made the difficulty increase more gradually, added hints to every problem, and emphasized the Chat feature of the website.

Infrastructure picoCTF is built on top of standard web development tools. We serve all pages statically from an nginx server running on Amazon EC2. Each page loads content dynamically through a separate API server running the Flask Python microframework [1]. We maintain persistence using a MongoDB instance running locally on the API server. We track site usage client-side with Google Analytics and on the server by logging events into the datastore. Problems are stored as BSON documents in MongoDB with the essential data including a title and the HTML description for the challenge. Each problem has a URI to a Python script for grading the correctness of submissions. Almost every query to the API is heavily cached using an instance of Memcached. The core infrastructure easily scaled with competition activity, though the shell server provided to students was often hindered by limited disk read and write speeds.

Soliciting Sponsorship We felt prizes were important to foster serious competition. In particular we believed that school awards would incentivize teachers to encourage students to participate. Due to restrictions on the funds received from the NSA we reached out to other sources to provide for prizes. We ultimately sent out dozens of requests to contacts in industry and at CMU. We found that clearly outlining the goals and emphasizing the scale of the competition was most convincing to funding sources. We do recommend approaching large corporations carefully as they often use centralized management systems for processing donation requests. On one occasion we failed to receive sponsorship from a large corporation because a separate entity in the company had already turned us down despite the enthusiasm of our contact.

Publicity We took a number of different approaches to publicity. News articles and interviews provided a strong flow of new registrations, but we believe most registrations resulted from the word of mouth initiated by a targeted email to members of the Computer Science Teachers Association (CSTA). Based on survey data, 60% of students heard about the competition from a teacher and 87% from a teacher, friend, or parent. 47% of teachers discovered picoCTF through the CSTA email and 41% through word of mouth. Social media campaigns and paid advertising was ineffective. We investigated placing ads in periodicals for high school teachers but cost thousands of dollars and months of notice.

General Lessons In creating picoCTF we gained a lot of valuable experience on organizing a competition of this scale. First, it is difficult for students to work during the semester as coursework takes precedence. Awarding course credit gives students to contribute more heavily. Second, hiring contractors is very time consuming as detailed documentation and requirements are necessary. The speed at which our design and technical requirements changed prohibited us from hiring despite having the funds. Lastly, when targeting participants outside of the traditional CTF community, polish in presentation and detailed copy is necessary: if the presence appears unprofessional, a teacher will not share it with their colleagues.

5 Impact

Based on website analytics (embedded JavaScript), datastore analysis (the persistent storage of teams, problems, and submissions), survey data[4], and anecdotal feedback, we believe picoCTF had a profound educational impact on high school students at an unprecedented scale. During the 10-day competition, 1,938 teams solved one or more challenges. Using survey data backed by analytics and IP logging, we believe between 8,000 and 10,000 students competed.

Demographics We targeted the competition at high school students in the United States. Problem submissions were overwhelmingly domestic across all users (90% domestic, 7% international, and 3% of unknown origin) and casual inspection of team affiliations shows predominately legitimate institutions. The 1,938 teams came from 955 different affiliations. Figure 4 shows the distribution of teams per affiliation.
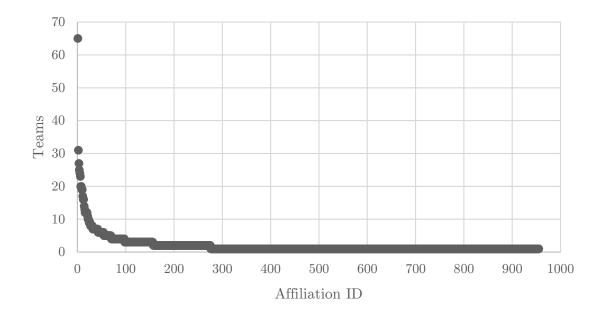

Figure 4: The distribution of teams per affiliation

Over 90% of teams were affiliated with a high school and individuals were mostly in grades 11 or 12 (see Figure 5). Teams were well represented across the United States with the geographic distribution shown in Figure 6. A large portion of students reported prior programming experience in object-oriented languages (61%) and on web applications (49%). Surprisingly 30% of students even claimed to have prior experience hacking, though the survey did not define the term. The vast majority of students become aware of the competition through a teacher (61%), classmate (19%), or parent (7%). Most students reported participating for fun or as a learning experience. In summary, the typical picoCTF 2013 participant was an 11th or 12th grade student with programming experience on a team organized by their teacher or classmate for fun.

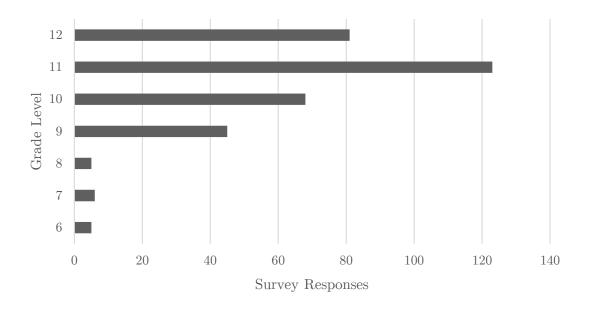[4]The survey can be found at `http://goo.gl/seSC0`

Figure 5: Reported grade distribution from competition survey

Educational Impact   The competition featured 57 problems across 5 major categories: forensics (15), cryptography (8), reverse engineering (9), web and scripting exploitation (13), and binary exploitation (11). Over the course of the competition we processed 172,482 submissions, of which 29,325 were correct. In preparing the competition we assigned point values (between 20 and 200) to challenges according to the estimated difficulty. Figure 7 shows the number of teams that solved a given challenge out of the number that attempted. Point values correlate inversely with challenge solves indicating accurate difficulty prediction ($r = -0.8$).

The challenges in picoCTF were designed to encourage students to learn and practice valuable technical skills above and beyond the traditional high school computer science curriculum. The game was divided into four levels, described in Section 3. Table 1 shows the number of teams to complete each level. We overview select problems in Table 2. For example, in *Try Them All!* we introduced 1,279 teams (many thousands of students) to salted password storage. Students demonstrated their understanding by implementing a brute-force dictionary attack on a leaked password hash. Examining a more traditional topic, *Byte Code* considers program representation, requiring students to either decompile a Java program or manually examine the byte code in a hex editor in search of a hidden key. Lastly over 90 teams solved *ROP 1*, a binary exploitation challenge on writing a return-to-libc attack. This form of return-oriented programming is a technique that troubles even graduate students, and yet, was solved by many hundreds of high school students. Overall, we successfully introduced thousands of students to complex computer security and computer science topics on both ends of our target spectrum from introductory to world-class.
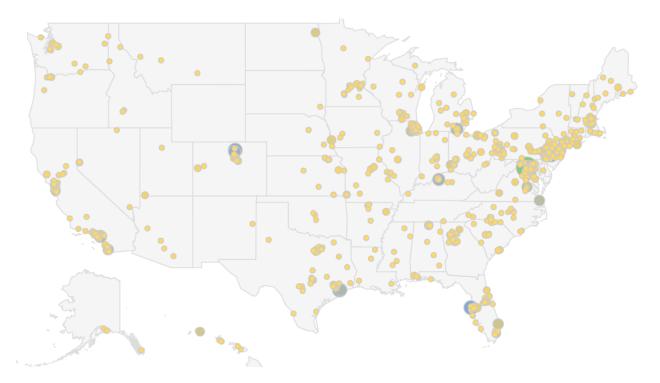
9

Figure 6: Geographic mapping of team affiliations. Circles scale with the number of affiliated teams.

Level	1	2	3	4
	(No Programming Experience)	(Introductory Programming)	(AP CS)	
Completions	1,541	1,297	930	3

Table 1: The number of teams completing the four levels of picoCTF

Supplemental Material To help introduce students to some of the topics and skills found in levels 1 and 2. Though we initially planned significantly more supplemental education materials, we did supply 9 lecture videos (totally 75 minutes) and a book chapter on program representation [4]. Over the course of the competition the video lectures received a total of 7,142 views. To further help students, we provided an IRC-based chat room. PPP members answered hundreds of questions and help foster a community among the most active competitors. The top two teams even plan to compete together in professional CTFs, starting with the 2013 DEF CON qualifier.

Performance Correlations Examining the survey we identified responses that correlated with higher average team scores. Unsurprisingly, we found that students with prior computer science experience, especially in discrete math and hacking, performed better on average. Additionally, the final score of a team was moderately correlated with the time spent on the competition ($r = 0.5$). We also found a correlation between using the basic problem viewer and higher team scores, indicating that serious competitors were less likely to use the game viewer.

Feedback We solicited feedback on the competition in our exit survey. Regarding content, students asked for a greater number of problems on web exploitation (30%) and cryptography (22%) and less binary exploitation (46%). Largely, students felt that the competition was an appropriate

Level	Challenge	Team Completions	Acquired Skills
1	First Contact	1,368	Network Traffic Analysis
2	CFG to C	1,321	x86 Assembly and Control-Flow Graphs
2	Try Them All!	1,279	Password Hashes, Salts, and Dictionary Attacks
3	DDoS Detection	615	Defensive Traffic Analysis
3	Byte Code	1,146	Program Representation
3	SQL Injection	571	Command Injection Attacks
3	RSA	228	RSA Implementation
4	Overflow 1	216	Buffer Overflow
4	ROP 1	96	Return-to-libc Attack

Table 2: A sample of picoCTF challenges and their educational contribution

difficulty and that 10-days was either sufficient (55%) or would have preferred more (40%). Teachers and students both reported that students put forth more effort and learned more than in a typical class. Lastly, out of the 36 teachers that responded to our survey, every one stated that they would encourage their students to compete again next year. Informally we also received a lot of feedback on social media and email.

Among the kind words and even poems[5], one note from a Pennsylvania high school teacher was especially touching:

> Wow! I haven't seen something like this light the fire of such a wide range of students in my 22 years of teaching computer science (or my own time spent studying CS & math in college through the 80's). Neither robotics, ACSL, face-face or online traditional programming contests, Logo, Alice, block based languages a la Scratch or AppInventor, early HTML development, or any other single CS phenomenon has ever inspired so many students to fight to get access in the computer lab after school and ask me cerebral questions such as bit-wise arithmetic or syntax questions on languages they haven't learned in school! Students with natural math abilities as well as average math intellectual skills, students who are the rebel hacking types as well as the goody two shoes kids, teams of girls and teams of guys and even seniors with full blown cases of senioritis are all coming out of the woodwork.
>
> ...
>
> THERE IS NO DOUBT IN MY MIND THAT THIS CONTEST WILL SINGLE-HANDEDLY ATTRACT MANY STUDENTS TO CAREERS IN CYBERSECURITY AND COMPUTER SCIENCE IN GENERAL!
>
> <div align="right">(Pennsylvania High School Instructor via Email)</div>

We also recieved a number of comments directly from students:

> My team and I have learned more in the last 5 days than we have in 2 years of computer class
>
> <div align="right">(Student via IRC)</div>

---

[5] http://drgnhmn.deviantart.com/art/picoCTF-368151415

Thanks for such a great competition! I learned an insane amount and definitely plan to get into more CTF's after this experience. I have a vast interest in computer security and computer science and after PicoCTF I really want to get into more types of competitions like this.

See you next year! (*Student* via Survey)

I thought this was a really awesome competition. Definitely the most fun I've ever had while competing. I wish this had existed since my freshman year.

(*Student* via Survey)

Some more samples of direct feedback can be found in Appendix A.

6   Looking Forward

We hope to build on the success of picoCTF 2013 to make an even greater impact in picoCTF 2014. To avoid much of the scheduling issues in the spring (e.g. SATs, AP exams, prom, graduation, etc.) we have announced picoCTF 2014 for the fall of 2014. We hope to use the extra time to better prepare a cohesive curriculum around the challenges and supply enough lectures and tutorials to guide a student through at least the first two levels, making picoCTF even more competitive to a massively open online course (MOOC).

In addition to the significantly improved educational materials we hope to provide a more friendly way for students to ask questions and receive answers. While functional IRC can be difficult to use and lacks any meaningful persistence, requiring competition organizers to repeatedly answer similar questions without advancing the conversation. We also plan to introduce automatically generated problem variants to allow teams to practice different skills (e.g. writing buffer overflows and identifying malicious traffic). Further, automatically generating problems allows new types of challenge evaluation where we could conceivably require a team to solve a challenge within a time limit or reward teams for solving many problem instances. Either way can be a motivation for students to generate programs that automatically solve challenge problems. Lastly we hope to improve our infrastructure to allow large-scale experiments on teaching methodologies as many proponents of MOOCs have advocated.

7   Conclusion

picoCTF 2013 reached nearly 10,000 middle and high school students across the United States. Students learned advanced technical skills, even some that can prove difficult to graduate students at a top university. We hope to expand on our success in picoCTF 2014 with a wider audience and a strong curriculum.

A   Direct Feedback Samples

> i've actually learned more about security and forensics from challenges like these
> more than my uni has taught me   (*Student* via IRC)

> This is probably random, but I'd like to give a really big thank you to everyone who helped put this together, because the more work I do the more obvious it becomes that there was loads of time and intelligence put into every bit of the competition.
>   (*Student* via IRC)

> This was a fantastic problem solving experience. The students were very engaged and excited to compete. I thought the contest was accessible by a wide range of students, due to the varying degrees of complexity and variety of problems.
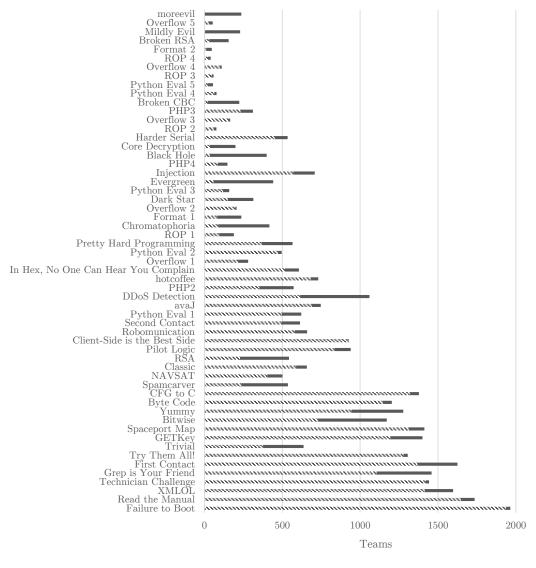> Good work!   (*Instructor* via Survey)

> This was a great way to supplement my unit on security and privacy. Thanks for the opportunity. Looking forward to the Fall CTF.   (*Instructor* via Survey)

References

[1] Flask Python Microframework. http://flask.pocoo.org/.

[2] shellinabox. https://code.google.com/p/shellinabox/.

[3] US Cyber Challenge: Cyber Quests. http://uscc.cyberquests.org/.

[4] Randal Bryant and David O'Hallaron. *Computer Systems: A Programmer's Perspective, 2nd Edition.* Prentice Hall, 2011.

[5] CTFtime. Team rating. http://ctftime.org/stats/, May 2013.

[6] Entertainment Technology Center. http://www.etc.cmu.edu/.

[7] Polytechnic Institute of New York University. http://www.poly.edu/csaw2012/highschool-cyberforensics.

[8] Team Osiris. http://www.etc.cmu.edu/projects/osiris/.

[9] The College Board. Computer science a course description. http://apcentral.collegeboard.com/apc/public/repository/ap-computer-science-course-description.pdf, 2010.

[10] The Plaid Parliament of Pwning. http://ppp.cylab.cmu.edu/.

[11] Allen Tucker, Fadi Deek, Jill Jones, Dennis McCowan, Chris Stephenson, and Anita Verno. A model curriculum for k–12 computer science. *Final Report of the ACM K-12 Task Force Curriculum Committee, CSTA*, 2003.

[12] Gregory B. White, Dwayne Williams, and Keith Harrison. The CyberPatriot National High School Cyber Defense Competition. *IEEE Security & Privacy*, 8:59–61, 2010.

Figure 7: The number of teams that successfully solved a challenge out of the teams that attempted. The challenges are sorted by decreasing point-value.