Using CTFs for an Undergraduate Cyber Education

Martin Carlisle, Michael Chiaramonte, and David Caswell
Department of Computer Science
United States Air Force Academy[1]

Abstract
Over the last five years, the United States Air Force Academy (USAFA) has participated in numerous Capture the Flag (CTF) and other cyber competitions. At first, this was simply an extracurricular club activity; however, as we have seen the impact on student motivation and learning, we have greatly increased student and faculty participation. Additionally, we have started to base entire for-credit courses on a CTF framework. In this paper we discuss our rationale for utilizing CTFs as part of our formal curriculum, as well as key lessons learned relating to student engagement and avoiding cribbing.

Introduction

Students at the United States Air Force Academy (USAFA) started competing in Capture the Flag (CTF) events for fun, without any formal organization or faculty involvement. In December 2010, we formally created the USAFA Cyber Competition Team. This team competes in international Capture-The-Flag (CTF) events held at most major cyber conferences, as well as in cyber defense competitions (e.g. the National Collegiate Cyber Defense Competition). Through our experience in fielding a cyber team, we have grown to appreciate students' significant learning from these competitions. Most notable is the increased motivation level of some students. Students would put in many hours trying to solve a CTF challenge, doing research on the web and implementing possible solutions. Their motivation was significantly greater than for their traditional class assignments. The learning also helped them with their regular coursework. Given these observations, over the last few years we have experimented with an expanded version of this approach by taking our cyber-related curriculum and converting it into a CTF-style classroom. In this paper, we discuss the type of curriculum we have folded into a CTF framework and how we have applied it in academic, training, and extra-curricular activities. We then discuss the impact that the CTF-driven curriculum has on our students. Finally, we discuss some of the challenges we faced with this approach and provide mechanisms that other schools can use to implement a CTF style classroom.

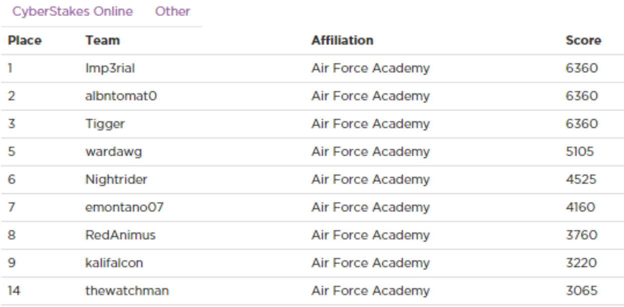
Encouraging Cyber at USAFA

At USAFA we have taken several complementary approaches to delivering Cyber content to the students. As a military service academy, we feel that all of our students should have a basic exposure to cyber concepts primarily from a defensive perspective. We accomplish this through fifteen lessons in our core computing course, which all freshmen are required to take. In this course, we provide several laboratory activities that provide hands-on experiences to help students understand the inherent risks and mitigations of the cyber environment. These activities are focused on a few fundamental topics including social engineering, malware, and the high-level vulnerabilities to national infrastructure. We approach each of the lessons with hands-on labs to understand what the purpose of the attack is, how the attacker would operate, and how the victim should respond.

Following the core course we have a Cyber Training elective. In this elective approximately 17% of the rising sophomores are exposed to cyber topics through a CTF architecture, CyberStakes Online, provided by ForAllSecure and funded by DARPA. This is a student-run program where the rising juniors and seniors provide mentoring and support while the sophomores work through the challenges. The focus of this training program is to provide a more detailed understanding of the different facets of the Cyber domain. In this CTF architecture, students are provided problems that have been categorized as basic tutorial, forensics, binary, reversing, web, or crypto. Under each of these categories the challenges are organized with points that increase consistently with the difficulty of the problems. With this structure students are given the flexibility to move through the categories they most want to learn about. This CTF approach provides us with several incentives that we use to encourage participation. First, students earn points which they can compare against other students as an ongoing competition (Figure 1). Second, we have created a local incentive

[1] Distribution A, Approved for public release, distribution unlimited. The opinions expressed in this article are the authors' own and do not reflect the views of the United States Air Force Academy, the Department of the Air Force, or the United States government.

program whereby students who correctly answer all questions over a threshold while accumulating an overall score over another threshold can earn their US Air Force Academy Cyber Wings. These students are then able to wear these wings on their uniforms as an official symbol of their accomplishment (see Figure 2).



CyberStakes Online Other

Place	Team	Affiliation	Score
1	Imp3rial	Air Force Academy	6360
2	albntomat0	Air Force Academy	6360
3	Tigger	Air Force Academy	6360
5	wardawg	Air Force Academy	5105
6	Nightrider	Air Force Academy	4525
7	emontano07	Air Force Academy	4160
8	RedAnimus	Air Force Academy	3760
9	kalifalcon	Air Force Academy	3220
14	thewatchman	Air Force Academy	3065

Figure 1: Scoreboard of our CTF environment

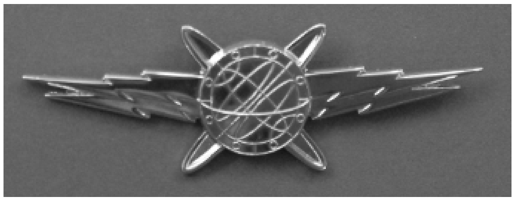


Figure 2: Cadet Basic Cyber Badge

Students who want to continue their cyber education can declare the Computer and Network Security major, join the Cadet Cyber Competition Team, and/or volunteer to lead the summer Cyber Training courses. Computer and Network Security majors will take several in-depth courses on cyber related technical and policy/legal related topics. Those who join the Cyber Competition Team compete internationally against undergraduate, graduate, and professional organizations in capture the flag, vulnerable-box, and network defense challenges. Finally, those who elect to serve as leadership of the Cyber Training program continue to work on our in-house CTF with the goal of enhancing and expanding the learning of subsequent offerings.

Gaming the curriculum

Bringing CTFs into the classroom continues our tradition of innovation to make the classroom more interactive and accessible. In 2004, we created a new flowchart-based programming environment, RAPTOR, to abstract away typical programming syntax and make algorithmic thinking more accessible to non-majors (Carlisle et. al 2004). USAFA computer science faculty have also developed videos (Bower, 2010, Carlisle, et al. 2010) to invert the classroom, allowing more time in class to explore and answer questions, moving more traditional lecture outside the classroom. More recently, while at USAFA, Adrian de Freitas brought gaming into the lecture hall through an interactive quiz experience, Classroom Live (de Freitas et al 2013). In Classroom Live, students are able to upgrade and progress their avatars through correctly answering questions.

With our Cyber curriculum, we have expanded on the inverted classroom approach to provide activities for students that range from large-scale Jeopardy style activities to multi-day exercise style events with external partners. We use the large scale exercises as culminating activities where students are matched against external partners for direct head-to-head competition. In the cyber curriculum these competitions are constructed to offer our students an ability to act as both cyber defenders and cyber attackers. In a defensive event, our students act as a blue team who are defending their electronic resources (network, data, etc.) from a competing organization, acting as red-team, who is actively engaging in some type of attacks to steal/break the resource. In the offensive exercise the roles are reversed. For either event we typically pair an experienced student with the team to coach them on what they should be looking for and what options they can take to respond. These events provide students a strong sense of realism and purpose for what they have learned leading into the events but they are typically very difficult to set up and are only useful in reinforcing concepts that they have mastered in previous, less all-inclusive, activities.

To teach the individual concepts of the cyber curriculum we have adopted CyberStakes Online, a DARPA-funded CTF architecture created by the authors of PicoCTF (Chapman et al 2014). The CTF structure allows students to work through the learning objectives at their own pace. Through its scoring system, they are each able to compete against themselves and also can see how they rank amongst their peers. This structure has enabled us to provide curriculum well beyond what we were previously able to accomplish in a more traditional lecture or even inverted classroom. Since students are able to progress at their own pace, and they have the sense of competition, we have found that the challenges themselves have provided sufficient motivation for most of the students to progress through the material. Hints provided with each of the challenges help students figure out what to research on the web to find a solution.

We also include team-based activities. These team activities span three genres: defensive exercises, offensive exercises, and individual-based cumulative scoring exercises. The last of those is essentially using the CyberStakes framework where groups of individuals are motivated to help each other learn by pitting small teams against each other and comparing the cumulative score of each team. This type of team exercise is easy to facilitate compared to defensive and offensive exercises where each team member has specific roles and must therefore operate together to achieve an objective.

Within the context of the curriculum, USAFA participates in one defense-only competitive exercise, the NSA's interservice Cyber Defense Exercise (CDX). (The USAFA Competition Team also participates in the National Collegiate Cyber Defense Competition). The CDX strives to place students in the role of network builders and operators fending off malicious attacks from external aggressors and naive or malicious users. This exercise is by far the most complex competition we do each year. Large amounts of time are spent by both the NSA and the student teams on developing and testing scoring systems, establishing and interpreting rules for red and blue team activities, building custom networks, and finding and training "white" cell staff to mediate the exercise. The plus side of this exercise is that it encompasses a wide array of student engagement from building, analyzing and assessing through defending a network. PPP (Plaid 2014) notes several downsides to defense-only exercises. The one that resonates with us the most is the lack of feedback. Students know that their systems have been attacked, but get very little feedback on how they could improve their performance. Additionally, we've discovered that defense-only exercises can be very demotivational, as students feel like they've been bullied by the red team and that they aren't capable.

Our experience is that red-blue exercises are a more engaging, less time-intensive means of teaching and learning team-based cyber offense, defense, and the interplay between the two. In these exercises we place teams on like infrastructures that they have not set up themselves and ask them to not only secure their infrastructure but to exploit the infrastructures of other teams. Points are awarded for thwarting attacks and successfully attacking opponents. There are many advantages of these types of exercises that lead us to favor this format to team activities:

1. *Realistic system security analysis and blue teaming.* In these red-blue exercises students are placed on top of a network architecture that they did not develop. This realistically represents most situations where a cyber security specialist is hired to help secure, operate or test an existing network. These exercises force students to make real time decisions on the state of their systems as they exist in a contested environment and implement any security measures they think are needed.

2. *Red teaming.* In red-blue exercises students have a chance to aggress against a dynamic adversary that is actively attempting to prevent intrusions. In this situation students need to define their objectives and weaponeer a means to achieve them. Objectives can include a number of things from disrupting a service to exfiltrating data.

3. *Cyber weapon reuse.* Unique to red-blue exercises is exposure to the concept of weapon reuse. In these exercises red teams can harvest exploits launched by others for use either back at the originator or against other teams. The level of weapon reuse is something that makes cyber warfare unique and is a valuable lesson when considering the higher-order effects of firing a cyber bullet. Although we have not used this as part of a class, one competition that really highlights this effect is the UCSB International Capture the Flag (Vigna et al 2014).

4. *The interplay between offense and defense.* An immensely beneficial experience gained from red-blue exercises is the interplay between offensive operations and defensive operations. During these exercises blue teams will aid red teams in two ways. First, they will identify cyber attacks used against their network and provide details to the red team to reuse the attack against others. Second they will identify and close vulnerabilities in their network all the while helping the red team build weapons that exploit these vulnerabilities so they can use these new weapons against our adversaries. Likewise the red teams aid the blue teams by observing attacks by other on the wire and by identifying vulnerabilities in adversarial networks. Details about these vulnerabilities and observed attacked are used by blue teams to further harden their defenses.

Achieving the high score!

Since its introduction, cyber gaming has had impressive effects on our curriculum, and student outcomes. From our basic cyber training course, our upper level cyber security class and through our cyber competition team cyber gaming is a resounding success. The primary gains from cyber gaming include improved student collaboration, increased motivation, increased feedback, and a willingness to engage in self-directed and lifelong learning.

While working through tough challenges and team based activities students learn to collaborate and teach each other. This move toward collaboration shows in other courses where our cyber focused students are more willing to engage their peers to help them learn and ask for help. This willingness to engage manifests in improved performance, better class interactions and appreciative students. In our Basic Cyber Operations course the most common positive student feedback is the courses' self-paced nature and the way it fosters teamwork and critical thinking.

That feedback is reflected in the courses' successes. In our most recent offering 96% of the students attained their Basic Cyber Operations Wings for high achievement. This achievement is even more impressive when you consider two additional facts: First almost 20% of the students from each class year matriculate through our training course; and second most of them did not elect to be in the course but were scheduled to take it as part of a mandatory military training regimen. That means a large number of less interested, less technical students successfully matriculated through a very technical cyber security course. In fact, the majority are not majoring in computing disciplines but still perform and enjoy the experience.

As students become accustomed to competitive cyber challenges the drive to continually solve harder and more puzzling problems grows. In our programing courses, our cyber students now engage in online programming and hacking challenges once they've completed the day's assignments. This effect is largest in our Python course where students began holding mini-competitions amongst themselves using online Python challenges.

Another result of cyber gamification is an increase in deeper student feedback and questions. It is our belief that because our cyber students engage in large amounts of self-directed activities they have naturally begun to reason about computing and cyber topics in a more mature and sound manner. This allows them to pierce the surface of topics and ponder questions that get to deeper understanding. This is supported by student feedback lauding our cyber courses as "great critical thinking courses," and "highly interesting courses where they learn a lot."

Finally, a genuinely pleasing observation we've made is that by the time our cyber students reach their junior and senior years they have developed a true desire to keep learning and experimenting. Relatively large numbers of our cyber students embark on projects because they are interested in trying to create solutions to hard problems. Our students frequently undertake part time projects outside of class to simply explore. In doing so they have created custom intrusion detection systems, proxy servers, domain name servers, penetration testing tools, and unique cryptographic tools.

The effects of cyber gaming are truly changing the classroom environment from one where the students rely on the instructor to one where the instructor simply facilitates and the students rely on each other and their own growing talents. This change produces observable improvements in student comprehension and student confidence. The results speak directly to Conrad Hughes' observation that "we should not forget that students still look up to erudition, to academic knowledge that they can emulate rather than looking to themselves as the foundation of knowledge or their peers who will work out problems in a group as the teacher moves about them facilitating, suppressing his/her presence and downplaying his/her convictions, knowledge and passion" (Hughes 2012).

Overcoming obstacles in CTF-driven curriculum

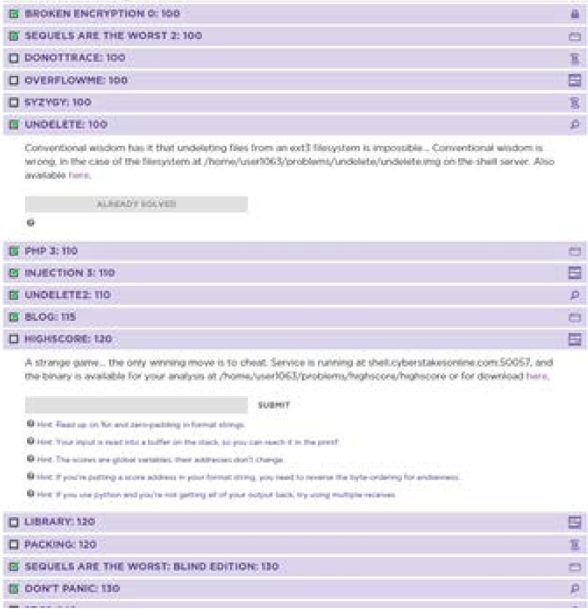
While the inverted nature of a CTF-style curriculum excels at motivating and teaching students to take responsibility and learn on their own, it is not a silver bullet. Developing, administering and controlling a CTF environment is fraught with challenges and faculty must be prepared to overcome or adapt. The biggest challenges to faculty are required overhead, controlling for academic integrity, extensibility, and appropriate depth.

The development of any competitive cyber curriculum, be it offensive or defensive in nature requires careful design to tease out meaningful learning objectives. This takes time and effort on the part of the instructor. This time commitment is compounded by the changing nature of the cyber environment and the constant need to refresh course work to modern technology. To minimize this overhead we deployed an externally-developed framework for hosting CTF challenges. This framework is key to the success of our individual-effort based cyber coursework. Specifically, it facilitates students by providing easy access to problems, hints, scoring and competition, and academic integrity.

One key feature of the CyberStakes framework we are using is that it automatically generating unique solutions to each problem for each student. This means that faculty members do not need to worry about students copying each other's answers. In a former framework we did discover that students would google write-ups of the questions and then simply submit that flag without actually solving the problem. Since each student has a unique key, they must solve the problem themselves. This allows students to work together to figure out a solution without simply copying the answer. Overall this framework allows an instructor to get more mileage from each problem and addresses key academic integrity concerns.

Another key aspect of the framework is its extensibility. Since the cyber domain continues to evolve, so too must our system be able to incorporate new problems. A significant feature of the CyberStakes framework is that it is highly adaptable. Problems can be added directly using a simple web form. This allows us to incorporate problems that we develop in-house as well as interesting problems that we find through the myriad of external CTF competitions our Cyber Competition Team competes in year round.

Another important problem is the level of difficulty of challenges. Sean Slade of the Association for Supervision and Curriculum Development states "An unsuccessful challenge is one that puts achievement just out of reach. A successful challenge asks the student to reach, push, and stretch their capacity." (Slade 2014). The extensibility afforded by the CTF helps us in adapting the paths of related problems so that we can provide students a progression of difficulty to help them learn the concepts rather than allowing them to get stuck by problems that are overly complex for their knowledge level. Furthermore, this gradation of problem complexity coupled with included web-based hints and guidance keep students engaged and limits the numbers who will grow overly frustrated and quit. Figure 3 shows the framework. Icons on the right show the categories of problems, and expandable hints help students know what to research to solve the problem.



☑ BROKEN ENCRYPTION 0: 100

☑ SEQUELS ARE THE WORST 2: 100

☐ DONOTTRACE: 100

☐ OVERFLOWME: 100

☐ SYZYGY: 100

☑ UNDELETE: 100

Conventional wisdom has it that undeleting files from an ext3 filesystem is impossible... Conventional wisdom is wrong, in the case of the filesystem at /home/user1063/problems/undelete/undelete.img on the shell server. Also available here.

ALREADY SOLVED

☑ PHP 3: 110

☑ INJECTION 3: 110

☑ UNDELETE2: 110

☑ BLOG: 115

☐ HIGHSCORE: 120

A strange game... the only winning move is to cheat. Service is running at shell.cyberstakesonline.com:50057, and the binary is available for your analysis at /home/user1063/problems/highscore/highscore or for download here.

SUBMIT

- Hint: Read up on %n and zero-padding in format strings.
- Hint: Your input is read into a buffer on the stack, so you can reach it in the printf
- Hint: The scores are global variables, their addresses don't change.
- Hint: If you're putting a score address in your format string, you need to reverse the byte-ordering for endianness.
- Hint: If you use python and you're not getting all of your output back, try using multiple receives.

☐ LIBRARY: 120

☐ PACKING: 120

☑ SEQUELS ARE THE WORST: BLIND EDITION: 130

☑ DON'T PANIC: 130

Figure 3: CyberStakes challenge web interface

All of our individual and team based activities are performed in our Cyber Training Range. This range is an isolated network which protects students from mistakenly acting on government or public systems without authorization. Furthermore this range hosts template virtual systems for a wide array of network appliances and services. This virtual repository facilitates quicker creation of realistic networks for offensive and defensive team exercises. To further speed the creation of these exercise network scenarios we are planning on deploying network traffic emulators for defensive forensic exercises and graphical drag and drop network ranges that greatly reduce the complexity of deploying virtual machines and will allow us to rapidly provision a wholly new network in minutes rather than hours or days.

Finally, introducing gaming to your curricula is always met with a positive student reception. We have found that students who are used to more traditional teaching styles where they are expecting to and believe they are supposed to learn everything they need from the instructor often get frustrated. To combat this we recommend introducing game based or inverted classrooms early in a student's colligate career to establish learning expectations. When we compared senior level courses that were offered while we transitioned to more inverted classrooms to sophomore courses offered at the same time the difference was stark. During this time our senior level cyber security courses were received with significantly more frustration and student resistance. In contrast, our sophomore programming and cyber training courses received feedback where less than 5% of the students rated the courses unfavorably.

Planning the sequel

From our perspective, we see the use of the CTF framework as providing several benefits to our students. Not only has it provided a fun and engaging format for teaching cyber concepts, but the very nature of the self-paced content has enabled our students to be more capable and motivated to tackle hard problems without direction. Students who have used the CTF architecture ask less but far more informed questions; they have shown greater personal responsibility for their own education and are willing to research their own solutions to problems rather than relying on the instructor or more experienced students. This engagement in the material has helped our students become more proficient in the technical material while improving their enjoyment of the academic experience.

While we feel that our current CTF framework has greatly helped the academic experience of our cyber content we continue to work to find new ways to improve our offerings. At the basic level, we continue to work through CTF problems from a variety of competitions and try to include those challenges we feel have a strong educational ability into our CTF structure. Further, we continue to add supportive hints to help lead students into finding answers to the CTF challenges without giving away the solutions. In Spring 2015, we are planning to run all of the assignments for our new reverse engineering course in the CTF environment.

To further aid students in their self-paced learning we have also begun putting together a Cyber skills Wikipedia style site to catalog the suite of knowledge embedded in the CTF questions. As this Wikipedia site has been student created, we have found it to be a strongly synergistic tool where students are able to continually craft its information to best communicate the various skills evaluated by the CTF. Feedback from students is that they have a lot of pride in their contribution to the Wiki and in their ability to write coherent educational articles without giving away the specifics of any of the challenges.

Conclusions

While have not conducted a rigorous scientific comparison of our CTF style against standard curricula, our observation and student feedback indicates that the CTF approach is highly effective at encouraging student learning of cyber security. Particularly, we have seen obvious increases in student motivation, a willingness for more self-directed learning, and the desire to push their own boundaries for knowledge. Based on these advantages we are looking into how to further move our curriculum into a CTF direction.

References

Carlisle, Martin, T. Wilson, J. Humphries and S. Hadfield. “RAPTOR: Introducing Programming to Non-Majors with Flowcharts”, *Journal of Computing Sciences in Colleges*, 19(4):52-60, April 2004.

de Freitas, Adrian and M. de Freitas. “Classroom Live: a software-assisted gamification tool”, *Computer Science Education*. 23(2):186-206, June 2013.

Martin C. Carlisle. “Using You Tube to enhance student class preparation in an introductory Java course”, *Proceedings of the 41st ACM technical symposium on Computer science education* (SIGCSE '10). ACM, New York, NY, USA, 470-474, 2010.

Slade, Sean. “Improving Schools: Hierarchy of Motivation.” Sept 2014. http://inservice.ascd.org/improving-schools-the-hierarchy-of-motivation/

Hughes, Conrad. “Passion for Beauty: A Model for Learning”, *Creative Education*. 3(3): 334-340, June 2012.

Peter Chapman, Jonathan Burket, and David Brumley. “picoCTF: A Game-Based Computer Security Competition for High School Students “, *2014 USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE '14)*, San Diego, CA. 18 August 2014.

Plaid Parliament of Pwnage. “Why CTF”, Online http://ppp.cylab.cmu.edu/wordpress/?p=1182. April 2014. Accessed 1 May 2015.

Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupé, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, Yan Shoshitaishvili. Ten Years of iCTF: The Good, The Bad, and The Ugly. *2014 USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE '14)*, San Diego, CA. 18 August 2014.