Collegiate Cyber Game Design Criteria and Participation

Bei-Tseng Chu
Gail-Joon Ahn
Steven Blanchard
James Deese
Richard Kelly
Department of Software and Information Systems
University of North Carolina at Charlotte
Charlotte, NC 28223
billchu@uncc.edu

Huiming Yu
Ashika Young
Department of Computer Science
North Carolina A&T State University
1601 East Market St.
Greensboro, NC 27441
cshmyu@ncat.edu

Abstract

Cyber games are gaining popularity in universities as a tool to further information security education. Recently prominent national and international collegiate cyber games were conducted and efforts are underway to institutionalize these games. This paper presents a set of design options for cyber games based on the author's experiences in organizing and participating in cyber games over the past three years. We will also discuss important considerations to incorporate cyber games into computing curricula.

1. Introduction

A cyber game is a competitive online exercise in which participants are engaged in activities either to prevent computer systems from being penetrated, or to penetrate computer systems. Denial of service activities are generally prohibited in cyber games. For the past three years, two of the authors (Chu and Ahn) have been engaged in designing cyber games as well as coaching students for national and international cyber games competitions. Two of our student teams placed first in the U. S. South in separate competitions. These competitions were The International Capture the Flag Competition (iCTF) and the National Collegiate Cyber Defense Competition (CCDC). One of the teams won the U.S. National Collegiate Cyber Defense Competition championship sponsored by the U.S. Homeland Security Department in 2006.

The primary purpose of this paper is to share our experiences in designing a successful cyber game. We will also share our experiences of how to prepare students for cyber games. Our experience has shown that cyber games are valuable education tools for the following reasons.

- Cyber games actively engage students in a highly interactive environment that keeps the students strongly motivated. Our department has enjoyed significant enrollment growth that can be attributed in part to a rigorous curriculum with a strong hands-on component.

- Students must master a comprehensive set of network and system administration skills and be able to apply them quickly to a variety of problems. Such skills are highly relevant to the current practice of the IT industry.

- With proper design, cyber games can promote creative problem solving.

- Cyber games require good team work coordination, skills that will help the students later in their IT careers.

Most of the reported experiences with cyber games, e.g. [1, 2, 3, 6], have been with class projects. Collegiate cyber games, while sharing many elements with class projects, have different characteristics including larger scale and more rigors in rules.

The first cyber games were held within the U.S. military and intelligence community where "red" teams attempted to penetrate the security posture of "blue" teams. The first civilian cyber game, Capture the Flag Contest, was held at DEFCON, the most prominent "computer hacker" convention, in 1996. U.S. military academies were the first academic institutions to institutionalize collegiate cyber games. An increasing number of universities have used cyber games as part of their curriculum. Cyber games can be designed to emphasize different skills sets and achieve different objectives. This paper outlines a set of design criteria that are important for designing cyber games.

6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)
0-7695-2841-4/07 $25.00 © 2007 IEEE

IEEE COMPUTER SOCIETY

2. Defensive vs. Offensive Game

In a defensive game, student participants do not engage in any attacking activities. Penetration attacks are performed by a team of judges, often referred to as the red team. In an offensive game, student participants engage in activities that attempt to penetrate computer systems. A red team is optional and often not used in offensive games. Participants often engage in defensive activities as well in offensive games.

Many proponents of defensive games are uncomfortable with ethical risks associated with teaching cyber attacking techniques in a university curriculum. Proponents of offensive games believe that a good understanding of attacking methods is essential for designing effective defenses and the risks associated with teaching attack techniques can be mitigated through appropriate ethics education.

3. Competition Content

A well designed cyber game must start with a set of clear objectives. The competition content must then be designed to achieve these objectives. In a cyber game, participants are presented with a set of scenarios, either all at the very beginning or throughout the competition. Scenarios can be classified as routine tasks, detective work, and problem solving.

Routine tasks may include patching systems with known vulnerabilities as well as routine administrative tasks such as setting up a directory and adding users. Routine tasks can be used to measure the mastery and proficiency of network and system administrative knowledge. Students are typically given a very large number of tasks that need to be accomplished within a short time window.

Detective work requires students to discover vulnerabilities/ malware that are specially designed for the competition. For example, a spying program may be set up to sniff passwords or a modified version of FTP with a command injection vulnerability may be provided.

In a defensive cyber game, students must identify such vulnerabilities in their system and take appropriate corrective actions (e.g. remove the spying program, modifying and recompiling the FTP program). In an offensive cyber game, students must not only take the appropriate defensive actions on their team's systems but also use such vulnerabilities to attack other teams. For example, a command injection vulnerability may be used to plant spyware which can be used to obtain the passwords necessary to break into other services.

Such tasks can be challenging and are aimed to test students' ability to discover new threats. Correction of the problems, once discovered, are usually relatively straight forward.

Both types of tasks discussed above do not require analyzing complex problems and design of solutions. An example that demands more problem solving skill might be to ask participants to set up a new web service utilizing other available services. Students must design and implement their work in a secure and timely manner. This type of scenario is rare in recent cyber game competitions.

4. Scale and Environmental Complexity

Small scale cyber games are often used as a capstone exercise for a course. Large scale cyber games, on the other hand, can be organized in a distributed way spanning multiple time zones.

Complexity of the cyber game environment is closely related to the scale of the cyber game. Fairness of the competition is paramount. All participants should have access to similar types of hardware and software.

One approach is to use a virtual environment, such as VMware. A standard set of images can be distributed and all participants are required to use these images. Cyber games using the virtual machine approach can easily scale to many participants in a highly distributed way. However, limitations of the virtual environment technology may make it difficult to configure robust networks consisting of different operating systems, network and security devices. Not all services are well supported in a virtual environment. Hardware demand for the machines involved may be quite high for reasonable performance. Therefore this approach tends to limit the complexity of the competition environment.

Another approach is to use a heterogeneous set of software and hardware devices. For example, each team may have a set of Windows, Linux, and Solaris machines together with routers and firewalls. An important advantage of this approach is that it allows the organizers to design more "real world like" scenarios. However, it is difficult to ensure that all teams would have the same initial configuration unless the organizers have physical control of all the hardware. Such a requirement can limit the number of people who can participate.

5. Rules and Scoring

A consideration of paramount importance in designing rules for cyber games is to ensure that participants with greater financial resources do not have an undue advantage. This can be addressed by considering both software and hardware used in the competition.

All participants should have access to the same software at the start of the competition. Freeware may be downloaded during the competition, but tools requiring

IEEE COMPUTER SOCIETY

payment should not be allowed. To ensure compliance, all network traffic from participants can be monitored. Participants should not be allowed to seek outside help during the competition. This includes the obvious such as emailing the coach, but also should preclude a participant from preparing resources specially designed for the competition. For example, someone with numerous resources may prepackage material especially for the competition and make them available via a website specifically created for the competition.

In small scale cyber games, it is feasible to ensure that all participants have access to very similar types of hardware. It is much more difficult to do so in large scale cyber games. In such cases, the competition content can be designed in such a way that participants with reasonable hardware will do almost as well as someone with more powerful hardware.

Task completion, availability of services, and penetration assessment are three categories to score cyber game participants. Game designers can choose to assign different weights depending on their particular goals. Task completion measures whether participants have completed the required tasks on time. Availability of services measures participant's ability to keep required services (e.g. web server or mail server) running. Penetration assessment measures a participant's ability to prevent attackers from accessing the computer system.

In an offensive game, penetration assessment also measures a participant's ability to design new ways to gain access to others computer systems. Extra points may be rewarded to participants who come up with original exploits or a penetration technique that is being used successfully for the first time.

To the extent possible, scoring should be automated. Scripts can be created to check for the availability of services, whether required tasks have been completed, and scan for vulnerabilities.

Monitoring network traffic to deter cheating is another import part of the cyber game infrastructure. Potential types of activities for monitoring include: downloading of software that is prohibited by rules, seeking outside advice (e.g. through email, chat, or voice over IP), attempts to tamper with the scoring mechanism, encrypted traffic to evade monitoring, and denial of service attacks. One possible approach may be to set up a network for the entire competition and make sure all Internet bound traffic goes through a centralized computer controlled by the organizer. Programs may be set up to automatically detect activities not allowed in the competition.

6. Case Studies

We use two successful cyber games as case studies to illustrate how the design criteria described here can be applied. The International Capture the Flag Competition started as a local class room exercise at the University of California at Santa Barbra [5]. It has many similar features as the DEFCON capture the flag competition. In 2005, 21 teams from universities in North America, Europe, South America, and Australia participated in iCTF05 competition. The National Collegiate Cyber Defense Competition was organized by the University of Texas at San Antonio with major sponsorship from the U.S. Department of Homeland Security. Four regional cyber game competitions were held across the U.S. (Southeast, Mid Atlantic, Southwest and Midwest). Regional champions and a team jointly fielded by five U.S. military academies participated in the National Collegiate Cyber Defense Competition.

6.1 iCTF 2005

The overall lay out of the 2005 iCTF competition network is illustrated in Figure 1. Each team had to have two machines at their site: a team box, and an image box. The team box was connected to the main box at the site of the competition organizer via a GRE tunnel. The image box had to run VMware and ran two images supplied by the organizer. The test image is used for trouble shooting and the vulnerable image is the image used in the competition. No further rules restricted how local networks could be set up by each team.

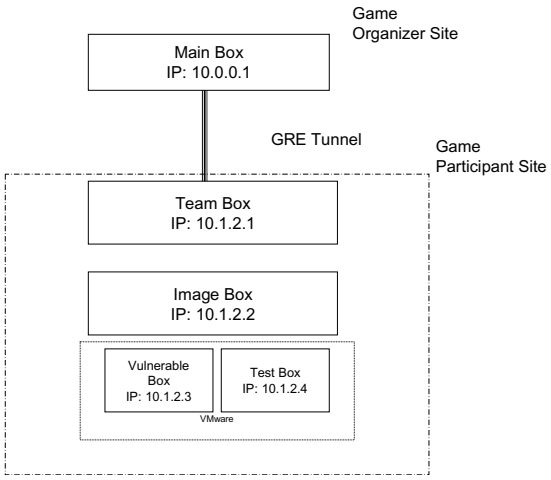

Figure 1. iCTF05 network layout

An encrypted VMware image based on Debian Linux was distributed shortly before the competition. The encryption key was emailed to teams to begin the competition. The image contained about 10 IP-based services, all designed for the competition. All except for one service were web pages written in PHP, Python, and/or JSP. An FTP service was also included. All

IEEE COMPUTER SOCIETY

services had multiple vulnerabilities. The web pages contained commonly known types of vulnerabilities such as command injection and SQL injection. The FTP service contained a number of vulnerabilities including buffer overflow and command injection [4].

The standard image contained a number of digital flags, implemented as hash values. The hash algorithm used was not announced. Flags always began with "MTNzEw", and ended with "==" (in base 64 encoding, it includes digits 31337, or "ELITE" in hacker speak). The scoring machine periodically logged into each team's image and refreshed the flags. One of the goals of the competition was for each team to find these flags in their opponent's machines. To receive credit, each team had to submit the found flags to the scoring machine via a web page. The scoring machine validated whether the flag was indeed a flag and it was the most recently planted flag.

To obtain these flags, each team had to exploit the vulnerabilities contained in the image. Teams were also encouraged to submit their exploits to the organizers. Points were awarded to teams who first discovered a known vulnerability and ways to successfully exploit it.

To defend against attacks, each team would apply appropriate patches to their system as well as modifying the vulnerable services provided to remove found vulnerabilities. However, team had to do that while maintaining the availability of the services as much as possible. Points would be deducted from a team for any unavailable service.

Any deliberate attempt to increase the volume of network traffic was not allowed. Interfering with scoring traffic was not allowed either. The source IP for the scoring mechanism was not predictable, thus one could not selectively block incoming traffic to prevent attacks. Students participating in the 2005 iCTF had to be full time students, with a maximum team size of 15 students.

6.2 CCDC 2006

In contrast to the virtual competition environment of iCTF 2005, the 2006 CCDC was hosted within one building. Besides teams of student participants, the competition had the following teams:

- Gold Team – Controlled the flow and timing of the events and scenarios (referred to as injections), and to serve as mediators for disputes and challenges.
- White Team – Judges and evaluators.
- Red Team – Penetration assessment.

All computers used in the competition were located on the same network. All Internet bound traffic went through the central router as illustrated in Figure 2.

Each team was assigned a set of computers and devices. Figure 3 illustrates the set up of the network for each team.

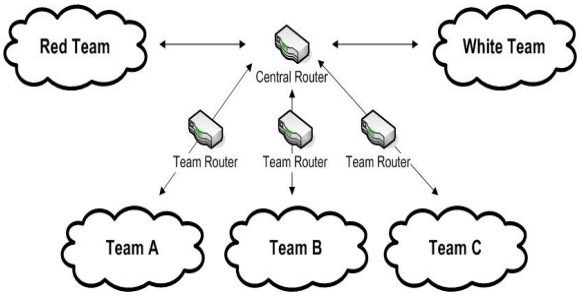

Figure 2. CCDC06 over all network architecture[8]

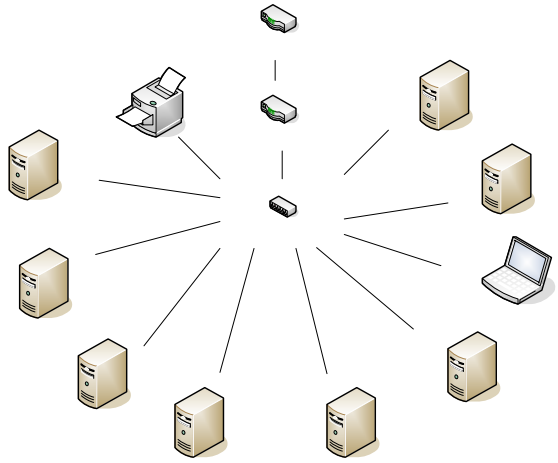

Figure 3. Network layout for each team [8]

The competition content was based on a set of real-world business scenarios. Some of the examples include:

- Employees have been using AIM protocol too much at work and the company wishes to block that service from being used. Solution: Set up a firewall rule to block the port used by the instant messaging protocol.
- Organize users into groups in Active Directory. With hundreds of users, this task is time consuming.
- A new network device was just announced by a vendor, install and configure that device. Students had to complete this task with little help as good technical support was not available.

Documentation and reporting were an important part of the competition. The business injects were modelled after real world business situations and requirements were given in the form of memos. Upon completion of an inject, each team had to submit reports along with required

IEEE COMPUTER SOCIETY

documentation. During the course of a two-day competition, a team may generate 150 pages of documents.

What makes this competition challenging is that teams must complete such task with very tight deadlines, working with machines with many unpatched vulnerabilities while under attacks from the Red Team.

Scoring was based on task completion, service availability, and penetration assessment by the Red Team. Services were probed periodically by automated scripts. Task completion was judged based on submitted documents as well as testing the services implemented. Once completed, the team was responsible for keeping the service running. An established service may be down for a number of reasons. For example completing a subsequent injection might interfere with a running service or a vulnerable service might crash when attacked by the Red Team.

Student teams were limited to eight full time students. Teams were not allowed to bring computers nor any digital media, although teams were allowed to bring books and other printed documents. Teams were allowed to download free software (either freeware or trial versions of commercial software). Other types of software cannot be used without authorization. All network traffic had to go through a central router (see Figure 2) and was subjected to monitoring.

6.3 Case Comparison

Table 1 compares these two competitions based on the design criteria described above.

Success of collegiate cyber games is ultimately judged by how they improve the quality of academic programs at the participating universities. Material used for the competition and experiences with the competitions may provide valuable instructional material and course feed back to participating universities. These benefits argue for wide participation in cyber games by interested schools.

7. Building a Successful Team

Besides having a high quality academic program, many other factors are essential to building a successful team for collegiate cyber games including team work, ethics, and diversity.

Teamwork is a key to any team's success in cyber games. A common problem is that team members are thrown together at the last minute. Lack of trust between team members can severely hamper the performance of the team. Key challenges include

- Lack of communication. Some of the students may not have good communication skills. Under time pressure, they may charge ahead with a certain task without communicating clearly with team members what they are doing. As a result team members may interfere with each others work.

Table 1. Summary of 2005 iCTF and 2006 CCDC design choices

	iCTF05	CCDC06
Defense vs. Offense	Offense (without red team)	Defense
Content	Focused on detective work	Emphasizes task completion with some considerations given to detective work and problem solving
Scale	International, fully distributed	Competitions conducted in a single location with the organizers controlling all the machines
Complexity of Environment	Consisted of a single Linux image loaded on VMware for each site. All sites are connected via a virtual network	Multiple machines and network devices with a mixture of operating systems
Rules	All competition network traffic had to be on the competition network. Teams were allowed to have external Internet access without monitoring	All traffic had to go through competition network. No external media allowed. Only freeware or approved commercial software was allowed.
Scoring	Based on service availability, flags captured, and original exploits. Except for evaluating original exploits, scoring is automated	Equally based on task completion, service availability, and red team assessments. A combination of manual and automated scoring.

IEEE COMPUTER SOCIETY

- Conflict resolution. Team members disagree on the best way to handle a particular situation. In one competition, fights broke out in one of the teams amidst heated disagreements.

Building trust among team member is key to good team work. It is important for members of the team to recognize and respect each others strengths. With better mutual understandings natural leaders may emerge to take responsibilities and coordinate with each other during competition. In preparing for collegiate cyber games, our teams spent a lot of time getting to know each other. We assigned team members to different groups of specializations, e.g. reviewing code to identify vulnerabilities, network set up, hardening Windows, and hardening Linux. Some students belonged to multiple groups others belonged to a single group. Besides serving as reviews of specifics skills, an important objective was for the team members to understand expertise of their teammates. The importance of such team building exercises is clearly far beyond winning the cyber game. These are the very same skills students need to succeed in their careers.

Students should develop a strong sense of ethics. Good approaches include case analysis, and having students develop their own code of ethics with appropriate guidance from faculty advisor.

Diversity of the IT work force is an important challenge for the computing community. Our experiences suggest that cyber games are an effective to attract minority students to the field of information security.

8. Conclusion and Future Work

Collegiate cyber games are still at a very early stage of development. Early evidence suggests that it is an excellent way to (a) develop student's hands on knowledge and problem solving skills that are highly relevant to the IT industry; (b) motivate students to purse IT as their career of choice; (c) emphasize team work and ethics; (d) attract minority students to IT.

However for cyber games to mature and become well established, such as achieving the status of the ACM programming contest, much more work is needed. We highlight two important areas of focus. First, while maintaining the hands on flavor of the games, we should promote student's creative design and problem solving skills. Second, in order to achieve the full benefit of the games, the games must be scalable so that more teams can participate.

9. Acknowledgements

This work is supported in part by grants from NSF: DUE 0516085, 0416042, and 0210076. We also wish to acknowledge the contribution of student team members: A. Faust, D. Cassidy, N. Conrad, D. Myers, D. Stone, S. Glumich, K. Stone, D. Underwood, A. Falivene, Z. Wadler, M. Dawson, K. Pearson, and U. Berry.

10. References

[1] P. Mateti, "A laboratory-based course on internet security", In Proceedings of the Thirty-Fourth SIGCSE Technical Symposium on Computer Science Education pages 252-256, ACM Press, 2003.

[2] M. Micco and H. Rossman, "Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates", In Proceedings of the Thirty-Third SIGCSE Technical Symposium on Computer Science Education pages 23-27, ACM Press, 2002.

[3] M. O'Leary. "A Laboratory Based Capstone Course in Computer Security for Undergraduates", In Proceedings of the Thirty-Seventh SIGCSE Technical Symposium on Computer Science Education pages 2-6, ACM Press, 2006.

[4] Open Web Application Security Project. http://www.owasp.org

[5] G. Vigna, "Teaching Hands-On Network Security: Testbeds and Live Exercises", Journal of Information Warfare 3(2): 8-25, 2003.

[6] J. Walden, "A Real-Time Information Warfare Exercise on a Virtual Network", In Proceedings of the Thirty-Sixth SIGCSE Technical Symposium on Computer Science Education pages 86-90, ACM Press, 2005.

[7] T. Wulf, "Implementing a minimal lab for an undergraduate network security course", J. Comput. Small Coll. 19(1): 94-98, 2003.

[8] http://utsa.edu/cias/CCDC/faq.htm

IEEE COMPUTER SOCIETY