Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

The National Collegiate Cyber Defense Competition: What are the next steps?

Gregory B. White, PhD, The University of Texas at San Antonio
LtCol Ronald C. Dodge, Ph.D., The United States Military Academy

Abstract – In 2005 the first regional competition was held in what has become known as the Collegiate Cyber Defense Competition. The following year four regional competitions were held along with the first national competition. In 2007 the national competition continued with state competitions being added to the overall plan. The National Collegiate Cyber Defense Competition is well on its way to being established as an annual event with more schools joining the event each year. This paper addresses what the next steps are for the competition if it is to continue to gain recognition among schools and to indeed be established as the single recognized collegiate cyber defense competition.

Index terms – Collegiate competitions, cyber defense exercise.

I. Introduction

The Collegiate Cyber Defense Competition (CCDC) was first held in March 2005 at The University of Texas at San Antonio. It included five schools from across Texas and was the direct result of discussions generated at a 2004 National Science Foundation sponsored workshop held in San Antonio to discuss the possibility of developing a national cyber security competition. The workshop brought together interested participants from government, academia, and industry. The participants agreed that a national competition would be of benefit and should be explored.[1] At the event, three schools from Texas were represented and the representatives from those schools decided to move ahead with the competition idea and form a Texas competition to be held in 2005. This was the genesis of the 2005 CCDC.

At the 2005 Colloquium for Information Systems Security Education (CISSE), the results of the Texas CCDC efforts were presented and an announcement made concerning the intention of conducting a National Collegiate Cyber Defense Competition (NCCDC) in 2006. [2] At the colloquium, a call for schools interested in both participating in the competition as well as those that might be interested in hosting a regional competition was made. The proposal was to conduct a series of regional competitions with the winning school from each of these competitions competing at the national competition held in San Antonio, Texas. Four schools conducted regional competitions. The winning school from each, plus a combined team from the military service academies, met in San Antonio in April, 2006 for the first national championship. The University of North Carolina – Charlotte won this inaugural event and plans were immediately begun on organizing the 2007 national championship competition. [3]

In April 2007 the winning teams from the regional competitions again met for the national championship. *<Since this paper is due before the competition is held, the results of the 2007 competition are unknown. The final version of the paper will include two sentences here to announce the 2007results.>* Plans have already been announced for the 2008 competition with additional schools already announcing their intention to create new regional competitions in their part of the country.

II. Current Status of the NCCDC

The CCDC and NCCDC are not the first cyber security competitions conducted. Several competitions have been held for a number of years including several in academia as well as other, such as the annual competition held at the DEFCON conference.[1] Early on in the discussion on the establishment of the NCCDC the issue of whether the competition would allow the participants to conduct offensive activity was held. While often viewed by some as more exciting, the decision was made to restrict the activity of participants in the NCCDC and its regional competitions to defensive activities – to activities associated with the defense of a network and its computer systems. The reason for this included the belief that defensive activity was what most students would be involved with upon graduation (the number of jobs requiring defensive skills far surpasses the number of jobs that require offensive skills), and the desire to ultimately seek a sponsor for the competition. The developers of the competition did not want it viewed as a forum for "developing the next generation of hackers". Focusing on defense would place the emphasis of the competition where it was felt that industry would want to see it and where it was actually most needed.

ISBN 1-933510-96-7/$15.00 ©2007 CISSE

While the rules have evolved since the first competition held in 2005, the actual format for the competition has changed only slightly. The NCCDC allows for teams of up to eight individuals, all of whom have to be full-time students as defined by their institution. The teams can contain a mix of students from different majors and can have both undergraduate and graduate students participating – though the number of graduate students per team is limited to two. The competition commences with each team being introduced to the network they will be expected to protect and keep operational. Each team is provided a fully operational network configured with a variety of hardware platforms running various pieces of software. Each team's network is identical in both hardware and software configuration. While the organizers guarantee that the network is functional, they do not guarantee that it is secure. The premise used in the competition is that each team has been hired to run and secure a small company's network. They do not have a chance to design the network, they must operate and protect what they are given. The teams are given a short period of time to begin to secure the networks before a red team is let loose on the networks. The red team consists of volunteers from government and industry organizations and simulates the hostile Internet environment that exists. The red team's goal is to penetrate the students' networks. General denial of service activities are not allowed unless they are part of a specific attack designed to gain unauthorized access to a network or system.

The teams are expected to maintain the operational aspect of their networks, to prevent intrusions into their network, and to respond to a variety of business activities that they will be given throughout the competition period. The business activities, referred to as "injects", simulate the type of activity that IT departments face on a daily basis in industry. The teams are scored on their ability to maintain the operational nature of their network, on the successful completion of the business injects, and on their ability to secure the network. A scoring engine begins checking the required services as soon as the competition begins. If a service is available the team receives a point. If the service is unavailable they do not. A timer is maintained for required services and after a certain period of unavailability, additional penalty points are applied. This is designed to represent service level agreements which are a common fixture within industry. The teams' ability to secure their network is gauged by their ability to prevent intrusions into their network. Depending on the level of access obtained by the red team, penalty points are assessed for every intrusion. The competition is designed to strike a balance between these three aspects of the scoring with the team that has the highest score at the end of the three days of competition being declared the winner.

Due to the format of the NCCDC, the number of teams that can participate is limited. The requirement to have identical hardware and software configurations results in a need for a tremendous amount of equipment thus realistically limiting the number of teams. The need to also ensure that red team activity is uniform across the teams also results in a limit to the number of teams that can be adequately tested (while there is some scripting of red team activity, most of the activity is not and when a team member is able to penetrate a network utilizing one tool or method the same needs to quickly be tried on the other teams as well). Both of these restrictions have led to a limit of between ten and twelve teams at a single competition.

This limit obviously places a severe restriction on the number of teams that can participate, and in the actual value of the competition, unless a method is used to select teams for the national competition. The concept of a regional structure was envisioned from the start with ten to twelve regional competitions being planned. This would result in maximum participation at the national level. Even with twelve regional competitions, if each competition used the same format there is still a limit of at most 144 schools that can compete hoping to qualify for the national event (twelve regional competitions each with twelve schools competing).

One of the decisions that was made early in the development of the competition was to open the event to both 2-year as well as 4-year colleges and universities. With this in mind, a limit of 144 schools is too restrictive and will not work to allow all schools that want to compete to do so. For this reason, another tier was also envisioned and was experimented with in 2007. This year, one of the regional competitions held state qualifying competitions to select the teams that would compete at the regional event. This increases the number of schools to over 1700 that have an opportunity to compete for the national championship. While in theory over 1700 schools could compete using such a structure, it is understood that there is not a uniform distribution of schools throughout the country and certain regions will have a larger concentration than others. For these areas, another tier can be added with divisional competitions that could extend the competition to one more level. Another possibility is to allow for a different format for the competition at the lowest tiers so that formats which could accommodate more schools could be used.

From the beginning, the NCCDC was designed to appeal to government and industry. This was done for several reasons including the desire to have it viewed as a beneficial event that could be used for both recruiting of students for jobs and would be attractive for potential sponsors. Being viewed as "hacker training" was not the

goal – the event was designed to be viewed as part of educational and training programs to develop "cyber defenders". The event has begun to attract some sponsors with the Department of Homeland Security (DHS) and Cisco Systems being the two largest. Cisco Systems, the largest corporate sponsor, has provided a tremendous amount of equipment to the competition which has facilitated the development of the network infrastructures used by the teams. DHS has provided funds in both 2006 and 2007 sufficient to bring the winners of the regional competitions to the site of the national event and to pay for their hotel accommodations while at the event. Other sponsors have provided equipment, money, food, or items for the competitors. Sponsorship is one of the priorities for the event planners for the 2008 competition.

III. Relationship with CAEIAE Schools

From the start, one of the issues of interest to DHS and other government organizations is the number of DHS and NSA designated National Centers of Academic Excellence in Information Assurance Education (CAEIAE). Up to this point, the majority of schools competing in the competition have not been CAEIAEs. One reason contributing to this is the fact that a large number of 2-year schools, which are not eligible for the CAEIAE designation, have been participating in the competition. A number of these have strong security programs and their students may transfer to 4-year institutions upon completion of their 2-year programs. Even when not factoring in these schools, CAEIAEs do not dominate the competition.

Examining the competition and its results provides an indication of some of the potential benefits of the NCCDC. The results in this case go beyond who won a specific competition. It refers to the larger impact that the NCCDC has on the security community. Already comments have been received from both faculty and students attesting to the benefits of these events. Students have become more interested in security, not just as a subject to take a course in, but as a possible career path. Academic programs have been changed as a result of faculty members observing the event and how their school's team fared during the competition. The increase in the number of schools competing in the various CCDC competitions has steadily risen since the first event in 2005. All of this has led some to recognize the potential benefits of the event and to actually propose for consideration the adoption by NSA and DHS of rules that would award points to schools who field a team for a competition, and additional points for schools that sponsor a CCDC competition, that can be used in the application for designation or re-designation as a CAEIAE.

IV. Potential of the NCCDC

It may be a bold statement, but the NCCDC has the potential to be as important to the advancement of computer security, especially in terms of student awareness of and interest in computer security, as the CAEIAE program itself. Because of its more all-inclusive nature, the NCCDC has the potential to reach more schools than does the CAEIAE program. The creation of a team takes a lot less involvement and commitment from a university than does inclusion in the CAEIAE program. Teams have been formed at universities with minimal involvement from faculty members. If there is a group of students interested in security and in fielding a team, they simply need a single faculty sponsor to become involved in a NCCDC event. This can result in more interest in security at institutions in which there is a minimal security faculty footprint. Research is an important part of becoming a CAEIAE but it is not required of a team or its sponsor – this again allows for more involvement in non-research oriented schools such as 2-year institutions.

Another factor that can contribute to the potential for the NCCDC becoming as important to security awareness as the CAEIAE program is the fact that it is a competition. Competitions of almost any sort are reported in the media. Winning a competition will result in press for the winning organization and for the event itself. With multiple tiers of security competitions, multiple winners will be crowned at the various levels and multiple stories generated. This, in turn, can raise the level of awareness in the event, the schools participating, and in security itself. With declining enrollments in information systems and computer security over the last few years, any event that may generate interest in IT-related majors may provide an added benefit for educational institutions. Security has been one of the areas that institutions have been using to attract potential students and the NCCDC can significantly help in this regard.

V. Future Plans for the NCCDC

While the NCCDC has come a long way since the original workshop in 2004 and the initial event in 2005, there is much that still needs to be accomplished. Chief among this is the development of a national governing body. Many excellent ideas were discussed by the participants in the 2004 workshop. There are a number of individuals at the workshop who have been involved in competitions for several years, the best know of which is the Cyber Defense Exercise (CDX) conducted for the U.S. military service academies. All of those involved in these other competitions have gained valuable insights into running cyber security competitions and the lessons they have learned should be used and not ignored. In addition, any

competition claiming to crown a national champion needs to have an independent body to oversee the many issues that will arise during a competition. Many of the competitions currently conducted would not stand up to the type of gamesmanship that can be expected should hundreds of teams become involved. Most are currently conducted in environments where "because that's the rule" would be an acceptable response to a dispute about a rule. One can't imagine the same argument being used at a National Collegiate Athletic Association (NCAA) basketball tournament or in professional sports such as the National Football League (NFL) or National Basketball Association (NBA). Such entities have governing bodies that address the many issues, such as changes to rules of the game/sport, that constantly arise. The same sort of entity needs to be developed for the NCCDC to institute early on the structure that will be used to address competition issues as the event develops. It is envisioned that the governing body will be composed of predominantly individuals from 2- and 4-year institutions that have security programs. Initially, individuals who have experience in conducting competitions will be sought to populate the board since an immediate task will be to develop not only the organization's by-laws but the governing rules for the competitions at the various levels.

The rules used in the competition have been under close scrutiny since the inception of the competition. Just like any other competition, the rules have evolved over time as issues have arisen not originally foreseen. Many issues have been settled at least temporarily but need to be examined by the larger governing body in order to gain more universal agreement. Issues such as participant eligibility still are a concern. Current competition rules state that competitors must be full-time students as defined by their institution. While this may be acceptable for traditional 4-year institutions, it limits participation by the 2-year institutions with non-traditional student bodies. The 2-year institutions often have a significant number of part-time students who are working on their degrees while also working in full-time jobs. Does disqualifying these individuals meet the goals and needs of the competition or should they be allowed? If the goal is to keep "ringers" from being able to participate (security professionals who may sign up for a single course just so they could form a team and compete) is the full-time requirement appropriate? An additional rule, somewhat addressing this issue, currently states that individuals should not be employed in the IT industry full-time or part-time for more than 20- hours per week.. Again the intent is to avoid "ringers" but does this disqualify students who may be working for a university's IT office or who are working as lab administrators or assistants? Should Help Desk experience disqualify individuals? Issues such as these are in need of clarification and careful consideration in order to insure that the goals of the competition are met without being overly restrictive in nature. At the same time, the rules need to be clearly delineated so that no misunderstandings occur because the rules are "up for interpretation". Having unclear, unrealistic, or overly restrictive rules can be detrimental to the competition and its broader acceptance by the community.

Another aspect of the competition that will need to be addressed by the governing body and those that are sponsoring the various competitions are the actual regional events. Currently selection of regional competition sites has been ad hoc and has been based on whoever was willing, or willing and first, to volunteer to conduct such a competition in a given portion of the country. Some regional competitions have rotated the event each year so a single school has not conducted the event each year. Others have kept the same location and sponsoring school. Some regions of the country are not currently represented (unless a team is willing to travel hundreds of miles) and regional sites need to be established. Determining where the sites should be located is an issue and is something else the governing body can greatly facilitate. The institutions that have sponsored the regional competitions have up to this point been allowed some leeway in the way they conduct their own competitions. They have been provided copies of the national rules, and teams that they send to the national event will have to abide by the national rules, so staying close to the national rules helped prepare their team for what would be seen at the national event – but it was not required. This has allowed the different organizers to test different ideas for the events which can be presented to the governing body for consideration. Ultimately, it is envisioned that a consolidated set of rules governing all levels of the competition should be constructed. This will ensure that participants in the different regional competitions will be subject to the same rules no matter which competition they participate in.

A significant issue that must be addressed is the continued funding of the NCCDC along with support to the regional competitions. The organizers of the NCCDC are searching for a "name sponsor" who sees the value of the competition and is willing to supply significant financial support to sustain the event. At the same time, no school has envisioned in its budget the need to support a cyber defense team nor money to conduct a regional competition. There is a cost with conducting a regional exercise – both in time and materials. At the national level, the organizers are looking for a sponsor that can help provide some support to the regional competitions as well so that the regional organizers do not have to add obtaining a sponsor for their event to the list of responsibilities when they agree to conduct the event. Alternatively, a sponsor can be sought for each of the regional competitions from an organization within the region's geographical boundaries that would be willing to adopt the regional competition. Since the costs associated

with the regional competitions is much smaller (on the order of a few thousand to as much as twenty thousand dollars depending on what they decided to support), obtaining regional sponsors could prove to be a much easier proposition than finding a major sponsor for the national competition.

There have been some discussions already about expanding the scope of the NCCDC. One item discussed is the expansion to an international competition instead of a US-only event. Since the Information Systems Security Association (ISSA) is one of the sponsors of the event, and ISSA is an international organization, they have been one of the entities recommending consideration of this expansion. The idea would be to have ISSA chapters help sponsor the various regional competitions and that international chapters be used to initially expand to an international event. (There already has been significant sponsorship of teams by some ISSA chapters in communities with schools that are competing. Expansion to international chapters is a natural extension of this.) Somewhat along this line, some government organizations have asked about the possibility of expanding the concept of the competition to include teams from industry as well. This would help serve to encourage security within the community at large and not just at the collegiate level. While this is indeed an intriguing idea, the organizers of the NCCDC currently do not have plans to expand to industry in the near future. At some point in the future it may be possible to address an open competition in which teams from any sector – government, academia, or industry – could compete but this would most likely be an extension of the NCCDC or possibly a completely separate event. It is believed that the concept of the competition is important enough for academia to warrant a collegiate-only competition.

Another possible expansion to the competition that has been discussed and that will occur within the next few years is the introduction of different events during the competition. A simple example of this would be to include a cyber forensics challenge at the competition for either individuals or teams to compete in. This would be along the lines of an NCAA track meet in which there are both individual and team events. The specific types of events that would be included are still being determined and how the overall national champion will be determined will be a subject that the governing body will have to address. Another related topic is the inclusion of an "attack and defend" portion of the competition. Many students enjoy the "thrill" of attempting to attack another system while having to defend their own. There are other collegiate and non-collegiate examples of this (the most notable having been the DEFCON competition) and students at the NCCDC have suggested that after the conclusion of the official portion of the defensive competition they be allowed to try some attacks on their own. The organizers of the NCCDC have not allowed this, and there are no plans at this point to include this in the future, but it is something that the governing body may wish to address. If they do, caution should be used to ensure that the overall theme of helping to develop the nation's cyber defenders and not the next generation of "hackers" should be kept in mind.

A final consideration is to determine whether the competition should expand to also include High School teams. There have been some High School cyber security competitions that have been conducted by different universities (most notably the competition at Iowa State University) but there is currently no recognized national cyber security High School competition. There are some significant differences between organizing and conducting a collegiate competition and a High School competition. Chief among these is the fact that there are many more high schools than there are colleges and universities. This means that the high school competition could potentially be many times the size of the collegiate event. Just as at the collegiate level, no funding is available for high school cyber defense teams which are use to local competitions. This also means that the number of high school competitions could also greatly outnumber the collegiate events. What ties that would exist between the competitions at the collegiate and high school levels should be examined (again by the governing body) but one simple solution is to keep them completely separate. Currently, the NCAA does not govern what a school district does with its competitions. The same could apply to cyber defense competitions where one level does not dominate the other but both are cognizant of the other's operations.

VI. A Separate 2-year competition

A significant part of the current NCCDC structure is the inclusion of 2-year institutions within the competition. The initial question that most have asked is whether these institutions are at a disadvantage over the larger 4-year organizations. So far this has not been shown to be the case. Teams from the 2-year institutions have fared very well against the teams from the larger institutions. Comments from faculty members at 2-year institutions have indicated that this may be due to the fact that 2-year institutions often focus more on the technical training aspects of securing a network and do not need focus on the theoretical aspects that are often seen at the larger institutions. Some have even suggested that this may give them an advantage in the competition. Whether either type of institution has an advantage can be debated and should be considered by the governing body. A discussion has occurred as to whether there should be a separate competition for the 2-year institutions. They certainly have shown their ability to compete in and to

organize competitions (see http://ccdc.morainevalley.edu/ for information regarding the Midwest Regional Collegiate Cyber Defense Competition hosted by Moraine Valley Community College for an excellent example of one of the regional competitions). It is the belief of the organizers of the NCCDC that it would be a loss for both types of institutions if the competition was split and separate events held. Having the various teams meet and mingle at the competitions helps both the community colleges and the 4-year schools involved. Students from one institution can talk to individuals from others where they may be considering continuing their education. Instructors can also mingle and discuss programs and courses with the ultimate winner being the programs at all institutions.

VII. Conclusion

The National Collegiate Cyber Defense Competition has made significant headway towards establishing a true national cyber security championship event. The foundation has been laid for not only a series of regional events leading to the national championship, but state competitions before the regional competitions to allow for any institution to compete. Much has been learned in the events that have been conducted so far and the forerunner for a set of standardized rules has been created. Several steps need to occur now for the competition to become established and recognized by institutions around the country. First is to obtain financial sponsorship of the event. Several organizations have expressed interest in the competition but it remains to be seen whether a "name sponsor" will step forward. The second important step is to establish a governing body for the NCCDC that can address the numerous issues regarding rules and expansion of the event to additional regional competitions. The last is the actual growth of the NCCDC itself so institutions from all areas of the country (and eventually from all interested nations) can participate.

VIII. References

[1] Hoffman, Lance and Ragsdale, Daniel, "Exploring a National Cyber Security Exercise for Colleges and Universities", Report No. CSPRI-2004-08, The George Washington University, Report no. ITOC-TR-04001, United States Military Academy.

[2] White, Gregory B., and Williams, Dwayne E., "The Collegiate Cyber Defense Competition", *Proceedings of the 9th Colloquium for Information System Security Education*, 6-9 June 2005, Georgia Institute of Technology, Atlanta, Georgia.

[3] White, Gregory B., and LCOL Dodge, Ronald C., "The National Collegiate Cyber Defense Competition", *Proceedings of the 10th Colloquium for Information System Security Education*, June 5-8, 2006, the University of Maryland – University College, Adelphi, MD.

[4] Lemos, Robert, "Cybersecurity Contests Go National", SecurityFocus, June 1, 2006, http://www.securityfocus.com/news/11394.