Creation of a Collegiate Cyber Security Championship Cup

Gregory B. White, Ph.D., Dwayne Williams, CISSP, *The University of Texas at San Antonio*

Abstract – A number of cyber security competitions currently exist. Some are aimed at high school students, some at professionals, and some at security professionals. By far the largest number of competitions take place at the collegiate level. Currently there is very little that ties these competitions together and at times it may seem that the competitions themselves are competing against each other. For these competitions to take the next step toward establishing themselves collectively as a recognized competition program they need to come together and establish a Collegiate Cyber Security Championship Cup and the program that would run it.

Index terms – Cyber Security, Collegiate Competitions, Cyber Defense, Exercises

I. Introduction

Competition and athletic events are part of our society. In almost every field competitions are held to establish who is the best practitioner in that field. All one has to do is flip through the many stations found on today's cable TV networks to find any number of sporting events or even competitions seeking to find the best in some field – such as cooking, spelling, or poker. Competitions are used to raise the level of interest that the general public has in a specific endeavor and to excite the participants themselves. A great example of this is what has happened in the game of poker over the last few years. Since the World Series of Poker began to be seen on TV, attendance at the events has continuously grown reaching a figure of 63,706 participants this last year. [1]

The field of cyber security has not been left out of this desire to see who is the best. Competitions have been conducted for several years at a variety of levels and in a variety of venues. Some competitions are held virtually while others are held in a specific location. In the field of cyber security the competitions hold an additional attraction for the competitors. Not only does the competition provide an opportunity for them to pit their skills against others, the competitions often provide an opportunity for the participants to do things that they normally would not have a chance to do in a school lab. This is especially true for the "hack and defend" type of competition where competitors attempt to break into the systems/networks of other competitors while defending their own. This sort of activity is normally not allowed in academic labs and environments so the competition provides a platform for the competitors to gain experience in an area the students might otherwise not have an opportunity to explore. Just as in other areas, the rise of these competitions, and the attention that they have begun to attract has helped them to grow and expand and there are now a number of them being held across the nation.

Dr Gregory White is an Associate Professor of Computer Science and the Director of the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio. Mr. Dwayne Williams is the Associate Director of Special Projects at the CIAS.

II. Cyber Security Competitions

Cyber security competitions have become increasingly popular over the past decade and encompass the entire spectrum of cyber security from offensive to defensive. Perhaps the longest running and arguably the most well known cyber competition is the Capture the Flag (CTF) contest held at the annual DEF CON competition. While the rules have changed over the years, the CTF pits teams of contestants against each other in a multi-day team on team competition. Competitors must protect their own systems while infiltrating resources of opposing teams. [2] While the CTF has traditionally emphasized offensive skills, defensive skills do play a critical role in the CTF. If a team is unable to secure and defend their own systems, they will not be successful at a CTF event. The 2011 CTF will take place June 3-5 and will run for a projected 53 hours.

The CTF model has been emulated by other cyber competition events, most notably the University of California at Santa Barbara's International Capture the Flag (iCTF). First held in 2004, the iCTF is described as a "multi-site, multi-team hacking contest in which a number of teams compete independently against each other." The iCTF differs from DEF CON's CTF in that the iCTF consists primarily of teams from academic institutions and involves more teams competing simultaneously from networks around the world. Early version of the iCTF gave each team identical systems to secure and defend while simultaneously attempting to disable their opponent's systems. More recent versions of the competition have become increasingly elaborate and

ISBN 1-933510-96-X/$15.00

involve scenario based challenges. The core emphasis of the iCTF, however, is still offensive in nature. [3]

Another variation of the CTF competition is Panoply, run by The University of Texas at San Antonio. Panoply varies from traditional CTF events in that teams compete for control of central resources and are only awarded points for possessing and maintaining identified critical services over a period of time. While no points are rewarded for offensive actions, teams must be able to scan and penetrate central resources. Teams attack only the central resources and are prohibited from attacking other teams but are allowed to take control of central resources away from competing teams. Once a resource is obtained, the team will have to prevent it from being taken by the other teams – thus they have to not only know how to exploit security holes in a system, they have to be able to know how to quickly patch the hole to prevent others from using the same hole to steal it away.

A well known cyber competition that has been in existence for several years is the United States Military Academy sponsored Cyber Defense Exercise (CDX). Founded in 2001, the CDX serves as a capstone course for information assurance programs at US military service academies. Unlike other competitive events, the CDX is a semester long project for the competitors. As part of the event, each team designs and builds their own networks to meet objectives laid out for the teams by CDX organizers. The "live" portion of CDX pits each team against an NSA sponsored Red Team – a group of individuals whose mission is to compromise the student networks. Unlike CTF events, the CDX downplays offensive skills for students and focuses on defensive skills such as secure network design, network operations, and incident response. The CDX is only open to US military academies. [4]

Similar to the CDX is the Collegiate Cyber Defense Competition (CCDC) program. Founded in 2005, the CCDC was the first competition that specifically focuses on the operational aspect of managing and protecting an existing "commercial" network infrastructure. Teams from two or four year colleges and universities are given identical small business networks and tasked to assess, secure, and defend those networks while maintaining critical services and responding to business tasks. During CCDC events, live Red Teams probe and attempt to penetrate student networks. The CCDC is a tiered competition structure with qualifying events that culminate in a national championship event. While teams do assess their own networks, CCDC primarily emphasizes defensive skills and network operations. [5]

Another noteworthy cyber competition is the DC3 Digital Forensic Challenge sponsored by the Department of Defense Cyber Crime Center (DC3). The DC3 Digital Forensic Challenge is unique in cyber competitions as it focuses on digital forensics, contains levels of competition from novice to expert, and allows both individuals and teams to compete.[6] Founded in 2006, the DC3 Digital Forensics Challenge contains multiple challenges (23 in 2011) that are separate and unique. Challenges are separated into 5 skill levels (100-500) with each level containing multiple challenges. Level 100 consists of "Novice" challenges with solutions that would be well known to experienced forensics examiners such as file signatures, hashing metadata, and so on. Level 200 challenges are more advanced and involve data hiding, registry modifications, file headers, and so on. Level 300 challenges are "Expert" level and are not guaranteed to have a solution or will have solutions that are no well known. Level 400 challenges have no known solution and involve parsing of communications, data hiding within files, and so on. Level 500 challenges are designed to challenge the development of new forensics tools based on defined requirements that are part of the challenge. Winners are selected from civilian, government, and international teams based on total points accumulated.

These are just a few of the cyber security competitions that allow collegiate competitors being held across the country. There are other collegiate events, as well as additional competitions aimed at other levels such as high schools or security professionals. The competitions are currently disparate with nothing that ties them together other than loose affiliations such as the tie between the CCDC and the CyberPatriot High School Cyber Defense Competitions. Creating a stronger tie between the various competitions would help strengthen all of them by raising the level of awareness of them. This leads to the idea of establishing a championship program for cyber security competitions.

III. Other Championship Cups

The idea of a special award being presented at the end of a competition season is not a new concept. The nature of competition leads to a desire to determine who the best in any given sport. Sports such as football, hockey and basketball have well established methods to crown an annual champion in that sport. This is true at both the collegiate and professional levels. The National Football League awards the Vince Lombardi Trophy to the winner of the Super Bowl. The Commissioner's Trophy is awarded to the Major League Baseball winner of the World Series. The National Hockey League awards the Stanley Cup to the winner of, appropriately enough, the Stanley Cup finals which is the culminating event of the playoffs in the league. On an international level, the *Fédération Internationale de Football Association(FIFA)* awards the FIFA World Cup to the winning team in the international soccer World Cup competition which, unlike the other championships mentioned here, only takes place

ISBN 1-933510-96-X/$15.00

every four years. Each of these championships has a very specific series of competitions leading to playoffs and the championship. Outside of some exhibition and preseason matches, all of the competitions fall under a governing body which establishes the rules all teams must follow. There is also a single recognized championship for each of these sports.

At the collegiate level, the National Collegiate Athletic Association (NCAA) has established rules for colleges to compete in a number of sports including the ones mentioned above. Championship systems have been established for the sports [7] with the best known being the championships in football and basketball. In basketball, for example, the winning team from the NCAA championship tournament receives a gold-plated NCAA national championship trophy in addition to the National Association of Basketball Coaches trophy. After many years, a championship system (though it is still hotly debated) was established for NCAA football and now the champion from this system is awarded the Bowl Championship Series trophy by the American Football Coaches Association.

Other sports, such as boxing, also have established champions and awards (or "belts" in the case of boxing) but there may be multiple governing bodies and thus multiple champions. In boxing, there are four main organizations, each with their own unique championship awarded to the champions in each of their weight classes. These organizations are the World Boxing Council, World Boxing Organization, World Boxing Association, and the International Boxing Federation. The goal of a champion in any one of these organizations is often to obtain as many of the belts as possible so they can claim the title of world champion in their weight category. Frequently there will be more than one individual holding any one of the given championship belts in a given weight class.

The nature of some sports may not lend itself to the clear establishment of a single national or world champion. Golf and stock car racing consist of a number of individual competitions often with very little tying them together. In an attempt to increase the public interest in the numerous stock car races in existence, the National Association of Stock Car Auto Racing (NASCAR) established the Sprint Cup as a championship award that could be presented to the top driver annually. The complete rules establishing the scoring system for the Sprint Cup are rather involved, but to provide a simplified explanation, the season is split into two seasons. The top drivers in the first part of the season can compete in the races that make up the second season which has been given the name of "The Chase for the Championship". Drivers earn points based on their finishing position in each race and can be awarded additional bonuses should they win a race or when they are the lead during a lap. What the Sprint Cup has done, beside increasing the public interest in NASCAR, is focus what might have remained a series of basically disparate races into a cohesive program leading to the crowning of a single champion.

Professional golf had a similar challenge as did stock car racing and the solution was again the creation of a single championship cup, in this case named the FedEx Cup. Golf has traditionally had a number of champions crowned for events such as the British Open, the U.S. Open, the PGA, and the Master's. The FedEx Cup was created to generate interest in the later part of the golf season when interest in the sport often waned. The FedEx cup, like the Sprint Cup, takes already existing events and turns them into a second season with an elimination system which mimics the playoffs found in many other sports. While the NASCAR Sprint Cup has succeeded in increasing public interest in stock car racing and its season, the FedEx Cup has not been quite as successful due to the fact of the popularity of the long established Master's. With the possible exception of a specific race, such as the Daytona 500, there wasn't a comparable stock car champion such as what the Master's provides the golf world. That said, the FedEx Cup has succeeded in increasing the interest in tournaments, that might not otherwise have had the public interest, due to their potential impact on the outcome of the FedEx Cup champion.

A less well-known championship series from which some lessons can be learned is the United States Dressage Federation's (USDF) year-end awards. [8] Scores for individual riders and horses are taken from different events throughout the year that may have been run by the USDF or the USEF (United States Equestrian Federation). In this case too, however, there is an overall licensing/governing body that addresses the rules for the different events. In this case, however, there are multiple awards presented at the end of the year for different categories. This might be a closer match to the cyber security competition environment.

IV. Creating a Cyber Security Championship Cup

The current collegiate cyber security competition environment is similar in many ways to professional golfing and stock car racing as well as equestrian events. A number of separate, currently disparate, competitions are occurring. In addition, in the case of cyber security competitions, there is no unified governing body and the rules and goals of the different competitions may be very different. Developing a championship system similar to any of the previously mentioned events will not be as easy without an overall governing body and unified set of

ISBN 1-933510-96-X/$15.00

rules. A system in which participation and levels of success in the different competitions provides points which can be accumulated and which lead toward the crowning of a national champion could initially be more easily established and is the logical first step. It is important to note that what is being proposed in this paper is not a championship event (such as is held for soccer, football, basketball, and a host of other athletic events) but rather a program which awards points to existing competitions based on factors still to be negotiated, and the school that receives the most points would be awarded the championship cup. This is more akin to the cups awarded in golf and NASCAR racing.

Establishing a cyber security competition championship program would require cooperation between the various hosts of the existing competitions on a number of levels. To begin with, the timing of the events should be coordinated so that not only would two competitions not be held at the same time, but the competitions should allow for enough time between them for students to prepare. Based on the different nature of the competitions, there might also be a natural progression that could be established and followed. Can certain competitions build upon other competitions? Can the skills learned in one better prepare competitors to compete in another competition?

The championship system would also have to address the relative weight of each of the competitions. Should the winners of each competition receive the same number of points or are some competitions more involved and therefore should be weighted heavier? How are competitions such as the CCDC program handled where some teams will compete at state qualifying, regional, and national events? Are teams awarded points each time they participate or are those teams that only compete in the state events awarded fewer points than those who advance to a regional or the national event? Does the size of the competition factor into the weight for the event or is there an assessment of the relative difficulty of the event and those competitions considered more challenging would receive a greater weight (an example of this would be the service academy CDX where only a few teams can compete but it can be argued that the level of the competition is very high)? How are competitions such as the CDX where only a few schools are eligible to compete handled? Is there a "menu" of competitions established from which a team can receive points for only a specific number of events – even if they compete in more? Are allowances made for two-year institutions or do they compete alongside four-year institutions with no differentiation being made or are there multiple divisions established so that two-year institutions only compete against two-year institutions and four-year colleges and universities against other four-year colleges and universities? How are graduate students handled – do they have the opportunity to compete alongside undergraduate students or is there a separate division organized for them?

Some of the competitions currently are aimed at the collegiate level. Others, such as the DC3 competition, allow for teams from more than the collegiate level. For competitions that allow for teams from various levels, a method to rank just the college teams is needed. This is not a difficult task and the DC3 competition is actually broken into multiple categories including U.S. graduate, U.S. undergraduate, and U.S. community college teams at the collegiate level. They also have a U.S. high school team category in addition to more open categories at the international and federal government levels.

The need to create a collegiate category in competitions that allow for other competitors brings up other eligibility questions. The most basic question to ask is who can qualify as a college student? This is just one of several eligibility questions that need to be addressed and agreed upon among the different competitions that would constitute the championship cup system. From a team perspective, what constitutes a team for an institution competing in the championship system? Do the same individuals have to compete on all teams from an institution that is participating in the system or can teams be formed for specific competitions with different members? This might be somewhat akin to a swimming or track and field competition where the "team" consists of a number of different individuals from the same institution but the same individuals do not participate in every event – they specialize in a few events or even a single event. From an individual competitor's perspective, does a participant have to be a full-time college student or can a part-time student participate? How many seasons is a student eligible to compete? How is the eligibility of a student verified? How, especially for the competitions that are virtual in nature, does the competition ensure that only eligible team members compete? Currently, the competitions have to mainly rely on the "honor" system and assume that the teams will follow the established rules. However, as the prestige and importance of the competition grows, especially if prize money, scholarships, or jobs are made available to winning team members, the temptation to "win at all costs" will increase and an established mechanism will need to be created to ensure compliance with established rules. The CCDC program is currently addressing some of these issues and may be used as an example of how to address them. A rules committee, made up of members from schools from each of the participating regions meets (via teleconference) on a regular basis to examine the rules to make sure there is a consensus on each rule and that all aspects are addressed. A similar mechanism would be needed if a championship cup system were established. This may eventually lead to the

ISBN 1-933510-96-X/$15.00

establishment of a governing body for the cyber competitions such as is found in the NCAA for college sports.

V. Benefits of a Cyber Security Cup

The establishment of a Cyber Security Cup could be very beneficial for a variety of reasons. First and foremost, it would raise the awareness of cyber security as a field of study and encourage more institutions to pursue and compete in multiple cyber competitions. In doing so, it would help lead to an increase in participation in these programs and in the field in general. Involvement in cyber competitions is a proven motivator for both faculty and students and has led to improvements in curriculum at institutions around the country. Cyber competitions provide opportunities for competitors to be involved in activities that they would not normally have a chance to do. In addition, there are very few activities at the collegiate level that provide an opportunity for computer science and information systems students to work in a team atmosphere that these competitions provide.

In addition to exposing students to the various disciplines and careers available in cyber security through various competitions, a Cyber Security Cup could be used to help establish a unified Common Body of Knowledge (CBK) as a reference for cyber security curriculums. While there is some overlap between cyber competitions, most cover one or more domains of cyber security that can be directly mapped to a CBK. Developing a CBK would allow faculty to adapt curriculum to the rapidly changing cyber security industry and would assist in the development of team guides and preparation materials for cyber competitions around the country. Competition organizers could also refer to a CBK when designing and preparing competition events. By soliciting input from government and industry, a unified CBK could be used to produce graduates that are more prepared to enter careers in cyber security fields. Development of the CBK for the championship cup would also help identify areas which may not currently be emphasized in any of the competitions, but should be. Development and use of a CBK for the competitions will help to organize what is now disparate competitions into a unified program that is helping to develop the cyber security professionals that the nation needs. Development of a CBK for the championship cup would take into consideration the work that has been done in this arena already by organizations such as the CBK identified by the $(ISC)^2$ and the work done on the Essential Body of Knowledge (EBK) by the Department of Homeland Security (DHS). [9, 10] In fact, the establishment of the CBK for the championship series may help to drive the development of a unified CBK for the field in general.

Another benefit of establishing a championship series was previously alluded to. Currently, there is no cooperation or coordination between the different events – each is truly its own event with no ties to the others. Establishment of the Cyber Cup program would help to bring all organizers together in order to de-conflict their individual events. Beyond simply de-conflicting, the coordination aspect could lead to a more organized approach to the events with potentially a plan for a logical seasonal progression through the events. Coordination would also apply to the CBK as has been mentioned.

A Cyber Security Cup "Championship Series" would also generate more public interest in cyber security and the individual competitions comprising the competition series. Public relations at each member event would refer back to the Cyber Security Cup, encouraging the public to learn more about other competitions. This cross promotion of activities would raise the visibility of every competition. It has long been the dream of the authors to have cyber security competitions be broadcast on an established television show such as ESPN and the development of the championship cup and the "championship series" could help make this dream come to pass. This in turn would help to raise the level of awareness of cyber security in the nation even more and would help to advertise each of the individual competitions.

VI. Conclusion

The authors believe that a collegiate cyber security championship cup would greatly enhance the visibility of cyber security for both students as well as the public in general. Raising the visibility of cyber security competitions at the collegiate level will also help generate more interest at the high school level where competitions such as the CyberPatriot High School Cyber Defense Competition is already making inroads. Industry and the nation need many more cyber security professionals than what is currently being produced. To do that requires a mechanism to excite students about the field and competitions have the benefit of doing that.

With the disparate nature of the current competitions that are being held, there is no immediate tie between them and the development of a championship system will take a great deal of work and cooperation between the entities that are currently conducting the competitions. The benefit to the individual competitions, and to the field in general, would be tremendous, however, and the authors believe that the idea would be well received by the different organizers of the events. Immediately developing a governing body for all of the events is not likely to happen in the immediate future – the competitions are too dissimilar and each has its own rich history and unique way of doing things. This, however,

ISBN 1-933510-96-X/$15.00

does not mean that a competition system could not be conducted. Rules that would govern participant qualifications could be worked out and a scoring system created that would include the current competitions that are being conducted as well as allowing for additional competitions that may be created in the future. Development of an NCAA-like governing body could be a task that is left for the future. The immediate first step is simply to bring the organizers of the major competitions together to start the dialogue and start working toward establishment of a National Collegiate Cyber Security Championship Cup. This is a very doable step.

Believing this to be a valuable endeavor, and believing that the establishment of a National Collegiate Cyber Security Championship Cup is feasible in the near term, the authors propose to bring together leaders of some of the competitions currently being conducted to begin discussing how a championship could be established and how the champion would be determined. The goal is to establish the initial rules for this championship recognizing the competitions currently in existence, as well as establishing rules that would govern the addition of new competitions that may develop in the future, by the end of the 2011-2012 academic year and to award the first National Collegiate Cyber Security Championship Cup at the end of the 2012-2013 academic year.

VII. References

[1] WSOP staff, "2010 World Series of Poker Shatters Attendance Record", July 2, 2010, www.wsop.com/news/2010/Jul/2962/2010-WORLD-SERIES-OF-POKER-SHATTERS-ATTENDANCE-RECORD.html, Mar 12, 2011.

[2] CTF Archive – Def Con, www.defcon.org/html/links/dc-ctf.html, Mar 11, 2011.

[3] The UCSB iCTF, ictf.cs.ucsb.edu/, Mar 11, 2011.

[4] ITOC Research, www.itoc.usma.edu/research/dataset, Mar 11, 2011.

[5] National Collegiate Cyber Defense Competition, www.nationalccdc.org, Mar 11, 2011.

[6] DC3 Digital Forensics Challenge, www.dc3.mil/challenge, Mar 11, 2011.

[7] NCAA Championship Season, www.ncaa.org/wps/wcm/connect/public/ncaa/championships, Mar 12, 2011

[8] "2011 USDF Competitor and Member Guide", http://magazine.usdf.org/usdf3, Apr 15, 2011.

[9] CBK, https://www.isc2.org/uploadedFiles/Education/Review_Seminars/CBK.pdf, Apr 15, 2011.

[10] Aitoro, Jill, "IT Security Essential Body of Knowledge", http://www.govexec.com/basics/itsecurity.htm, April 15, 2011

ISBN 1-933510-96-X/$15.00