THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

CSPRI
CYBER SECURITY POLICY & RESEARCH INSTITUTE

The United States Military Academy

Exploring a National Cyber Security Exercise for Colleges and Universities

Lance J. Hoffman
Daniel Ragsdale

This report provides an overview of existing cyber security exercises, explores the feasibility of generalizing those exercises to a national exercise, describes the structural and resource-related issues of hosting a cyber security exercise, and outlines the mission and goals of a potential governing body for such exercises.

Report No. CSPRI-2004-08
The George Washington University
Cyber Security and Policy Research Institute

Report No. ITOC-TR-04001
United States Military Academy
Information Technology and Operations Center

August 24, 2004

Exploring a National Cyber Security Exercise for Colleges and Universities

Lance J. Hoffman[1]
Daniel Ragsdale[2]

Abstract

This report provides an overview of existing cyber security exercises, explores the feasibility of generalizing those exercises to a national exercise, describes the structural and resource-related issues of hosting a cyber security exercise, and outlines the mission and goals of a potential governing body for such exercises.

[1] Computer Science Department, The George Washington University, Washington, DC 20052, lanceh@gwu.edu

[2]Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY 10996, Daniel-ragsdale@usma.edu

Table of Contents

Introduction

On February 27 and 28, 2004, a group of educators, students, and government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises for post-secondary level students similar to the annual Cyber Defense Exercise (CDX) held among the students of the various U.S. military service academies. The military model and other smaller efforts were described, and numerous ideas, opportunities, and challenges were brought forth. This report attempts to capture the concepts discussed at the workshop. It provides an overview of existing cyber security exercises, opens questions related to generalizing those exercises to a national exercise yet to be defined, describes the structural and resource-related issues of hosting a cyber security exercise, and outlines the mission and goals of a potential governing body for such exercises.

What Is a Cyber Security Exercise?

There are at least four examples of what could be called a cyber security exercise.

Organized Competition among Service Academies

The U.S. military service academies' CDX was designed in 2001 as an inter-academy competition in which teams design, implement, manage, and defend a network of computers (see Appendixes L3, L7, and L14). A team of security professionals from various government agencies participate in the exercise as attackers.

Any offensive activity by an academy is heavily penalized. The event, now held annually, stresses the application of skills learned in the classroom as students attempt to keep their networks functional while a group of professional security experts "attacks" the networks repeatedly over the course of several days. The participants must build a secure network including several legacy applications. The must both install and secure the applications they employ to meet service requirements, and build defensive measures around systems that may not be altered. By focusing on the defensive tasks in network security, each student has the opportunity to truly understand the fundamental concepts and can spend time conducting forensic analysis. This helps avoid an inadvertent attack that spills outside the "network sandbox". While many might argue that the likelihood of such an occurrence happening is small, one such event can be catastrophic to the exercise.

The greatest drawback of the CDX is its rigid nature. Students are strictly limited in both the time frame of the exercise and the actions that can be taken during the exercise. This structure does, however, provide a strong reference from which to gauge the relative performance of each participant.

Small, Internal, Continuous "Capture the Flag" Exercise

In contrast to the large-scale, multi-institution event the CDX represents, a student group from the University of Texas at Austin has established a small-scale, internal, continuous cyber security exercise. The students created their own isolated network to practice system defense, and it evolved into an ongoing, online, offense-oriented competition. Teams of attackers are assigned objectives and gain points when they achieve the objectives by a designated scoring system. No time constraints are involved, so individual participants can take part at any time (see Appendix 4). The hardware was donated, and the students are responsible for managing and maintaining both the hardware and the online exercise.

This structure offers maximum flexibility at minimum cost. However, it lacks integration into an established curriculum and thus misses the opportunity to be used as a formal capstone exercise that provides a focal point for an advanced information assurance course. Additionally, any perception that students are using university resources to "learn to hack" in an unsupervised environment might cause concern among the administration and others.

National "Capture the Flag" Exercise

What began as a classroom exercise in a course on network security at the University of California, Santa Barbara, grew into a competition among teams around the United States. Teams are given a system, configured by the organizers. The system contains a number of undisclosed vulnerabilities. The teams have a limited time to set up their own systems and then are allowed to attack each others' systems at will. Each team attempts to find the vulnerabilities in the given system so that they can fix or protect their system and, at the same time, exploit this knowledge to compromise the system of other teams. A successful compromise allows a team to access and modify specific hidden information on another's system (i.e., "the flag"). This allows a scoring system to determine the current status of the competition and assign points to each team. Points are also assigned to teams that maintain their services active and uncompromised. Therefore, each team has to defend its own system to maintain functionality, such as web access and network connectivity. (See Appendix 5.)

This scenario shares some characteristics of the previous one. In particular, it requires the students to engage in offensive actions to win. Introducing students to the attack process and actually requiring them to employ such skills each raise legal concerns. Specifically, what happens if an attack unintentionally leaks outside the exercise network (since virtual private networks [VPNs] are not guaranteed to be secure)?

Semester-Long Class Exercise

At Texas A&M University, a graduate-level advanced security class engages in a cyber security exercise throughout the whole semester. Students are divided into teams of attackers (hackers) and defenders (system administrators); a third group oversees the

exercise and imposes the same limitations on the students as the university network imposes on all its users. Access is limited to a private network, and defenders must keep the network running at all times. At the end of the semester, both teams disclose what they were able to accomplish. Grading is subjective and focuses on the successful attempts of each team (see Appendix 6).

This exercise also has students engaging in attack activities, although in a supervised scenario, and thus also raises the potential legal concerns cited above. In addition, each student group only has the hands-on experience for its own mission. The exercise may be somewhat less competitive than if the school were competing against a rival school.

These different types of exercise are summarized in Table 1.

Table 1. Summary of Cyber Security Exercises

	Organized Competition Among Service Academies	*Small, Internal, Continuous Exercise*	*Regional "Capture the Flag" Exercise*	*Semester-Long Class Exercise*
Student offense component		**X**	**X**	**X**
Student administrative component	**X**			**X**
Isolated exercise network		**X**		**X**
VPN exercise network	**X**		**X**	
Inter-school competition	**X**		**X**	

Goal and Benefits of Cyber Security Exercises

All of the cyber security exercises described involve hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program, i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace (in this case, the defense, not the attacks). The exercises combine legal, ethical, forensic, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure.

Therefore, the goal of a cyber security exercise might be described as follows:

> To provide a venue for practical education in the implementation of all strategies, tools, techniques, and best practices employed to protect the confidentiality, integrity, authenticity, and availability of designated information and information services.

A Uniform Structure for Cyber Security Exercises

It has been suggested that a uniform structure for cyber security exercises be set up. The goals of creating a uniform structure for cyber security exercises might include the following:

1) Providing a template from which any educational institution can build a cyber security exercise

2) Providing enough structure to allow for competition among schools, regardless of size or resources

3) Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance

Rules and Guidelines

Workshop participants identified the following concerns that should be addressed by a standard set of rules.

Eligibility: Workshop participants agreed that participation should be limited to post-secondary school students for the immediate future. Commercial or government agencies should have opportunities to play a supporting role, but the focus should remain on the academic exercise for now. By limiting exercises to educational institutions, organizers will be better able to gain support from faculty, university leaders, and national educational and professional societies.

Resources: The guidelines should specify options for setting up networks for an exercise. Attention must be given to creating (a) level playing field(s) so institutions with greater resources (e.g., hardware with fast processors and access to high bandwidth for communication) do not have an outright advantage. Software and tools that can be used should be available to all participants and limited to open-source or pre-approved programs from an approved software list. Participants should not be allowed to use evaluation copies of commercial software. This ensures all schools have access to the same set of tools to employ. This does not imply that a school should disclose its list of software to other schools – each participant is still required to conduct the research needed to employ the most secure network possible.

Legal issues: Guidelines should offer specific methods for recognizing and meeting legal obligations when planning and conducting an exercise. Various legal considerations are discussed below.

Limitations: Rules should define in writing as thoroughly and clearly as feasible what strategies and practices are and are not allowed. Two distinct sets of rules should be devised: one for attackers and one for defenders. Referees should also have clear guidelines. Referees should be independent of both the defending and attacking teams since they may be used to ensure fairness of the conduct of a competition. They also, dependent upon their experience, may add value to the learning experience by providing

insight and guidance in the form of an After Action review. This is where much of the learning occurs. (See Appendix 11.)

Scoring: A uniform method of scoring should allow teams of all sizes to compete. An objective and relatively simple scoring algorithm will allow teams or even individuals to engage in an internal cyber security exercise and compare themselves with those taking part in a more formal, competitive exercise. Both automated and manual scoring approaches should be considered. If possible, additional points should be awarded for realistic solutions that preserve functionality, e.g., those that allow other network users to continue working, use e-mail, and access the Internet at an acceptable speed. It may be helpful to implement an ongoing (or real-time) assessment mechanism and possibly post scores during the exercise. (At least one workshop participant felt that this type of competition would not scale to a national level because of difficulties involved in coordinating referees and ensuring a level playing field, and suggested removing the competitive element at the national level, pointing out that individual schools could always set up isolated competitions with one another if they considered their students and curricula to be roughly equivalent.)

Penalties: Consequences for violating the rules should be determined at the outset. Ethical considerations should be made clear. Participants should agree to adhere to the spirit, as well as the letter, of the rules.

Assessment: During the exercise, communication among all participants is critical. Because of the adversarial relation that develops between the attackers and the defenders, the referees should be the conduit for all information requests. Rules should address how and how much information should be shared among teams during an exercise. It may be helpful to consider incentives for sharing information.

The exercise must be assessed after completion. Specifically, where and when attacks occurred, whether they were identified, and how they were addressed is important to know, so that an accurate assessment can be made of the participants' understanding of the network activity. Setting up a secure network is good only until the first compromise. After that, participants must demonstrate that through forensic analysis, they fully understand and can document what happened. In general, the format and framework of a post-event assessment should be determined at the outset; how and how much information learned should be shared after the event should be determined.

Post-event disclosure: Once an exercise is completed, teams should be required to disclose all the tactics they used during the exercise. Tactics and strategies from past competitions should be readily available.

(Note: Numerous ideas were proposed throughout the workshop; some were thought to be beyond the scope of a standardized cyber security exercise. Some of those concepts are noted in Appendix 9.)

Legal Considerations

It may be assumed that the sole purpose of a cyber security exercise is training, and federal laws allow agencies to conduct vulnerability assessments for the purpose of security. However, to the extent that exercises may involve some use of real data and may affect real users of a real interactive system, organizers and participants should be aware of applicable state and local laws and regulations as well as institutional regulations regarding the following:

- Unauthorized intrusion
- Unauthorized access to data in transmission
- Unauthorized access to stored data
- Fourth Amendment limitations on government actors
- Individual privacy rights
- Contractual obligations

Organizers must take every reasonable step to ensure that no protected information is even put at risk, let alone compromised during any form of exercise. Functionally this equates to segregating the networks used for the exercise from production or support networks. Ideally, the only systems ever connected to the exercise network are those directly involved in the exercise. If such separation is not possible, than additional measures may be required to insure proper information protection.

A more realistic (and possibly more damaging) scenario is the use of exercise systems to intentionally or accidentally harm an innocent third party, potentially resulting in downstream liability. The concept of downstream liability is gaining interest and momentum in the legal communities. Lawsuits have been filed (e.g., FTC v. Guess Jeans: http://www.securityfocus.com/news/5968, FTC v. Eli Lily: http://www.ftc.gov/opa/2002/01/elililly.htm) and there are several white papers and articles on the issue. More on this can be found at "Downstream Liability for Attack Relay and Amplification" at http://www.cert.org/archive/pdf/Downstream_Liability.pdf, "Poor Tech Security Can Mean Lawsuits" at http://www.williamsmullen.com/news/articles_detail/122.htm, and "Downstream Liability – The Next Frontier" at http://www.nocinfragard.org/docs/rasch.ppt.

Organizers should assess their authority to access the system, manipulate the system, and access specific data. To do so, they should determine what systems, data, and authorities will be involved or affected. Organizers should seek permission to conduct an event from responsible parties. The entire procedure of the exercise (from planning through post-event disclosure) should be explained clearly to ensure that responsible parties give their fully informed consent. Students who participate in information assurance courses often are required to sign such an understanding of the concerns involved. See Appendix 15 for an example used in the Department of Engineering Management and Systems Engineering at The George Washington University. See Appendix 12 for the authorization memorandum issued by the United States Military Academy for its attacking team.

Organizers should screen participants and develop a plan to address civil liability or criminal activity, should it arise. Before sharing or publishing information, organizers and participants should consider the level of sensitivity of the information.

The exercise offers hands-on experience in a competition important to learning how to defend computer systems. Its main focus is not training to attack systems. It is important to point this out to university administrators and to the public in advance, during, and after the exercise to avoid expectations by participating students of a "fun hacking game" to defuse criticisms by those who may consider the exercise likely to cause more harm than good.

Appendix 8 contains a memo to organizers, players, and sponsoring organizations from legal staff in preparation for a cyber security exercise. This memo may serve as an example for organizers of future cyber security exercises.

Structural Considerations for a Cyber Security Exercise

There are at least four possible structural models for a cyber security exercise:

- Participants are given requirements and services they are to provide and must develop their own systems/networks to provide them.
- Participants are given specific systems and services to provide and must develop protections for them.
- Participants are given specific systems and a network configuration and must protect them.

A major decision is whether to conduct an event with multiple teams at one site (centralized) or at multiple sites (distributed). A distributed exercise requires fewer resources, but a centralized exercise enhances the excitement of competition. Because a centralized event would require establishing an isolated network for the exercise, it may more successfully limit the likelihood of damaging or malicious information traveling outside the realm of the exercise via the Internet. The availability of other university computer systems will affect the scheduling of the event.

The logistical issues identified below should be considered by (an) institution(s) exploring the possibility of establishing a cyber security exercise.

Personnel/Participation

- Scope of participation, e.g., members of a club, all students in a class, students across the university, or students from several universities
- Minimum and maximum number of participants
- Conditions of participation
- Qualifications and affiliations of referees or mediators

Tools

- Isolated network (if participants have access to the Internet, justify in writing beforehand). Consider simulating connectivity, e.g., creating a shadow server that gives the appearance of the Internet.
- Ensure equity of tools, advance notice, and hardware.
- All teams should have equivalent bandwidth; the following questions should be addressed in advance:
    - What bandwidth is required?
    - Are filters or rate limiters already in place?
    - Will bandwidth-oriented, application-specific denial of service (DoS) attacks be allowed?
    - Will general DoS attacks be allowed?
    - Can additional bandwidth be purchased or rented for the duration of the exercise?
    - Should organizers develop a list of approved websites that teams can access during the exercise, e.g., sites with tools that can help patch new vulnerabilities as they develop?
    - Will dedicated bandwidth conflict with Internet service provider or carrier?

Other

- Duration of preparation time
- Parameters for "pre-attack" setup, intelligence gathering, and surveillance
- Duration of the event
- Active/inactive periods of attack
- Types and areas of vulnerability
- Ensuring consistency of attacks, so all defending teams are subject to the same types and variety of attacks
- Definition of a "functional" system, i.e., participants should ensure the system can be navigated by naive users and not just technical experts

Resources and Costs

The costs of a cyber security exercise can be separated into six areas:

- Procurement
- Maintenance
- Internal personnel
- External support
- Management
- Facilities

This section provides some general observations on related costs. Some more detailed treatments of costs are provided in Appendix 10.

Procurement: For some institutions, the cost of obtaining appropriate hardware may be more than they can absorb, especially if the hardware is dedicated for the exercise only. The costs increase linearly with the number of teams involved. In some cases, it may be possible to borrow or rent equipment, establishing a central repository where participants can pick up and return equipment. The use of virtual machines would cost significantly less.

Maintenance: The cost and frequency of technical upgrades should be considered in budgeting and planning.

Each institution should maintain archives documenting its exercise, which would involve only negligible costs for the institution. The governing body will maintain technical reports, documents, scores, etc.

Internal personnel: Faculty members typically require release time or support time approved by their departments to oversee cyber security exercise properly. Both administrative and technical staff support are also needed.

External support: In some cases, obtaining the services of an external team of professionals in information assurance to act as attackers, referees, and/or controllers may be appropriate.

Management: If there is an overall governing body (local, national, or other), its costs would have to be covered. Fees or dues from the exercise and/or its participants, as well as from possible sponsors, are likely sources of revenue.

Facilities: The cost of procuring laboratory space for the exercise should be considered; it is expected the cost would increase in relation to the number of teams involved at a given site. Ancillary costs related to facilities include the cost of hooking the computers up to the Internet for the duration of the exercise.

Evaluating the Costs and Benefits

While the costs may seem daunting, it should be remembered that many institutions have found ways to minimize the cost of organizing exercises by obtaining donated resources and encouraging volunteer support. It may be helpful to initiate an exercise on a small scale, such as through a group study project or in the context of a special topics course.

Institutions should carefully weigh the many benefits of such an exercise against the potential monetary costs. Cyber security exercises provide an opportunity for students to apply their skills in a real-world scenario such as that likely to be found in a large corporation, a military coalition, a government agency, or a university. The exercise also offers lessons in teamwork, leadership, and coordination, as participants may be forced to react to change and to work with students or faculty from other departments.

Among the most significant costs is the time of faculty members involved. Great effort is needed to prepare students for an exercise, set up laboratories, and oversee and mentor students working in the laboratories for the duration of an exercise. These efforts take time away from other faculty responsibilities; therefore, faculty may require recognition by or even permission from the department to plan and implement an exercise. The exercise may be (and probably should be) integrated with one or more classes in a computer security and information assurance curriculum. Eventually, if an exercise becomes commonplace at an institution, the burden on faculty decreases, as fewer resources and innovations are required to maintain the exercise.

(Another factor in the equation would be whether the institution would keep the upgraded laboratories and equipment for instruction, etc.)

Governance

A central governing body with broad expertise is needed to establish and disseminate rules and framework. This body would be responsible for the following:

- Collect information about existing cyber security exercises, evaluate the pros and cons of the various models, and make the findings available to others.
- Define the goals and objectives of a structured cyber security exercise.
- Develop a framework for a cyber security exercise in an academic setting.
- Develop standard rules, parameters, and scoring mechanisms for cyber security exercises with an eye toward growing from single-school or small regional exercises to a national competition.
- Issue initial guidance for cyber security exercises.

On a more general level, it would also be appropriate for the governing body (or a portion of it) to

- facilitate resources,
- seek financial or other support and sponsorship for regional or national cyber security exercises,
- coordinate with external agencies to enable a cyber security exercise/event,
- promote the educational benefits of cyber security exercises to academic institutions,
- support and disseminate research that furthers the goal of initiating and growing cyber security exercises, and
- explore the feasibility of developing a national-level competitive cyber security exercise.

This organization could have members representing a wide spectrum of interests and expertise, including technological, legal, academic, governmental, and commercial. A non-voting advisory board might include representatives of the federal government, corporations, or others.

Such a board might explore affiliation with another national organization such as the Institute of Electrical and Electronics Engineers (IEEE) or the Association for Computer Machinery (ACM). This would provide several benefits. First, the parent organization may be able to provide resources for the event execution. Second, university administrators might be more willing to support such an activity if it is "recognized" by a well-known and respected organization. An analogous event might be the ACM programming competition.

A number of workshop participants are already in the process of establishing a governing body (see Appendix 13). Once board members are elected, the governing body will turn its attention to collecting detailed information about existing cyber security exercises and developing rules and guidelines for a standardized cyber security exercise. Eventually, the governing body will explore how to link various individual exercises to create regional, national, or even international competitions.

A patent and trademark is being sought for the Cyber Defense Exercise (CDX) as implemented by the Service Academies, which may have legal implications for others organizing their own cyber security exercises or for a national exercise. Dan Ragsdale and Wayne Schepens filed the patent to protect the CDX as envisioned and implemented by the service academies and prevent misrepresentation of event sponsorship. They were both involved in the workshop described in this report and in its planning. Given the fluid legal situation here, organizations creating or describing a similar competition should probably avoid using the term "Cyber Defense Exercise". This report uses "cyber security exercise" throughout, except when specifically describing the Cyber Defense Exercise participated in by the service academies.

Conclusion

The workshop identified the various approaches taken in structuring cyber security exercises and illuminated the technical, legal, ethical, educational, and financial considerations involved. The consensus was that such exercises are worthy of the considerable effort required to plan and implement them. Creating a standard structure for cyber security exercises would have multiple benefits: it would provide a framework that would enable more institutions to initiate an exercise, allow students from schools of all sizes to compete against one another, and pave the way for regional and national competitions. One key missing item was a governing body. The development of a governing body will facilitate the creation of rules and guidelines; a governing body will also foster communication, promote the benefits of cyber security exercises, and provide support for institutions.

Acknowledgments

This workshop would not have taken place without the hard work of several individuals. A steering committee met well in advance of the event and then was involved in a continuous email meeting to set the agenda (Appendix 2) for the workshop and to determine and invite the individuals who ultimately attended. That committee was

composed of the co-principal investigators (Lance Hoffman and Dan Ragsdale), their colleagues immediately supporting them (Tim Rosenberg and Ron Dodge), Wayne Schepens, Doug Jacobson, and Venkat Pothamsetty. Their affiliations are given in the roster of attendees in Appendix 1. Tony Stanco of The George Washington University and Hun Kim of the Department of Homeland Security contributed as members of this group also, but were unable to attend the actual workshop. Gale Quilter was in charge of the logistical arrangements, assisted by Kevin Guerrieri. Dana Trevas wrote the first draft of this report and also provided editorial support. Sujit Rathod coordinated the final manuscript preparation.

Work on this project was supported in part by National Science Foundation grant 0342739.

Appendices

Appendix 1. Cyber Security Exercise Workshop Participants

PARTICIPANT LIST

February 26 – 28, 2004
La Mansion del Rio Hotel
San Antonio, TX

George Bakos
Senior Security Expert
Institute for Security Technology Studies
Dartmouth College
45 Lyme Road, Suite 104
Hanover, NH 03755
Phone: 603-646-0665
Fax: 603-646-0666
Email: gbakos@ists.dartmouth.edu

Matt Bishop
Associate Professor
Department of Computer Science
University of California, Davis
One Shields Avenue
Davis, CA 95616-8562
Phone: 530-752-8060
Fax: 530-752-4767
Email: bishop@cs.ucdavis.edu

George Chamales
Student
University of Texas at Austin
711 B. W. 35th
Austin, TX 78705
Phone: 512-565-0507
Fax: 512-475-6183
Email: george@overt.org

Keri Chisolm
Assistant Network Administrator
Mississippi State University
Computer Science and Engineering
PO Box 9637
Mississippi State, MS 39762
Phone: 662-325-1518
Fax: 662-325-8997
Email: kchisolm@cse.msstate.edu

Art Conklin
Student
University of Texas at San Antonio
6900 N Loop 1604 West
San Antonio, TX 78249
Phone: 210-379-3671
Fax: 210-458-6311
Email: aconklin@utsa.edu

David A. Dampier
Assistant Professor
Mississippi State University
Computer Science and Engineering
PO Box 9637
Mississippi State, MS 39762
Phone: 662-325-8923
Fax: 662-325-8997
Email: dampier@cse.msstate.edu

Ronald Dodge
Director, Information Technology and Operations Center
Department of Electrical Engineering and Computer Science
West Point
601 Thayer Road, Room 109
West Point, NY 10996
Phone: 845-938-5569
Fax: 845-938-3807
Email: Ronald.dodge@usma.edu

Charles Wesley Ford, Jr.
Chairman
University of Arkansas at Little Rock
2801 South University
Little Rock, AR 72204
Phone: 501-569-8134
Fax: 501-569-8134
Email: cwford@ualr.edu

J.D. Fulp
Lecturer
Naval Postgraduate School
833 Dyer Road
Monterey, CA 93943
Phone: 831-262-4855
Fax: 831-656-2814
Email: jdfulp@nps.navy.mil

Derek Gabbard
Chief Technology Officer
CDXperts
PO Box 7904
Ann Arbor, MI 48107
Phone: 734-604-0204
Fax: 734-367-0458
Email: Derek@cdxperts.com

Seymour Goodman
Professor, International Affairs and Computing
Co-Director, Georgia Tech Information Security Center
Georgia Institute of Technology
781 Marietta Street, NW
Atlanta, GA 30332-0610
Phone: 404-385-1461
Fax: 404-894-1900
Email: Goodman@cc.gatech.edu

Lance J. Hoffman
Distinguished Research Professor
Computer Science Department
The George Washington University
Washington, DC 20052
Phone: 202-994-4955
Fax: 202-994-4875
Email: lanceh@gwu.edu

Doug Jacobson
Director, Information Assurance Center
Iowa State University
2419 Coover Hall
Ames, IA 50011
Phone: 515-294-8307
Fax: 515-294-8432
Email: dougj@iastate.edu

Willis Marti
Associate Director for Networking
Texas A & M University
Teague, MS-3142
College Station, TX 77843-3142
Phone: 979-845-0372
Fax: 979-847-8643
Email: wmarti@tamu.edu

Clifford Neuman
Director, Center for Computer Systems Security
USC Information Sciences Institute
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292
Phone: 310-822-1511
Fax: 310-823-6714
Email: bcn@isi.edu

Venkat Pothamsetty
Software Engineer
Cisco Systems
12515 Research Boulevard
Austin, TX
Phone: 512-378-1675
Email: vpothams@cisco.com

Daniel Ragsdale
Director, Information Technology Program
Department of Electrical Engineering and Computer Science
West Point
West Point, NY 10996
Phone: 845-938-4628
Fax: 845-938-4628
Email: daniel.ragsdale@usma.edu

Tim Rosenberg
Associate Research Professor
Computer Science Department
The George Washington University
Washington, DC 20052
Phone: 202-994-9516
Fax: 202-994-4875
Email: trosenbe@gwu.edu

Anthony Ruocco
Associate Professor
School of Engineering
Roger Williams University
One Old Ferry Road
Bristol, RI 02809
Phone: 401-254-3334
Fax: 401-254-3562
Email: aruocco@rwu.edu

Wayne J. Schepens
Founding Partner
CDXperts Inc.
504 Heavitree Garth
Severna Park, MD 21146
Phone: 410-987-4484
Fax: 410-987-4484
Email: wayne@cdxperts.com

Ryan Smith
Student
University of Texas
2606 Rio Grande, Apt 203
Austin, TX 78705
Phone: 972-814-8968
Email: ryansmith@mail.utexas.edu

Erich J. Spengler
Principal Investigator
NSF Regional Center for Systems Security and Information Assurance
10900 South 88th Avenue
Palos Hills, IL 60465
Phone: 708-288-5361
Fax: 708-974-0078
Email: spengler@morainevalley.edu

Anthony V. Teelucksingh
Trial Attorney
Department of Justice/CCIPS
128 Overbrook Road
Baltimore, MD 21212
Phone: 202-514-1026
Fax: 202-514-6113
Email:Anthony.teelucksingh@usdoj.gov

Krizi Trivisani
Chief Security Officer
The George Washington University
44983 Knoll Square Drive, Suite 339
Ashburn, VA 20147
Phone: 202-345-2182
Fax: 703-726-3622
Email: krizi@gwu.edu

Giovanni Vigna
Assistant Professor
University of California, Santa Barbara
Department of Computer Science
Santa Barbara, CA 93106
Phone: 805-893-7565
Fax: 805-893-8553
Email: vigna@cs.ucsb.edu

Donna Warwas
Computer Security Engineer
Air Force Information Warfare Center
402 Greig Street, Building 179
San Antonio, TX 78226
Phone: 210-925-3749
Fax: 210-925-5087
Email: donna.warwas@lackland.af.mil

Gregory B. White
Director
Center for Infrastructure and Security
University of Texas
6900 North Loop 1604 W
San Antonio, TX 78249
Phone: 210-458-6307
Fax: 210-458-6311
Email: gwhite@utsa.edu

Appendix 2. Workshop Agenda

Thursday, February 26, 2004

1800-2100 Reception

Friday, February 27, 2004

0800-0810 Welcome
Lance Hoffman and Dan Ragsdale, co-Principal Investigators

0810-0815 Meeting logistics
Gale Quilter, meetingsguru.com

0815-0845 Self-introductions

0845-1000 Cyber Defense Exercise to Date: Lessons Learned
History of CDX
Possible future directions for similar exercises
Formal assessment
Do's and Don'ts
Dan Ragsdale
Legal issues
Anthony Teelucksingh
Technical issues
Wayne Schepens

1000-1015 BREAK

1015-1100 Reactions and Raising of Any Missed Issues

1100-1130 Discussion

1130-1145 Assignments to Working Groups

1145-1200 Charges to Working Groups (chairs and reporters designated before meeting)

1200-1300 WORKING LUNCH

1300-1500 Working Group Meetings
1. Venue, duration, and refereeing
2. Use of the actual Internet
3. Eligibility, governance, costs, and prizes

1500-1515 BREAK

1515-1600 Presentations of WG meeting results (1-5 slides each, 10 min. each)

1600-1700 Discussion of these results
"Collection" of slides "published", available to attendees by 1900

Saturday, February 28, 2004

0800-0900 Reactions to "Collection of slides" and WG meeting results

0900-0930 Reorganizing Working Group topics and composition

0930-0945 Charges to New Working Groups

0945-1000 BREAK

1000-1200 New Working Groups (4-6) meet

1200-1300 LUNCH

1300-1345 Presentations of New Working Group meeting results

1345-1445	Reactions to new WG meeting results
1445-1900	FREE TIME FOR MOST ATTENDEES (during which early draft visual presentation of workshop results is created by Steering Committee)
1900-2200	WORKING DINNER
	2000-2030 Early Draft Presentation of Workshop Report
	2030-2100 Feedback to Early Draft
2200	Adjournment

Appendix 3. United States Military Academy Cyber Defense Exercise (CDX)

The CDX has developed into an extraordinary educational experienced for the students and midshipmen who take part in the exercise. It provides an excellent capstone exercise for these students during which their knowledge of information assurance concepts and their skills in protecting and defending information systems are assessed in the context of realist, true-to-life scenario. During the four years that this exercise has been conducted three significant benefits emerged; education, leadership development, and research opportunities.

The CDX provides three significant benefits; education, leadership development, and research opportunities. The comments provided during after action reports and summary papers unanimously stated that the educational experience provided by the CDX was one of the most rewarding experiences while in school. The participating students, seniors in their fifth semester of concentrated study in Computer Science, begin the semester by analyzing the problem and follow up with a network design, an implementation of that network, their own vulnerability assessment, and then the four-day exercise. Their implementation includes major applications requirements (web pages, electronic mail, databases, video conferencing, desk top applications) as well as a robust infrastructure (DNS services, bridges and routers, a honeynet, a firewall, a proxy server, an intrusion detection capability and a backup and recovery facility).

These student activities build on and use every aspect of their by-then five semester computer science education – a program whose initial emphasis is on foundational knowledge and skills that are then reinforced by numerous project-oriented applications. They have not been trained in the particular technologies they now confront. From Linux to MAC OS X, from firewalls to DNS servers to file servers, from email to web servers, this exercise demands that they quickly learn the strengths and weaknesses of their assigned network component, identify threats and vulnerabilities, assess risk, find and apply safeguards. They learn what they have learned in this curriculum: to "drop down" into an unfamiliar situation and learn what they have to learn, fast.

As computer science majors, the students had taken the list of required theoretical and programming courses but were never presented real world problems that were dynamic in nature. For example, each student at some point was required to develop a database. While this is certainly a task they will perform in the real world at some point, it is very static and "canned". The Cyber Defense Exercise presented the students with a dynamic environment where they needed to respond to the changing tactics and techniques of a very skilled live opponent.

As important as this exercise was as the application of their intensive five semester computer science education, perhaps it is more significant as the culmination of their eight semester education in leadership. Military academies place a heavy emphasis on leadership. As with the educational rewards, the exercise leadership was cited in after action reports as one of the participants' most challenging leadership experiences. This is a significant statement given that the academies are designed to challenge the students

from the day they arrive to the day they graduate. In 2004, 32 students organized themselves in two short months to design, build and defend a complex network. The intricacies involved in leading a large group of students in an exercise where most are applying new skills are a large challenge even for experienced leaders.

The third area of tremendous usefulness and potential is in research. The exercise provides the opportunity to evaluate new and existing technologies and policies, conduct human interaction and management research, and forensic analysis. The typical exercise results in a tremendous amount of data from application, host, network, IDS and firewall logs.

The exercise also produced two unexpected benefits. First, the coordination during the exercise by members of the "attack" team, who normally do not work together, provided insight into complimentary procedures. Second, since the skill and the knowledge levels of the participants has improved so dramatically over the past four years, the CDX has become an excellent testing ground for new and emerging concepts in information assurance.

More information regarding the USMA CDX can be found at www.itoc.usma.edu/cdx.

Appendix 4. University of Texas Cyber Security Exercise

We believe that the best way to defeat your enemy is to think like your enemy, and then use that foresight to stay one step ahead of them. We have incorporated this ideal as the main focus of our capture the flag exercises. Our exercises give us an opportunity to reinforce the security practices taught in our class lectures, by allowing students to gain first hand experience using blackhat tools and tactics to exploit security weaknesses in a secure and monitored environment.

The architecture of our exercise is setup to allow students access to the target network through an *ssh* gateway. While ideally we would like the network to be completely separated from the Internet, we've found it just isn't practical. Depending on their complexity, our exercises can span anywhere from a week to two months or beyond. Also, all of our participants are all undergraduate students and participate on a completely volunteer basis. So they don't always have a lot of time to dedicate, but they can drop into the network and work when they do have some free time. Our current setup has one gateway/firewall machine that only allows *ssh* in, and drops all outbound attempts. Each team has their own attack computer on the network. They have full control of this computer, which they are also responsible for protecting from the other teams.

Once the competition starts, a team is provided the address of the target network and a list of objectives. The competition ends after all objectives are completed. Each team earns points based on the objectives they've completed, and how well they've documented and reported their activities. Invariably each round, students will come up with different creative attacks on both the target network and the other teams' computers, and they will receive bonus points depending on the originality and difficulty of the attack. Administration and judging of each round is carried out by the same person who designed the round, an undergraduate senior.

The scenarios may range anywhere from a single host with a software vulnerability to a complex e-commerce environment with a firewall, IDS, and honeynet. The vectors of attack change with every round of our competition, but the topics we've covered have included buffer overflows, heap overflows, SQL injection, weak passwords, directory traversal, *ssh* vs. *telnet*, and the principle of least privilege, just to name a few.

Rules have been the toughest thing to evolve over the years. When the participants first get the rules, they will hold them up to the light, find all the holes and use those holes to their full advantage. There are two ways that we found to deal with this: try and find all the holes and have a large comprehensive rule set, or have a very simple rule set whose spirit encompasses all the holes. We chose to do the latter of the two. We have made our environment as "self-enforcing" as possible; our only rules are that you can't commit any denial of service acts, and you can't try to circumvent the outbound restrictions of the network to access the Internet.

Appendix 5. University of California, Santa Barbara, Cyber Security Exercise

The Capture the Flag contest is a multi-site, multi-team hacking contest in which a number of teams compete independently against each other.

This exercise is the latest of a series of live exercises organized as part of the graduate course on "Network Security and Intrusion Detection" taught at UCSB by Professor Giovanni Vigna. Previous versions of this exercise are described in the paper: G. Vigna, "Teaching Hands-On Network Security: Testbeds and Live Exercises," Journal of Information Warfare, vol. 3, no. 2, pp. 8-25, 2003.

The most recent live exercise was different because instead of having the students of the class compete against each other, it involved different teams at different universities and institutions. The exercise is loosely based on the DEFCON "Capture the Flag" contest. This exercise is different from the DEFCON contest because it involves several educational institutions spread across the nation. The DEFCON contest includes locally connected teams only. In addition, the DEFCON contest has always involved a limited number of teams. We developed a new network solution that allows a large number of teams to participate.

The goal of each team is to maintain a set of services available and uncompromised throughout the contest phase. Each team can (and should) attempt to compromise other teams' services. The services to be provided are implemented as part of an operating system installation running as a VMware image. Each service has a number of associated flags. Initially, the flags are set to the flag of the team that set up the VMware host. The goal of each team is to keep their flag uncompromised, while trying to change the flags of other teams to their own.

During the contest phase of the exercise, the scoring software connects periodically to each service and checks the corresponding flag values. If the service is not available, the team receives no points. If the service is up and the flag is the flag of the team managing the host, the team gets some points. If the service is up but the flag is set to the one of another team, the other team gets some points.

Note that each time a flag is tested its value is substituted with a new value computed by applying a secret hash function to the original value. Therefore, simply rebooting a host on a regular basis will not grant points since the hash value will be restored to the original value at each reboot.

Rules

It is not possible or feasible to list all the rules and the exceptions to rules that apply. When deciding if an attack/protection technique is fair or not, students are urged to think about the fact that the goal of this exercise is to learn about protecting/attacking a system in a live situation. They are encouraged not to focus on "breaking" the scoring system,

but instead to concentrate on developing/deploying effective (and realistic) defense and attack techniques.

Below is the current list of rules. These rules might be changed during a particular instance of the competition, as more issues are raised by the participants.

- It is forbidden to launch denial-of-service (DOS) attacks. This is particularly critical, given the limited duration of the exercise (4 hours). No floods, no DNS poisoning, no obviously destructive behavior.
- Excessive traffic generation will be penalized, whether or not the traffic is part of a DOS attack. Generating traffic from a host that a team has compromised to penalize the owner team is considered unfair practice.
- It is possible to patch the services, provided that the patch is made available to the organizers by sending an email to them. This will allow the organizers to make sure that a patch will not block the scoring system. If this is not done, the services will be considered as non-functional.
- The scoring mechanism will access random pages at random times, in addition to checking for the flag values. Blocking access to the service functionality that is not associated with flag verification is equivalent to having the service not available.
- It is not possible to perform attacks outside the VPN. For example, attacking a team's VPN router using its routable address (i.e., the address that is visible on the Internet) is not allowed. All the traffic for the exercise must be contained within the VPN.
- It is allowed to attack any host of a team's subnetwork. The attacks are not necessarily limited to the host system provided by the organizers. For example, if one compromises the target system of Team 1, he/she may try to compromise the host that is running the VMware application.

More information regarding the UCSB Capture the Flag Exercise can be found at http://www.cs.ucsb.edu/~vigna/CTF/.

Appendix 6. Texas A&M Cyber Security Exercise

Advanced Networks and Security, CPSC 665, is a graduate level course to educate students about aspects of computer security important to future administrators. Part of this course is a semester-long hands-on exercise that gives students greater insight and understanding of the nature of computer security issues by allowing attempts to penetrate a live, but isolated, network environment. Students role play as normal users or attackers or system administrators and class discussion emphasizes understanding from multiple points of view.

A single *gold team* sets up a network of hosts offering services consistent with those offered by a university network. With this in place several *black teams* attempt to circumvent security features of the network. The ultimate goal of a black team is to gain control of a host with out being detected. Black teams are assigned hosts outside the 'campus', but are also given user accounts on the department systems.

The *platinum* team, consisting of two faculty and support staff, serves as referees and guides for both black and gold teams. The gold team is formed by selecting key individuals in the semester prior to preparation. Additional members are added once class starts, based upon their expertise in network administration. The gold team administers the sandbox network and is responsible for defending the systems while still providing required services.

Law prohibits attempting to compromise hosts. Therefore special care must be taken with this type of exercise so that actions taken by students do not affect hosts outside of the exercise. To facilitate this separation a *sandbox* network has been constructed in the Network Engineering Lab. This is a reference to the measures taken to enclose the network in a manner that ensures "safety" and isolation. This access point is setup to prevent any actions in the sandbox from escaping the exercise. Network monitoring is also done at this point to ensure students are acting within the guidelines of the class. These are important aspects, to maintain a continuation of this course.

It is important for students to be able to distinguish the transition from public or academic networks where the activities encouraged in this class are not only prohibited but can raise criminal charges. Thus, mechanisms for protecting the students from inadvertently sending attacks to network nodes outside of the sandbox are critical, as well as preventing real life hackers from using the sandbox as an attack platform. The sandbox is intended to emulate a computer science department on a typical campus and is broken up into 3 logical networks: the Black (Internet), Campus, and Department networks. Not shown are systems used as traffic generators. This was done to lessen the artificiality of all traffic being security related. At semester's end, each team presents its activities and lessons learned.

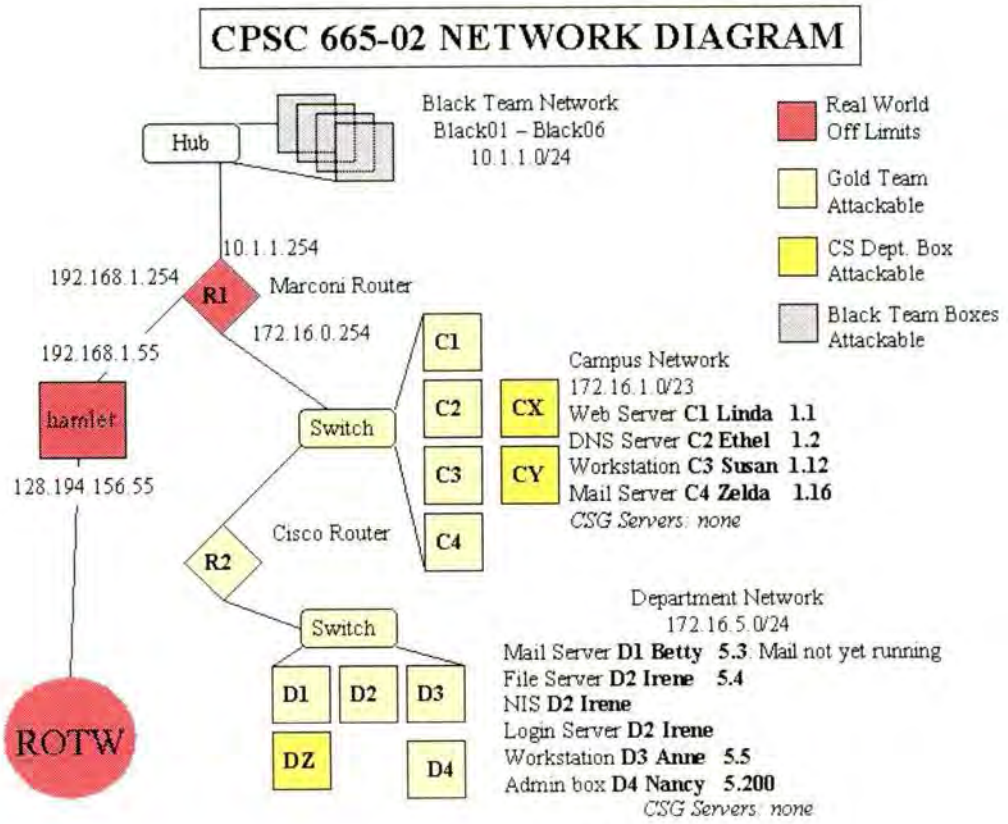


Figure 1 Network Layout

Appendix 7. The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education

THE CYBER DEFENSE EXERCISE: AN EVALUATION OF THE EFFECTIVENESS OF INFORMATION ASSURANCE EDUCATION

Wayne J. Schepens
National Security Agency
Information Technology Operations Center
United States Military Academy

West Point, NY 10996
Wayne-Schepens@usma.edu
845-938-7674

Daniel J. Ragsdale, John R. Surdu
United States Army
Information Technology and Operations Center
United States Military Academy

West Point, NY 10996
{dd9182 | dj6106}@usma.edu
845-938-2056/2407

Joseph Schafer
United States Army
U.S. Naval War College
Newport, RI
kj6rl@arrl.net
401-848-6200 x3816

ABSTRACT

The US Military Academy at West Point issued a challenge to the five United States service academies to participate in an inter-academy Cyber Defense Exercise (CDE). This exercise was initiated and implemented by faculty and cadets assigned to the US Military Academy, West Point, with funding and direction provided by the National Security Agency. The concept of "defending the network" was derived to evaluate cadet skills and the effectiveness of the Information Assurance (IA) education invoked at West Point. The Cyber Defense Exercise served as the final project for senior-level Computer Science majors enrolled in the Information Assurance (IA) course. The IA - Service Academy Group for Education Superiority (IA-SAGES), a group formed to plan, develop and share IA curriculum, proposed that all US service academies teaching an IA course participate in the exercise. The US Air Force Academy and US Military Academy accepted the challenge to compete in 2001.

The *distributed* facility in which this exercise will be conducted is known as the Cyber Defense Network (CDN). It was designed and developed by a West Point cadet (student) team, and is an extension of the Information Warfare Analysis and Research (IWAR) Laboratory. To understand the function of the CDN, it is necessary to understand all the resources at the disposal of USMA for IA education.

The IWAR Laboratory is an isolated laboratory used by undergraduate students and faculty researchers at the US Military Academy. It is a production-like, heterogeneous

environment and has become a vital part of the IA curriculum at West Point. The military range analogy is used to teach the students in the class that the exploits and other tools used in the laboratory are weapons and should be treated with the same care as rifles and grenades. This paper describes the structure of the laboratory and how it is used in classroom instruction. It describes the process used to create the IWAR and the Cyber Defense Exercise (CDE). Finally, this paper describes the concept of the 2001 Cyber Defense Exercise and expectations for future participation.

INTRODUCTION

The Information Technology and Operations Center (ITOC) is a focal point for Information Assurance education at USMA. Soon after its creation in 1999, the ITOC built the Information Warfare Analysis and Research (IWAR) Laboratory. This facility was designed to support undergraduate education and faculty research at West Point. It was developed with the thought in mind that, one day, each US Service Academy would have similar resources and curriculum in which to train; therefore, representatives from the service academies created the Information Assurance – Service Academy Group for Education Superiority (IA-SAGES) in June 2000.

The mission of this working group is to share IA curriculum, resources, and experiences in order to align each academy's IA program in a similar fashion. The service academies are training the future leaders of America, who in their future roles will rely daily on the integrity of information. The founders of the IA-SAGES conceived a Cyber Defense Exercise (CDE) in which participating academies would match information assurance wits against one another. Several hurdles had to be overcome to make this a reality; however, the concept was quickly accepted. This exercise serves as a real-world educational experience, and the inter-service rivalry generates interest in the growing field of IA.

This report describes how the CDE became a reality, the development of the Cyber Defense Network (CDN) to support the CDE, and the plans for its first execution. It describes the vital role that the IWAR Lab plays in teaching information assurance and preparing undergraduate students majoring in computer science to "defend the network" against professional security evaluators, known as Red Teams.

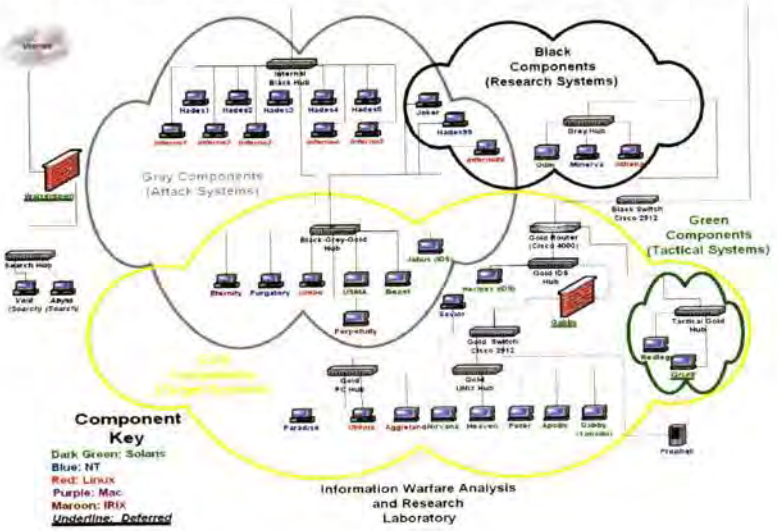


Figure 1: IWAR Laboratory

BACKGROUND

The nation that will insist upon drawing a broad line of demarcation between the fighting man and the thinking man is liable to find its fighting done by fools and its thinking by cowards. - Sir William Butler, 1874

The U.S. military is rapidly changing to take advantage of information technology from the Army's Advanced Warfighting Experiments to the Navy's Network-Centric Global Wargames. Tomes argues that we are so far ahead, no adversary will threaten us with information warfare for twenty years [1]. Carver counters that, although we have the tools to defend ourselves, we are not using them, and we are blundering toward another Pearl Harbor [2]. The fact that nearly half of the nations employed in U.S. Y2K remediation efforts have been identified as using offensive information warfare supports Carver's pessimism [3]. George Surdu, Global Director of Information Systems, Technology, and Services at Ford Motor Company, said that most of Ford's Y2K code was written in India and Israel [4]. The wide dissemination of hacker tools, lack of designed-in security in virtually all Department of Defense (DoD) information systems, and increasing DoD use of commercial communications infrastructures makes the prospect of asymmetrical threats horrifying. Each day it becomes increasingly plausible that young hackers working for a foreign power could cripple critical information systems. Recently the Army has placed as much emphasis on defending its information infrastructure as it had spent on Y2K remediation [5].

History teaches us that "technology permeates warfare," but the technological advances do not necessarily govern or even influence strategy and tactics immediately [6]. The mission of the U.S. Military Academy is to prepare future military leaders. A basic technical literacy is required of all cadets. For computer science majors, one of the most popular courses is the Information Assurance (IA) course. The goal of Information Assurance education at West Point is to improve awareness of security issues associated with information system. To this end, cadets get a broad appreciation for the policy and ethical considerations of Information Operations along with a strong grounding in the hands-on, technical aspects.

INFORMATION ASSURANCE COURSE OBJECTIVES

Upon graduation, all cadets are commissioned as officers in the U.S. Army. Many of them will be responsible for the security of critical Army information systems. The IA course, therefore, is designed to provide a firm foundation in the fundamentals of information assurance. With this foundation, recently commissioned lieutenants have in their toolbox the intellectual skills needed for continued self-education.

The protection and defense of physical locations is a notion with which all cadets are comfortable. All cadets have had the benefit of no less than three years of military training and education by the time they take the IA course. A tenant of military planning and operations from as long ago as Sun Tzu and Julius Caesar is that knowing the tools, tactics, vulnerabilities of ones opponent as well as oneself leads to victory [7]. To

establish an effective defense you must have a good understanding of your own vulnerabilities. In addition, you must be aware of the techniques that your adversary might employ to exploit those vulnerabilities. These ideas have direct applicability in the cyber domain.

In the IA course, cadets learn many offensive techniques. Cadets write malicious applets and viruses. They use port scanners, network sniffers, and vulnerability scanners to find the holes in a system's defenses. They use scripts, Trojan horses, and other tools to gain root-level access to target hosts. The purpose of all this familiarization, however, is not to make them hackers. The purpose is to give them an appreciation for the tools used by potential adversaries as well as the vulnerabilities of currently fielded or commercially dominant information systems and how those vulnerabilities might be exploited. Information ethics are emphasized throughout this learning process to strengthen moral character.

For the IA course to be successful, it is necessary to provide an environment that facilitates active learning and provides maximum opportunity for hands-on experiences for the cadets [8]. It was quickly determined, however, that nearly all of the tools and capabilities needed for this hands-on experience could not be installed in any of the general-purpose computer laboratories for both legal and practical reasons. This led to the creation of an Information Warfare Range, like those used for conventional weapons training.

Once the IWAR Range was developed, it was time to create the "sandbox" for actual wargames to be held. Since the goal from the onset of this IA course has been to educate in the context of defense, defense of a network would be the objective for the wargame. The sandbox needed to consist of a network that would mimic the function, form, and fit of an information infrastructure used to support a base or organization in which a future lieutenant might be assigned. After learning various offensive and defensive techniques throughout the semester, cadets would be assigned to defend the network, while professional Red Teams would remotely access, attack, and identify vulnerabilities associated with the system. This Cyber Defense Exercise would serve to not only test their defense skills but also to allow the faculty to evaluate the effectiveness of their education.

IWAR RANGE

As part of their training, cadets are taught the military concepts of offense and defense as well as tactics like reconnaissance and "defense in depth." Additionally, by the time they are eligible for the IA course they will have had significant basic classroom and field military training experiences. This training includes familiarization and/or qualification with various weapons systems on weapons ranges. These ranges provide a safe and authorized location to conduct training. Leveraging this knowledge, the IWAR Laboratory is introduced to the cadets as an IWAR range. While the IWAR Laboratory (Range) also facilitates faculty research, this paper focuses on the laboratory itself and how it supports the IA course.

By describing the IWAR as a range, instructors leverage several important concepts from conventional weapons training. First, the range is a special, isolated space. Just as one may fire automatic weapons on a rifle range at various targets and launch missiles at other targets, so too can cadets launch cyber attacks from their firing position (cadet computer terminals) at the IWAR Range target computers (also within the isolated laboratory). Second, it is unthinkable to fire an automatic weapon at a crowd of people from one's barracks room; it should also be unthinkable to use any of the cyber attacks from one's barracks room - *or anywhere outside the IWAR laboratory.*

Recall that the IWAR is a completely isolated laboratory with no physical connection to the outside world.

The IWAR Laboratory is divided into four networks. The Gray network is the "attack" side of the network. Cadets have their workstations on the Gray sub network. Each cadet team has one host workstation, but each workstation uses VMware to run various operating systems on the same physical machine. These operating systems include Window 2000™, Windows NT™, Window 98™, and Redhat™ Linux. Cadets have Administrator and root accounts in each of these environments. They also have user accounts on all other Gray sub network machines. An example of how these systems are used for instruction is this: for an in-class exercise cadets use their Windows NT™ virtual machines to download a malicious applet from their Linux virtual machine on the same physical hardware. The malicious applet then does "bad things" to the Windows NT™ machine. Also, on the Gray network are servers on which the cadet teams have user-level accounts. These "low-hanging fruit," fruit that is easy to take off the tree, allow the cadets to launch "insider" attacks.

The Gold network hosts the target systems. These are a series of Unix (Solaris™ and Irix™), Linux, Windows NT™, and Macintosh™ workstations and servers. Several machines are Gray/Gold, meaning that they are targets, but they are on the Gray subnet and thus "low-hanging fruit." Except for those machines that are also Gray, users do not have accounts on Gold machines. This makes attacking these hosts harder. In addition, Gold machines are on the other side of routers, switches, and firewalls, again creating a realistic heterogeneous environment. The Gold network helps cadets appreciate the capabilities and vulnerabilities of firewalls and routers. Also wrapped in the Gold sub network is the Green sub network on which tactical command and control systems are attached.

Faculty members use the Black network for information assurance research. Due to the placement of the machines and the switch (shown in the topology), researchers can work on both offensive and defensive projects on the Black network.

Two machines in the laboratory are not connected to any of the IWAR networks. Cadets use these machines for hunting the Internet for offensive and defensive tools. They can then copy these tools to disks and hand-carry them to an IWAR Range machine. Cadets physically remove these Internet connected boxes from the network when not in use. This

isolation, along with some other techniques, reduces the likelihood that external hackers will compromise these machines. In this way the IWAR Range should avoid having these systems serve as launching points for attacks against other Internet resources.

Together the sub networks that make up the IWAR Range provide a valuable resource for teaching cadets how to defend systems against attackers. The Gray network allows cadets to get an appreciation for insider attacks while the Gold network gives them an appreciation for outsider attacks. The Green network allows cadets to explore the vulnerabilities of Army tactical systems. Finally, the Black network allows faculty to conduct research in the same isolated facility.

THE "MAKING OF" IWAR

All four of the isolated and non-routable networks comprising the IWAR form a realistic, production-like environment of heterogeneous systems. Initially four criteria constrained the design of the range. First, the design must allow minimal possibility of misuse for damage to other systems. Second, on-hand resources should be used whenever possible. Third, time was limited. Finally, the laboratory needed to fit into one classroom.

After investigating several possible designs involving all manner of access controls and firewalls, we decided that the most expedient and least risky method of reducing the possibility of misuse would be to electrically and physically isolate the range from all other networks. In our worst nightmares we envisioned a New York Times headline, "Network Attack Lab at West Point used to destroy XX," where XX is your favorite external site.

On-hand resources were used because of constraints on both time and money. The primary means of achieving these goals was to use "rescued machines." These machines were those that were five to ten years old and that the administrators had removed from main production use after replacing them with newer models.

The West Point Department of Electrical Engineering and Computer Science maintains a "Tech Area" where many of these old machines awaited turn-in and donation to other organizations. We rescued several of these machines to form the core or our initial IWAR. Typical of these machines were a dozen generic, 60MHz Pentium boxes with old monitors and four SUN IPC and IPX boxes.

This rapid initial success helped identify several "underutilized" machines with which to augment the IWAR. These machines consisted of three old SGI computers that had been early Web and graphics servers and two old, dual-processor, Pentium servers that had been used for domain controllers and file servers on the Gray and Gold Windows NT™ domains. Support personnel located some equipment that had been procured for old projects, such as networking components and an Imac, that were transferred into the lab.

Since the IWAR Range is completely isolated, a more secure method for the students to access resources on the Internet was needed. The goal was that the cadets should be able

to search for and download information from even the most untrusted of sites without risking damage to any other systems. Two 90 MHz Gateway PCs, loaded with a very limited and secure version of Linux serve this purpose. Forcing the user shell to Netscape and requiring the presence of a Zip disk as the home directory further secured these computers. In addition, these two *Search boxes* are connected to the Academy network through a production firewall donated by the Academy's Directorate of Information Management.

Of greater concern was the risk that the IWAR network would be compromised and used to attack external sites than the possibility that someone would gain access to the limited resources on these search boxes. The search boxes are easily rebuilt from a *ghost* image since there are no home directories on the hard drive. The Zip disk was chosen since it would allow a relatively simple method of transferring files downloaded from hacker sites into the isolated IWAR range. Zip disks are also not in widespread use throughout the rest of the Academy, thus reducing somewhat the chance that someone would transfer these weapons to the main networks.

Early enthusiasm and achievements in the IWAR garnered some scarce dollars that were used to upgrade some of the rescued machines and procure essential networking, upgrading, and space-saving components. Rescued or redirected networking components included mostly inexpensive hubs. Primarily due to space considerations each cadet team uses a single hardware system, loaded with a variety of operating systems running in virtual machines.

Running many virtual machines on a single hardware platform significantly consumes memory and CPU cycles. New motherboards, memory, and Zip drives in the Gray machines helped to improve the performance of these machines from dismal to acceptable.

The classroom in which IWAR Range resides had been previously separated into two sides by a divider with a door to the hallway from each side. The *attack* machines were located on one side of the solid room divider and the target machines were located on the other side. This close proximity but isolation of the attack and target machines simplified administration and setup of the lab. Additional administrative simplification was achieved by *ghosting* most of the systems and using Sun Microsystems administrative servers and tape backups to allow rapid reconstruction of the systems.

The most important space, power, and heat saving components were the use of KVM (Key, Video, and Mouse) switches for nearly all of the Gold target systems. In addition to space, heat and power proved to be huge constraints on the number of systems that could be reasonably set up in one classroom. With KVM switches, four sets of Keyboards, Mice, and Monitors provide interfaces for all 25 gold systems, significantly reducing the space, power, heat, and clutter on the Gold network.

In addition to a heterogeneous hardware environment, the IWAR provides a wide variety of production quality network applications and services. These include Domain Name

Service (DNS), WINS™, authentication and replication with Domain Controllers, Network Information Service (NIS), and NIS+. Also provided are web servers, mail servers, Network File System (NFS), Samba™, LanMan™, and additional services. Common production configurations were adopted. For example we ran Microsoft Internet Information Server™ (IIS) and Exchange on the Windows NT™ servers and Apache on the Linux and Sun servers.

The Gray/Gold servers were configured with old and unpatched versions of the operating systems (e.g., Redhat™ 2.1 and Windows NT™ 4 with no service packs applied) and applications. Additionally, these boxes were located on the Gray subnet on the same hub with the attack machines. The students also had user accounts on these servers. Thus, the students could log onto the Gary/Gold servers and easily sniff the network and attempt well-known exploits to upgrade their privileges from user to root or administrator. The Linux boxes and Linux virtual machines on the student's boxes participated in the Sun NIS Domain. The attack boxes were members of the Gray NT domain controlled by another Gray/Gold server.

Conversely, the main Gold boxes operated with the latest patches and versions of the operating systems (e.g., RedHat 7.0 and Windows NT™ 4 SP6a), patches, and applications. After gaining some confidence in attacking the "low hanging fruit" of Gray/Gold, students could move onto the "treetop fruit" of the Gold domain. NIS+ was used on the Sun and Linux boxes in the Gold domain. One of the first requirements of the course was for the students to map the entire network.

Students used a wide variety of tools and a shared home directory environment for all of the systems with which they had privileges. The shared environment was achieved with Windows NT™, Linux, and Sun logon scripts and NFS and SMB mounts. The students could easily transfer exploits from among any of their environments and use development tools from Linux, Sun, and Microsoft to compile their code. Finally, recognizing the relative difficulty of using the search boxes and the time constraints for undergraduate students in a Computer Science elective, numerous "hacker tools" were cataloged on a Gray/Gold site.

A lab of enormous complexity and heterogeneity emerged in a matter of weeks. Despite the time and resource constraints the entire IWAR range was built in four weeks and cost less than $20,000.

Since this initial development and preliminary upgrade, interest in this local, unique resource has risen both in academia as well as industry. Government and military organizations have provided funding to support ITOC research efforts, enabling the ITOC to perform a complete upgrade of the Grey network. For instance, each cadet in the IA course has his or her own workstation on the Gray network now.

IS IWAR WORTH THE EFFORT?

The creation of the IWAR involved significant time and resources. Weeks went into the design of the IWAR Range, and four more weeks were devoted to its construction. While the IWAR made extensive use of rescued hardware, it still cost $20,000 to get started. The question that should be asked is "does this expenditure of resources result in greater educational efficacy?"

There is great intuitive appeal to the notion that the hands-on experience provided by the IWAR Range is more effective than PowerPoint™ slides and white boards. When the cadets actually implement an attack or exploit they must also describe how they would defend against such an attack. Later in the course they must implement these defensive measures in securing a network against external attack. This not only provides practical experience as both an attacker and a defender but it exercises their ability to think critically, analyze, and synthesize.

The comments received in end-of-course critiques were statements like "A great course that will be very applicable to my future career. I am very grateful for the experience. Learning and experimenting was [sic] the best thing," [our emphasis] "Best course I have taken, hands down," and "[I learned] that nothing is secure [you need to be] careful of everything and anything you do." This end-of-course feedback provided anecdotal evidence of the efficacy of the course. The ITOC plans to conduct experiments to conclusively demonstrate this efficacy as future work.

Almost as soon as the IWAR was built and used to teach the Information Assurance class, other departments became interested in it. One semester after its completion, the Department of Social Sciences began teaching a course in the IWAR focusing on policy of cyber warfare. Because many cyber warfare policy makers are ignorant of the technology for which they are decreeing policy, a large component of this course at West Point involves hands-on orientation to a number of exploits, attacks, and defensive measures. Several times the Fundamentals of Information Technology course, a mandatory course for all Plebes (freshmen) has used the IWAR to emphasize a topic. More and more classes at West Point are considering making use of the IWAR Range in the future even if that use is only for one or two class periods.

HOW DID THE CYBER DEFENSE EXERCISE COME ABOUT?

Since the early stages of IWAR development, USMA had thought of initiating an inter-academy Cyber Wargame. These thoughts began to take shape during the first meeting of the Information Assurance – Service Academy Group for Education Superiority (IA-SAGES) in June 2000. Representatives from the US Military Academy (USMA), US Naval Academy (USNA), and US Air Force Academy (USAFA) explored the idea of establishing a network to host a Cyber Defense Exercise. It was agreed to focus on the defensive aspect of information operations as it aligned well with the goals of the IA programs being developed at the academies. It also directly related to the goals employed by the National Information Security (INFOSEC) Education and Training Program, which had instituted NSA Visiting Fellows within the USMA and USNA. It was,

therefore, decided to pursue the means to create the "sandbox" and begin to outline the logistics behind hosting such an event.

Shortly after this meeting, an unrelated request to the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) for resources to support research and education in Public Key Encryption resulted in a landfall of acquisitions. The PKI PMO offered to provide funding to supply USMA with a PKI lab to consist of ten Windows-based workstations and two Sun Servers. In return USMA would educate future officers in a system that is currently being deployed DoD-wide. Once the word was out the Naval Postgraduate School (NPS) and USAFA became interested in acquiring similar resources and the PKI PMO was quick to accommodate the request.

The delivery of the PKI lab equipment provide a means of furnishing all the members of the IA-SAGES with the resources they would need not only to perform PKI education, but also to support a Cyber Defense Exercise. The minimum computers, networking components, and software required at each of the five US service academies and NPS to support a PKI-enabled Cyber Defense Exercise were determined. This plan was proposed and the PKI PMO whole-heartedly endorsed the concept.

The Chairman of IA-SAGES then set out to convince the USNA, US Merchant Marine Academy (USMMA), and US Coast Guard Academy (USCGA) to participate in the exercise. USNA and USMMA agreed to accept the equipment with the expectation that they would require a year to ramp up their IA programs prior to participating in the Cyber Defense Exercise.

Funding was in place and the stage was set for the USMA, USAFA, and NPS to participate in the first Cyber Defense Exercise in the spring of 2001. The remaining tasks were to design and build the "sandbox", identify and coordinate the Red Teams willing to participate, and establish the execution plan for the 2001 event.

DESIGNING AND IMPLEMENTING THE "SANDBOX"

With continuing focus on educating cadets in the area of Information Assurance while employing a multi-disciplinary approach, the ITOC decided it was important to capture the learning experience associated with the gathering of requirements, design, and construction of the Cyber Defense Network (CDN). The effort was perfect for a non-Computer Science major Information Systems Design course capstone project. A project team made up of four students majoring in Economics, Geography, and International Relations were assigned this task. USAFA wished to participate in the development as well. As a result, they assigned a cadet majoring in Computer Science and enrolled in an independent study to join the USMA project team.

The USMA project team was tasked to: (1) design a network (Cyber Defense Network) include various operating systems, network services, databases, and applications typical of military and commercial information infrastructures; (2) provide secure, remote connectivity to the CDN for Red Teams; (3) ensure the CDN is electronically separated

from the academy backbone; (4) and provide installation instructions and ghost CDs so the identical configuration could be copied at all the participating schools. The CDN as delivered to each academy would be intentionally weak in IA safeguards. This would give students enrolled in the Information Assurance course and opportunity to practice their newly acquired skills in "defending the network". Cadets will have about two weeks to implement IA measures using what they have learned in their respective courses. An Internet-hosted Virtual Private Network, PKI-enabled and off-limits to the students during the exercise, would provide a way for Red Teams to evaluate the security posture each academy team achieved.

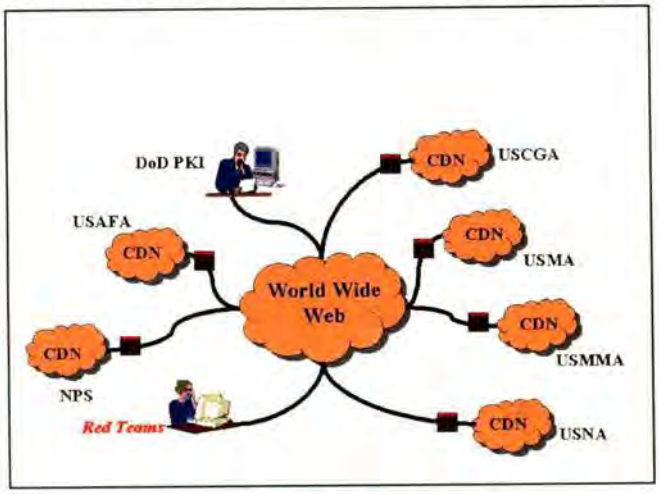


Figure 2: Inter-Academy Cyber Defense Exercise Conceptual Diagram

It is important to note that cadets developing the CDN will not participate in the Cyber Defense Exercise.

The cadet project team enthusiastically accepted ownership of this effort and went above and beyond what was normally required of capstone project teams. A Cyber Defense Exercise summit was held at the USAFA in January 2001, which served as a program review. The cadets delivered a briefing to the DoD PKI PMO, faculty involved with the CDE, and the US Air Force Red Team on their design and implementation plan. They gathered input to create draft Rules of Engagement (ROE) and outline the milestones associated with conducting the 2001 Cyber Defense Exercise.

The final Cyber Defense Network design consists of platforms running Sun Solaris™, Linux, Windows 2000™, Windows 98™, and Windows NT™ operating systems. Internet access is provided to allow for downloading the latest patches and software updates. These systems are configured to provide various services such as: IIS, ColdFusion™, database servers, Web servers, file servers, and

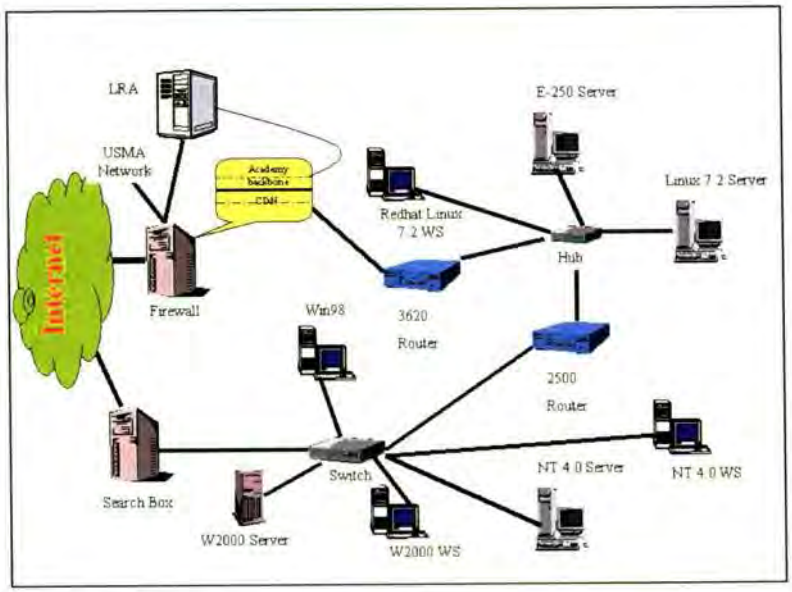


Figure 3: Cyber Defense Network Architecture

application servers. The final design for the VPN is still under development. The long-term solution is to use V-One Smartgate™ software in conjunction with a Gauntlet™ firewall hosted on a Sun Solaris™ platform. This will allow the DoD PKI to provide authentication and encryption between the CDN and the Red Teams; however, the current design relies on a series of CISCO routers to provide point-to-point encryption and authentication between each CDN and Red Team.

WHO WILL ATTACK?

The CDE concept involves independent parties to evaluate the performance of the cadets in securing the network. As early as September 2000, the 92nd Aggressor Squadron, US Air Force IWAR Center, Kelly Air Force Base, learned about the CDE through a chance meeting with an ITOC member at an IA conference. They immediately expressed interest in supporting as a Red Team. They briefed their organization and mission at the Cyber Defense Exercise summit, and they were accepted as a Red Team for the CDE. After a bit more coordination, they agreed to provide evaluation criteria that will be used to objectively determine a winner. They also indicated even if remote connectivity were not provided, they would be willing and able to support an on-site Red Team effort for each school.

After a briefing to the NSA Executive Command in January of 2001, the Defense Information Operations Group offered to provide a Red Team to support the exercise. This relationship has already proven to be of immense value. Due to problems each school encountered configuring the VPN, the NSA Red Team has taken the lead in establishing remote connectivity and has agreed to review and comment on the evaluation criteria provided by the 92nd Aggressor Squadron.

The third and final Red Team to join the exercise is from the Land Information Warfare Activity, US Army. In order to ensure the exercise is fair, each Red Team will attack each of the three participating schools during different time periods. They will each provide an independent final report and recommendation to the Cyber Defense Exercise Board. The Cyber Defense Exercise Board, made up of representatives from each US service academy, Red Team, and the NSA will decide the winner of the IA trophy.

EXECUTION OF THE 2001 EXERCISE

The overall mission of the CDE is to minimize the risk of a security breach while ensuring necessary operational services are maintained. It is also imperative, should a security breach take place, it does not go undetected. Cadet teams participating in the exercise are assigned to subordinate missions and will have four weeks to develop security implementation plans and ten days to work hands-on to secure the network.

During the Red Team attacks, the cadets will be required to electronically transmit the "Order of the Day" to all workstations within the Cyber Defense Network while maintaining confidentiality and integrity. This transmission must provide a system status and indication and evaluation of any known intrusion and/or attack. It is possible that the

Red Teams may introduce vulnerabilities while entering the CDN. Since the CDNs will not be manned by cadets 24 hours a day, any vulnerabilities introduced will be left for a period of time to give cadets the opportunity to search and record intrusions. Once this time expires the Red Teams will return the CDN to its original state for the next Red Team.

The cadets will be provided with system documentation including network diagrams, hardware and software resources, operating systems, and services included within the CDN. They will be encouraged to use this information, all they have learned in their studies, and any other ethical means at their disposal to immediately commence planning for the secure configuration of the CDN. In addition, they will be provided with the Rules of Engagement (ROE), which outlines the necessary operational services and limitations imposed to ensure fair competition.

No social engineering or attempts to introduce vulnerabilities into an opposing academy's infrastructure are authorized. This had to be addressed as the question arose from cadets, "...can we have insiders introduce malicious code to our opponents systems?"

Upon completion of the one-week attack period, the Red Teams will provide their independent After Action Reports (AAR) and recommendation to the Cyber Defense Exercise Board. The board will have one week to review and select a winner. The winning academy will be presented the NSA Information Assurance Director Trophy (currently under contract for procurement).

CONCLUSIONS AND FUTURE EXPECTATIONS

The US Military Academy, US Air Force Academy, and the Naval Postgraduate School will compete in the 2001 Cyber Defense Exercise. There is strong interest among faculty at the US Merchant Marine Academy and the US Naval Academy to compete in the future. Because NPS is a graduate program, it will not compete for the NSA IA Director's Trophy; however, since word has spread, there is interest in expanding the exercise to include graduate programs that are certified as Centers of Excellence in Information Assurance.

The NSA IA Director's trophy will be a traveling award and will reside with the winning academy for the academic year. This award will serve to advertise and generate interest among students nation-wide to learn about Information Assurance.

The results of the exercise will be out briefed by the Red Teams and discussed with each cadet team through a planned video teleconference. Results will also be evaluated to determine how well prepared the cadets were for the exercise. This information will serve as feedback to make future improvements to the IA course. It will also be valuable to see how the cadets perform as compared to real-life operational organizations undergoing similar Red Team evaluations.

Upon completion of the exercise, the expectation is for the CDN at USMA to be disconnected from the Internet and used by a newly formed student organization that is focused on information assurance topics. This group will be a Special Interest Group (SIG) of the student Association of Computing Machinery (ACM) chapter at West Point. The group's full name will be the Special Interest Group for Security, Audit, and Control (SIGSAC). Cadets in the group will have an opportunity to reconfigure the network into Red and Blue teams. They will then try to replicate exploits that appear in popular news media, and experiment with a variety of defensive software products and firewalls. This will provide a healthy outlet for cadets' interested in this topic. It provides an unstructured, but supervised, environment for them to learn about these technologies in a fun, unthreatening, and un-graded manner. This free play will be supplemented with demonstrations by external consultants, faculty, and other cadets experimenting in this area.

The CDN will revert back to its original purpose, providing a facility for the conduct of the Cyber Defense Exercise, each spring so that it may be used in conjunction with the IA course. The CDN will be returned to its baseline configuration using the Ghost CDs and installation procedures provided by the PKI-Enabled VPN CDE Rapid Set-up cadet development team. It should be noted that the workload for cadets at USMA does not allow for cadets to branch out into many different areas. Fortunately, the resources provided in the Cyber Defense Network and by the SIGSAC give cadets, especially those who are not majoring in Computer Science, an opportunity to experience Information Assurance exercises throughout their cadet careers. These cadets could be thought of as participating in intramural or junior varsity athletics. Through their involvement in SIGSAC and by taking prerequisites courses they are preparing themselves for playing at the varsity level during their senior year when they participate in the CDE exercise. More importantly, they are preparing themselves for the time when all of them, as commissioned officers will be responsible to protect and defend the many critical information system upon which our Army depends.

REFERENCES

[1] Robert R. Tomes, "Boon or Threat? The Information Revolution and U.S. National Security," *Naval War College Review*, vol. LIII, pp. 21-38, 2000.

[2] Curtis A. Jr. Carver, "Information Warfare: Our Next Task Force Smith," Unpublished Research Paper. Fort Leavenworth: U.S. Army Command and General Staff College, 1997.

[3] Terrill D. Maynard, "International Implications and the NIPC," in Proc. *InfowarCon 99*, Washington, September 6-9 1999.

[4] Surdu, George, Global Directory of Information Systems, Technology, and Services, Ford Motor Company, personal conversation, October 2000.

[5] Robert Turk and Shawn Hollingsworth, "Information Assurance: Army prepares for next generation of warfare," *Army Communicator*, vol. 25, pp. 34-35, 2000.

[6] John Arquilla and Don Ronfeldt, "In Athena's Camp: Preparing for Conflict in the Information Age," Santa Monica: RAND, 1997.

[7] Michael I. Handel, *Masters of War: Classical Strategic Thought*, Second Revised and Expanded ed. London: Frank Cass, 1996.

[8] Richard M. Felder, "Reaching the Second Tier -- Learning and Teaching Styles in College Science Education," *Journal of College Science Teaching*, vol. 23, pp. 286-290, 1993.

Appendix 8. Model Legal Memo for Cyber Security Exercise Participants and Organizers

Legal Issues for Cyber Defense Exercise (CDX)

The Cyber Defense Exercise (CDX) originated as an annual competition between student teams from the five U.S. Service Academies as an educational experience for the participants. As conceived, the Exercise utilizes information assurance concepts in protecting and defending information systems in the context of a realistic but controlled scenario with student teams of defenders. In one sense, the CDX is a simulation in that the entire exercise is subject to strict controls and isolated from production networks. On the other hand, the CDX is an authentic experience because the attacking teams exploit real network and system vulnerabilities. Similarly, the defending team must use available resources to respond to attacks as they occur.

This paper will provide a brief overview of the legal issues under federal law. However, counsel should also review applicable state law where it may vary from federal law. In addition, this paper assumes that the CDX is for an educational purpose related to information assurance and does not include law enforcement, counter-intelligence, or intelligence purposes. Finally, this paper does not constitute legal advice which should be obtained from legal counsel fully familiar with all of the facts of the proposed CDX including the scope of the exercise, and the expected participants.

The Legal Framework

Conceptually, a CDX is similar to vulnerability assessment and its related exercise, penetration testing. However, as an educational exercise, the purposes of a CDX are quite different. Generally, federal law does not prohibit or otherwise regulate cyber defense exercises such as vulnerability assessment or a CDX. However, in the course of planning for a CDX, counsel should consider the following legal risks:

1. unauthorized intrusions into or damage to a network or computer system may violate federal law. 18 USC §1030;

2. unauthorized access to or disclosure of stored data may violate the Electronic Communication Privacy Act. 18 USC §2701 et. seq;

3. unauthorized data interception may violate the Wiretap Act. 18 USC §2510 and 18 USC §3121;

4. civil lawsuits for damage to third-parties; and

5. universities and colleges may have contractual or statutory privacy obligations to participants.

1. *Computer Fraud and Abuse Act*

The CFAA is the principal federal statute that applies to a variety of criminal conducted directed at computers systems and networks. Network crimes are those crimes that attack the confidentiality, integrity, and availability of a computer or network. There are three types of network crimes that are widely recognized: computer intrusions, malicious code disseminations, and denial of service attacks. In addition, the CFAA also criminalizes causing damage to a computer system.

For example, 1030 section 5(A) makes it a criminal offense to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause $5000 or more in damage without authorization to one or more protected computers. For purposes of section 5, a protected computer is essentially any computer connected to the Internet or otherwise facilitates an interstate or foreign electronic transmission. Other provisions criminalize intentionally accessing a computer without authorization and recklessly, or in some cases, negligently causing damage. The CFAA also provides for civil suits by persons whose computers or networks have been damaged.

The CFAA, by its terms, does not preclude applicability to mock environments such as a CDX. However, it is also clear that the touchstone for liability under the CFAA is authorization to intentionally access the computer system and in some cases, authorization to damage those systems. Plainly, the consent and authorization of the owners of the hardware to use the system in a CDX is essential. The organizers should obtain the permission from the relevant parties for any network that will be touched during the exercise, and for any data that resides on or transits the network. This is a critical but not necessarily a trivial task because it may not be immediately apparent which systems are affected or who is authorized to give consent for the entire system. The authorizing official should understand the network, the legal implications, and computer security. The necessary approvals are correspondingly more difficult to obtain if the CDX is not limited to an isolated test network, but instead is conducted over the Internet.

2. *Electronic Communication Privacy Act (ECPA)*

ECPA imposes limitations on accessing stored data and disclosing stored data to others, including government investigators, for network operators that provide communication services to the general public. For the most part, ECPA provides privacy protections for email. Generally, ECPA prohibits accessing, without or in excess of authorization, a network and obtaining or altering a communication where the communication has not yet been retrieved by the intended recipient on the network. Since the CDX network should not be a production network, the CDX network will not operate as a communication provider to members of the general public. To make this point clear, the CDX network should also not offer email services to the participants.

3. *Wiretap Act and the Pen/Trap statute*

The Wiretap Act and the Pen/Trap statute regulate the real-time interception of electronic data as it traverses a network. The statutes cover two aspects of electronic data: transactional data such as packet headers, and content data such as the packet payload. Transactional data means the "dialing, routing, addressing, and signaling information" associated with a communication. Content means the substance of the communication such as the body of email, IRC chats, and the contents of files. Like the CFAA, there is no exception as such for a CDX or for non-production networks generally. The provisions of the Wiretap Act and the Pen/Trap statute apply with equal force to isolated, non-production networks as they do to networks open to general users, unless the interception of the communication falls within an exception.

The most likely applicable exception is the consent of the participants to the real-time monitoring of their communications. This consent should not be presumed because of a participant's role in the competition. Instead, consider a consent form with disclosure of the monitoring, signed by each participant, including the attacking team.

4. *Civil lawsuits for Damage to Third-Parties*

The risk of damage to third-parties is probably the most variable legal risk in operating a CDX because the likelihood of such damage in a controlled environment may be difficult to foresee. If a CDX is operated on an entirely closed network without any possibility of attack traffic leaking into production networks, then the risk of participants causing damage to non-CDX equipment or data is reduced. However, it is prudent to be smart about selecting member for both the attacking teams and the student participants. The rules, scope and purpose of the exercise should be made clear to all participants, including the consequences for violating the rules. A background check for the attacking team is not unreasonable. Furthermore, diligence by the organizers to ensure that the CDX stays within the scope of the planned exercise as it unfolds will help to identify and address unforeseen developments quickly and appropriately.

5. *Contractual or Statutory Privacy Obligations*

Finally, universities and colleges frequently have privacy obligations to students that may be based on university policies or guidelines, or applicable state statutes. These privacy protections may impose other obligations for which an informed consent by the participants is required.

Conclusion

Careful planning for CDX is the key to a successful exercise, and careful planning should include an understanding of the legal issues that may arise. Participation by legal counsel in the planning of the CDX can avoid potential legal pitfalls.

Appendix 9. Related Ideas beyond the Scope of a Standardized Cyber Security Exercise

Several ideas were suggested at the workshop that seemed beyond the scope of traditional or "standardized" cyber security competitions. These ideas may encourage non-standard activities that will inform everyone's experience in running these exercises. Familiarity and know-how so far is largely limited. The group with the most experience, the military academies, function in an environment somewhat different than that of civilian educational institutions, and their environment may not be easily generalized to the civilian institutions.

The ideas below may also may inspire groups to try modifications to the Current (military academy) CDX, and some of these modifications may give us more knowledge of the advantages and disadvantages of both the traditional and other methods of running these exercises.

In addition, some of these ideas are necessary to make a competition academically valid – notably correlating a cyber defense competition with an appropriate curriculum. If that is done, educators can more easily make the case that a cyber security competition augments lecture and classroom instruction.

These ideas follow:

- Pit student attackers against student defenders.
- Create a competition season that includes leagues and graduated levels of competition.
- Correlate curriculum development with a cyber security exercise.
- In addition to the defenders and attackers, create a "user" team. The users would be individuals who are not experts in computer science who need access to the system to perform a function unrelated to security. How quickly and easily they can accomplish their goals would be considered in the scoring.
- Pair a defender team with a user team.
- Develop a long-term software engineering project to design, implement, and test a secure but functional system, improving it with lessons learned from a cyber security exercise.

Appendix 10. Cost Estimates

These cost estimates are approximations. Costs may vary widely, depending on the hardware and software involved, the expertise of the personnel involved, and how much of these resources are donated.

Procurement
A baseline cost for a dedicated network of $60,000 per team per site (assuming a single team consists of six to 20 individuals) is estimated for the first year. Subsequent years costs would encompass only maintenance and upgrades as needed. If an existing network is used, costs could be completely mitigated based on local resources.

Maintenance
Technical upgrades would be expected to cost $5,000–$10,000 per team per site to ensure an even playing field and include such items as wireless access and voice over Internet protocol. Software upgrades may be free or very cheap and may involve use of open source software or, for Windows software, the Microsoft developers' network ($400/year for academic users). These costs assume a dedicated network. Costs using existing resources would be significantly less.

Personnel
Administrative support (e.g., coordinating the logistics of the event, recruiting participants, and publicizing the event) is estimated to involve about 40 person-hours. Technical support to maintain the hardware and software varies by implementation, but is similar to that associated with the management of any small network.

External Support
It is estimated that hiring an external team of attackers would cost $15,000. This estimate assumes the attackers are full-time professionals in information assurance who would spend about 1 week total preparing for the exercise, taking part, and debriefing. Referees may cost approximately $5,000 per site; they would be expected to spend about 1 week total preparing for the exercise, taking part, and debriefing. Controllers would spend approximately 200 hours setting up scenarios, equipment lists, monitoring, etc., and would cost approximately $20,000. These costs assume that an external resource provides the services. Faculty and students could provide many of the services mentioned, and potentially lower this cost considerably.

2004 Inter-Service Academy Cyber-Defense Exercise Directive (v2)

1. Simulated Scenario:

The country of Purple has recently undergone a bloody civil war and has splintered into two states, one calling itself The People's Republic of Red and the other calling itself The Federated States of Orange. Each state is vying for international recognition and aid. The United States, along with a coalition of the willing, has begun relief efforts to bring needed medical supplies and food to the newly formed country of Orange, which has embraced democracy. The coalition has been very critical of the policies of the newly formed Red state, citing human rights infractions and Red's authoritarian ruler's disregard for the people of Red as being contrary to good order and stability in the region.

The multinational coalition has begun to build up forces in the region, and has begun to plan for five bases of operations – each with its own computer networking infrastructure. Each of these bases will be responsible for building and maintaining its own Cyber Defense Network (CDN) to support all required services needed by the deployed coalition forces. As there is still a great deal of unrest and insurgency on each side in the civil war, there are many threats to information and to personnel at the regional commands. Threats against the information maintained within the coalitions networks can be expected from Red cyber-attack forces as well as from untrustworthy entities (possible Red insurgents) within each command. We must assume that Red forces may have some knowledge of the information technology architecture, and that they may also have access via external hosts. Red forces can be expected to attempt to access the allied Global Liberation Unified Network GLU and adversely impact coalition operations by obtaining and/or manipulating information deemed critical to the allied mission.

The Combined Forces Command will be staffed as follows:

Wayne Schepens, CC – Combined Forces Commander, wayne.schepens@cfhq.cdx

Chris Benjes, C3 – Director of Operations, chris.benjes@cfhq.cdx

Rob Millot, C4 – Director of Logistics, rob.millot@cfhq.cdx

Derek Gabbard, C6 – Director of Communications, derek.gabbard@cfhq.cdx

One to Three Liaison Officers per Regional Command

Regional Commands:

USAFA	Adams (adams.cdx)
USCGA	Franklin (franklin.cdx)
USMA	Hancock (hancock.cdx)
USMMA	Jefferson (jefferson.cdx)
USNA	Washington (washington.cdx)
AFIT	Harrison (harrison.cdx)

Requirements:

a. Implement a Windows 2000 Domain. Each CDN will implement a child Windows 2000 Domain Controller which will be joined to the .cdx Windows 2000 tree. The tree root Windows 2000 Domain Controller will be located at CFHQ, and will be named revere.cdx. All users on each CDN must have valid user accounts in their respective domains and have capability to utilize file and print services. Must offer public share folders to host critical Command and Control and other exercise information.

b. Create and maintain a Local Personnel Database (LPD) to provide the following information via a publicly available Web Site (secured via SSL or TLS):
   i) Organizational Chart and telephone listing – available to the entire .cdx domain
   ii) Regional Weather Forecasts (updated at least every 2 hours)
   iii) Status of services (red (inoperable), yellow (intermittent or partially available), green(fully available) available only to local site and CFHQ members
   iv) All local members PKI certificates (public keys)

   Although this database is to be managed locally, CHFQ must be able to perform immediate updates via a web interface.

c. Implement email services. CFHQ has chosen Email as its primary electronic means for communication. Each CDN will implement Email and establish means for all forward deployed Liaison Officers (LO) (On-site White Cell members) to access Email. All personnel will be required to use DoD PKI certificates for access and transport of sensitive information. Users must be able to remotely access web-based Email. Each local user (*all participating students*) must have an Email account and the capability to log in and access machine utilities. CFHQ staff requires local email accounts on each CDN. The command standard for e-mail is Exchange Server 2000 with Outlook Web Access (OWA).

d. Establish a Local Registration Authority (LRA) to support secure Email between regional commands enabling any remote user to download any local user's public key certificate. (Faculty/students at each school will be required to issue DoD PKI certs for all local users including LOs.) Each participant at the regional commands must have a PKI certificate, and each public key must be available through the command's web page.

e. The command standard for desktop is Windows 2000. Liaison Officers will require continuous access to a workstation. Note: Liaison officers must have unfettered/unmonitored access to a Windows 2000 host on the local CDN as well as a local e-mail account.

f. Situation Reports (SitRep) describing suspicious activity must be securely delivered electronically to C4 and C6 daily upon commencement of the Exercise NLT 2400 hrs EST. Report content is described in ANNEX A.

g. Provide command leaders with audio and video conferencing on-line.

h. An Inventory Control Database (ICD) must be maintained by each regional command. It is to be locally created and maintained and should be accessible to CFHQ and all LOs. The database must be viewable (via a web browser). Changes made locally must immediately be reflected via the web interface. Critical elements of information required includes: for all hardware – make, model and serial numbers; for all network equipment -- host names, IP addresses, and MAC addresses; for all software -- local commands Approved Software List and software versions.

i. Each regional command must maintain a local DNS. CFHQ will maintain the primary DNS server.

j. Maintain a dedicated host configured and administered by CFHQ. This host will be used for service verification and/or vulnerability scanning of other regional command networks. This host will have a local IP address and must have external access but will not be used to access any services on the local network. This machine will not be used to attack local CDNs.

k. Provide completed Concept of Operations (CONOPs) to describe plans and architectures as well as user information necessary to meet all Directive requirements NLT 14 April 2004. Comprehensive network diagrams mapping all services to hosts, account information and instructions for user access, lists of key personnel and contact information, as well as instructions for obtaining PKI credentials shall be included. (CONOPs will only be shared with the White Cell. Be complete, as your score will rely upon these documents.)

2. Execution

a. Commander's Intent: All CDN services/applications must be available for use by the coalition forces for the duration of the exercise, and no intrusions or attempted intrusions into the CDN shall go undetected. Unless otherwise noted within the requirements, all information to be shared among regional commands shall only be offered statically; external regional commands must not be able to manipulate information. The mission will rely on the availability and integrity of all required information. Provide survivability to all aspects of information and functionality. Be prepared for the unexpected.

b. Due to past communication problems, the Commander is prohibiting the implementation of host based firewalls.

c. Timeline: The CDX will be conducted in four phases (all times are US EST).

i) Phase 1 – Design and implementation, installation, configuration and planning, 26 Jan 04 through 16 Apr 04. Network architecture and software integration must be established based on the Directive requirements. Apply all information assurance knowledge and available tools to harden the CDN to the maximum extent possible. Security tools must be open source or freely available to government and/or academic institutions. These tools, as well as any other software used during the exercise, must be listed on the White Cell Approved Software List (see ROE for submittal instructions). *White Cell will be on site from 16 Apr 04 through the duration of the exercise.*

ii) Phase 2 – Active/Anomaly/Report/Recovery cycle, 1200 hrs 19 Apr 04 through 1400 hrs 22 Apr 04.

(1) Active: CFHQ requires each regional command to maintain its functional capabilities continuously throughout Phase 2. Downtime for system maintenance will be considered so long as the requests are for time outside the window of regular duty hours defined as 0930-1630, EST. Requests must be made during regular duty hours and gain approval in advance by the C4 and/or C6. Downtime will be limited to 2-hour increments and one event per 24 hours. **Scoring begins during this phase. All teams will start with 0 points and will earn points based on lack/loss of availability and compromise of information/systems. Downtime will commence when the school is notified by the White Cell. LOW SCORE WINS. Each CDN must be manned by at least one student throughout duty hours.**

(2) Anomaly: White Cell will introduce pre-defined anomalies at regularly scheduled intervals throughout Phase 2. Be prepared to inherit systems and/or establish new functional capabilities. Also be prepared to handle forced loss of capability and/or introduction of malicious code for which each team will need to recover. Include documented recovery plans within the SitRep.

(3) Report: Coalition teams must send a Situation Report (SitRep) containing the information shown in ANNEX A to CFHQ via a PKI encrypted and signed Email. The SitRep shall be received by the White Cell no later than 2359 on each active day (19-22 Apr).

(4) Recovery: Coalition teams may work to identify anomalies created as a result of the attacks and try to recover any systems that have been infected throughout the entire exercise.

iii) Phase 3 – Post exercise deliberations, 22 Apr 04 through 30 Apr 04. The Red Force and White Cell representatives will jointly prepare an After Action Report and submit a recommendation of the CDX 2004 winner based upon a review of: a) the relative defensive postures presented by each regional

command's CDN, b) the effectiveness and usability of redundant systems and recover from injected anomalies and c) the accuracy and detail of the SitReps received by CFHQ. The NSA IA Director's Trophy will be presented to the winning team. (The winning school will need to coordinate with the NSA Fellows to settle on a date and time for Mr. Wolf to visit and present the trophy.)

d. Subordinate Unit Missions: To be assigned as necessary at the discretion of each regional command.

e. Rules of Engagement (ROE):

i) No one other than designated Red Force participants shall partake in any form of offensive information/computer warfare. The CDX is a defense and survivability exercise for the coalition participants. Any unauthorized offensive action by any member of a coalition team will disqualify that team from the competition.

ii) All machines/devices/boxes used within the CDN must be included on the Approved Hardware List provided by the White Cell.

iii) All software used within the CDN must be included on the Approved Software List created and maintained by the White Cell. Each CDN will have its own Approved Software List. Approval requests may be submitted anytime prior to 16 April 2004 and shall be sent to software@cdxperts.com. If your CDN implements software not on your list, you are in violation of the rules of engagement and will be subject to a penalty of 250 points. Strict adherence to licensing agreements will be enforced.

iv) Phase 2 will be a time when White Cell and Red forces are exercising the network. Each team must provide an "on-call" faculty or staff member who is able to contact a student representative in order to troubleshoot network or service problems. Loss of functional capability will be reported to each team, they then will have an opportunity to utilize back-up means to provide functionality. Repairing or replacing services within 1 hour will incur no penalty, assuming a compromise has not occurred. **The physical or logical disconnection of any network resource will introduce an immediate penalty unless done in conjunction with approved Downtime.**

v) Penalty points will be awarded to teams sending SitReps un-signed and transmitted in cleartext. In addition, a penalty will be assessed if the Red Force is able to intercept and read an unprotected SitRep.

vi) The involvement of faculty and staff will be limited to "background" support throughout all phases of the CDX. Though this is admittedly a subjective call, the ethical intent is for the substantive portion of the exercise to be a

predominantly student run evolution. Faculty and staff are allowed to provide some degree of assistance in carrying out tasks that students have, of their own volition, identified as necessary and prudent; though actual hands-on "keyboarding" from faculty or staff shall be excluded to all but the most basic systems administration type tasks; i.e., low level systems details that are not typically taught as part of IA coursework.

vii) To win the exercise you must have incurred the least amount of points. Points are earned based on services not being available or information/systems being compromised. These penalty points will be assessed if the CDN requisite services are not available during the Phase 2. This policy ensures a larger penalty imposed upon teams for unavailable services rather than exploited services. Guidance for team scoring is outlined in ANNEX B.

viii) Further requirements for network services may be levied by CFHQ at any time, and systems and services may be delivered for incorporation into the CDNs in the form of Virtual Machines or actual services.

ANNEX A: CDX 2004 Situation Report (SitRep) Format *(Limited to 3 pages)*

The SitRep will serve to provide a status of the operational capability of each regional command's CDN and the effectiveness their intrusion detection and reaction capability. The SitRep must be transmitted to CFHQ as specified in the Directive requirements. The following fields must be addressed though style and specific information content is left to each team's discretion:

Operational Capability:

Overall system status (narrative)

Service status (address all Directive requirements)

Intrusion Detection:

Suspicious activity in the last 24 hours

Type of attack(s)

Source and destination IP addresses (each attack)

Ports accessed (or attempts thereof)

Damage incurred

Reaction/response taken

Expected enemy activity in the next 24 hours

Anomaly Reaction/Response:

Modified USER Instructions for services:

ANNEX B: CDX 2004 Scoring Criteria / Format

During Duty Hours: No service (>3 hours) renders a 200-point penalty. Loss for 1-3 hours renders 100-point penalty. Loss of integrity renders a 100-point penalty for each service or data compromise. Degraded service (less secure than required) renders a 50-point penalty.
Outside Duty Hours or during any Hands-off Period: Loss of service renders a 100-point penalty.
Subjectivity will be left to White Cell and Red Force discretion.

Requirement	Degraded Service	Loss of Integrity	Down for 1-3 Hours	No Service >3 Hours
A. CDN W2K Domain Services available				
B1. Personnel Information database available via Web				
B2. CFHQ update capable				
C1. Local Users able to send and receive email to and from CFHQ and other CDNs				
C2. Remote Users able to send and receive e-mail using local CDN accounts				
D. Local Registration Authority: Available (regional commands can download local Public Certificates)				
E. Unfettered and unmonitored W2K Workstation access and local domain account access available to LO				
F. SitRep Secure Delivery *(4X points)*				
G. Audio and Video Conferencing				
H. Inventory Control Database: Available and Local Edit Capable				
I. Local DNS				
J. Remote host				

ANNEX B page 1 of 1

Appendix 12. Sample Authorization Memorandum for Attackers

<date>

MEMORANDUM THRU

<Participating Organizations Network Operations Office>

FOR *<Attack Team Organization>*

SUBJECT: Security Evaluation Authorization

1. The purpose of this memorandum is to provide authorization to *<Attack Team Organization>*in conducting a security evaluation of the Cyber Defense Network (CDN) hosted at the *<team Organization>*, between *<start date>* and *<end date>*. We would like you to participate in the Cyber Defense Exercise as described, within the Cyber Defense Exercise (CDX) Directive. The CDN will be virtually isolated from the <team *Organization>*computing infrastructure.

2. The *<Team Organization>* has constructed and fielded a Cyber Defense Network, which virtually represents a production-like information infrastructure. This network provides the students in the Information Assurance class the resources to practice their skills in a secure configuration. This network will not host real data; its sole purpose is to exist as a sandbox to support the exercise.

3. The focus of the exercise for the students will be in maintaining services and integrity. The exercise will be hosted within a Virtual Private Network (VPN). This VPN will provide connectivity between all participating schools, the Red Force, and the White Cell. It will provide encrypted paths to specific IP ranges to support remote Red Force activity. Traffic penetrating the bounds of the VPN will be limited to HTTP, FTP, and DNS and will only be offered prior to *<date and time>*. This traffic will be denied upon commencement of the exercise. It is critical that you limit your attack to resources only residing through the predefined IP range. Please contact the point of contact for this memorandum at any time that you feel you may have exceeded your boundary.

4. This exercise represents the final exam for the cadets. Their goal is to employ the skills they have learned to defend this computer network. Your role will be to penetrate the systems within the Cyber Defense Network, disrupt the availability and integrity of services, evaluate the security posture, report on your findings, and recommend a winner with the input of the White Team to be certified by the Exercise Director.

5. The point of contact for this memorandum is the undersigned..

/signed/

Appendix 13. Movements towards a Governing Board

At the workshop, a great deal of interest was shown in establishing a central committee or national board to coordinate future Cyber Defense Exercise work. Tim Rosenberg and Ron Dodge agreed to serve as organizing agents to establish the governing body and facilitate the election of a board. They have identified the following necessary steps:

- Incorporate the governing body as a not-for-profit organization so it may accept donations
- Create bylaws
- Evaluate the patent application of the CDX and, if appropriate, determine whether a licensing agreement is needed

The following board guidelines are being considered for action:

1. PURPOSE:
The Steering Committee is a group of individuals responsible for general operating policy, procedures, and related matters affecting the CDC national board as a whole, with the follow charges:
1.1 Establish the basic committee organization and prepare it for formal elections not later than 1 November 2004.
1.2 Establish national board constitution.
1.3 Facilitate communications between schools wishing to participate in a Cyber Defense Competition (CDC).

2. COMMITTEE MEMBERSHIP
2.1 The initial steering committee shall be made up of six positions. The positions are: three committee officers: chair, co-chair, and secretary, and three standing sub-committees chairs: funding, rules, and communications.
Remaining interested personnel shall contribute as subcommittee members or as appointed by the board.
2.2 Each member shall serve until the steering committee holds formal elections (not later than 1 Nov 2004).
2.3 Each organization can have no more then one member on the Committee or a given sub committee.

3. STEERING COMMITTEE SELECTION
3.1 Nomination process is a two week period, where each workshop attendee can nominate two possible committee members. This is done by sending an email to Ron Dodge (ronald.dodge@usma.edu). The nominations will be confirmed.
3.2 Nominees will be sent an email confirming their desire to accept the nomination.
3.3 After the two week nomination period, there is a one week voting period. Each workshop attendee can cast one vote for each open position. Voting will be conducted by sending an email to Ron Dodge (ronald.dodge@usma.edu). The votes will be confirmed. The top winners take the positions.

4. TIMELINE
Summer 2004: Comments on initial plan (open to all on the steering committee list)
Fall 2004: Nomination period for six initial formal positions (open to all workshop attendees)
Fall 2004: Voting (open to all workshop attendees).

Ron Dodge will continue coordinate the establishment of the steering committee until all positions have been filled (Fall 2004).

Tim Rosenberg will continue to explore the benefits of incorporating or falling in under an existing organization (ACM, etc...) and report his recommendations to the new steering committee.

Architecture of a Cyber Defense Competition*

Wayne J. Schepens and John R. James[1]
Electrical Engineering and Computer Science Department
United States Military Academy
West Point, NY 10996, U.S.A.
John-James@usma.edu
Wayne-Schepens@usma.edu

Abstract – *This paper describes the effort involve in executing a Cyber Defense Exercise while focusing on the White Cell and Red Forces activities during the 2003 Inter-Academy Cyber Defense Exercise (CDX). These exercise components were led by the National Security Agency and were comprised of security professionals from Carnegie Mellon University's CERT, the United States Air Force, and the United States Army. This hands-on exercise provided the capstone educational experience for information assurance students at the U. S. service academies. The White Cell developed the scenarios and anomalies, established the scoring criteria, refereed the exercise, and determined the winner based on the effectiveness of each academy to minimize the impact to their networks from the Red Forces network intelligence gathering, intrusion, attack and evaluation. To understand better all that is involved this paper takes advantage of the authors three years of experience in directing the activities associated with the planning and execution of the 2003 exercise.*

Introduction

Designed to fill the CAPSTONE requirement for the United States Military Academy's Information Assurance course in 2001, the Cyber Defense Exercise (CDX) pits teams of cadets from each of the five US service academies against security experts within the Department of Defense. Each team is challenged to design, implement, and manage an operational network of computers. Management of various platforms (Windows, LINUX, Solaris, FreeBSD, etc.) is required and services such as web, email, public key infrastructure, and database sharing must be provided. Students are encouraged to establish architecture, policy, and procedures that invoke a defense-in-depth and defense-in-breadth posture to keep the aggressors at bay. To keep the playing field level, security measures are limited to open source freely available tools. Strategies and techniques employed by the students that were tested on the CDX battlefield have provided industry, academia, and government with valuable lessons. These lessons are related to work in network mapping, port scanning, vulnerability scanning, password integrity checking, network

Figure 1. NSA Information Assurance Director's Trophy

[1] This work was partially supported by an endowment establishing the Adam Chair in Information Technology. The views expressed herein are those of the authors and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

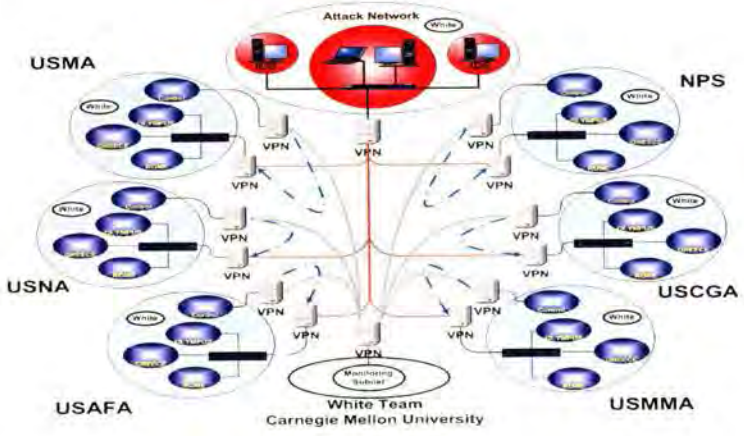
monitoring tools, intrusion detection systems, host-based and network-based firewalls, and layer-two bridges.

As the competition begins, the National Security Agency (NSA) - led Red Force identifies vulnerabilities and launches repeated attacks on each network over a four-day period. Students have the ability to enter into direct cyber combat in an effort to keep services on-line and running. Teams are then evaluated on maintaining services as well as efforts to recover from and prevent future security breaches. The winner is presented the NSA Information Assurance Director's Trophy. West Point held the title in the first two years of the competition; however, the US Air Force Academy took home the trophy in 2003, Figure 1.

The CDX has resulted in an intense rivalry between the academies and has become a staple of each academy's information assurance curriculum. The DoD's investment in this project has already reaped extraordinary benefits and the sky is the limit. The CDX should serve as a model for inter-agency programs as there are several players involved each year whose vision and dedication make this effort a success. In just three years the number of personnel involved in carrying-out and participating in the exercise has grown from approximately 40 to over 300.

The CDX consists of three main components: the *Blue Forces* consisting of the five US service academies, the Naval Postgraduate School and the Air Force Institute of Technology[3]; the *Red Forces* consisting of the National Security Agency, the Air Force 92nd Information Warfare Aggressor Squadron, and the Army 1st Information Operations Command; and the *White Cell* consisting primarily of personnel from Carnegie Mellon University and led by Mr. Wayne Schepens. This paper focuses on the responsibilities and activities of the Red Forces and the White Cell in establishing an effective cyber defense competition.

White Cell Lays the Groundwork



The White Cell developed the scenarios and anomalies, established the scoring criteria, refereed the exercise, and determined the winner based on the effectiveness of each academy to minimize the impact to their network of the Red Forces malicious activities.

[3] AFIT and NPS competed in a separate competition that was run in parallel with the service academy competition.

Scenario

Completing the scenario early is essential to enable each participant time to provide input. Six months is adequate, but no matter how much time is provided the White Cell must be persistent because if the input does not come by way of comments during the planning stages it will come by way of complaints during the execution stages.

The military academies use exercises to capture realistic situations and put future military officers in positions in which they are expected to encounter upon graduation. The 2003 CDX scenario was as follows:

A multi-nation coalition force has initiated a liberation operation against the hostile country of Red. The coalition combatant force is to be supported by a network architecture known as the Global Liberation Grid (GLG). The coalition is depending on the United States X Academy to establish a command to support this network. The GLG will consist of seven commands located in various places throughout the world, each requiring their own Cyber Defense Network (CDN) in order to create, maintain, and share critical mission information. The physical infrastructure to provide connectivity between these commands will be the responsibility of the National Security Agency. It will be each commands responsibility to design, develop, and implement the hardware/software necessary to host a CDN capable of meeting a specific set of requirements.

Threats against the information maintained in this network can be expected from Red cyber-attack forces as well as from untrusted entities within each command. We must assume that the Red forces may have some knowledge of the GLG architecture, and that they may also have access via external hosts. Red forces can be expected to attempt to access the allied CDN and adversely impact allied operations by obtaining and/or manipulating information deemed critical to the allied mission. The Red forces are <u>not</u> expected to perform network availability attacks, as their operational doctrine favors surreptitious information exploitation over the more overt denial of service attack profile.[4]

This scenario laid the burden on each academy to define an adequate architecture and software implementation to support the mission. It also made clear that the objective of the Red Forces was one of security evaluation and data acquisition through compromise rather than a brute force attack. This scenario was played out at each academy based on providing the following requirements:

Requirements:

- *Headquarters has chosen email as its primary electronic means for communication. Implement email and establish means for forward deployed personnel (White Cell) to access email. These personnel will be required to use DoD PKI certificates for access and transport of sensitive information. They must be able to remotely utilize either web or application based email, therefore you*

[4] Inter-Service Academy Cyber-Defense Exercise Directive, dated 9 January 2003.

must provide for both. Each local user must have an email account and capability to login and access machine utilities. HQs will establish 20-30 user accounts in order to distribute mission update information as required.

- *It is critical for coalition partners to know the organization make-up of each command and be able to find contact information. Therefore you must provide a web based organizational chart and telephone and email directory.*
- *Situation Reports (SitRep) describing operational capabilities must be securely delivered electronically to xxxxx@.cdx.*
- *A supply database for each command must be locally managed based on updates provided by Headquarters. The database shall be updated on a daily basis and should be made statically available to each command. Supply officer at HQs must have edit capability. Updates to supply data will be sent daily via attachments to email.*
- *Establish a Local Registration Authority (LRA) to enable external users to download any local users public key certificate. HQs will need a way to push public certificates to each command's LRA providing means to initiate secure communications. This push must be executed using means other than email.*
- *Unless otherwise noted, all information deemed to be shared among outside commands should only be offered statically, outside commands must not be able to manipulate information.*
- *The mission will rely on the availability and integrity of all required information. Provide survivability to all aspects of information and functionality.*
- *Provide command leaders with audio and video conferencing on-line.*
- *The command standard for desktop is windows 2000.*
- *HQs will maintain the main DNS server. Each command must maintain a local DNS.*
- *Provide complete concept of operations, account information, network diagrams, and provided service to HQs.*
- *Be prepared for the unexpected. Establish means to evaluate the functionality and security of your local CDN. Establish means to monitor CDN activity and be prepared to respond with redundant functionality and report known compromises.*[2]

Students were warned to be prepared for the unexpected as anomalies were injected with absolutely no warning and the Red Forces owned a rogue box on each academy's CDN capable of launching stealthy attacks. The mission's success relied upon the availability and integrity of all required information and survivability of the networks functionality. In order to maintain an effect network over a one-week active period, students would have to design and build with information assurance as a cornerstone…something we all should be doing don't you think?

Schedule of Engagement

After months of hard work in analyzing the requirements, conceptualizing and defining a design, and implementing a functional product the time came to face the enemy. Although all involved were primed as always to start, glitches here and they make

all involved wish for more time to prepare. Some students spend 20 hours per day in the lab during the weekends preceding the exercise. This level of effort is obviously put forth for more than just a grade.

Early in the academic year each academy agreed to a common week of attack in which students would stand watch in their respective labs throughout the day while the White Cell utilized their systems manually and by way of automated tools both locally and remotely and the Red Forces performed their art. In order to ensure a clean start, the White Cell started verifying functionality and services a few days prior to the exercise for any school interested. They helped trouble shoot and get everyone on same page to ensure the best fight for all. This proved to be extremely valuable because in the past two exercises the Red Forces were requested to hold back on the first day of activity while everyone made ready. It seemed no matter how much time was given, the final tweaking came down to the last minute for all involved. A valuable lesson in ensuring adequate testing prior to going live is learned by faculty and students alike.

During the evenings of the exercise, students spend their time recovering, thinking of new and eloquent solutions and back-up plans, and documenting the results of the day's exploits and modifications to their system's configurations. The effectiveness of their efforts will be reflected in the scoring.

Anomalies

Each day without warning, anomalies are injected into the scenario. These operational irregularities test the student teams' and/or their systems ability to react on the fly. They can be as complex as requiring each team to stand up an anonymous FTP server based on a commanders order to share information rapidly and readily to the other commands or as simplex as requiring a student to give up a system password as if someone was not diligent in providing password protection. They may include requiring all hands to man their battle stations such that no one is left to monitor logs and provide real time systems administration or they may be introduced as a piece of malicious software injected on a specific platform or service waiting for a specific time or event to execute. An anomaly may require a student user to load the latest intriguing piece of software made available via the Internet, which may introduce a new vulnerability, or it may require the student to fall back to an earlier version of software that is vulnerable to a well-known exploit. Whatever the anomaly, all participants are exposed equally and their actions, procedures and policies to address them are evaluated.

Organization

The *top-level architecture* of the CDX is shown in Figure 2. As indicated in the figure, each of the schools local area networks had two Virtual Private Network (VPN) nodes, one for providing services to each of the other participating schools, the White Cell and the Red Forces and another for the competing teams to evaluate their own systems from the vantage point of an outsider.

The use of the VPNs during the CDX provides an environment to conduct the exercise and to evaluate and "test drive" software before placing it into a production environment. It is intended to protect the integrity of the exercise as well as ensure any offensive measure taken by the Red Forces does not make it to the outside world. Any offensive action taken by the participating students is strictly prohibited and grounds for disqualification as only the Red Forces have the appropriate legal authority to attack.

White Cell members are located at each participating school to serve as a local referee and are directed by leadership located at a Headquarters stationed in Maryland. The White Cell uses a combination of automated tools and manual evaluation to determine service availability and the degree of compromise. They utilize a scoring criterion that invokes penalty points for loss of services and/or compromises and provides redemption points for effective reporting. Penalty points assessed for service degradation are dependent upon time of outage while penalty points assessed for compromise depend upon root or user level access. It is critical to have coverage remotely and on-site as well as to work closely with the Red Force leaders to ensure de-confliction between cause and effect.

Post-Exercise Deliberations

Upon the conclusion of the exercise the White Cell works closely with the Red Forces to certify the rank and order of each team and as a result the winner of the CDX. In addition, they document the results and accounts of the activities throughout the exercise to provide and after action report for each school. They also conduct a telephone conference with all interested participants, which serve as an effective venue for learning.

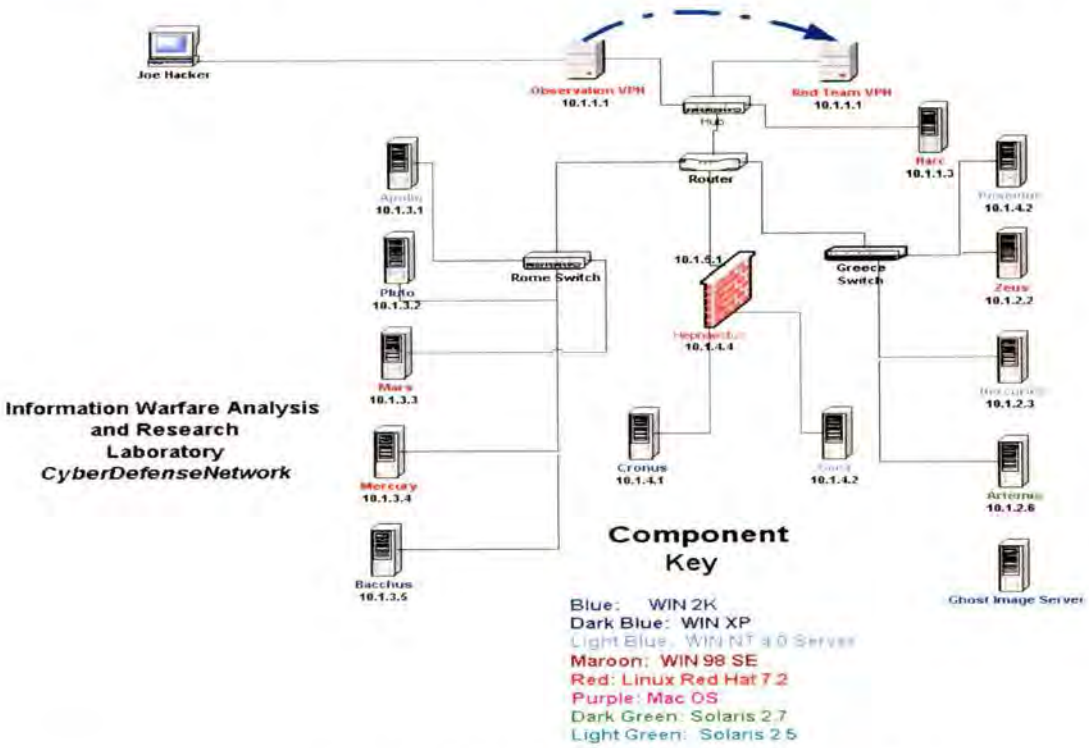


Figure 3. Cyber Defense Network circa 2002

This gives the students and faculty and opportunity find out all that the Red Forces knew and how successful or unsuccessful they were in exploiting their network. Sitting in on this meeting provides outstanding evidence to how effective an educational tool this exercise really has become. Undergraduate students demonstrate their understanding of computer science at the graduate studies level. Strategies and techniques employed by these students go on to serve as examples that the NSA and CERT utilize to teach to industry professionals.

Red Forces Organization and Activities

The Red Forces provided the insider and outsider threat during the cyber defense exercise. They also were involved in providing valuable input to the White Cell during the planning and preparation phases. They are only limited in their tasks to avoid distributed Denial of Service (DoS) attacks to agreed upon times in the exercise since doing this early in the game could greatly the limit the learning experience for all involved.

Organization

While the White cell had elements at each of the Cyber Defense Network (CDN) nodes and Headquarters, the Red Forces were all gathered together operating at a location outside of Baltimore, Maryland. The Red Forces were linked to the CDX VPN and could see all of the traffic over the VPN linking the service academies together. They were on the network but were limited in privileges to services available to all coalition partners. They also ran a rogue machine at each academy for which they have administrative privileges. The intent of the rogue boxes was to throw off the participants in efforts to preclude them from filtering based on IP ranges. If they locked out IP ranges that required services they would be heavily penalized.

Activities

Figure 3 shows the range of operating systems and network components used in CDX 2002. For CDX 2003, while all teams had the same hardware, each team could pick the operating system used to provide a required service. The Red Forces went through a sequence of activities to perform network intelligence gathering, execute intrusion attempts, conduct network attacks, and evaluate the effectiveness of their attacks.

A tcpdump file (about 500Mbytes) is available for the traffic over the net during the 2002 CDX. This data is almost totally malicious in nature since during the 2002 exercise the schools were required to provide a service but not to actively use the service. During 2003 there was considerably more non-malicious traffic over the net since all schools were required to use the net to submit periodic reports and send messages, traffic generators were utilized by the Red Forces to hide their attacks, and the White Cell actively exhausted the services required to be provided. However, technical problems prevented creation of a tcpdump file of the 2003 traffic. For the 2004 CDX we expect to

again increase the friendly network traffic and a tcpdump file is expected to be available for the 2004 exercise. Contact either author to obtain the 2002 data.

Conclusions

In this paper, we have presented a summary of some of what is involved in executing a Cyber Defense Exercise. Lessons learned are plentiful and continue to help us make this a better experience for the participants each and every year. Students have repeatedly told us that the CDX is the best educational activity they have experienced at the USMA. Red Forces individuals have also repeatedly informed us that they have both enjoyed participating in the CDX as well as benefited professionally from participating in the CDX. The CDX has been made possible by extensive support from the National Security Agency (NSA) Public Key Infrastructure (PKI) Management Office.

The benefits of the CDX are realized both at the highest levels of the DoD as well as the lowest levels at the academies. For example, the excitement of the CDX coupled with West Point's 2001 and 2002 victories, sparked interest among the entire corp of cadets. As a result, the first ever student information assurance group was formed at West Point. The club, affiliated with the Association for Computing Machinery (ACM) Special Interest Group for Security Audit and Control (SIGSAC) has now grown to over 450 student members (over 10% of the entire corps of cadets) representing each of the 13 academic majors. The first student chapter of its kind, SIGSAC includes a wide range of interdisciplinary activities and has members from every academic department. In fact in there second year of existence they earned honors from IEEE as student chapter of the year.

The CDX has proven to be an effective vehicle in increasing information assurance awareness, facilitating ethical education and debate, providing leadership development opportunities and generating excitement in students for information assurance.

References

[1] J. Schafer, D. J. Ragsdale , J. R. Surdu, and C. A. Carver,"The IWAR range: a laboratory for undergraduate information assurance education," presented at Consortium for Computing in Small Colleges, Middlebury, Vermont, 2001.

[2] D. W. Welch, D. J. Ragsdale, and W. Schepens, "Training for Information Assurance," *IEEE Computer*, pp. 2-9, 2002.

[3] W.J. Schepens, D.W. Welch, and D.J. Ragsdale, "A Lesson in Cyber Defence," *Defence Systems International: Critical Information Systems*, June 2002.

Appendix 15. Sample Legal Liability Release Form

Student Certification and Agreement

I, _____, hereby certify that I have been given a copy of and have read and understand the Code of Conduct, and I agree that I will act at all times in accordance with that code. I understand that GWU takes its ethical obligations very seriously and violations will not be tolerated. I fully understand that GWU and its students must conduct the Program's activities in accordance with the highest possible ethical and legal standards. I know that I am responsible for ensuring that my personal conduct is above reproach. As a condition of studying in the Information Security Management Program at GWU, I agree that violations of the standards described in the Code of Conduct shall be made known immediately to my appropriate faculty member(s) and that violations will result in dismissal from the Program and failure to receive the Certificate or a degree with a concentration in information security management. I understand that this is a zero tolerance policy and that no second chances are given.

I agree to take all reasonable precautions to assure that sensitive University or faculty information, or information that has been entrusted to my fellow students or me by third parties (such as the students' employers), will not be disclosed to unauthorized persons. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the faculty or the person who is the designated information owner or custodian.

I also understand specifically that GWU provides computer systems and networks for my use in academic studies and that I am not permitted to use those computer systems and networks for personal business or for any activities not related to my academic studies. I understand that GWU audits and monitors the use of those computer systems and networks and that I have no right to privacy or expectation of privacy when I use computer systems and networks provided to me by GWU.

_____
Signature

_____
Printed Name

_____ _____
Student Number Date

S/N 052001-2