DEVELOPING CYBER WARRIORS FROM COMPUTER ENGINEERS *et al.*

Barry E. Mullins
Department of Electrical & Computer Engineering
Air Force Institute of Technology

Abstract

This paper discusses the development of a successful cyber warfare curriculum for computer and electrical engineering students at the Air Force Institute of Technology (AFIT). We leverage two traits exhibited by many engineers as we continually improve the curriculum. First, engineers are inherently inquisitive and notorious for disassembling things to better understand how they work. Second, the most effective pedagogical technique is to make the subject interesting and fun. This paper describes how we teach various computer-related topics by first teaching how things (e.g., computer networks and computer architecture) work in prerequisite courses and then teaching the students how to "break" them using cyber operations in our Cyber Attack course. We find students truly learn when challenged with defeating a computer protocol or architecture.

This paper outlines our cyber warfare curriculum with emphasis on our Cyber Attack and Cyber Defense course sequences. The paper focuses on methods used to teach the various phases of cyber attack to computer and electrical engineers, computer scientists, cyber operators as well as other technical majors. The paper also addresses our participation in the US National Security Agency-sponsored Cyber Defense Exercise (CDX). The overarching goal of the curriculum is to provide students with an understanding of how to attack and defend in the cyber domain using the CDX, as well as numerous course-oriented exercises, as proven effective teaching tools.

Identifying and collecting metrics for determining success in any course can be difficult. We use the results of national exercises (e.g., CDX), student feedback in the form of anonymous online critiques and test scores as our metrics. Results show the students are learning the finer points of computer systems as they hone their cyber warrior skills necessary to defend our information systems.

Introduction and Motivation

Securing information systems from intentional or unintentional information disclosure has quickly become one of our nation's top priorities. There are countless published examples of corporations and organizations loosing data due to cyber attacks. A recent high-profile example is the cyber attack on Google; this incident, codenamed Operation Aurora, was a highly sophisticated and targeted attack on Google's corporate infrastructure resulting in the theft of intellectual property[1,2]. It has been postulated there are even more unpublished or announced cyber attacks. Given the negative ramifications, including weakened consumer confidence, many corporations are leery of publicizing the fact that they have experienced a cyber attack. U.S. lawmakers are proposing a bill requiring corporations to report these attacks[3]. Cyber attacks are now acknowledged as significant threats to various nations' security[4-10]. Even seemingly innocuous attacks can have ramifications as illustrated by the 2009 U.S. Presidential election in which Sarah Palen's Yahoo email account was hacked[11]. Furthermore, attacks are now targeting SCADA (Supervisory Control And Data Acquisition) networks. SCADA networks refer to industrial and infrastructure control systems which typically include manufacturing, production, power generation, water treatment and distribution, oil and gas pipelines, and electrical power transmission and distribution including nuclear power. In fact, the highly-publicized Stuxnet malware is causing great concern over the future safety of our citizens given much of our critical infrastructure relies on potentially vulnerable information systems[12].

The time-tested adage goes "The best defense is a good offense". It behooves everyone involved in designing, using, and securing computing systems to thoroughly understand the realm of potential attacks against their systems in order to understand how to better defend against the attacks. Our definition of computing system extends beyond laptop and desktop computers; we include embedded systems including cell phones as well as SCADA networks.

The Air Force recognizes the vast damage possible through cyber attacks and added cyberspace to its mission statement[13]. Other military services and corporations also recognize the threats and are taking steps to mitigate them. Naturally, education plays a pivotal role in creating cyber warriors to support this persistent and potentially deadly threat. Many universities have developed a course or two to address this need. In 1996, AFIT created a cyber operations curriculum to educate our students and future leaders on the finer points of attacking and defending computing systems as well as the vast capabilities and limitations of cyber warfare[14].

The paper is organized as follows: the next section presents our Cyber Operations curriculum; this is followed by a discussion of cyber challenges and exercises we participate in to assess our student's comprehension of cyber warfare; the next section presents assessment results; and a final section which concludes the paper.

AFIT's Cyber Operations Curriculum

We define Cyber Operations (CO) as those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. Cyber Operations encompass most of the technological aspects of Information Operations (IO). To support CO, professionals must be cognizant of the tools, techniques, and practices required to defend, attack and exploit these resources. At the technical level, CO encompasses multiple scientific disciplines such as[15]:

- Computer and network defense, attack, and exploitation
- Cryptography
- Computer forensics
- Systems security engineering and operations
- Application software security
- Threat and vulnerability assessments and analyses

Our CO curriculum is designed to develop competency in a wide range of areas of computer engineering and computer science emphasizing security-related topics particular to cyber operations[15]. The curriculum consists primarily of the following courses taken in the order shown in Figure 1. The courses are described in the next section.

Fall	Winter	Spring	Summer
CSCE 525	CSCE 528	CSCE 628	CSCE 527
CSCE 526	CSCE 629	CSCE 725	
	CSCE 625		

Figure 1. Cyber Operations Curriculum Flow.

Prerequisite and Ancillary Courses

Developing competency in a wide range of computer engineering and science disciplines requires several courses. These courses are presented as either supporting or core in this paper in the sense that the supporting courses are still critical but not the focus of the paper. Supporting courses are either prerequisites or significantly enhance our core attack and defense courses and are discussed first.

CSCE 525 Introduction to Information Warfare

This course studies the nature of Information Assurance (IA), Information Operations (IO), Information Warfare (IW) and their ramifications for military operations and national security. It provides a foundational understanding of information operations doctrine and an overview of the various aspects of IO/IW. Emphasis is on cyber warfare and operations in cyberspace. The course examines military and national infrastructures including SCADA systems, vulnerabilities, interdependencies, threats, and

opportunities for exploitation. Students are expected to exit the course with a basic knowledge and understanding of information and cyberspace operations and their impact on warfare and national security. This course uses the text *Conquest In Cyberspace: National Security and Information* by Libicki as well as several current papers and news articles to spur discussion.

CSCE 526 Secure Software Design and Development

This course discusses the theory and techniques associated with the design of secure software and its protection. Topics include the policy and doctrine associated with software security and protection, designing systems for limited access and span of control, buffer overflow, authentication, trust management, and race conditions. This course uses the text *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them* by Howard, LeBlanc and Viega.

CSCE 527 Cyber Forensics

This course discusses cyber forensics and its effects on both information warfare and traditional forensic sciences. Students gain insight into the computer's role in crime, and the digital evidence available in a computer related investigation. Topics include the legal ramifications of evidence gathering, chain-of-custody, and methods for evidence preservation, identification, extraction, documentation, and interpretation as well as the tools available. This course uses the text *Incident Response and Computer Forensics* by Prosise, Mandia and Pepe.

CSCE 625 Information Systems Security, Assurance and Analysis I

This course examines the security of computer systems and networks using the tools provided by propositional and predicate logic to discover underlying principles of security. The course synthesizes elements from computer networking, operating systems security, and data security within an analytic framework. Topics include access control matrices, protection models, confidentiality, integrity, representing identity, flow and confinement, malicious logic and intrusion detection. Students taking this course learn about threats to information resources, countermeasures and their fundamental limitations. The course uses the text *Computer Security: Art and Science* by Bishop.

CSCE 725 Reverse Code Engineering

This course provides the foundations necessary to begin Reverse Code Engineering (RCE), which requires knowledge of both hardware and software architecture. This course focuses on Intel Architecture (IA32) executing Windows operating systems (OS) and applications. The goal of this course is to provide the foundations necessary towards software vulnerability discovery, exploitation development, and malware analysis. The course does not have a required text; course material is derived from Intel and Microsoft manuals in addition to reading various sections of the following texts:

- *Exploiting Software: How To Break Code* by Hoglund and McGraw
- *The IDA Pro Book* by Eagle
- *Hacker Disassembling Uncovered* by Kaspersky
- *Microsoft Windows Internals* 2005 by Russinovich and Solomon
- *Rootkits* by Hoglund and Butler
- *Reversing, Secrets of Reverse Engineering* by Eilam

Cyber Defense Courses

Our cyber defense sequence is split across two courses—CSCE 528 and CSCE 628. These courses are scheduled to coincide with the annual CDX exercise sponsored by the National Security Agency (NSA). The CDX is a competition designed to give students the opportunity to learn and demonstrate best practices in defensive information assurance. The fundamental objective is to design and implement a network which provides numerous IT services specified by the NSA and defend it against an onslaught of cyber attacks from NSA attackers[16].

CSCE 528 Cyber Defense and Exploitation I

This course discusses the hardware/software tools and techniques associated with the protection and exploitation of computer systems and networks. Students learn how to design and build a secure network including numerous networking services offered by most organizations in preparation for the CDX, which is described in more detail later. Emphasis is placed on the planning and designing of the services and infrastructure. Course topics include the DoD and USAF policy and doctrine associated with the protection of communication resources, intrusion detection systems, firewalls, honeypots and honeynets, span of control and accessibility, and use of various commercial and DoD tools for system protection and exploitation. The class is divided into teams, and each team is responsible for select services. The number and composition of teams vary each year based on the mandated services. A representative breakout of teams by services is shown in Table 1.

CSCE 628 Cyber Defense and Exploitation II

This course is a continuation of CSCE 528. Students use the tools and techniques learned in CSCE 528 to implement their plan and actually build their secure network and services. CSCE 628 provides ample lab time to prepare the network before the actual exercise, which occurs about halfway through the quarter. After the CDX, the remainder of the spring quarter consists of unstructured lab time in which students explore various aspects of the network and research incidents, attacks, and exploits they saw during the exercise. The students are able to conduct "what if" scenarios as well as investigate how the CDX exercised their areas of responsibility (functional areas). We also use this time to allow the students to learn more about the other functional areas; each team provides a briefing to the class detailing how they secured their area/services.

Cyber Attack Course (CSCE 629)

This course provides an introduction to the use of cyber attack. Students learn how to attack and exploit computing resources using hardware and software tools and techniques. Course topics include defining targets, gathering intelligence, exploiting and attacking targets, maintaining access/control of targets, and assessing attack success. We emphasize the fact we do not simply train our students how to use tools; we educate them on engineering and science involved as well as the foundational techniques used to attack and exploit. In other words, it is relatively easy to train someone to open a tool, configure it and launch it; this person is called a script kiddie and often has no understanding of the underlying techniques used to perform the requested action. Although not a course requirement, each student should be able to design and build their own attack tool at the end of this course based on their education.

Course Text

The text for this course is *Counter Hack Reloaded - A Step-by-Step Guide to Computer Attacks and Effective Defenses*, second edition by Ed Skoudis and Tom Liston. This is an outstanding text due to its treatment of how exploits work; it is not a

Table 1. AFIT CDX Team Composition.

Team Duties	**Team Size**
Team leaders	2
Firewalls, intrusion detection, external Domain Name Service (DNS)	2
Windows active directory, internal DNS, Exchange, Outlook, Outlook web access	3
Desktop services, video teleconference, public-key infrastructure, service monitoring, vulnerability scanning	4
Internet web server, MySQL database server	2
File sharing (public and private), incident response	2
IP security, peer-to-peer, client services	3

simple dictionary of tools and how to use them. The primary mission of the course is to teach why vulnerabilities exist, how to exploit them manually and using a tool which matches very nicely with this text. AFIT is on the quarters system, and classroom time is limited; therefore, the attack aspects from the text are emphasized even though the text provides outstanding defensive methods, techniques and tactics. The students receive this defensive information in CSCE 528 and CSCE 628. We also use the following texts as references:

- *Metasploit The Penetration Tester's Guide* by Kennedy et al.
- *BackTrack 5 Wireless Penetration Testing* by Ramachandran

Typical Course Flow

Table 2 shows the course flow and how the material is divided into seven areas which follow the typical stages of a successful cyber attack. Each area is presented during lecture followed by an accompanying lab. Since cyber attack is very much a hands-on activity, we find the students only truly learn by implementing the techniques and tactics discussed in class as well as using associated tools.

The course is taught using two-hour blocks for two days a week. Table 3 shows a representative detailed schedule. This schedule provides a breakout of the relative time spent on each topic as well as days dedicated entirely to lab time. Although lab time is not listed for each topic, the students are often given some time during class to work on the labs. With that said, most students have to finish the labs as homework.

Table 3. CSCE 629 Course Schedule.

Date	Text Chapter	Topic
5-Jan	1	Intro
7-Jan	5	Reconnaissance
12-Jan	6	Scanning
14-Jan	6	Scanning
19-Jan	6	Scanning
21-Jan	7	Exploit - Buffer Overflow
26-Jan	7	Lab time
28-Jan	7	Exploit - Password attacks
2-Feb	7	Lab time
4-Feb	7	Exploit - Web app attacks
9-Feb	8	Exploit - Network attacks
11-Feb	8	Exploit - Network attacks
16-Feb	9	Exploit - DoS attacks
18-Feb	10	Maintain Access
23-Feb	11	Covering Tracks
25-Feb		Exam
2-Mar		Final Project
4-Mar		Final Project
9-Mar		Final Project
11-Mar		Final Project

Table 2. Cyber Attack Topic Areas.

Topic Area	Tools Discussed
Reconnaissance	Wayback Machine, Whois, various Google directives, gcc
Scanning	Nmap, Nessus, Ipconfig, Ping, Traceroute, native Windows commands
Buffer Overflows / Exploitation	Nessus, Metasploit, gcc to compile various vulnerable programs, native Windows commands
Password Attacks	Fgdump, Cain, Ophcrack, John the Ripper, native Windows commands
Web App Attacks / Session Cloning / SQL Injection	Webgoat, Burp Proxy
Network Attacks including Wireless Attacks	Arpspoof, Dnsspoof, Ettercap, Netcat, native Linux commands, native Windows commands, aircrack-ng, Cain
Maintaining Access / Covering Tracks	Elitewrap, Covert_tcp, alternate data streams

Assessment Tools

The following tools are used to assess student performance. As shown in Table 3, one in-class, individual-effort exam is given toward the end of the quarter and covers all course material; the exam accounts for 30% of the grade. Given our students typically work in teams after graduation, all other assessment tools require the students to work in teams of two. Two projects (10% of the course grade) require the students to synthesize course material. The first project requires the students to research an existing attack tool and prepare a report describing how to load it and start it in sufficient detail such that fellow classmates can load and use the tool. The second project requires the students to create a custom lab, including the possibility of writing custom tools, based on methods and techniques not discussed in class. The seven labs account for 35% of the course grade; as mentioned, these labs are highly interactive and provide an opportunity for the students to experience and experiment with the techniques discussed in class.

In lieu of a final exam, a final project in the form of a Capture the Flag exercise is used. The final project comprises 25% of the grade and requires each team of two students to penetrate at least eight computers (targets) using information gathered during reconnaissance and discovered on various targets during the exercise. Team score is based on the number of targets penetrated as well as the number of user accounts successfully compromised. Compromising a user account typically involves two steps—learning the username of an account and then cracking (or otherwise determining) the user's password. Not all user accounts are equal; some are easier to compromise than others. Points are awarded based on the level of difficulty of learning the account names and cracking the passwords.

Cyber Challenges

Assessing our courses continues to be an important and ongoing effort. Beyond the student feedback discussed later, we also use external exercises to determine how our students compare to other universities.

NSA-Sponsored Cyber Defense Exercise (CDX)

The CDX is designed to give students the opportunity to learn and demonstrate best practices in defensive information assurance. This annual competition is sponsored and administered by the National Security Agency and gives the military service academies as well as the two military graduate schools, AFIT and the Naval Postgraduate School (NPS), an opportunity to assess their cyber skills. The NSA, in consultation with the schools, determines the services the schools must provide during the exercise. These services are meant to emulate a production operation. The schools are not directed on how to provide the services or how to secure them. As a result, each school typically creates a unique infrastructure to provide and secure the services. After the schools create their networks, the NSA attacks them during a week-long exercise in mid-April. The team with the fewest compromises is deemed the winner and awarded the NSA Information Assurance Director's Trophy. Since AFIT and NPS are graduate schools, they do not compete for the trophy but are scored using the exact same techniques and can be recognized as top performers if their score is the highest. A more detailed description of the CDX can be found in the references[14,16].

Beginning in 2009, the NSA invites AFIT and NPS to send students to participate on the attacking team called the Red Cell. The students operate side-by-side with the NSA's finest to attack networks of other schools. This gives the students an outstanding opportunity to exercise what they learned in the Cyber Attack course the previous quarter. Feedback from these students has been very favorable thus far.

Since the CDX is limited currently to military schools, other schools should seek out similar challenges such as the National Collegiate Cyber Defense Competition[17] and get involved.

DC3 Digital Forensics Challenge

The Department of Defense Cyber Crime Center (DC3) sponsors an annual digital forensics challenge called the DC3 Digital Forensics

Challenge. According to the executive director of DC3, the challenge "is a call to the digital forensics community to pioneer new investigative tools, techniques and methodologies"[18]. The challenge offers teams from around the world the opportunity to solve "approximately 20 different unique, single based challenges ranging from basic forensics to advanced tool development"[18]. Participants are asked to solve challenges similar to the following with increasing order of difficulty[18].

- Level 100: Challenges with a solution well known to experienced examiners (e.g., File Signatures, Suspicious Software, Hashing Metadata, etc.)
- Level 200: Challenges with a solution, but having a degree of difficulty (e.g., Data Hiding, File Headers, Passwords, Registry, etc.)
- Level 300: Difficult challenges that may have a solution, but it is not well known (e.g., Encryption, Parsing, etc.)
- Level 400: Challenges with no known solution (e.g., Communication Recovery/Parsing, Concealment of information within computer files, etc.)
- Level 500: Challenges that involve Digital Forensic tool development based on defined requirements (e.g., tools, methodologies, etc. for known Digital Forensic investigation issues)

Results

Assessing the success of any program is difficult. We use a variety tools to determine the success of our cyber operations program such as the results of the CDX exercise and the DC3 challenge for external validation. We use student feedback for internal assessment.

As mentioned, we have participated in the annual CDX exercise since 2001. We have attained the highest score seven out of the last eight years. The students use the expertise learned in our Cyber Attack course to determine how hackers and penetration testers think and operate. They then learn how to secure their network in our Cyber Defense courses. We have found this combination of courses in this order to serve our students well.

AFIT has participated in the DC3 Digital Forensics Challenge the past four years. We were the grand champions in 2007 (team name of Cyber Warriors) and were the U.S. winner (DC3 Prize) in 2009 (team name of Little Bobby Tables) primarily as a result of our Forensics and Cyber Attack courses.

Thus far, student feedback has been phenomenal! Students made the following comments about the Cyber Attack course:

"The course was challenging yet fun."
"I learned so much it's ridiculous!"
"By far, this is the highest quality educational course I've ever taken in my military or educational career."
"His course is not easy, but the challenges he presents make the students better."
"The final project [the capture the flag project] was awesome."
"Liked the mixture of lecture and labs…kept it interesting."
"The final project enhanced my knowledge of computer networks in a way that no other networking course ever has."

Test scores since curriculum inception also indicate students are truly learning computer networking, Internet applications, computer architecture, and how to solve difficult problems using sound engineering practices. In fact, one student commented, "I thought I knew computer networking, but it wasn't until I finished your course [Cyber Attack] that I now truly know networking."

Numerical feedback from all four years the course has been offered is outstanding. Table 4 contains the questions asked of the students as well as their averaged responses on a 5.00 scale. Reluctantly, questions 13 and 14 were not asked during 2008 and 2009.

Although not a formal assessment metric, course enrollment can be another indicator of course success if the course is not required of all students. Student enrollment in these courses continues to

increase each year despite a relatively flat school enrollment. The enrollment in Cyber Attack has grown from 20 in 2008 to 45 in 2011. Enrollment in the Cyber Defense courses has also seen similar increases the past three years. These numbers are very encouraging and seem to indicate the courses are serving our students well. In fact, many local employees sit in on the Cyber Attack course to learn more about the subject or hone their skills.

Conclusions

Cyber attack and defense is a critical facet of day-to-day business for all organizations now and into the foreseeable future. Our curriculum provides a solid foundation to computer and electrical engineers, as well as other students, in the finer points of defending our information systems. A successful defense should start with a clear understanding of the offensive techniques and tactics that might be used to compromise a system. Therefore, our curriculum leverages a very successful Cyber Attack course to better teach cyber defense.

Student responses to the courses have been phenomenal with many testimonials attesting to the value of the courses to not only teach cyber topics, but to also teach the finer points of computer and network systems by investigating how the systems are vulnerable and how to break them. We are very pleased most students indicate the courses are "fun", which is the goal.

Based on the success of our cyber curriculum, the Center for Cyberspace Research (CCR) at AFIT is expanding our educational mission to include two new continuing education courses—Cyber 200 and Cyber 300[19]. Cyber 200 is designed to refresh and provide more breadth to cyberspace professionals six to eight years after their initial cyberspace training. Cyber 300 is designed to provide a broad background at the strategic level in "cyber concepts, including

Table 4. Student Feedback for CSCE 629, Cyber Attack.

Question		**2008**	**2009**	**2010**	**2011**
1	The objectives for this course were made clear at the beginning of the course.	4.92	4.93	4.90	4.83
2	The objectives of this course were met throughout the quarter.	4.92	4.93	4.90	4.83
3	The text (or other materials) for this course was helpful.	5.00	4.86	4.80	4.91
4	The methods of evaluation (exams, papers, etc.) were appropriate for this course.	4.85	4.93	5.00	4.55
5	Overall I think that this course will be valuable to my education.	5.00	4.93	4.90	4.83
6	Overall, I think that this course will be valuable to my professional career.	5.00	4.85	4.70	4.65
7	This course was taught at the appropriate level of difficulty.	4.85	4.93	5.00	4.78
8	I had the opportunity to learn a lot in this course.	5.00	4.93	5.00	4.91
9	The required prerequisites (If any) prepared me for the course.	4.92	4.93	4.70	4.43
10	The work I was required to do helped me learn the course material.	5.00	4.93	5.00	4.91
11	Please rate the overall quality of this course based on factors such as content, relevance, etc., on a scale of 1 to 5 (5 is the highest score).	4.92	4.86	4.90	4.52
12	Please rate the overall quality of course instruction on a scale of 1 to 5 (5 is the highest score).	5.00	4.86	4.90	4.70
13	The use of the labs enhanced my learning.	--	--	4.90	5.00
14	The final project (capture the flag) accessed what I learned during the course.	--	--	4.90	5.00

capabilities, limitations and vulnerabilities and their associated application and employment in joint military operations"[19].

Acknowledgements

The author acknowledges the funding and support of the Center for Cyberspace Research. The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

References

1. D. Drummond, A new approach to China, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html, last accessed 6 January 2011.

2. McAfee, Operation Aurora, http://www.mcafee.com/us/threat_center/operation_aurora.html, last accessed 6 January 2011.

3. Bill to require private sector reporting of cyber attacks, http://www.federalnews radio. com/index.php?nid=150&sid=2123868, last accessed 6 January 2011.

4. BBC News, Cyber attacks and terrorism head threats facing UK, *BBC News*, http://www.bbc.co.uk/news/uk-11562969, last accessed 6 January 2011.

5. J. Bliss, U.S. Nuclear Plants Vulnerable to Cyber Attacks, Analysts Say, http://www.bloomberg.com/news/2010-11-17/u-s-nuclear-plants-vulnerable-to-cyber-attacks-analysts-say.html, last accessed 6 January 2011.

6. S. Gorman and S. Fidler, Cyber Attacks Test Pentagon, Allies and Foes, http://online.wsj.com/article/SB10001424052748703793804575511961264943300.html, last accessed 6 January 2011.

7. T. McCarthy, Cyber Attacks Jeopardize Superpower Status, http://www.cbsnews.com/stories/2010/04/22/eveningnews/main6422768.shtml, last accessed 6 January 2011.

8. J. Meserve, Sources: Staged cyber attack reveals vulnerability in power grid, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US, last accessed 6 January 2011.

9. M. Malseed, U.S. Government Faces Growing Cyber Threat, http://ohmygov.com/blogs/general_news/archive/2010/10/07/us-government-faces-growing-cyber-threat-infographic.aspx, last accessed 6 January 2011.

10. Student Guide for Masters Programs, Air Force Institute of Technology, 21 June 2010

11. K. Zetter, Palin E-Mail Hacker Says It Was Easy, http://www.wired.com/threatlevel/ 2008/09/palin-e-mail-ha/, last accessed 6 January 2011.

12. N. Falliere, L. Murchu, and E. Chien, W32.Stuxnet dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, last accessed 6 January 2011.

13. M. Gettle, "Air Force releases new mission statement", *Air Force Print News*, http://www.af.mil/news/story.asp?storyID=123013440, last accessed 6 January 2011.

14. B. E. Mullins, T. H. Lacey, R. F. Mills, and R. A. Raines The Morphing of a Cyber Operations Curriculum at AFIT *IAnewsletter*, Vol. 10 No. 1 Spring 2007, pp. 26-30, http://iac.dtic.mil/iatac/IA_newsletter.jsp.

15. D. Dombey, Pentagon warns of security threat, http://www.ft.com/cms/s/0/e1a1ce6e-03d7-11e0-8c3f00144feabdc0.html #axzz 181OoEB4r, last accessed 13 December 2010.

16. B. E. Mullins, T. H. Lacey, R. F. Mills, J. M. Trechter and S. D. Bass, "How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum," *IEEE Security and Privacy*, Vol. 5, No. 5, September/October 2007, pp. 40-49.

17. National Collegiate Cyber Defense Competition, http://www.nationalccdc.org/, last accessed 6 January 2011.

18. DC3 Digital Forensics Challenges, http://www.dc3.mil/challenge/#, last accessed 6 January 2011.

19. Cyber 200 and 300 Course Information, http://www.afit.edu/en/ccr/centerprograms.cfm?a=cyber, last accessed 6 January 2011.

Biographical Information

Barry E. Mullins is an Associate Professor of computer engineering in the Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson AFB OH. He received a B.S. in computer engineering (cum laude) from the University of Evansville in 1983, an M.S. in computer engineering from the Air Force Institute of Technology in 1987, and a Ph.D. in electrical engineering from Virginia Polytechnic Institute and State University in 1997. He served 21 years in the Air Force, teaching at the U.S. Air Force Academy for seven of those years. He is a registered Professional Engineer in Colorado and a member of Tau Beta Pi (engineering), Eta Kappa Nu (electrical and computer engineering), Phi Beta Chi (science), Kappa Mu Epsilon (mathematics), IEEE (Senior Member), and ASEE. His research interests include cyber operations, malware analysis, computer/network security, computer communication networks, embedded (sensor) and wireless networking, reverse code engineering, and reconfigurable computing systems. Mullins has won numerous teaching and research awards, including the 2011 Cage H. Crocker Outstanding Professor Award, 2010 IEEE Eta Kappa Nu C. Holmes MacDonald Outstanding Teaching Award, 2010 Air Force Science and Engineering Educator of the Year, AFIT Instructor of the Year (Dr. Leslie M. Norton Teaching Excellence Award), AFIT Instructor of the Quarter twice, AFIT Eta Kappa Nu Outstanding Teaching Award for Electrical and Computer Engineering, and the AFIT Professor Ezra Kotcher Award Teaching Excellence Award for outstanding curriculum development. During his time at the Air Force Academy, he also received the U.S. Air Force Academy's Outstanding Academy Educator Award, as well as the Brig. Gen. R. E. Thomas award for outstanding contribution to cadet education twice.