### Faculty Contact Information

[kcardwel@faculty.ed.umuc.edu](mailto:kcardwel@faculty.ed.umuc.edu)

### Course Materials

Title: Hacking: The Next Generation

Author: Dhanjani, Rios & Hardin

Copyright: 2009

Publisher: O'Reilly & Associates, Inc.

ISBN: 9780596154578

For textbooks, visit <https://webtext.europe.umuc.edu>.

### Course Description

(Formerly IFSM 457.) Prerequisites: CSIA 302 (or CMIT 265) and CSIA 303.

In-depth analysis of differences between cyberterrorism and cyber crime and the motivations that drive cyber adversaries. The goal is to assess cyberterrorism and cyber crime related vulnerabilities, understand the use of network analysis tools, and identify the differences between computer network defense and offense and the difficulties associated with a global threat space. Students may receive credit for only one of the following

courses: CSIA 457, IFSM 457, or IFSM 497C.

### Course Outcomes

After completing this course, you should be able to 1. interpret and communicate the concepts, terminology, and motivations associated with cybercrime and cyberterrorism, and translate problems into viable solutions 2. research and apply industry and government best practices regarding cybercrime and cyberterrorism mitigation strategies to protect the organizational mission 3. analyze existing cybersecurity capabilities and develop and adjust strategy to address changing threats

4. evaluate and select appropriate analysis tools and techniques to mitigate cyberterrorism and cybercrime threats

### Course Introduction

This course provides an in-depth analysis of the differences between cyberterrorism and cybercrime and the motivations that drive all types of cyber adversaries. By the end of this course, you will be able to assess

cyberterrorism- and cybercrime-related vulnerabilities and develop and implement mitigation strategies to deter the exploitation of systems and networks by adversaries. You will gain a deeper understanding of the use of network analysis tools and will be able to identify the differences between computer network defense and computer network offense and the difficulties associated with a global threat space.

Concepts learned in this course will be directly applicable to careers in information assurance and cybersecurity.

### Grading Information and Criteria

A standard 100-pt scale, with grades of A (90-100) B (80-89), C (70-79), D

(60-69) , and F (0-59) (superior, above average, average, below average, unacceptable).

Weekly Conference Responses, homework and participation 25%

Project 1 10%

Project 2 30%

Project 3 20%

Final Exam 15%

The grading scale, based on 100 points, is as follows:

A = 90-100

B = 80-89

C =  70-79

D =  60-69

F = 0-59

### Other Information

The University of Maryland University College regulations are strict about the assignment of an Incomplete. Please consult the Undergraduate Catalog for further Do not expect an Incomplete in the course unless you have serious personal problems very close to the end of the term or have official TDY orders or other documentation of official duties.

Information on Grading policies:

Late Policy: The assignment, participation (discussion Topics and Web

Activities), and exams should be submitted on time. Students have a long lead-time in which to prepare, ask questions, and seek help. Therefore, unless a major accident, illness, or work assignment (with supporting

documentation) prevents a student from submitting work on time, 10% will be docked from each late assignment's grade.

Extra Credit: Extra credit is not normally given.

Attendance: Although attendance is not counted in the grade, Weekly

Participation is, and it is an important part of the learning process

online.

Writing and Research: Effective writing is critical to the intellectual life of university students and graduates within the workplace. Effective managers are usually effective communicators. Your work in this course must demonstrate your ability to master and effectively communicate course content. Efficient writing:

\*Meets the needs of the reader

\*Adequately covers the subject

\*Uses expected conventions of the format and organizations

\*Demonstrates use of credible reasoning and evidence

\*Satisfies standards of style and grammatical correctness

\*Requires 100% compliance with UMUC's zero-tolerance policy regarding

plagiarism.

### Project Descriptions

All projects are to be in Microsoft Word or RTF format.  References are required for all work.  Papers are to be single-spaced 10 or 12 point font, in Times Roman or Arial script.

Project One:

5-7 page paper on SCADA and Critical Infrastructure Systems.

Project Two:

5-7  Mobile devices and how they threaten or security

Project Three

5-7 pages on sophisticated malware and how anti-virus cannot protect us

### Course Schedule

Week 1

16 Jan

Introduction

Hacking Methodology

Chapter 1: Intelligence Gathering

Reconnaissance

Week 2

23 Jan

Chapter 2: Inside out Hacking

Scanning

Gaining Access

Maintaining Access

Week 3

30 Jan

Chapter 3: The Way it Works

Terrorism and Security

National Security Policy

Covering the tracks in hacker attacks

Group Assignments and Coordination Tasks

\*\*\* Project One: SCADA and Critical Infrastructure Systems

Week 4

6 Feb

Airline Travel

Privacy and Surveillance

Chapter 4:Blended Threats

Chapter 5: Cloud Insecurity

ID Cards and Security

Group Task - The Cloud

Week 5

13 Feb

Security and Disasters

Chapter 6: Abusing Mobile Devices

Economics of Security

\*\*\* Project Two: Group - The risk of mobile devices to our networks

Week 6

20 Feb

Psychology of Security

Chapter 7: Infiltrating the Phishing Underground

Chapter 8: Influencing Your Victims

Chapter 10: Business of Security

Week 7

27 Feb

Cybercrime and Cyberwar

Chapter 9: Hacking Executives

Chapter 10: Case Studies

\*\*\* Project Three: GROUP Sophisticated malware and why anti-virus cannot help us

Week 8

5 Mar

Computer and Information Security

Reference Materials

Review for the Final Exam

\*\*\* Final Exam

### Faculty Bio

Kevin Cardwell spent 22 years in the U.S. Navy, during this time he tested and evaluated Surveillance and Weapon system software, some of this work was on projects like the Multi-Sensor Torpedo Alertment Processor (MSTRAP), Tactical Decision Support System (TDSS), Computer Aided Dead Reckoning Tracer (CADRT), Advanced Radar Periscope Discrimination and Detection (ARPDD), and the Remote Mine Hunting System (RMHS). He has worked as both software and systems engineer on a variety of Department of Defense projects and early on was chosen as a member of the project to bring Internet access to ships at sea. Following this highly successful project he was selected to head the team that built a Network Operations Center

(NOC) that provided services to the commands ashore and ships at sea in the Norwegian Sea and Atlantic Ocean . He served as the Leading Chief of Information Security at the NOC for six years prior to retiring from the U.S. Navy. During this time he was the leader of a 5 person Red Team that had a 100% success rate at compromising systems and networks.

He currently works as a free-lance consultant and provides consulting services for companies throughout the world, and as an advisor to numerous government entities within the US and UK . He is an Instructor, Technical Editor and Author for Computer Forensics, and Hacking courses. He is technical editor of the Learning Tree Course Ethical Hacking and Countermeasures and Computer Forensics. He is author of the Controlling Network Access course. He has presented at the Blackhat USA Conferences. He is a contributing author to the Computer Hacking Forensics Investigator V3 Study Guide and The Best Damn Cybercrime and Digital Forensics Book Period.

He is a Certified Ethical Hacker (CEH), Certified Security analyst (E|CSA), Qualified Penetration Tester (QPT), Certified in Handheld Forensics, Computer Hacking Forensic Investigator (CHFI) and Live Computer Forensics Expert (LCFE), and holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas. His current research projects are in Computer Forensic evidence collection on "live" systems, Professional Security Testing and Advanced Rootkit technologies. He developed the Strategy and Training Development Plan for the first Government CERT in the country of Oman, he servers as a professional training consultant to the Oman Information Technology Authority, and is currently developing the team to man the first Commercial Security Operations Center in the country of Oman and is working with the Malaysian Government as Master Course Developer for the Asia/Pacific Cyber Security and Forensics Centre of Excellence,