MORGANSTATEUNIVERSITY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

EEGR480 Introduction to Cyber Security
Credits: 3
ONLINE
COURSE SYLLABUS

Instructor: Dr. Farzad Moazzami
Office: SEB, RM 334
Telephone No. (443) 885-4204
Email Address: Farzad.Moazzami@morgan.edu
Office Hours:

References
Recommended:
Other reference material as provided via Bb

Catalog Description
This course will provide a basic introduction to of all aspects of cyber-security including business, policy and procedures, communications security, network security, security management, legal issues, political issues, and technical issues. This serves as the introduction to the cyber security track in electrical and computer engineering department.
Prerequisite: EEGR 317; Recommended Co-requisite: EEGR 410

Course Requirements
This course is an elective course for all engineering undergraduate students, especially those with the computer engineering, networks, communications concentration, or cyber security interest. This course relates heavily to the EEGR410/481/482/483 series.

Course Objectives
This course provides students basic knowledge and skills in the fundamental theories and practices of Cyber Security. Upon completion of the course a student is expected to have met the following six (6) course objectives COs). These course objectives are tied to weekly objectives found in each module.

- CO1: Understand the broad set of technical, social & political aspects of Cyber Security
- CO2: Appreciate the vulnerabilities and threats posed by criminals, terrorist and nation states to national infrastructure
- CO3: Understand the nature of secure software development, operating systems and data base design
- CO4: Recognized the role security management plays in cyber security defense
- CO5: Understand the security management methods to maintain security protection
- CO6: Understand the legal and social issues at play in developing solutions.

Detailed Schedule
<table>
<thead>
<tr>
<th>Content</th>
<th>Date</th>
<th>Reference</th>
<th>Topic</th>
<th>Assignmen</th>
</tr>
</thead>
</table>
| Module 1    | TBD   | Chapter 1 | Chapter 1 Introduction (CO1,CO2)  
1.1 What Is Computer Security?  
1.2 Threats  
1.3 Harm  
1.4 Vulnerabilities  
1.5 Controls | M1        |
| Module 2    | TBD   | Chapter 2 | Chapter 2 Toolbox: Authentication, Access Control, and Cryptography (CO1,CO2,CO3)  
2.1 Authentication  
2.2 Access Control  
2.3 Cryptography | M2        |
| Module 3    | TBD   | Chapter 3 | Chapter 3 Programs and Programming (CO2,CO3,CO4)  
3.1 Unintentional (Non-malicious) Programming Oversights  
3.2 Malicious Code—Malware  
3.3 Countermeasures | M3        |
| Module 4    | TBD   | Chapter 4 | Chapter 4 The Web—User Side (CO2,CO3)  
4.1 Browser Attacks  
4.2 Web Attacks Targeting Users  
4.3 Obtaining User or Website Data  
4.4 Email Attacks | M4        |
| Module 5    | TBD   | Chapter 5 | Chapter 5 Operating Systems (CO3,CO4,CO5)  
5.1 Security in Operating Systems  
5.2 Security in the Design of Operating Systems  
5.3 Rootkit | M5        |
| Module 6    | TBD   | Chapter 6 | Chapter 6 Networks (CO2,CO3,CO4)  
6.1 Network Concepts  
6.2 Threats to Network Communications  
6.3 Wireless Network Security  
6.4 Denial of Service  
6.5 Distributed Denial-of-Service Strategic Defenses: Security Countermeasures  
6.6 Cryptography in Network Security  
6.7 Firewalls  
6.8 Intrusion Detection and Prevention Systems  
6.9 Network Management | M6        |
| Module 7    | TBD   | Chapter 7 | Chapter 7 Databases (CO3,CO4)  
7.1 Introduction to Databases  
7.2 Security Requirements of Databases  
7.3 Reliability and Integrity  
7.4 Database Disclosure  
7.5 Data Mining and Big Data | M7        |
| Module 8    |       |           | ORAL MIDTERM EXAM                                                      |           |
| Module 9    | TBD   | Chapter 8 | Chapter 8 Cloud Computing (CO3,CO4,CO5)  
8.1 Cloud Computing Concepts  
8.2 Moving to the Cloud  
8.3 Cloud Security Tools and Techniques  
8.4 Cloud Identity Management  
8.5 Securing IaaS | M9, P9    |
| Module 10 | TBD | Chapter 9 | Module 10 | TBD | Chapter 9 – Privacy (CO4,CO5)  
9.1 Privacy Concepts  
9.2 Privacy Principles and Policies  
9.3 Authentication and Privacy  
9.4 Data Mining  
9.5 Privacy on the Web  
9.6 Email Security  
9.7 Privacy Impacts of Emerging Technologies  
9.8 Where the Field Is Headed |
|----------|-----|-----------|-----------|-----|-------------------|
| Module 11 | TBD | Chapter 10 | Module 10 | TBD | Chapter 10 Management and Incidents (CO3,CO4,CO5,CO6)  
10.1 Security Planning  
10.2 Business Continuity Planning  
10.3 Handling Incidents  
10.4 Risk Analysis  
10.5 Dealing with Disaster |
| Module 12 | TBD | Chapter 11 | Module 10 | TBD | Chapter 11 Legal Issues and Ethics (CO3,CO4,CO5,CO6)  
11.1 Protecting Programs and Data  
11.2 Information and the Law  
11.3 Rights of Employees and Employers  
11.4 Redress for Software Failures  
11.5 Computer Crime  
11.6 Ethical Issues in Computer Security  
11.7 Incident Analysis with Ethics |
| Module 13 | TBD | Chapter 13 | Module 10 | TBD | Chapter 13 Emerging Topics (CO5,CO6)  
13.1 The Internet of Things  
13.2 Economics  
13.3 Computerized Elections  
13.4 Cyber Warfare |
| Module 14 | ORAL FINAL EXAM | | | | |

**Format:** Online

**Grading:**

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework</td>
<td>40%</td>
</tr>
<tr>
<td>Research Projects</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm Exam</td>
<td>15%</td>
</tr>
<tr>
<td>Discussion Board</td>
<td>10%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>15%</td>
</tr>
</tbody>
</table>
NOTE: Any material submitted that is substantially copied from other students without citation or from the Internet will receive a zero grade.

Notes: Expectations and Requirements
1. Students are expected to log on to Bb 3 times a week.
2. Students are expected to be actively engaged on the discussion board conversations.
3. Homework and other assignments are due by midnight of the given due date. Late penalty will be deducted for late submission.
4. A programming assignment might be given in lieu of a quiz.
5. Academic misconduct or cheating during an exam will result in an F grade for the course.