Catalog Description
This course will provide the basic concepts in the many aspects of security associated with today’s modern computer networks including local area networks and the internet. It includes the fundamentals of network architecture, vulnerabilities, and security mechanisms including firewalls, guards, intrusion detection, access control, malware scanners and biometrics.

Prerequisite: EEGR 317

Course Objective:
This course will provide the basic concepts in the many aspects of security associated with today’s modern computer networks including local area networks and the internet. It includes the fundamentals of network architecture, vulnerabilities, and security mechanisms including firewalls, guards, intrusion detection, access control, malware scanners and biometrics.

Specific topic coverage includes

- Network Security Landscapes
- Security Principles and Practices
- Operating Systems and Applications
- Network Security Fundamentals
- Communication
- The Security Threats and Response Integrated Cyber Security
- Privacy in Computing
- The Internet of Things
- Data Acquisitions and Analytics

Upon successful completion of this course, a student will have met the following six (6) course objectives (COs). These course objectives are larger goals for weekly objectives found in each module.

- **CO1**: Articulate the network security landscape as it pertains to cyber security past and present
- **CO2**: Understand guiding security principles and practices including processes and policies of systems management
- **CO3**: Identify risks and methods for improving security of operating systems and applications including web browsers, domains and servers
- **CO4**: Explain the fundamentals of security for network protocols and wireless technologies
- **CO5**: Be knowledgeable of the various communications for maintaining security such as secret communications like cryptography and covert communications steganography; explain how these are applied in email, on servers and across networks

- **CO6**: Recognize integrated cyber security for different types of devices (smartphones, computer tablets etc.) and how security is validated on computer systems

- **CO7**: Apply the knowledge of Intrusion Detection and Prevention Systems and their components for threat detection and response.

**Point Rubric/ Assessment**

Grades will be assigned as follows:

- 90 – 100%  
  A
- 80 – 89 %  
  B
- 70 – 79%  
  C
- 0 – 70%  
  F

20 points: Midterm Examination

20 points: Final Examination

- Both examinations are cumulative and given in a varied format. An in-class review will be held prior to each examination.

30 Points: Quizzes

- Quizzes vary from five to ten questions and may be in any format. (3 Quizzes worth 10 points each) *Quizzes cannot be made up.*

20 Points: Homework and Assignments

- Presentations will be 10 minutes and topic areas will cover weekly course objectives and Raspberry Pi assignments.

10 Points: Class Participation – Attendance

- Your interaction with your instructor and fellow students occur through your presentation of news articles, homework assignments best practices relating to Cyber Security-Network Security Related Topics.

(When necessary, I use standard mathematical rounding rules to round grades to the nearest whole number when assigning letter grades.

**Late Work**

Unless and otherwise noted, all assignments must be completed by 8:00 on the due date and all times are Eastern Standard Time. Late work (*Homework Assignments only*) will be dropped one point for each day that is late. If you have an extenuating circumstance or need special accommodations, please contact me before the due date, and I will try to work something on.

**Receiving Feedback**

I will grade and return assignments to you within 7 days following the due date. You can review your grades by going to the *My grades* link in the right course menu.
# Course Outline
Below is an outline of weekly lessons and activities.

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Chapter Reading</th>
<th>Exams/Quizzes/Assignments</th>
</tr>
</thead>
</table>
| 1 Jan, 2016 | **Module1: Network Security Landscape**  
- State of Network security: cyber security  
- New Approaches to Cyber Security: General Trends, The changing faces of cyber security  
- Interfacing with the organization: An Enterprise Security Methodology, Key Questions to Manage Risk, Database | Chapter 1  
Chapter 2  
Chapter 3 | *Introduction on BB*  
*Post summary of (Module-1 on BB)* |
| 2 | **Module2: Security Principles and Practices**  
- Access control: Control Models, Types of Access Control Implementations, Identification and Authentication, Databases and Remote Access | Chapter 4  
Chapter 5  
Chapter 6 | **Homework # 1**  
(Chapter 4-6) |
| 3 | **Module2: Security Principles and Practices (continued)**  
**Module3: Operating Systems and Applications**  
- Unix and Linux Security: The Focus of Unix/Linux Security, Physical Security, Controlling the Configuration, Operating UNIX Safely, Hardening UNIX | Chapter 7  
Chapter 8  
Chapter 9 | **Post summary of (Chapter 7-9 on BB)** |
<table>
<thead>
<tr>
<th>4</th>
<th><strong>Module 3: Operating Systems and Applications (continued)</strong></th>
</tr>
</thead>
</table>
|  | ● Web security: What’s HTTP ?, How HTTP works ?, Server Content, Client Content, State, Attacking Web Servers, Web Services  
|  | ● Electronic mail (E-mail) Security  
|  | ● Domain name System: DNS Basics, Purpose of DNS, Setting Up DNS, Security Issues with DNS, DNS Attacks, Designing DNS, Master Slave DNS, Detailed DNS Architecture, DNS SEC  
|  | Chapter 10-14  
| 5 | **Module 4: Network Security Fundamentals** |
|  | Chapter 15-16  
| 6 | **Module 4: Network Security Fundamentals (continued)** |
|  | ● Firewalls: Firewalls, Firewall Rules, The Use of Personal Firewalls  
|  | Chapter 17-19  
|  | **Quiz #1**  
|  | (Module 1-3)  
|  | **Post summary of**  
|  | (Chapter 15-16 on BB)  
|  | **Project 1** (TCP Wireshark)  
|  | **due by end of week 7**  
|  | **Homework # 2**  
|  | (Summary on Module -4)
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>Chapter/Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><strong>Module5: Communication</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Secret communication: What is Cryptography, General Terms, General</td>
<td>Chapter 20-21</td>
</tr>
<tr>
<td></td>
<td>Cryptography Principles, The Four Cryptography Primitives, Putting These</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primitives together to Achieve CIA, Proprietary Versus Open Source</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Algorithms, Attacks on Hash Functions, Quantum Cryptography</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Covert communication: Where Hidden Data Hides, Where did it Come From,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Where is it going, Overview of Steganography, Steganography Compared to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptography, Types of Steganography, Products that Implement Steganography,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Steganography Versus Digital Water Marking, Goals of Digital Water Marking,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><strong>Module5: Communication (continued)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Application of secure/covert communication: E-mail, Authentication</td>
<td>Chapter 22</td>
</tr>
<tr>
<td></td>
<td>Servers, Working Model, Public Key Infrastructure, Virtual Private</td>
<td>Homework #3 (Chapter 20-22)</td>
</tr>
<tr>
<td></td>
<td>Networks, Secure Sockets Layer/ Transport Layer Security, SSL Handshake</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><strong>Spring break</strong></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><strong>Module6: Security Threat and Response</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Intrusion detection and response: Intrusion Detection Mechanisms,</td>
<td>Chapter 23-24</td>
</tr>
<tr>
<td></td>
<td>Honeypots, Incident Handling</td>
<td>Post summary Chapter 23-24 on BB</td>
</tr>
<tr>
<td>11</td>
<td><strong>Module6: Security Threat and Response (continued)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security assessment, testing and evaluation: Information Assurance</td>
<td>Chapter 25</td>
</tr>
<tr>
<td></td>
<td>Approaches and Methodologies, Certification and Accreditation, DIACAP,</td>
<td>Quiz #2 (Module 4-5)</td>
</tr>
<tr>
<td></td>
<td>Federal Information Processing Standard 102, OMB Circular A-130, The</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National Institute of Standards and Technology Assessment Guidelines,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Penetration Testing, Auditing and Monitoring</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><strong>Module7: Integrated Cyber Security</strong></td>
<td>supplement materials</td>
</tr>
<tr>
<td></td>
<td>- Smartphone and mobile device security</td>
<td>Project #2 (IDS Snort) due by end of week 14</td>
</tr>
<tr>
<td>13</td>
<td><strong>Module7: Integrated Cyber Security (continued)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Validating your security: Overview, Current</td>
<td>Chapter 26-28</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Homework #4 (Module 6)</td>
</tr>
</tbody>
</table>
### State of Penetration Testing, Formal Penetration Testing Methodology, Steps to Exploiting a System, Exploiting the System, Uploading Programs, Keeping Access: Back doors and Trojans, Covering One’s Tracks

- **Data protection:** Identifying and Classifying Sensitive Data, Creating a Data Usage Policy, Controlling Access, Using Encryption, Hardening end points and Network Infrastructure, End Point Security, Insider Threats and Data Protection
- **Putting everything together:** Critical Problems Facing Organizations, General Tips for Protecting a Site, Security Best Practices

| 14 | presentations | Final exam |

### References

**Textbook (Required)**


All readings will come from the textbook. You can order from through MSU Bookstore or via online resources.


**Additional Reading**

Raspberry Pi


National Institute of Standards and Technology (NIST)


IoT News Network

[http://www.iotnewsnetwork.com](http://www.iotnewsnetwork.com)

MIT Technology Review

[http://www.technologyreview.com](http://www.technologyreview.com)
Krebs on Security

http://krebsonsecurity.com

Department of Homeland security-critical Infrastructure sectors

http://www.dhs.gov/critical-infrastructure-sectors

United States Computer Emergency Readiness Team

http://www.us-cert.gov

Chronology of Data Breaches

https://www.privacyrights.org/data-breach