MORGAN STATE UNIVERSITY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COURSE SYLLABUS
FALL, 2015
ONLINE EEGR.481 INTRODUCTION TO NETWORK SECURITY
CREDITS: 3

THIS COURSE IS A SENIOR ELECTIVE IN THE ECE DEPARTMENT.

INSTRUCTOR: THIERRY WANDJI
EMAIL: KETCHIOZO.WANDJI@MORGAN.EDU

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.

Week	Topics	Chapter Reading	Exams/Quizzes/ Assignments
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	Chapter1 Chapter2 Chapter3	***Introduction** on BB ***Post** summary of (Module-1 on BB)
2	**Module2: Security Principles and Practices** ● Information System Security Principles: Key Principles of Network Security, Formal Processes, Risk Management, Calculating and Managing Risk ● Information System Security Management: Security Policies, Security Awareness, Managing the Technical Effort, Configuration Management, Business Continuity and Disaster Recovery Planning, Physical Security, Legal and Liability Issues ● Access control: Control Models, Types of Access Control Implementations, Identification and Authentication, Databases and Remote Access	Chapter4 Chapter5 Chapter6	**Homework # 1** (Chapter 4-6)
3	**Module2: Security Principles and Practices (continued)** ● Attacks and Threats: Malicious Code, Review of Common Attacks, External Attack Methodologies Overview, Internal Threat Overview **Module3: Operating Systems and Applications** ● Windows security: Windows Security at the Heart of the Defense, Out-of-the-Box Operating System Hardening, Installing Applications, Putting the Workstation on the Network, Operating Windows Safely, Upgrades and Patches, Maintain and Test the Security, Attack against the Windows Workstation ● Unix and Linux Security: The Focus of Unix/Linux Security, Physical Security, Controlling the Configuration, Operating UNIX Safely, Hardening UNIX	Chapter7 Chapter8 Chapter9	**Post summary** of (Chapter 7-9 on BB)

4	**Module3: Operating Systems and Applications (continued)** ● Web browser and client security: Web Security and Client Risk, How a Web Browser Works, Web Browser Attacks, Operating Safely, Web Browser Configurations ● 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 ● Server security : General Server Risk, Security Design, Operating Servers Safely, Servers Applications, Multi-level Security and Digital Rights Management	Chapter 10-14	**Quiz #1** (Module1-3)
5	**Module4: Network Security Fundamentals** ● Network Protocols: Protocols, The Open System Interconnect Model, The OSI Layer, The TCP/IP Model, TCP/IP Model Layers, Internet Protocol, VOIP ● Wireless Security: Electromagnetic Spectrum, The Cellular Phone Network, Placing a Cellular Telephone Call, Wireless Transmission Systems, Pervasive Wireless Data Network Technologies, IEEE Wireless LAN Specifications, IEEE 802.11, IEEE 802.11 Security, Bluetooth, Wireless Application Protocol, Future of Wireless	Chapter 15-16	**Post summary** of (Chapter 15-16 on BB) **Project 1** (TCP Wireshark) **due by end of week 7**
6	**Module4: Network Security Fundamentals(continued)** ● Network Architecture Fundamentals: Network Segments, Perimeter Defense, Network Address Translation, Basic Architecture Issues, Subnetting, Switching and VLANs, Address Resolution Protocol and Media Access Control, Dynamic Host Configuration Protocol and Addressing Control, Zero Configuration Networks, System Design and Architecture Against Insider Threats, Common Attacks ● Firewalls: Firewalls, Firewall Rules, The Use of Personal Firewalls	Chapter 17-19	**Homework # 2** (Summary on Module -4)

	● Intrusion Detection and Prevention: Intrusion Detection Systems, Response to Intrusion Detection Systems,		
7	**Module5: Communication** ● Secret communication: What is Cryptography, General Terms, General Cryptography Principles, The Four Cryptography Primitives, Putting These Primitives together to Achieve CIA, Proprietary Versus Open Source Algorithms, Attacks on Hash Functions, Quantum Cryptography ● Covert communication: Where Hidden Data Hides, Where did it Come From, Where is it going, Overview of Steganography, Steganography Compared to Cryptography, Types of Steganography, Products that Implement Steganography, Steganography Versus Digital Water Marking, Goals of Digital Water Marking,	Chapter 20-21	**Midterm exam**
8	**Module5: Communication (continued)** ● Application of secure/covert communication: E-mail, Authentication Servers, Working Model, Public Key Infrastructure, Virtual Private Networks, Secure Sockets Layer/ Transport Layer Security, SSL Handshake	Chapter 22	**Homework #3** (Chapter 20-22)
9	Spring break		
10	**Module6: Security Threat and Response** ● Intrusion detection and response: Intrusion Detection Mechanisms, Honeypots, Incident Handling	Chapter 23-24	**Post summary** Chapter 23-24 **on BB**
11	**Module6: Security Threat and Response (continued)** ● Security assessment, testing and evaluation: Information Assurance Approaches and Methodologies, Certification and Accreditation, DIACAP, Federal Information Processing Standard 102, OMB Circular A-130, The National Institute of Standards and Technology Assessment Guidelines, Penetration Testing, Auditing and Monitoring,	Chapter 25	**Quiz #2** (Module 4-5)
12	**Module7:Integrated Cyber Security** ● Smartphone and mobile device security	supplemental materials	**Project #2** (IDS Snort) **due by end of week 14**
13	**Module7: Integrated Cyber Security (continued)** ● Validating your security: Overview, Current	Chapter 26-28	**Homework #4** (Module 6)

	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

Texbook (Required)

Eric Cole, Ronald Krutz, James W.Conley ,**Network Security**, Second Edition,Copyright 2009,Print ISBN:978-0-470-50249-9,Print ISBN:978-0-13-239077-4

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

Technological Requirement and Supplies: Raspberry Pi (http://wwww.raspberrypi.org)

Additional Reading

Raspberry Pi

http://www.raspberrypi.org

National Institute of Standards and Technology (NIST)

http://www.nist.gov

IoT News Network

http://www.iotnewsnetwork.com

MIT Technology Review

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