# MIS 5209 - Securing Digital Infrastructure

## About the Instructor:

Brian Green (?@temple.edu)
http://community.mis.temple.edu/?/
https://www.linkedin.com/in/isprof
Phone: 856/283.2136
Google+: brian.green@gmail.com
Online Office hours: By appointment.

## Class Location and Time:

ONLINE 5:30 – 8:15, Monday (starting August 29, 2016)

## Course Description:

Examines issues related to securing the components of a company's electronic infrastructure. In this course students will study the hardware and software components, including networks, firewalls, operating system virtualization and cloud interfaces, their potential security vulnerabilities and approaches to securing their operations. Students become familiar with Digital Infrastructure at both the conceptual and practical level through lecture, in-class activities and homework exercises.

## Course Objectives:

- Be able to examine an organization's network, identify the components, understand the risks inherent in the network and suggest mitigation approaches.
- Be able to understand and use a variety of modern encryption methods.
- Be able to understand and use a variety of data integrity methods.
- Be able to understand and use trust measures.
- Be able to identify the components and protocols used in modern applications, understand the inherent risks, and suggest mitigation approaches.

## Required Text & Readings:

- Gregory, P., McNary, K., La Scola, E. (2015). *CISSP Guide to Security Essentials*. 2 Ed., Boston: Cengage Learning.
- Cole, E. (2016) Network Security. 2 Ed., Boston: Wiley

# Evaluation & Grading

| | |
|---|---|
| *Practical Assignments* | 20% |
| *Written Assignments* | 20% |
| *Case Presentations* | 5% |
| *Midterm Exam* | 20% |
| *Final Exam* | 30% |
| *Class Participation* | 5% |

## Course Assessment Overview

This course has 4 parts; the first is an introduction, with the proceeding three sections covering the major topics in infrastructure security at the network, device, and data levels. Each of the four sections is defined in the course outline, along with the subjects covered in each. There will be three exams throughout the course; while they are not cumulative, each unit relies heavily on the material covered in proceeding units. While the focus of the exam in each unit will cover the learning objectives in that unit, the previous units are a prerequisite. Exams are online, and must be completed during the assigned examination window (typical 72 hours) and may not be completed after the deadline.

## Participation

There are both synchronous and asynchronous participation activities in this course. In both cases, it is expected that the activities are completed during the intended unit. Participation activities completed before or after the intended week will not be considered a graded deliverable. While participation is a relatively insignificant portion of your final course grade, regular and meaningful participation is strongly encouraged.

***Synchronous activities:***

Although this course is conducted online, there will be weekly class meetings facilitated by WebEx (a web conferencing platform). Students should have a computer with a webcam (included on most laptop computers), microphone and speakers (you may find the use of a headset to be more convenient). These sessions may include traditional interactive lectures, group exercises, and presentations by other students. Your attendance and active participation in these weekly class meetings is mandatory.

***Asynchronous activities:***

In addition, each week there will be discussion topics, to which students can post comments and opinions. The purpose of these discussions is to stimulate conversation about the course material among the class members, and replicate the meaningful discussion that might take place in a face-to-face class meeting. Although this activity is graded, there are no "correct" answers. This is a subjective exercise, where student participation is valued over accuracy of content. There is no "quota" for participation in discussion threads, but I will be looking for meaningful contribution to the conversation. Meaningful contribution can involve discussions that clarify course material among students, students that bring their experience or industry knowledge about a particular relevant topic to the class, and thoughtful responses to the discussion prompts.

## Case Presentations

Throughout the course, there will be six case study readings tangentially related to the topics covered in the course. All students will be asked to review the case, and be prepared to discuss during a weekly class meeting. In addition, each case will have several students assigned as SME's, who will be responsible for presenting the case to the students, and facilitating discussion of the case. You will be assigned your case at the beginning of the term, and may work with the other assignees for that case to coordinate your efforts. The case presentation can include any presentation modality you choose, and should also include prompts for class discussion, as well additional insight from your research on the case.

## Written & Practical Assignments

In addition to the aforementioned graded activities, there will be written and practical assignments to give students the opportunity to demonstrate their understanding of the course material. Many of the topics and class discussions will cover both theoretical and practical applications in network security. For example, we may discuss cryptography and its mathematical underpinnings, but we will also discuss protocols and tools for real world applications. As such, you will be able to demonstrate your understanding of the topic in the written assignments, while demonstrating their application in the hands-on practical assignments.

***Written Assignments ("WA" in schedule)***

In some units of study, you will find questions for the written assignment. The appropriate length of your responses to the questions is that which is necessary to adequately answer the question. Students should not feel obliged to provide narrative form answers to all questions; in many cases, bullet lists, tables or charts may be more appropriate. Use your judgement to determine the best method to convey the answer most concisely. Where appropriate, be sure to include citations, though formal APA formatted citations and footnotes will not be necessary in these rather informal assignments.

***Practical Assignments ("PA" in schedule)***

In some units of study, you will find hands-on exercises, where you will be asked to apply the concepts covered in the reading and assignments using tools, protocols and applications that demonstrate their use. It is expected that all students have proficiency with the command prompt and basic networking in Microsoft Windows in order to complete these assignments. Students will be required to install tools and utilities in Microsoft Windows, and are expected to have access to computers in which to complete these assignments. It should be expected that these will need to be completed on your own computer, and not computers available for use in a public space such as a library, your workplace or institutional facilities. Deliverable for each exercise will vary, and will be defined in each assignment.

## Course Outline:

- 1: Introduction
    - Defining infrastructure
    - IT Security Triad
    - Course overview
    - Lab environment
- 2: Access Controls
    - Identifications and Authentication
    - Centralized Access Control
    - Decentralized Access Control
    - Access Provisioning Life Cycle
    - Access Control Attacks
    - Testing Access Controls
- 3: Systems Software Security
    - Operating Systems
    - Windows Security
    - Linux/Unix Security
    - Server Security
    - Threats and Countermeasures
- 4: Applications Software Security
    - Client/Server Applications Security
        - Web Security
        - Email Security
        - Client/Server Applications Security
    - Application Models and Technologies
    - Software Development Life Cycle / Secure Coding
    - Applications Security Controls
    - Databases and Data Warehouses
    - Threats and Countermeasures
- 5: Cryptography Protocols
    - Synchronous protocols:
        - DES

        - 3DES
        - AES
        - RC4
    - Asynchronous protocols:
        - RSA
    - Hashing and Trust:
        - Message Digest
        - SHA
- 6: Practical Cryptography
    - Applications and Uses of Cryptography
    - Encryption Methodologies
    - Cryptanalysis
    - Key Management
    - Attacks and Countermeasures
- 7: Business Continuity & Disaster Recovery Planning
    - Business Continuity (BC) and Disaster Recovery (DR) Planning
    - BC/DR testing
    - BC/DR Architectures
- 8: Security Operations
    - Applying Security Concepts to Computer and Business Operations
    - Records Management Security Controls
    - Backups
    - Anti-Virus Software and Other Anti-Malware Controls
    - Remote Access
    - Administrative Management and Control of Information Security
    - Resource Protection
    - Incident Management
    - High Availability Architectures
    - Vulnerability Management
    - Change Management and configuration Management
    - Operations Attacks and Countermeasures
- 9: Physical & Environmental Security
    - Site Access Controls
    - Secure Siting
    - Equipment Protection
    - Environmental Controls
- 10: Security Architecture & Design
    - Security Models
    - IS Evaluation Models
    - Computer Hardware Architecture
    - Computer Software Architecture
    - Software and System Security Threats and Countermeasures
    - Cloud Security Threats and Countermeasures
- 11: Network Protocols
    - ISO OSI
    - TCP/IP
    - Topologies and Cabling
    - Routing / Switching

    - Wired and Wireless Network Technologies
- 12: Telecommunications & Network Security
    - Wired and Wireless Network Technologies
    - Network Authentication, Access Control
    - Firewalls
    - Virtual Private Networks
    - Intrusion Detection Systems
- 13: Risk Management, Legal, Regulations, Investigation, & Compliance
    - IT Security Supporting Mission, Goals and Objectives
    - Risk Management
    - Security Management
    - Personnel Security
    - Computer Crime
    - Incident Response
    - Investigations
    - Computer Forensics
    - Professional Ethics

## Citation Guidelines

If you use text, figures, and data in reports that was created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

## Plagiarism and Academic Dishonesty

Plagiarism and academic dishonesty can take many forms. The most obvious is copying from another student's exam, but the following are also forms of this:

- Copying material directly, word-for-word, from a source (including the Internet)
- Using material from a source without a proper citation
- Turning in an assignment from a previous semester as if it were your own
- Having someone else complete your homework or project and submitting it as if it were your own
- Using material from another student's assignment in your own assignment

Plagiarism and cheating are serious offenses, and behavior like this will not be tolerated in this class. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course, to expulsion from the program.

## Student and Faculty Academic Rights and Responsibilities

The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02) which can be accessed through the following link: http://policies.temple.edu/getdoc.asp?policy_no=03.70.02

## Grading Criteria

The following are the criteria used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

| Criteria | Grade |
|---|---|

| | |
|---|---|
| The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are no mechanical, grammatical, or organization issues that detract from the ideas. | A- or A |
| The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals. | B-, B, B+ |
| The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions. | C-, C, C+ |
| The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material. | Below C- |

## Fall 2016 Schedule

| **Week** | **Topic** | **Reading:** | **Assignments:** | | | |
|---|---|---|---|---|---|---|
| | | | **Case** | **Written** | **Practical** | **Discussion** |
| 1 | Introduction | | | | PA1.1 | D1.1 |
| 2 | Access Controls | *Gregory*: pp.37-67<br>*Cole*: pp.109-125 | C2.1 | WA2.1 | PA2.1 | D2.1 |
| 3 | Systems Software Security | *Cole*: pp.145-253<br>*Gregory*: pp.88-89 | | WA3.1 | | D3.1 |
| 4 | Applications Software Security | *Gregory*: pp.95-123<br>*Cole*: pp.255-427 | C4.1 | WA4.1 | PA4.1 | D4.1 |
| 5 | Cryptography Protocols | *Gregory*: pp.572-629<br>*Cole*: pp.176-189 | | | PA5.1<br>PA5.2<br>PA5.3 | D5.1 |
| 6 | Practical Cryptography | *Cole*: pp.190-202 | C6.1 | WA6.1 | | D6.1 |
| 7 | **Midterm Exam** | | | | | |
| 8 | BC / DR | *Cole*: pp.140-166 | C8.1 | WA8.1 | PA8.1 | D8.1 |
| 9 | Security Operations | *Cole*: pp.257-282 | C9.1 | WA9.1 | PA9.1 | D9.1 |
| 10 | Physical/Environmental Security | *Cole*: pp.294-317 | C10.1 | WA10.1 | PA10.1 | |
| 11 | Security Architecture & Design | *Cole*: pp.330-360 | C11.1 | | PA11.1 | D11.1 |
| 12 | Network Protocols | *Cole*: pp.381-405<br>*Gregory*: pp.431-458 | | WA12.1 | PA12.1 | D12.1 |
| 13 | Telecom & Network Security | *Cole*: pp.405-412<br>*Gregory*: pp.459-568 | | WA13.1 | PA13.1<br>PA13.2<br>PA13.3 | D13.1 |
| 14 | Rick Management & Compliance | *Cole*: pp.2-22,220-246<br>*Gregory*: pp.809-847 | | | | D14.1<br>D14.2<br>D14.3 |
| 15 | **Final Exam** | | | | | |