# MIS 5214 – Security Architecture
# Spring 2020

## Instructor

David Lanter
Office: 209C Speakman Hall
Email: David.Lanter@temple.edu
e-Profile: http://community.mis.temple.edu/dlanter/
Office hours: Wednesdays 1:00 PM – 3:00 PM, and by appointment

## Class Location and Time

| Location | Day | Time |
|---|---|---|
| 1810 Liacouras Walk, Room 420 | Wednesdays | 9:00 AM – 11:30 AM |

## Class Website:

https://community.mis.temple.edu/mis5214sec004spring2020/category/01-introduction/

## Description

In this course you will study and learn about how: organizations plan, design and develop enterprise security architecture, IT security capabilities are aligned with business goals and strategy, and IT system security architectures and capabilities are assessed.

## Objectives

1. Learn key Enterprise Security Architecture concepts
2. Develop an understanding of contextual, conceptual, logical, physical and component levels or security architectures and how they relate to one another
3. Learn how security architectures are planned, designed and documented
4. Gain an overview of how security architectures are evaluated and assessed
5. Gain experience working as part of team, developing and delivering a professional presentation

## Textbook and Readings

- **Corporate Computer Security – Global Edition**, Fourth Edition, 2015, Boyle, Randall J. and Panko, Raymond R., Pearson, ISBN 13: 978-1-292-06045-3

- Weekly readings will also be found under the SCHEDULE menu on the class website, including:
  - National Institute of Standards and Technology (NIST) Special Publication 800 Series documents describing federal government security policies, procedures and guidelines
  - Federal Information Processing Standards (FIPS)
  - Federal Risk and Authorization Management Program (FedRAMP) documents and templates
  - Articles from OWASP, Microsoft, U.S. Department of Homeland Security, and other sources

- Case studies and a reading are available as a course pack for purchase from Harvard Business Publishing available at: https://hbsp.harvard.edu/import/692284

## Class Schedule

| Unit # | Topics | Date |
|---|---|---|
| 1 | Introduction | 1/15 |
| | The Threat Environment | |
| 2 | System Security Plan | 1/22 |
| 3 | Planning and Policy | 1/29 |
| 4 | Case Study 1 "*A High-Performance Computing Cluster Under Attack: The Titan Incident*" | 2/5 |
| | Cryptography | |
| 5 | Secure Networks | 2/12 |
| 6 | Firewalls, Intrusion Detection and Protection Systems | 2/19 |
| 7 | **Mid-Term Exam** | 2/26 |
| | *Spring Break* | 3/4 |
| 8 | Case Study 2 "Cyberattack: The Maersk Global Supply-Chain Meltdown" | 3/11 |
| | Access Control | |
| 9 | Host Hardening | 3/18 |
| 10 | Application Security | 3/25 |
| 11 | Data Protection | 4/1 |
| 12 | Incident and Disaster Response | 4/8 |
| 13 | Team Project Presentations | 4/15 |
| 14 | Team Project Presentations | 4/22 |
| 15 | **Final Exam** | |

## Readings

| Unit # | Readings |
|---|---|
| 1 | • Boyle and Panko: Chapter 1 The Threat Environment<br>• Ross, J.W., Weill P., and Robertson D.C. (2008), "Implement the Operating Model Via Enterprise Architecture" (in the Harvard Business Publishing course pack) |
| 2 | • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management, pp.84-95<br>• NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems"<br>• "FedRAMP System Security Plan (SSP) High Baseline Template" |
| 3 | • Boyle and Panko, Chapter 2 Planning and Policy<br>• NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 8 – Security Planning, pp.67-77<br>• NIST SP800-60V1R1 "Guide for Mapping Types of Information and Information Systems to Security Categories", pp.1-34<br>• FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems", pp.1-9 |
| 4 | • Boyle and Panko, Chapter 3 Cryptography<br>• NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations", pp.1-44<br>• NIST SP 800-53Ar4 " Assessing Security and Privacy Controls for Federal Information and Information Systems", pp.1-28 |
| 5 | • Boyle and Panko, Module A "Networking Concepts" and Chapter 4 "Secure Networks"<br>• NIST SP 800-145 "The NIST Definition of Cloud Computing"<br>• An Introduction to DDoS – Distributed Denial of Service Attack<br>• Public Key Infrastructure and X.509 Public Key Certificates |
| 6 | • Boyle and Panko: Chapter 6 Firewalls<br>• Basile, C., Matteo, M.C., Mutti, S. and Paraboschi, S, "Detection of Conflicts in Security Policies", in Vacca, J.R. (2017) Computer and Information Security Handbook, Third Edition, Chapter 55. pp. 781-799. |
| 8 | • Boyle and Panko, Chapter 5 Access Control<br>• NIST SP 800 63-3 "Digital Identity Guidelines"<br>• NIST SP 800 63A "Digital Identity Guidelines Enrollment and Identity Proofing"<br>• NIST SP 800 63B "Digital Identity Guidelines Authentication and Lifecycle Management" |
| 9 | • Boyle and Panko, Chapter 7 Host Hardening<br>• NIST SP 800-123 Guide to General Sever Security |
| 10 | • Boyle and Panko, Chapter 8 Application Security<br>• OWASP Top 10<br>• OWASP Attack Surface Cheat Sheet |
| 11 | • Boyle and Panko, Chapter 9 Data Protection |
| 12 | • Boyle and Panko, Chapter 10 Incident & Disaster Response<br>• NIST SP 800 34r1 Contingency Planning Guide for Federal Information Systems |

## Assignments

Course assignments, readings and case studies have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts. You are responsible for completing the weekly readings prior to class and posting your assignments to the class website.

You will find the readings for each week posted to the class website under the SCHEDULE menu item. Be sure to check for updates to the list of readings for the week one week prior to each class. In addition to readings, you will also find resource materials and details of problem solving assignments for the coming week's class under the SCHEDULE menu:

SCHEDULE -> First Half of Semester/Second Half of Semester -> Week#-Topic**.**

In addition to completing the reading assignments, you are also responsible for submitting the following deliverables on-time, according to the schedule provided:

1. **One Key Point Taken from Each Assigned Reading:** To facilitate preparation and active participation in class you are required to summarize and discuss one key point you took from each assigned reading.

   Each **Thursday** you will find a series of posts on the class web site referencing the readings and assignments for the coming week. There will be one post corresponding to each reading assigned that week. Post a few sentences of thoughtful analysis about one key point you took from each assigned reading by **midnight Sunday** the week they are due.

2. **One Question You Would Ask Your Fellow Classmates to Facilitate Discussion.** Among the posts provided for the coming week you will find one specifically designated for posting a question to ask your fellow classmates to facilitate discussion of the coming week's topic. Post your question by **midnight Sunday** the week it is due.

3. **Problem Solving Assignments:** Occasionally you will be asked to solve a problem or answer specific questions. For these assignments you will be asked to submit your solution or answer(s) as a written document, or informational diagram in PDF file format. (You may produce diagrams using a graphic drawing software tool of your choosing, e.g. Microsoft Visio, draw.io, PowerPoint, etc.) Upload your assignment saved in PDF format to Canvas by **midnight Sunday** the week it is due.

   ***Document submission instructions:*** *Put your name, class section number and the week of the assignment in the top-left corner of the header of the document. Name your submitted document file using the following naming convention and upload it to your Canvas. File naming convention: course number (MIS5214), followed by a dash ("-"), followed by your name (first-last), followed by an underscore ("dash"), followed by the unit of the assignment. For example: MIS5214-David-Lanter_Unit3.pdf.*

## Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. In addition to fulfilling your weekly assignments you are required to:

1. **Comment on your classmates' discussion questions and/or key points they took away from the readings:** Read your classmates' discussion questions and key points they took away from the assigned readings, and contribute at least three (3) substantive posts that include your thoughtful answers to their discussion questions and/or comments on the key points made about the readings. Your posting of your three comments is due **Tuesday by noon.**

2. **Post an article to the "In the News" Post:** Contribute a link and a brief summary. Be prepared to discuss in class an article you found about a current event in the Information Security arena. An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome. The deadline for posting is **Tuesday by noon.**

Evaluation online and in-class will be based on what you contribute, not simply what you know. **Frequency** and **quality** of your contributions are equally important.

***Note: Late submissions for participation deadlines will result in no (0) credit earned for Comments and In the News articles.***

## Case Studies

You will prepare and participate in two case study analyses during the semester. I will provide several questions to help you prepare to discuss each case study. Answer the questions in a way that demonstrates the depth of your understanding of the security and audit concerns represented by the case.

Case study analysis is a 3-phase process:

i. Individual preparation of each case study analysis is done as a homework assignment that has you answering questions intended to prepare you for contributing in a group discussion meeting.

   Your analysis of the case will prepare you to learn from what others say. To fully benefit from the interchange of ideas about a case's problem, however, you must possess a good understanding of the facts of the case and have your own ideas. Studying the case, doing your homework and answering the questions readies you to react to what others say. This is how we learn.

ii. Group discussions are informal sessions of give and take. Come with your own ideas and leave with better understanding. By pooling your insights with the group you advance your own analysis. Discussions within small groups is also helpful for those uncomfortable talking in large classes to express their views and gain feedback.

iii. Class discussion advances learning from the case, but does not solve the case. Rather it helps develop your understanding why you need to gain more knowledge

and learn concepts that provide the basis of your intellectual toolkit you develop in class and apply in practice.

Upload your answers to the case study questions to your Canvas folder no later than **Sunday at Midnight** of the week it is due. Below is the schedule for the Case Studies:

| Class | Case Study | Due | Discussion |
|---|---|---|---|
| 4 | Case Study 1: "*A High-Performance Computing Cluster Under Attack: The Titan Incident*" | 2/2 | 2/5 |
| 8 | Case Study 2: "Cyberattack: The Maersk Global Supply-Chain Meltdown" | 3/8 | 3/11 |

Your written answers to the questions should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Be sure to include each question (including number) along with the answers in your document. Do not prepare a separate cover page, instead put your name, the class section number (MIS5214), and the case name in the top-left corner of the header.

*You will name your submitted document file and upload it to your Canvas using the following file naming convention: class section number (MIS5214), followed by a dash ("-"), followed by your name, followed by a dash, followed by the Case for the assignment.*
*For example: MIS5214-David-Lanter-Case1.pdf.*

***Note: Late submissions for a Case Study's deadline will result in no (0) credit earned.***

## Team Project

By class 4, students will be organized into teams that work together on case studies and on the Team Project. Each team will be responsible for researching, developing and presenting a system security plan for a cloud-based enterprise information system. The plan will include technical specifications and diagrams illustrating the security architecture of an information system. The team will develop and deliver a 15-minute presentation on the system's security architecture, followed by 15-minutes of questioning by the other project teams.

Below is the schedule for the Team Projects:

| Unit # | Team Project Schedule | Due |
|---|---|---|
| 8 | 1st Draft System Security Plan (SSP) | 3/11 |
| 10 | 2nd Draft SSP | 3/25 |
| 12 | 3rd Draft SSP | 4/8 |
| 13 | Presentation of Final Deliverables | 4/15 |
| 14 | Presentation of Final Deliverables | 4/22 |

## Exams

There will be two exams given during the semester: Mid-Term and Final exams. Together these exams are weighted 20% of your final grade.

Below is the Exam schedule:

| Unit # | Exam | Date |
|---|---|---|
| 7 | Mid-Term | 2/26 |
| 15 | Final | 4/29 |

You will have a fixed time (e.g. 120 minutes) to complete the exam. Mid-Term Exam will occur during class on February 26, and Final Exam will occur during finals week during class time on April 29. In general, the final exam will be cumulative.

A missed exam can only be made up in the case of documented and verifiable extreme emergency-situation. No make-up is possible for Final Exam.

## Weekly Cycle

As outlined above in the **Assignments, Participation, Case Studies and Team Project** sections, much of your learning will occur as you prepare for and participate in discussions about the course content. To facilitate learning the course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

| When | Actor | Task | Type |
|---|---|---|---|
| Thursday | Instructor | Post readings & assignment questions | Assignment |
| Sunday midnight | Student | Post key points, question, (& answers) | Assignment |
| Sunday midnight | Student | Case study answers | Assignment |
| Tuesday noon | Student | Post 3 comments and In The News article | Participation |
| Wednesday | Both of Us | Class meeting | Participation |

## Evaluation and Grading

| Item | Weight |
|---|---|
| Assignments | 20% |
| Participation (in class and online) | 20% |
| Case Studies | 20% |
| Team Project | 20% |
| Exams | 20% |
| | **100%** |

| Grading Scale | | | |
|---|---|---|---|
| 94 – 100 | A | 73 – 76 | C |
| 90 – 93 | A- | 70 – 72 | C- |
| 87 – 89 | B+ | 67 – 69 | D+ |
| 83 – 86 | B | 63 – 66 | D |
| 80 – 82 | B- | 60 – 62 | D- |
| 77 – 79 | C+ | Below 60 | F |

## Grading Criteria

The following criteria are 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- |

## Late Assignment Policy

An assignment is considered late if it is turned in after the assignment deadlines stated above. No late assignments will be accepted without penalty unless arrangements for validated unusual or unforeseen situations have been made.

- Participation and case study contributions cannot be turned in late. If you miss contributing prior to the deadlines for class that week you will receive no credit for it.
- Assignments will be assessed **a 20% penalty** each day they are late. No credit is given for assignments turned in over five calendar days past the due date.
- You must submit all assignments, even if no credit is given. **If you skip an assignment, an additional 10 points will be subtracted from your final grade in the course.**
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

## Citation Guidelines

If you use text, figures, and data in reports that were 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

All work done for this course: papers, examinations, homework exercises, blog posts, laboratory reports, oral presentations — is expected to be the individual effort of the student presenting the work.

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

## Additional Information

| | |
|---|---|
| **Availability of Instructor** | ▪ Please feel free to contact me via e-mail with any issues related to this class. I will also be available at the end of each session. Please note that these discussions are to address questions/concerns but are NOT for helping students catch up on content they missed because they were absent.<br>Note: I will respond promptly when contacted during the week<br>▪ I am available to meet personally with you:<br>✓ Immediately after class<br>✓ During office hours<br>✓ By appointment prior to class<br>✓ By appointment by phone |
| **Attendance Policy** | ▪ Class discussion is intended to be an integral part of the course. Therefore, full attendance is expected by every student.<br>▪ If you are absent from class, speak with your classmates to catch up on what you have missed. |
| **Class Etiquette** | ▪ Please be respectful of the class environment.<br>▪ Class starts promptly at the start time. Arrive on time and stay until the end of class.<br>▪ Turn off and put away cell phones, pagers and alarms during class.<br>▪ Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class.<br>▪ Refrain from personal discussions during class. Please leave the room if you need to speak to another student for more than a few words. If a student cannot refrain from engaging in private conversation and this becomes a pattern, the students will be asked to leave the classroom to allow the remainder of the students to work.<br>▪ During class time speak to the entire class (or breakout group) and let each person "take their turn."<br>▪ Be fully present and remain present for the entirety of each class meeting. |