MIS 5214 – Security Architecture
Spring 2022

Instructor

David Lanter
Office: Speakman 209C and online via Zoom
Office Hours: Via Zoom by appointment
Email: *David.Lanter@temple.edu*
e-profile: *http://community.mis.temple.edu/dlanter/*

Class Format: Hybrid
Class Meetings: Wednesdays, 5:30pm – 8:00pm
Where – Online: *Zoom Meeting*
Where – In-Class: 1810 Liacouras Walk, Room 420, for Units 11-14
Website: https://community.mis.temple.edu/mis5214sec703spring2022/welcome-to-security-architecture/
Canvas: https://templeu.instructure.com/courses/107728

Course 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.

Course 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

Credit Hours: 3

Textbook and Readings

- **Corporate Computer Security**, 5th Edition, 2021, Boyle, Randall J. and Panko, Raymond R., Pearson, ISBN-13: 9780135823248

- Weekly readings described under READING below Class Schedule can 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/897080

Class (Unit) Schedule

Unit #	Topics	Date
1	Introduction	1/12
	The Threat Environment	
2	System Security Plan	1/19
3	Planning and Policy	1/26
4	Case Study 1 "*A High-Performance Computing Cluster Under Attack: The Titan Incident*"	2/2
	Cryptography	
5	Secure Networks	2/9
6	Firewalls, Intrusion Detection and Protection Systems	2/16
7	**Mid-Term Exam**	2/23
	Spring Break	3/2
8	Case Study 2 "*Data Breach at Equifax*"	3/9
	Access Control	
9	Host Hardening	3/16
10	Application Security	3/23
11	Data Protection	3/30
12	Incident and Disaster Response	4/6
13	Team Project Presentations	4/13
14	Team Project Presentations	4/20
	Course Review	
	Final Exam	4/27

Readings

Unit #	Readings
1	• Boyle and Panko: Chapter 1 The Threat Environment • 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 • NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems", pp. 18-26 • "FedRAMP System Security Plan (SSP) High Baseline Template"
3	• Boyle and Panko, Chapter 2 Planning and Policy • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 8 – Security Planning, pp.67-77 • NIST SP800-60V1R1 "Guide for Mapping Types of Information and Information Systems to Security Categories", pp.1-34 • FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems", pp.1-9 • NIST SP 800-53r5 "Security and Privacy Controls for Information Systems and Organizations", pp.1-17 • NIST SP 800-53B "Control Baselines for Information Systems and Organizations", pp. 1-15 • NIST SP 800-53Ar4" Assessing Security and Privacy Controls for Federal Information and Information Systems", pp.1-28
4	• Boyle and Panko, Chapter 3 Cryptography • Case Study 1 "A High-Performance Computing Cluster Under Attack: The Titan Incident" (in the Harvard Business Publishing course pack)
5	• Boyle and Panko, Module A "Networking Concepts" and Chapter 4 "Secure Networks" • NIST SP 800-145 "The NIST Definition of Cloud Computing" • An Introduction to DDoS – Distributed Denial of Service Attack • Public Key Infrastructure and X.509 Public Key Certificates
6	• Boyle and Panko: Chapter 6 Firewalls • 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 • NIST SP 800 63-3 "Digital Identity Guidelines" • NIST SP 800 63A "Digital Identity Guidelines Enrollment and Identity Proofing" • NIST SP 800 63B "Digital Identity Guidelines Authentication and Lifecycle Management" • Case Study 2 "*Data Breach at Equifax*" (in the Harvard Business Publishing course pack)
9	• Boyle and Panko, Chapter 7 Host Hardening • NIST SP 800-123 Guide to General Sever Security
10	• Boyle and Panko, Chapter 8 Application Security • OWASP Top 10, Introduction • How to use the OWASP Top 10 as a standard

	• How to start an AppSec program with OWASP Top 10 • OWASP Attack Surface Cheat Sheet
11	• Boyle and Panko, Chapter 9 Data Protection
12	• Boyle and Panko, Chapter 10 Incident & Disaster Response • 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.

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:

Unit #	Case Study	Due	Discussion
4	Case Study 1: "*A High-Performance Computing Cluster Under Attack: The Titan Incident*"	1/30	2/2
8	Case Study 2: "*Data Breach at Equifax*"	3/6	3/9

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 and section number (MIS5214-703), 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 and section number (e.g. MIS5214-703), followed by a dash ("-"), followed by your name, followed by a dash, followed by the Case for the assignment.
For example: MIS5214-703-David-Lanter-Case1.pdf.

Note: Late submissions will result in loss of 50% credit earned.

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.

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 Rough Draft System Security Plan (SSP) review	3/23
10	2nd Draft SSP review	3/30
11	3rd Draft SSP review	4/6
12	Presentation of Final Deliverables	4/13
13	Presentation of Final Deliverables	4/20

Draft System Security Plans: For these assignments you and your team should schedule time and meet with your instructor to review and gain feedback on your security architecture solution. You may produce system and security architecture diagrams using a graphic drawing software tool of your choosing, (e.g. https://app.diagrams.net/, PowerPoint, Microsoft Visio, etc.)

Final deliverable 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 name of the assignment. For example: MIS5214-David-Lanter_2ndDraft-SSP.pdf.

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	3/3
	Final	5/4

You will have a fixed time (e.g. 120 minutes) to complete the exam. Mid-Term Exam will occur during class on February 23, and Final Exam will occur during finals week during class time on May 4. 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 from readings, question for classmates	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	25%
Participation	25%
Team Project	25%
Exams	25%
	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 comments and In The News articles cannot be turned in late. If you miss contributing prior to the deadlines for class that week you will receive no credit for it.
- Late Assignments will be assessed **a 50% penalty** each day they are late.
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

University Policies

TEMPLE AND COVID-19

Temple University's motto is Perseverance Conquers, and we will meet the challenges of the COVID pandemic with flexibility and resilience. The university has made plans for multiple eventualities. Working together as a community to deliver a meaningful learning experience is a responsibility we all share: we're in this together so we can be together.

Attendance Protocol and Your Health

Instructors are required to ensure that attendance is recorded for each in-person or synchronous online class session. The primary reason for documentation of attendance is to facilitate contact tracing, so that if a student or instructor with whom you have had close contact tests positive for COVID-19, the university can contact you. Recording of attendance will also provide an opportunity for outreach from student services and/or academic support units to support students should they become ill. Faculty and students agree to act in good faith and work with mutual flexibility. The expectation is that students will be honest in representing class attendance.

Video Recording and Sharing Policy

Any recordings permitted in this class can only be used for the student's personal educational use. Students are not permitted to copy, publish, or redistribute audio or video recordings of any portion of the class session to individuals who are not students in the course or academic program without the express permission of the faculty member and of any students who are recorded. Distribution without permission may be a violation of educational privacy law, known as FERPA as well as certain copyright laws. Any recordings made by the instructor or university of this course are the property of Temple University. Any unauthorized redistribution of video content is subject to review by the Dean's office, and the University Disciplinary Committee. Penalties can include receiving an F in the course and possible expulsion from the university. This includes but is not limited to: assignment video submissions, faculty recorded lectures or reviews, class meetings (live or recorded), breakout session meetings, and more.

Code of Conduct Statement for Online Classes Online Behavior

Students are expected to be respectful of one another and the instructor in online discussions. The goal is to foster a safe learning environment where students feel comfortable in discussing concepts and in applying them in class. If for any reason your behavior is viewed as disruptive to the class, you will be asked to leave and you will be marked absent from that class. Please read the university policy concerning disruptive behavior:

> ***The disruptive student is one who persistently makes inordinate demands for time and attention from faculty and staff, habitually interferes with the learning environment by disruptive verbal or behavioral expressions, verbally threatens or abuses college personnel, willfully damages college property, misuses drugs or alcohol on college premises, or physically threatens or assaults others. The result is the disruption of academic, administrative, social, or recreational activities on campus.***

Online Classroom Etiquette

The expectation is that students attending online courses will behave in the same manner as

if they were in a live classroom. Be courteous and professional in your location, attire and behavior. Specifically, your location should reflect a clean and professional appearance - not a bedroom, crowded conference room, loud restaurant/bar, etc. Your attire should mirror what you might wear to a live classroom. We expect that students will not disrupt class through visuals or verbal outbursts, such as but not limited to, conversations with other people in the room, engaging in inappropriate behavior while you are in class or distracting the class in any other way. In addition, students should refrain from doing something in their online class that they would not do in a live classroom. which includes eating large meals, drinking alcohol, vaping, getting up often and leaving the online class (not staying at their computer). You should arrive on time and leave when the class is over. If there is an emergency of some kind, notify your faculty member via email or the chat function in Zoom.

Student and Faculty Academic Rights & Responsibilities

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The University has a policy on Student and Faculty Academic Rights and Responsibilities (Policy #03.70.02) which can be accessed at policies.temple.edu.

Inclement Weather Policy

Please be advised that while Temple University campuses may close for inclement weather, online courses are not on-campus and therefore are still expected to meet. Your instructor will contact you regarding any adjustments needed in the event of a power outage or severe circumstances. Should you have any questions, please contact the professor.

Academic Honesty

Learning is both an individual and a cooperative undertaking. Asking for and giving help freely in all *appropriate* setting helps you to learn. **You should represent only your own work as your own.** *Personal integrity* is the basis for intellectual and academic integrity. Academic integrity is the basis for academic freedom and the University's position of influence and trust in our society. University and school rules and standards define and prohibit "academic misconduct" by all members of the academic community including students. You are asked and expected to be familiar with these standards and to abide by them. A link to Temple's Policy on Academic Dishonesty can be found at the following link: https://grad.temple.edu/resources/policies-procedures

Disability Statement

Any student who has a need for accommodations based on the impact of a documented disability or medical condition should contact Disability Resources and Services (DRS) in 100 Ritter Annex (drs@temple.edu; 215-204-1280) to request accommodations and learn more about the resources available to you. If you have a DRS accommodation letter to share with me, or you would like to discuss your accommodations, please contact me as soon as practical. I will work with you and with DRS to coordinate reasonable accommodations for all students with documented disabilities. All discussions related to your accommodations will be confidential.

Temple University's Technology Usage Policy

This site includes information on unauthorized access, disclosure of passwords, and sharing of accounts. https://secretary.temple.edu/sites/secretary/files/policies/04.71.11.pdf