MIS 5214 – Security Architecture
Spring 2024

Instructor

Jose Gomez, CISSP
Office Hours: Via Zoom by appointment
Email: *tuf82656@temple.edu*
e-profile: *https://community.mis.temple.edu/members/jose-gomez/profile/*

Class Format: Online

Class Meetings: March 3 - March 9, 8:00 AM – 12:00 PM Beijing Time

Class Location: Zoom Link

Website: Security Architecture - MIS 5214 Website

Canvas: Canvas Link to Course 5214

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

Required Textbook and Readings

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

- Unit (class) 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, and other sources

- Case studies and a reading are available as a course pack for purchase from Harvard Business Publishing available at: BNAI Security Architecture 5214 | Harvard Business Publishing Education

Class Schedule

Unit #	Topics
0a	Introduction
0b	The Threat Environment
1a	System Security Plan
1b	Planning and Policy
2a	Case Study 1 *“A High-Performance Computing Cluster Under Attack: The Titan Incident*”
2b	Cryptography
3a	Secure Networks
3b	Firewalls, Intrusion Detection and Protection Systems
4a	**Mid-Term Exam**
4b	Case Study 2 *“Data Breach at Equifax”*
5a	Access Control
5b	Host Hardening
6a	Application Security
6b	Data Protection
7a	Incident and Disaster Response
7b	Team Project Presentations
8	Team Project Presentations / Review
	Final Exam

Assignments

The readings, questions, and case study assignments have been chosen to bring the real world into class discussion while illustrating fundamental concepts.

1. **Readings:** Below is the reading schedule you are responsible for completing. Complete each reading and answer reading discussion questions posted to the class website before the first class:

Unit #	Readings
0b	• 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 BNAI Security Architecture 5214 | Harvard Business Publishing Education) • NIST SP 800-100 "Information Security Handbook: A Guide for Managers", Chapter 10 Risk Management pp.84-95
1a	• NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems" • "FedRAMP System Security Plan (SSP) Low Moderate High Baseline Master Template • FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems"
1b	• 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 SP 800-60V1R1 "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 Reference • NIST SP 800-60V2R1 "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"
2a	• Case Study 1: "A High-performance computing cluster under attack: The Titan Incident", (in the BNAI Security Architecture 5214 | Harvard Business Publishing Education)
2b	• Boyle and Panko, Chapter 3 Cryptography • NIST SP 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations", pp. 1-44 • NIST SP 800 53Ar4 "Assessing Security and Privacy Controls for Federal Information and Information Systems", pp. 1-28
3a	• Boyle and Panko, Module A "Networking Concepts" and Chapter 4 "Security Networks • NIST SP 800-145 "The NIST Definition of Cloud Computing" • An Introduction to DDoS – Distributed Denial of Service Attack

	• Public Key Infrastructure and PKI Elements
3b	• 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.
4b	• Case Study 2 "*Data Breach at Equifax*", (in the BNAI Security Architecture 5214 | Harvard Business Publishing Education
5a	• 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"
5b	• Boyle and Panko, Chapter 7 Host Hardening • NIST SP 800-123 Guide to General Server Security
6a	• 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
6b	• Boyle and Panko, Chapter 9 Data Protection
7a	• Boyle and Panko, Chapter 10 Incident & Disaster Response • NIST SP 800 34r1 Contingency Planning Guide for Federal Information Systems

2. Answer Questions: Questions for each topical unit are available on the class website, under "READING & CASE STUDY QUESTIONS". Post your answer to each of the questions as you work through the readings **by the Saturday before our first face to face class at midnight**.

To do so, click "Leave a Comment". Provide a paragraph or two of thoughtful analysis as your answer to each question. Late submissions of answers will result in lost credit for the assignment.

- **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.

Case Studies: Case study analysis will be conducted in three phases:

i. **Individual preparation** is done as homework assignment questions you answer that will prepare you to contribute in group discussion meetings. It 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** will be conducted during class as 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.

You will find the questions for each case study posted on the class website under READING & CASE STUDY QUESTIONS. You will not post your answers to the case study questions on the class website. Instead you will upload two files to Canvas: One file will contain your answers to Case Study 1's questions, and the second file will contain your answers to Case Study 2.

Upload your answers to the case study questions to Canvas no later than the **Saturday before our first face to face class together at Midnight**.

Your written answers to the case study 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.BNAI), and the case name in the top-left corner of the header.

Name your submitted document file and upload it to Canvas using the following file naming convention: class section number (MIS5214-BNAI), followed by an underscore ("_"), followed by your name (last-first), followed by an underscore ("_"), followed by the Case for the assignment.

For example: MIS5214-BNAI_Gomez_Jose_Case1.pdf for the first case study, and MIS5214-BNAI_Gomez_Jose_Case 2.pdf for the second case study.

Below is the schedule for the Case Studies:

Unit	Case Study
1c	Case Study 1: *A High-performance computing cluster under attack: the Titan incident*
3b	Case Study 2: *"Cyberattack: The Maersk Global Supply-Chain Meltdown"*

Participation

Your participation in class discussions is critical. Evaluation is based on you consistently demonstrating your thoughtful engagement with the material. Assessment is based on what you contribute. The frequency and quality of your contributions are equally important.

Team Project Presentation

During Unit #1b students will be organized into project teams. Each team will identify an information system and follow up throughout the week by developing a system security plan (SSP) for the information system which they will present to the class during Units #7b/#8. Each team will present their SSP in 15 minutes and answer questions posed by the members of the other teams during a question and answer (Q&A) session.

Below is the schedule for the Team Projects:

Unit #	Team Project Schedule
2	1st Draft System Security Plan (SSP) review
3	2nd Draft SSP Review
4	3rd Draft SSP Review
7b	Presentation of Final Deliverables
8	Presentation of Final Deliverables

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
4a	Mid-Term
	Final

Mid-Term Exam will occur during class on March 4, and Final Exam will be made available in Canvas and must be completed on March 9. 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.

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 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.***

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 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.

Online exam proctoring

Proctorio or a similar proctoring tool may be used to proctor exams or quizzes in this course. These tools verify your identity and record online actions and surroundings. It is your responsibility to have the necessary government or school issued ID, a laptop or desktop computer with a reliable internet connection, the Google Chrome and Proctorio extension, a webcam/built-in camera and microphone, and system requirements for using Proctorio or a similar proctoring tool. Before the exam begins, the proctor may require a scan of the room in which you are taking the exam.

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