MIS 5214 – Security Architecture
Spring 2025

Instructor

Paul Warner

Email: paul.warner@temple.edu

Class MIS Community Web Site:

https://community.mis.temple.edu/mis5214sec951spring2025/welcome-to-security-architecture/

Class Canvas Web Site: https://templeu.instructure.com/courses/156069

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 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: https://hbsp.harvard.edu/import/1264447

Class Schedule

Unit #	Topics
0a	Introduction
0b	The Threat Environment
1a	System Security Plan
1b	Planning and Policy
1c	Case Study 1 *"A High-Performance Computing Cluster Under Attack: The Titan Incident"*
2a	Cryptography
2b	Secure Networks
2c	Firewalls, Intrusion Detection and Protection Systems
3a	**Mid-Term Exam**
3b	Case Study 2 *"Cyberattack: The Maersk Global Supply-Chain Meltdown"*
3c	Access Control
4a	Host Hardening
4b	Application Security
4c	Data Protection
5a	Incident and Disaster Response
5b	Team Project Presentations
5c	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" https://hbsp.harvard.edu/import/1264447 • 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"
1c	• Case Study 1: "A High-performance computing cluster under attack: The Titan Incident", https://hbsp.harvard.edu/import/1264447
2a	• 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
2b	• Boyle and Panko, Module 1 "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
2c	• 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.
3b	• Case Study 2 "Cyberattack: The Maersk Global Supply-Chain Meltdown", https://hbsp.harvard.edu/import/1264447
3c	• 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"
4a	• Boyle and Panko, Chapter 7 Host Hardening • NIST SP 800-123 Guide to General Server Security
4b	• Boyle and Panko, Chapter 8 Application Security • OWASP Top 10 • OWASP Attack Surface Analysis Cheat Sheet
4c	• Boyle and Panko, Chapter 9 Data Protection
5a	• 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 and Case Studies are available on the class website, under "QUESTIONS ABOUT THE READINGS AND CASE STUDIES. Post your answer to each of the questions on the course website as you work through the readings with the goal of completion before the first class. 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.**

Case study analysis will be conducted in three phases:

i. **Individual preparation** is done by answering the case study questions. This 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** 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.

Below is the schedule for the Case Studies:

Unit	Case Studies
1a	Case Study 1: *A High-Performance Computing Cluster Under Attack: The Titan Incident*
2b	Case Study 2: *Cyberattack: The Maersk Global Supply-Chain Meltdown*

Come to class prepared to discuss all of your answers to topical unit questions and case study questions in-detail.

- **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.

Your answers to the case study questions must be submitted no later than the **Saturday before our first face to face class together**.

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 #5b/#5c. 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)
3	2nd Draft SSP
4	3rd Draft SSP
5b	Presentation of Final Deliverables
5c	Presentation of Final Deliverables

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
3a	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	20%
Participation	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. Note: I will respond promptly when contacted during the week ▪ I am available to meet personally with you: ✓ Immediately after class ✓ During office hours ✓ By appointment prior to class ✓ 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. ▪ 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. ▪ Class starts promptly at the start time. Arrive on time and stay until the end of class. ▪ Turn off and put away cell phones, pagers and alarms during class. ▪ 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. ▪ 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. ▪ During class time speak to the entire class (or breakout group) and let each person "take their turn." ▪ Be fully present and remain present for the entirety of each class meeting.