ITMS 575 SYLLABUS

ITMS 575 Zero Trust Architecture: Design and Implementation

Hours: 3 credit hours / 45 contact hours

Instructor: TBD

Textbook, title, author, and year:

a. *Zero Trust Networks: Building Secure Systems in Untrusted Networks 2nd Edition*. Razi Rais, Christina Morillo, Evan Gilman & Doug Barth, 2024
b. NIST Special Publication 800-207 *Zero Trust Architecture.* Oliver Borchert, et.al. 2023
c. NIST Special Publication 1800-35B *Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics.* Oliver Borchert, Alper Kerman et.al. 2023
d. NIST Special Publication 1800-35C *Implementing a Zero Trust Architecture Volume C: How-To Guides.* Oliver Borchert, Alper Kerman et.al. 2023
e. NIST Special Publication 1800-35D *Implementing a Zero Trust Architecture Volume D: Functional Demonstrations.* Oliver Borchert, Alper Kerman et.al. 2023

Specific course information

a. **Catalog description:** Students will examine Zero Trust architecture focusing on its design and implementation as a model that treats all network hosts as exposed to the internet and assumes the network is always at risk. The course explores the transition from traditional perimeter-based defenses to zero trust strategies that directly incorporate authentication protocols, authorization protocols, and encryption into the network's infrastructure. Utilizing NIST Special Publication (SP) 1800-35, students will learn how to apply zero trust concepts across different organizations.
b. **Prerequisites:** ITMS 548
c. **Elective**

Specific goals for the course

a. Program Educational Objective
   - Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
   - Through collaborative coursework and projects, students will learn to address cybersecurity challenges by leveraging insights from diverse disciplines, enhancing interdisciplinary communication skills to effectively collaborate with experts from different backgrounds to build a holistic approach to cybersecurity problem-solving.
   - Upon completion, students will possess strategic leadership skills to assess cybersecurity risks, develop mitigation strategies, and ensure compliance with legal standards, preparing them to be an effective leader in cybersecurity initiatives within organizations.

b. Course Outcomes:
   Each successful student will gain an in-depth understanding of the fundamental principles of the zero trust model, including how to design and implement these architectures using existing technologies. They will gain practical experience through case studies and projects that apply zero trust principles in real-world scenarios, following NIST SP 1800-35 guidelines.
c. **Course student outcomes:**
   - Describe and implement the zero trust model and its core components such as trust engines, policy engines, and context-aware agents
   - Develop strategies used to transition from perimeter-based security models to comprehensive zero trust architectures
   - Apply zero trust principles to protect network, data, workloads, devices, and users.
   - Analyze and employ NIST SP 1800-35 guidelines for designing and deploying zero trust networks
   - Evaluate and apply lessons learned from case studies that document various organizations' journeys toward adopting zero trust
   - Engage in a hands-on project that requires the application of course concepts to design zero trust solutions

Topics to be covered

a. Introduction to Zero Trust: Understanding Fundamentals and Model Development
b. Architectural Design of Zero Trust Networks: Planning, Diagramming, and Implementing using current technology.
c. Applying Zero Trust to Specific Domains: Data, Workloads, Networks, Devices, Users, and Analytics
d. Advanced Zero Trust Concepts: Adversarial Viewpoints and Future Challenges
e. Practical Implementation: NIST SP 1800-35B Architecture and 1800-35C How-To Guides
f. Case Studies and Project Work: NIST SP 1800-35D Functional Demonstrations and Risk Management
g. Final Project: Designing and presenting a Zero Trust solution in an organizational context