ITMS 475 SYLLABUS

ITMS 475 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 1800-35B *Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics.* Alper Kerman et.al. 2023
c. NIST Special Publication 1800-35C *Implementing a Zero Trust Architecture Volume C: How-To Guides.* Alper Kerman et.al. 2023
d. NIST Special Publication 1800-35D *Implementing a Zero Trust Architecture Volume D: Functional Demonstrations.* 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 448
c. **Elective**

Specific goals for the course

a. Program Educational Objective
   2. Perform requirements analysis, design and administration of computer and network-based systems conforming to policy and best practices, and monitor and support continuing development of relevant policy and best practices as appropriate.
   4. Design and implement an enterprise security program using policy, technology, and awareness to implement appropriate controls and technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
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 assist in the implementation of the zero trust model and its core components such as trust engines, policy engines, and context-aware agents
   - Describe 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 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
   - Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions **(ABET Computing Criterion 3.1)**
   - Communicate effectively in a variety of professional contexts **(ABET Computing Criterion 3.3)**
   - Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline **(ABET Computing Criterion 3.5)**
   - Apply security principles and practices to maintain operations in the presence of risks and threats. **(ABET Cybersecurity Criterion 3.6)**
   - Assist in the creation of an effective project plan

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: NISTP SP 1800-35D Functional Demonstrations and Risk Management
g. Final Project: Designing and presenting a Zero Trust solution in an organizational context