CAREER: *Trusted-Zero-Trust*: A Reference Model Framework for Designing, Implementing, and Evaluating Zero Trust in Mission-Critical Cyber-Infrastructures

Carlos Rubio-Medrano, Texas A&M University - Corpus Christi

Motivation. Due to an always-evolving and increasingly-effective threatscape, Zero-Trust is gaining a momentum as a much-needed paradigm for the cyber-protection of mission-critical infrastructures. First coined a few years ago, it is actively recommended by experts in industry and the US Government, which plans to transition into Zero-Trust for better protecting cyber-infrastructures of national interest.

Problem Statement. Despite this growing interest, **there is a lack of well-defined methodologies to design, implement, and evaluate Zero-Trust deployments**. Concretely, the following shortcomings are identified: (i) *Lack of a Comprehensive, Formal Definition.* Despite being based on a set of well-known, previously-explored methodologies, e.g., Identity Management, Authorization, Continuous Monitoring, etc., there is still no consensus on the nature and number of methodologies that must be considered, including they should interact with each other. (ii) *Lack of Evidence-backed Methodologies, Recommendations, and Best Practices.* Moreover, there are insufficient practical, evidence-based descriptions on how to effectively design, implement, and deploy Zero-Trust, such that not only vulnerabilities and attacks can be better handled, but also new and legacy technologies can be taken into account. (iii) *Lack of Evidence-backed Efficiency Assessments.* Finally, there is a lack of evidence on the effectiveness of Zero-Trust that convincingly justifies the organizational efforts, costs, and time needed for a successful deployment.

Proposed Approach. In order to address these shortcomings, I propose the development of ***Trusted-Zero-Trust*, a reference model framework for designing, implementing, and evaluating Zero-Trust-inspired protections for modern cyber-infrastructures**, For such a purpose, the following research thrusts will be conducted: (i) *Analyzing and Defining Zero-Trust.* First, we will organize existing methodologies and techniques, as well as the interactions between them, in a hierarchical model that serves as a reference for practitioners to identify different levels of expected functionality, complexity, and maturity of existing and future Zero-Trust deployments; (ii) *Designing and Deploying Zero-Trust.* Next, leveraging our reference model, a series of case studies will be conducted in collaboration with existing cyber-infrastructures for scientific resource sharing and educational support, ultimately resulting in a series of recommendations and best practices for successfully designing, implementing, and deploying Zero-Trust; (iii) *Evaluating and Assessing Zero-Trust.* Finally, using the products of the two previous thrusts as an input, a framework for evaluating, assessing, and improving Zero-Trust will be introduced, so future practitioners can meet domain-specific needs, justify investments, and provide more effective cyber-protections.

Intellectual Merit. This project will provide answers to the following research questions: (i) *What are the basic blocks of Zero-Trust?*, e.g., the composing methodologies, techniques, paradigms, and their interactions. (ii) *How to better implement Zero-Trust?*, e.g., the steps, recommendations, and best practices; (iii) *How to assess the cost of implementing Zero-Trust?*, e.g., the organizational efforts and costs; (iv) *How to measure the effectiveness of Zero-Trust?*, e.g., the threats/attacks that Zero-Trust can prevent/counteract.

Education Plan. This project will leverage *Trusted-Zero-Trust* to educate a stronger and diverse workforce pipeline in three different educational thrusts as follows: (i) *Organizations.* A series of seminars and consulting materials will be developed for organizations in both industry and academia to transition from existing cyber-protections into one (or more) reference levels as described by *Trusted-Zero-Trust*; (iii) *Professionals*. In addition, a credentialing system based on *Trusted-Zero-Trust* will be developed for IT professionals to design, implement, and evaluate Zero-Trust solutions in different levels of expertise; (iii) *Institutions.* Finally, being Texas A&M University - Corpus Christi (TAMU-CC) a Hispanic-Serving Institution (HSI), students from underrepresented groups will be recruited and exposed to the different cybersecurity topics. Also, the industry and academia connections to be developed as a part of the different research thrusts of *Trusted-Zero-Trust* will contribute to internships, courses, workshops, and laboratories as a part of the upcoming BS and MS programs focused in Cybersecurity at TAMU-CC.