

**Talk title:** Towards a Rigorous Approach for Zero Trust in the 5G Core

**Abstract:** By combining technologies such as Network Function Virtualization and Service-Based Architecture with decentralized and cloud deployments, the fifth generation of cellular networks (5G) aims for unprecedented Quality of Service, and use-cases in smart industry, emergency operations, remote medicine, and more. The increased attack surface introduced by this transition as well as the critical nature of the 5G communications require, more than ever before, a rigorous analysis of 5G security. In this talk, we analyze the security implications introduced in the 5G Core, and the existing security solutions proposed in the 5G standard. We explore the model of Zero Trust Architecture (ZTA) and we discuss how it is supported by the 5G Core standard. With Virtualization and Cloud deployment being significant factors in the increase of the attack surface, we expand ZTA principles to include the software and hardware of the deployment stack. We leverage Trusted Execution Environments (TEEs) to ensure confidential computing on untrusted deployments and our analysis shows how our proposed model handles the increased attack surface and reinforces the ZTA principles in the 5G Core, without any changes to the 5G standard. Finally, we provide experimental results that demonstrate the overhead incurred by our model in terms of performance and monetary cost.

**Team members:** Norbert Ludant, Marinos Vomvas, Guevara Noubir (Northeastern University)