Resilient Mission Computer

By: Hamed Okhravi

The Resilient Mission Computer (RMC) effort focuses on researching and developing a foundationally secure computer system design in which important security properties are inherent. In this talk, we focus on two aspects of such a design. First, we study the largest class of vulnerabilities in modern operating systems that arise from the over-privilege in their monolithic design. To prevent these vulnerabilities, we leverage security features available in commodity processors to enforce fine-grained compartmentalization of the OS. We describe the design, implementation, and evaluation of such compartmentalization for the Linux OS. Second, we study the caveats of leveraging safe programming languages in conjunction with unsafe ones in modern applications. We illustrate how *cross-language attacks* allow an attacker to bypass safety guarantees built into modern language. In addition, we describe the implementation and evaluation of defenses that prevent such attacks and enable secure usage of safe programming languages.