Title: Confidential Computing across Multiple Devices

Speaker: Jon Lange, Distinguished Engineer, Microsoft

Abstract:

Confidential Computing is emerging as a new set of security promises for cloud-based computing, but what does it mean for hardware implementation? This talk will discuss the basics of confidential computing, including architectures on CPU hardware, and will discuss what is required of any device to claim to support confidential computing, techniques that devices can use to interact with one another to accelerate confidential workloads, and standard protocols that are emerging to facilitate this device interaction.

Bio:

Jon Lange is a Microsoft Distinguished Engineer who has spent the last several years defining the confidential computing architecture for Microsoft Azure, partnering with CPU designers and other hardware vendors to develop that architecture, and building the core infrastructure for hardware-based confidential computing support in the Azure host operating system.