Virtualization has undergone a revitalization over the past decade due to increased system performance and the support for virtualization in commodity hardware. Industry is adopting virtualization to reduce operating costs and improve reliability. Academia is looking to improve experiential learning opportunities and building scalable computer laboratories. The resulting "race to the cloud" has brought to light some of the challenges associated with virtualization.

This minitrack includes 3 papers that cover a range of virtualization topics, and a panel/open-forum.

The panel/open-forum is entitled Specialized Virtualization Environments for Cyber Operations Education Support, and will focus on the use of virtualized to Cyber Operations education and training. We expect this to be an interactive forum, and will be actively seeking audience participation and discussion. The forum will be moderated by Efstatios Gavas (NYU-Poly), and the speakers will include:

• Steven M. LaFountain (Associate Directorate for Education and Training (ADET) at the National Security Agency) will discuss the National Centers of Academic Excellence (CAE) in Cyber Operations Program, which is intended to be deeply technical, firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

• Kara Nance (University of Alaska Fairbanks) will discuss the RAVE infrastructure, capabilities, and the challenges in the context of developing the faculty expertise required to education the next generation of cyber operations professionals.  

• Richard M. (Dickie) George (Johns Hopkins University Applied Physics Lab), will discuss the threat/adversary model, what information is being targeted, and how cyber professionals can address the needs of the nation. The need today has shifted from rocket scientists to cyber warriors – it’s this new breed of scientist that the cyber ops program is creating, and they will serve many roles. He will go over some of those roles – red team, hunter, malware analyst, reverse engineer, and active defender - with the emphasis on the importance of applying virtualized laboratory training to real world problems.

• Chris Eagle (Naval Post Graduate School), will discuss scenarios and use of virtualized environments for malware analysis education, especially as it relates to cyber operations.

The three papers selected for this minitrack cover the range from the development of hardware support for virtualization to the use of virtualization in academic and commercial environments.

In Building a Hypervisor on a Verified Protection Layer, Mike Dahlin et al, discuss their ongoing work aimed at separating the virtualization layer into a small, trusted, and verified component that manages control of the virtualized environment, and an untrusted component that is responsible for providing a given VM with a virtualized hardware environment in which to execute.

In Identifying Weaknesses in VM/Hypervisor Interfaces Kara Nance and Lucas McDaniel describe work they performed to build an analysis and testing environment for various VM/hypervisor interfaces, with the goal of identifying security vulnerabilities that could allow VM “break out” to occur.

Finally, in Cloud-Based Virtual Computing Laboratories, Burd, Luo, and Seazzu discuss the migration of in-house physical and virtual labs to cloud-based versions, and the associated challenges and benefits that such a migration can involve.

The papers in this session show that virtualization is a multi-faceted domain, with a wide range of potential applications, an active research community, and demand for classes and research projects in the academic community.