Abstract: Embedded system security and reliability challenges have been exacerbated by the complexity inherent in the software stack of next generation handheld devices and the aggressive push for multi-core technology. On-chip distributed memories are becoming a necessity with the adoption of multiprocessor systems, and are expected to occupy up to 94% of on-chip real estate. In order to regulate the power consumption of multiprocessors, techniques such as aggressive voltage scaling (AVS) are being deployed at the cost of introducing faults into the memory hierarchy. Moreover, as technology scaling continues to be driven forward and techniques such as AVS continue to be deployed, the increase in on-chip memories makes them the most vulnerable to soft-errors. As applications with different degrees of assurance and criticality are deployed on these multiprocessor platforms, new challenges emerge in terms of protection against software based side channel attacks, exploits such as buffer overruns, and permanent/transient faults. In this talk, I will present SeReVraL, a secure and reliable virtualization layer for on-chip distributed memories. I will first introduce the technology behind SeReVraL and will proceed to discuss a framework for secure software execution exploiting SeReVraL.

Biography: Luis Bathen is a Ph.D. candidate from the University of California, Irvine. He is associated with the Center for Embedded Computer Systems at UCI. His research interests are in embedded systems security, reliability, and virtualization. He is interested in building secure and reliable software/hardware products. He is an Intel/GEM fellow, UCI President’s Dissertation Year fellow, and Eugene Cota-Robles (ECR) fellow. He has worked for Intel and IBM Research, where he has published several conference papers and journals, as well as filed 5 patents (one granted through USPTO). He has made major contributions to several IBM products including IBM’s high-end storage controllers (AMP Technology), IBM’s TPC/Leopard Suite, and IBM’s General Parallel File System. He holds a B.Sc. from UC Irvine.