Title: Securing Systems with Isolated Execution

Abstract: One of the challenges in securing today’s computing systems is how to efficiently protect critical parts of security-sensitive applications from attacks that are launched using untrusted or compromised system software layers. Modern operating systems (OS) and virtualization layers are growing into large and very complex pieces of code. Due to their large size and complexity, it is virtually impossible to design them without exploitable vulnerabilities. Despite a plethora of protection techniques, many recent attacks that exploit vulnerabilities in systems code that bypass existing protections have been successfully demonstrated. Instead of attempting to prevent software bugs or mitigating all possible routes for their exploitation, a fundamentally different approach is to completely isolate security-sensitive parts of application code from potentially compromised system software layers. With significant interest from many hardware vendors including Intel, ARM, AMD and IBM, isolated execution has potential to become a future standard of secure computing.

In this talk, we first introduce Iso-X – a flexible hardware-managed architecture for supporting isolated execution. Isolation in Iso-X is achieved by creating and dynamically managing compartments (isolated software modules) to host critical fragments of code and associated data. Iso-X provides fine-grained isolation at the memory-page level, flexible allocation of memory, and a low-complexity, hardware-only trusted computing base. Iso-X requires minimal additional hardware, a small number of new ISA instructions to manage compartments, and minimal changes to the operating system. In the second part of the talk, we examine some future challenges faced by the isolated execution environments. In particular, we discuss the vulnerability of isolated systems to side-channel attacks and covert channels due to shared physical hardware resources. We then demonstrate several such new attacks that apply to both traditional and isolated systems, and describe possible mitigation strategies.

Bio: Dmitry Evtyushkin in a Ph.D. candidate in the Department of Computer Science at Binghamton University. He received his undergraduate degree from Moscow Institute of Electronics and Mathematics, Moscow, Russia, in 2011. His research interests are in the areas of computer architecture and secure system design, with specific focus on architectures for isolated execution and investigation of covert channels and side channels through shared processor resources. His work was published in leading conferences and journals, including MICRO, CCS, TACO and TDSC. He is a recipient of Binghamton Graduate Student Award for Excellence in Research.