Abstract:
Modern operating systems consist of large, monolithic blobs of complex code, and are plagued with vulnerabilities that allow perpetrators to exploit them for profit. This, coupled with the sophistication of modern adversaries, makes the need for effective and targeted defenses more critical than ever. In this talk, I will present our work on developing novel protection mechanisms and exploit prevention techniques that improve the security posture of commodity operating system kernels. In particular, I will discuss kR^X and XPFO, two projects whose goal is to harden contemporary OSes, against attacks that exploit memory safety vulnerabilities in kernel code, without entailing super-privileged software (e.g., a hypervisor or VMM). In addition, I will talk about ret2dir, a new kernel exploitation technique that we developed, which unveils how standard OS design approaches can significantly weaken the effectiveness of deployed, state-of-the-art kernel defenses.

Bio:
Vasileios (Vasilis) Kemerlis is an Assistant Professor of Computer Science at Brown University. His research interests are in the areas of systems and software security, with a focus on OS kernel protection, automated software hardening, and information-flow tracking. His work on kernel security has been profiled by press and social media outlets, including LWN.net, the Linux Journal, Dark Reading, >>>> and Hacker News, won the first prize in the Applied Security Research Paper competition, at the Cyber Security Awareness Week (CSAW) 2014, and led to the adoption of kernel hardening techniques >>>> from OpenBSD and Qualcomm's MSM Android. In addition, Vasilis has contributed to the design and implementation of Microsoft's primary solution for automatically triaging crash dumps, which is now part of the Windows Error Reporting Platform. In the past, he was a member of the Solaris Core Kernel team at Oracle, where he worked on adding support for full Address Space Layout Randomization (ASLR) in the Solaris OS. Lastly, Vasilis has co-invented the first cache-based side channel attack that can be entirely executed from JavaScript context, which resulted in Apple and Mozilla limiting the time
resolution of JavaScript's performance API (as a mitigation to the proposed attack), and the Tor Project decreasing the time precision of JavaScript entirely. Vasilis holds a PhD (2015), MPhil (2013), and MS (2010) in Computer Science from Columbia University, and a BS (2006) in Computer Science from Athens University of Economics and Business.