GUEST LECTURE ANNOUNCEMENT
Computer Science Department - University of Crete
Seminar Series:
CyberSecurity in Spring: The Spring of CyberSecurity

Defending against Memory Corruption and Transient Execution Attacks

by **Michalis Polychronakis, Stony Brook University**

April 14th, 2022 18:00

https://zoom.us/j/95822937119

Host: Evangelos Markatos, Computer Science Department, University of Crete

Abstract

The exploitation of memory corruption vulnerabilities in popular software is among the leading causes of full system compromise and malware infection. At the same time, the leakage of sensitive data through the exploitation of memory disclosure vulnerabilities is becoming an increasingly important threat. To make matters worse, the threat of data leakage has been exacerbated by the recent spate of transient execution attacks, which can leak otherwise inaccessible process data through residual microarchitectural side effects. In this talk I will present our work on software specialization, the goal of which is to restrict the operations an attacker can perform as part of vulnerability exploitation, and on selective data protection, which prevents data leakage attacks by protecting sensitive user data in memory.

Short Biography

Michalis Polychronakis is an associate professor in the Computer Science Department at Stony Brook University. He received the BSc ('03), MSc ('05), and PhD ('09) degrees in Computer Science from the University of Crete, Greece, while working as a research assistant in the Distributed Computing Systems Lab at FORTH-ICS. Before joining Stony Brook, he was an associate research scientist at Columbia University. His research aims to improve the security of computer systems and networks, build defenses against malicious software and online threats, reinforce the privacy of our online interactions, and enhance our understanding of the internet and its darker sides. He has published more than 100 peer-reviewed papers, many of them in top venues such as IEEE S&P, USENIX Security, ACM CCS, ISOC NDSS, EuroSys, and USENIX ATC, and is the recipient of the DARPA Young Faculty Award (2018) and the NSF CAREER Award (2018).