Private and Trustworthy Computing:
Better Hardware Security with Homomorphic Encryption

Nektarios Tsoutsos
New York University

Wednesday, March 28, 2018
11:00 am – 12:00 pm
HUB Room 3

Abstract:

From financial information and medical records to shopping habits and Internet searches, computing devices are the virtual containers of sensitive information for millions of users. At the same time, the proliferation of privacy attacks, such as state-wide surveillance attempts revealed from whistle-blower cases, federal agencies compelling private companies to develop unsafe software, and high-profile compromises of cloud service providers undermines the users' trust on contemporary computing paradigms. As it is evident from the recent Meltdown and Spectre side-channel vulnerabilities, one root cause to these problems is that modern computer architectures have always been designed for performance, and security protections are traditionally addressed as patches, continuously trying to outsmart adversaries.

A key observation is that any side-channel leakage is harmless as long as sensitive information remains encrypted during processing, which motivates the use of special cryptographic methods such as homomorphic encryption. This talk discusses the design of encrypted processors that support privacy outsourcing based on a single-instruction computer architecture. To achieve trustworthy computation on encrypted data in light of soft errors and maliciously injected faults, this talk presents integrity and fault-tolerance countermeasures that enable real-time error detection using judiciously defined metadata. In addition, open research problems in encrypted data processing will be discussed, such as the design of homomorphic circuits and encrypted processors with multiple instructions.

Short Bio:

Nektarios Tsoutsos is a security researcher focusing on hardware security, applied cryptography, computer architecture, and cyberphysical systems. He received the Ph.D. degree in computer science from New York University in 2018, and the M.Sc. degree in computer engineering from Columbia University in 2010. Dr. Tsoutsos holds a patent on encrypted computation using homomorphic encryption and has published articles on privacy outsourcing, fault tolerance, memory authentication, privacy-preserving benchmarks, hardware Trojan designs, additive manufacturing security, homomorphic e-voting attacks, as well as intellectual property protection using Intel's software guard extensions. From 2015 to 2017 he was the organizer of the Embedded Security Challenge event that is held annually in North America, Europe, India and the Middle East as part of NYU's Cyber Security Awareness Week. In 2014 he joined Intel's Security Center of Excellence for six months, while from 2010 to 2012 he worked as an advisor in the information security industry.