Anton Burtsev
aburtsev@uci.edu
https://www.ics.uci.edu/~aburtsev/

Title: Building the Future Operating Systems: Fast, Secure, and Cloud-Scale

Abstract: Despite numerous ways in how the use of computer systems has evolved over the last decades, the software engineering technology behind the very core of the systems stack—an operating system kernel—remains unchanged since early computer systems. Starting as a relatively simple software layer, four decades ago operating systems were designed to provide isolation and multiplexing of hardware. Two decades ago, security attacks against these systems were a pastime for small communities of hobbyists, and we were running these systems on a single general CPU. Today, systems with essentially the same architecture and security model are required to operate in the face of targeted security attacks sponsored by a multi-national malware economy, commercial espionage, and government intelligence agencies. If modern commodity operating systems are centered around general-purpose processors, the next generation of systems will inherently rely on diverse, heterogeneous hardware ranging from many-core processors like Intel Xeon Phi that contains up to 72 processor cores and graphical processing units (GPUs) to specialized hardware accelerators, like specialized machine-learning chips and field-programmable gate arrays (FPGAs) re-programmed on demand for a specific task. In a hardware-accelerated environment that consists of many diverse execution units, the execution of a program is no longer a conventional thread tied to a single CPU, but a graph of small computations scheduled on a set of hardware accelerators each implementing a part of the program logic. And if historically the use of datacenters was a rare exception in the domain of high-performance computing, most daily workloads ranging from social networks to personalized health medicine rely on a computational power and storage capacity of a cloud.

This talk describes three new operating system projects that aim to develop the next generation of operating systems designed to resist targeted security attacks, leverage heterogeneous hardware, and provide security and privacy of data in a cloud. RedLeaf is a new operating system, and associated formal verification tools for implementing provably secure and reliable systems in the Rust programming language. Redshift is a new operating system for developing applications that leverage performance of a heterogeneous hardware-accelerated system. Horizon is a novel cloud architecture aimed at providing data and computation security within a cloud.