Trustworthy software execution is increasingly demanded in multiple situations, including the cloud computing environment where customers execute their software in cloud servers, and in edge computing where computing may be performed on the edge nodes. Customers require strong privacy and security guarantees from a secure trust base in hardware. Recognizing this, chipmakers recently introduced secure execution environment, such as Intel SGX and AMD SEV. A key component of secure execution environment is memory encryption and integrity verification. In this talk, I will give a short overview of key milestones in memory encryption and integrity verification technologies. Then, I will discuss how these technologies are not adequate in providing secure execution environment in the future, for several reasons. First, the threat model is incomplete. The pervasiveness of side channel vulnerabilities and attacks in both cloud servers and edge nodes can bypass the protection provided by SGX and SEV. This is evident in the recent Spectre and Meltdown security vulnerabilities. Second, these technologies are not compatible with new memory technologies that are coming online, such as 3D-stacked DRAM, and non-volatile main memory (NVMM). Third, they are too expensive for use in Internet of Things (IoT) devices, especially ones that require low power consumption or ones with intermittent energy supply.

In the second portion of the talk I will discuss my thoughts on emerging topics on cybersecurity research, and my thoughts on making cluster collaboration successful.