Writeup for the talks of Dr. Dan Williams 10/15

Submitted by: Provakar Mondal

Dr. Dan Williams is an Assistant Professor in the Department of Computer Science at Virginia Tech joined in August 2021. Before that he spent 10 years as a research staff at IBM.

Dr. Williams's research interests lie in the field of operation systems, security, cloud. He likes to investigate new mechanisms for process sandboxing and isolation. In a short, improving the security and efficiency of the fundamental computing systems that our society depends on is the area where Dr. Williams's research interests are focused.

In the seminar, Dr. Williams talked about serverless cloud computing. As an example, he mentioned **MicroVM** that is secure and efficient. Then he talked about **KASLR** that rises in the age of micorVMs. He used visualization to depict the cloud workloads trends.

The advantages of serverless systems are thought to run code without provisioning or managing servers, event-driven, fine-grained elasticity, millisecond metering. But for this, it is required a lightweight unit of execution. VMS has better isolation but the problem is that they are heavyweight and if boot-up time is applied that is also costly. Then the era of virtualization has appeared to make a practical solution for this problem.

In the seminar, Dr. Williams pointed out MicroVMs as lightweight guests and lightweight monitors. As a result, they can boost fast. Then he introduced a question, how to MicorVMs boot quickly, and answered the question by saying MicorVMs cut out bootstrap or legacy as legacy stacks give compatibility.

Later Dr. Williams described details of Linux boot. **bzImage** is usually an image of the Linux kernel. It contains Bootstrap loader, Compressed kernel, and "relocations". Booting a bzImage is the process where the monitor loads bzImage into guest memory and transfers control to the guest (bootstrap loader), then the bootstrap loader copies compressed kernel out of the way, the bootstrap loader decompresses kernel, and finally parses kernel ELF. After that Dr. Williams showed experiments data used in Firecracker boot time. MicroVMs boot faster by modifying Firecracker to support bzImage boot and 20%-36% performance improvement over LZ4 in boot time through the direct boot.

In the later phase of the talk, Dr. Williams talked about KASLR and its unfortunate omission as it has the chance to leak information and one information leak can give it all away and its kernel is not designed to protect information.

Dr. Williams then talked about in monitor randomization and explained the intuition behind the design. In this design, bootstrap steps are unnecessary in an already bootstrapped virtualized environment, expensive relocation can be avoided, the kernel is loaded once into its final resting place.

Dr. Williams provided a very informative and nice presentation. Many deep things about computing systems were presented. He also used nice comparison results and images to attract the attention of the attendee.