Operational Visibility and Security Analytics Designed for Cloud

Canturk Isci
IBM TJ Watson Research Center

12/19/2017 at 10:30 am
CoRE 301

Abstract

We are witnessing a major shift in the foundations of computing. There is an accelerating growth in the scale and the variety of cloud platforms, emerging runtimes, and new programming models. Cloud computing discussion has shifted from mere utility and density to cloud-native services and design patterns. Emerging cloud services allow users to define and provision complex, distributed systems with unprecedented simplicity and agility. With the push of a button entire stacks of software can be instantiated within minutes with various configurations and customizations. Automation, continuous integration and delivery further simplify the entire lifecycle management of modern born-on-the-cloud applications. However, these advances also bring in new research challenges. Operational visibility into the complex, distributed applications, cloud runtimes and the underlying infrastructure is becoming a persistent pain point across end-users and providers for operational and security insights. As system and configuration complexity grows, data-driven operational analytics for security, compliance, configuration and resource management emerge as key areas of new innovation, where traditional solutions remain ineffective or insufficient.

In this talk I will present an overview of the cloud evolution, emerging runtimes and design patterns. I will describe the challenges arising from this evolution and where existing techniques fall short. I will then present our recent work on cloud operational visibility and analytics that tackles some of these challenges. I will describe a unique approach to leveraging cloud abstractions and implementation principles to achieve unmatched deep and seamless visibility into cloud instances, and using this deep visibility to develop operational and security analytics for the cloud. I will overview two outcomes of this approach, Agentless System Crawler and the Vulnerability Advisor service. I will discuss our journey developing the foundations of the visibility and security services for IBM Cloud Containers. I will share our

experiences working with a production cloud and the key real-world use cases. I will provide an overview of our current research directions, open problems and opportunities in this area.

Bio

Canturk Isci is a Principal Researcher, Manager and Master Inventor in IBM TJ Watson Research Center, where he leads the Cloud Monitoring, Operational and Security Analytics team. He currently works on deep introspection based monitoring techniques for cloud, and their application to novel operational, security and DevOps analytics. He is the technical lead for IBM Vulnerability Advisor for Containers and for Agentless System Crawler. His research interests include operational visibility, analytics and security in cloud, virtualization, energy-efficient and adaptive computing. Prior to IBM Research, Canturk was a Senior Member of Technical Staff at VMware, where he worked on distributed resource and power management. He has a B.S. from Bilkent University, an M.Sc. with Distinction from University of Westminster, UK and a Ph.D. from Princeton University.

Faculty Host: Abhishek Bhattacharjee