THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

RESEARCH SEMINAR

Execution Flow Instrumentation and Its Applications

Dr Xuhua DING
Associate Professor
School of Computing and Information Systems
Singapore Management University
Singapore

***Date* : 20 December 2023 (Wed)**
***Time* : 10:00 am - 11:00 am**
***Venue* : N002**

Abstract

In this talk, we begin with an introduction to Execution Flow Instrumentation (EFI), a powerful dynamic analysis approach that interleaves the instruction flows of the target thread and of the analysis thread together without mixing up their code. EFI thus combines the advantages of code instrumentation and hardware-aided event trapping but without their drawbacks. We then present OASIS which is a system infrastructure that realizes EFI. On top of OASIS, a user can run her user-space analyzer to conduct dynamic analysis upon a kernel- or user-thread running in a guest virtual machine with guaranteed security and transparency. Applications of OASIS based EFI go beyond conventional dynamic analysis. It allows us to build a kernel symbolic execution engine (named as KRover) without involving intermediary representation or dynamic binary translation. It can also be applied in cloud platforms to introspect and repair malfunctioning virtual machine.

About the Speaker

Dr Xuhua Ding is currently an Associate Professor of Computer Science and Lee Kong Chian Fellow at the School of Computing and Information Systems, Singapore Management University. He has over twenty years of research experience on cybersecurity, spanning across applied cryptography, privacy-preserving protocols, network security, and system/software security on x86 and ARM platforms.