Securing Modern Systems by Preventing Information Leaks

Widely used systems such as operating systems and web servers are implemented in unsafe programming languages for efficiency, and system designers often prioritize performance over security. Hence, these foundational systems inherently suffer from a variety of vulnerabilities and insecure designs that have been exploited by adversaries to launch critical system attacks. Two typical goals of these attacks are to leak sensitive data and to control victim systems.

In this talk, I will first explain why, in modern systems, preventing information leaks can be a general defense that not only stops data leaks but also defeats control attacks. Then, I will present three ways to prevent information leaks: eliminating information-leak vulnerabilities in code, re-designing system mechanisms against information leaks, and protecting certain sensitive data from information leaks. Correspondingly, I have developed three tools, which impose negligible performance overhead while automatically and reliably securing complex systems. In the end, I will discuss how to secure both widely used and emerging systems in various dimensions.

Kangjie Lu is a Ph.D. candidate in Computer Science at the Georgia Institute of Technology. His research interests include security and privacy, program analyses, and operating systems. He is particularly interested in automatically uncovering and addressing fundamental security problems, and securing widely used systems while preserving their reliability and efficiency. In addition to papers published in top-tier security conferences (CCS, NDSS, and USENIX Security), his research has resulted in many important updates in the Linux kernel, the Android OS, and Apple's iOS. During his Ph.D. study, he worked as an intern at NEC Labs America and Samsung Research America, and as a visiting scholar at the Max Planck Institute for Software Systems (MPI-SWS).