Recent cyberattacks involve various actors including diverse adversaries, where each actor plays subtle but prominent roles. It is essential to understand the real-world actors from various aspects to mitigate security threats and protect end-users from the threats. In this talk, I will present fundamental findings from several measurements and user studies exploring and understanding the unique behaviors of adversaries as well as benign software developers that cause various security incidents. First, I will discuss the malicious actor, adversaries: particularly, how they abuse the Code-Signing Public Key Infrastructure (PKI) by exploiting the weaknesses in other actors (i.e., certificate authorities, publishers, and end-users). Second, I will describe why benign software developers often fail in secure development and present blueprints for improvement. Finally, I will conclude by discussing my future research directions in understanding new security threats and actors from emerging technologies (e.g., IoT).

Bio:
Doowon Kim is a Ph.D. candidate in the Department of Computer Science at the University of Maryland, College Park. His research focuses on data-driven security and usable security. Specifically, he investigates the root causes of security threats by better understanding actors (e.g., adversary and end-users) involved, with data-driven and human-centered perspectives. Moreover, his work covers the Code-Signing PKI, the Web PKI, and the security behaviors of benign software developers. His research has resulted in a real-world impact on the Code-Signing PKI and has generated interest from media such as Ars Technica, The Register, Schneier on Security, and Threatpost. He is a recipient of the NSA Best Scientific Cybersecurity Paper Award and Ann G. Wylie Dissertation Fellowship.