COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

DUC BUI

Assessment of Privacy Risks in Mobile and Web Applications

Tuesday, May 17, 2022
2:30 – 4:30pm
3725 BBB
Virtual

ABSTRACT: The ubiquity of mobile apps and online services, which collect data in all corners of users' daily lives, stresses the need for assessing their increased risk to user privacy. While the applications widely utilize privacy policies to inform users of their data practices, the policies are difficult and time-consuming for users to comprehend due to their great length and use of legal language. More importantly, the actual implementation of data practices and opt-out choices are not always consistent with the stated privacy policies and user privacy preferences.

First, I present PI-Extract, an automated framework that extracts and presents data practices stated in privacy policies to help users read and understand them easily and fast. A user study shows that PI-Extract's presentation significantly improves the users' reading comprehension of policy texts. Second, I develop PurPliance, an automated system that detects the inconsistencies between the data-usage purposes stated in the privacy policy and those of the actual execution behavior of an Android app. I create a formal model to represent and verify the data usage purposes in the extracted privacy statements and data flows to detect policy contradictions in a privacy policy and flow-to-policy inconsistencies between network data flows and privacy statements. The evaluation results of the end-to-end detection of contradictions have shown a significant improvement over a state-of-the-art method. Finally, I create end-to-end automated systems to analyze the flow-to-policy consistency of the privacy practices of websites, online trackers, and browser extensions. Specifically, ConsentChk detects the inconsistencies between a website's data collection via cookies and the cookie consent preferences of users. OptOutCheck analyzes the (in)consistency between online trackers' data collection and the opt-out choice statements in their privacy policies. ExtPrivA checks the discrepancies between browser extensions' data collection and their privacy disclosures. These systems found a large number of online services and browser extensions whose actual behavior was not consistent with their disclosed data practices. The automatic analysis techniques offer an effective and scalable privacy assessment that benefits all stakeholders of the Web and mobile ecosystems, including users, developers, and regulators.

CHAIR: Prof. Kang Shin