CURRENT TOPICS IN PRIVACY SEMINAR

CarnegieBosch INSTITUTE

Carnegie Mellon University privacy ENGINEERING

Igor Bilogrevic - Google

Enhancing Safety on the Web with On-Device ML

Abstract

The web is a powerful platform for developers and users, enabling the former to provide personalized experiences and sophisticated services to the latter. Most users experience the open web through their browser, which is their agent in the online world. Safety is a critical aspect in the online world, and browsers have different ways to mitigate online threats. In this talk, I will cover two recent advances in web safety: notifications spam mitigation and distributed browser fingerprinting detection. Most notification prompts are not granted by users, but they constitute a potential threat vector for subsequent online abuses (e.g., phishing). To decrease the notification spam in Chrome, we designed, evaluated and deployed an on-device ML model that decides whether to show a less visible permission prompt depending on the browsing context and the users' past actions in such context. Regarding browser fingerprinting, which is a privacy-invasive technique to extract a quasi-unique device identifier from the browser's properties and device characteristics, we designed and evaluated a novel detection approach based on federated learning with differential privacy guarantees.

Bio

Igor is a Staff Research Scientist working to bring novel machine learning and AI features for privacy and security in products. His mission is to make technology simpler, safer and smarter for the users. By default. He has a PhD on applied cryptography and machine learning for privacy-enhancing technologies from EPFL (Switzerland). Previously, he worked in collaboration with the Nokia Research Center on privacy challenges in pervasive mobile networks, encompassing data, location and information-sharing privacy. He has spent a summer at PARC (a Xerox Company), conducting research on topics related to private data analytics. He is a co-inventor on several patents filed by Nokia, PARC and Google. He is interested in several domains that are related to the applications of machine learning and AI to privacy and security, such as web browser privacy and contextual intelligence.

Seminar delivered remotely

TUESDAY, FEBRUARY 25TH **Hamburg Hall, 1002 and Zoom**