# Privacy-Preserving Data Synthesis and Inference Attacks

Vincent Bindschaedler
University of Illinois at Urbana-Champaign (UIUC)

2/19/2018 at 10:30 am
CoRE 301

## Abstract

A challenging problem in data privacy is privacy-preserving data publishing. Straightforward approaches such as removing identifiers to ensure anonymity do not provide meaningful protection against inference attacks. In this talk, I will describe a new framework to share sensitive datasets in a privacy-preserving way. I will show how to construct a mechanism to synthesize full data records using a probabilistic generative model. A key feature of this technique is that privacy is not achieved by modifying the generative model or adding noise. Instead, a privacy test is used to decide whether each synthesized record can safely be published. On the theoretical front, I will show that appropriately randomizing the privacy test yields differential privacy. On the experimental front, I will apply the framework to various types of data, including census microdata, location trajectories, and images.

## Bio

Vincent Bindschaedler is currently a PhD candidate in Computer Science at the University of Illinois at Urbana-Champaign (UIUC). He received his MSc and BSc from EPFL. His research interests include data privacy, applied cryptography, and the intersection of machine learning with security and privacy. His recent work focuses on privacy-preserving data sharing and understanding side-channels threats.

Faculty Host: Badri Nath