A U S H A N G

FREIE UNIVERSITÄT BERLIN

Fachbereich Mathematik und Informatik

Promotionsbüro, Arnimallee 14, 14195 Berlin

D I S P U T A T I O N

Donnerstag, 17. November 2022, 15:00 Uhr

WebEx

Disputation über die Doktorarbeit von

Frau Franziska Boenisch

Thema der Dissertation:

Secure and Private Machine Learning

Thema der Disputation:

What Trust Model is Needed for Federated Learning to be Private?

Die Arbeit wurde unter der Betreuung von **Prof. Dr. M. Margraf** durchgeführt.

Abstract: In federated learning (FL), data does not leave personal devices when they are jointly training a machine learning model. Instead, these devices share gradients with a central party (e.g., a company). Because data never "leaves" personal devices, FL was promoted as privacy-preserving. Yet, recently it was shown that this protection is but a thin facade, as even a passive attacker observing gradients can reconstruct data of individual users.
In this talk, I will explore the trust model required to implement practical privacy guarantees in FL by studying the protocol under different trust assumptions regarding the central party. I will first show that in vanilla FL, even a central party that passively observes the gradients can reconstruct individual users' training data points. Then, I will present state-of-the-art methods that allow an actively malicious central party to amplify reconstruction success. Finally, I will present defense methods that are intended to protect FL against this type of attacks and motivate why most of them still fail to yield privacy guarantees under the presence of an untrusted central party. I will conclude the talk by an outlook on what it will take to achieve privacy guarantees in practical FL implementations.

Die Disputation besteht aus dem o. g. Vortrag, danach der Vorstellung der Dissertation einschließlich jeweils anschließenden Aussprachen.

Interessierte werden hiermit herzlich eingeladen

Der Vorsitzende der Promotionskommission
Prof. Dr. M. Margraf