Machine Learning and Privacy: Friends or Foes?

Vitaly Shmatikov (Cornell Tech)

Machine learning is eating the world. Modern machine learning methods, especially deep learning based on artificial neural networks, rely on the training data collected from millions of users to achieve unprecedented accuracy and enable powerful AI-based services.

In this talk, I will discuss the complex relationship between machine learning and digital privacy. This includes new threats, such as adversarial use of machine learning to recover hidden user data, and new benefits, such as privacy-preserving machine learning that protects the confidentiality of training data while constructing accurate models.