# Attacks on Federated Learning

- Attack 1: Data poisoning attack [1].

**References**

1. Shafah and others: Poison frogs! targeted clean-label poisoning attacks on neural networks. In *NIPS*, 2018.