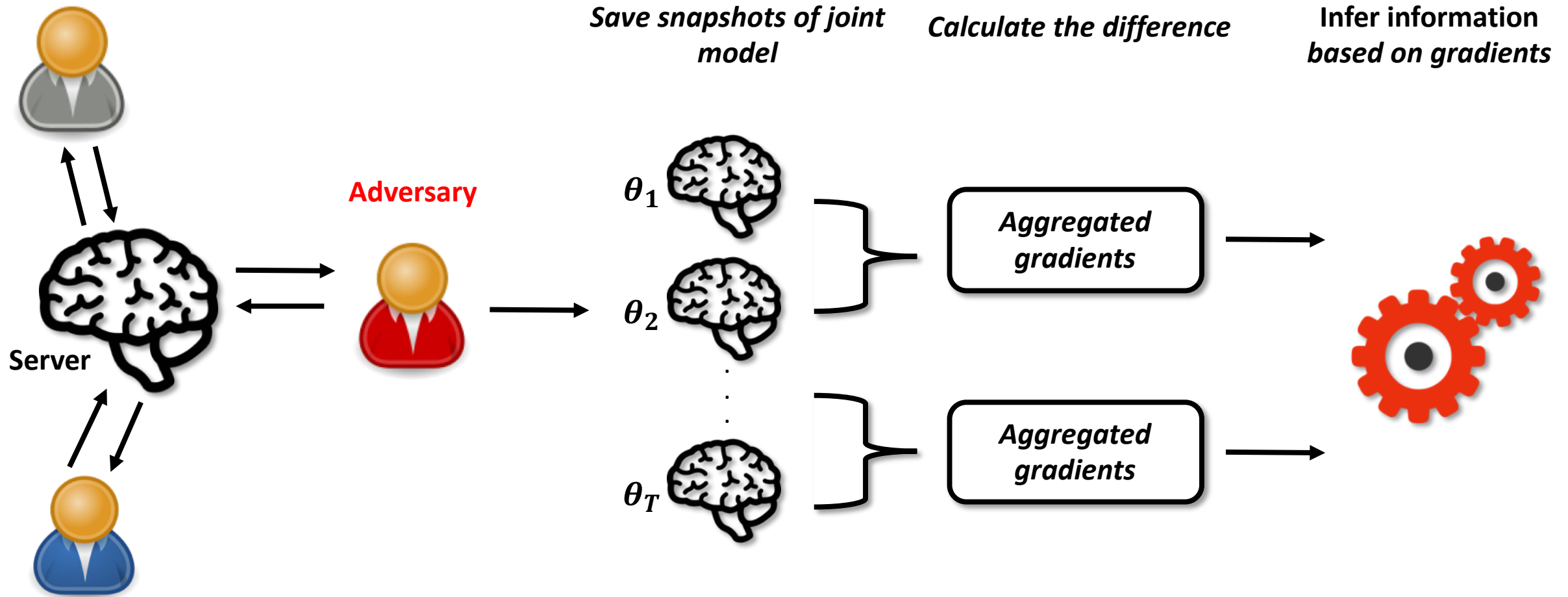# Passive Property Inference Attack

Luca Melis, Congzheng Song, Emiliano De Cristofaro, Vitaly Shmatikov. Inference Attacks Against Collaborative Learning. Under Submission.

Active Property Inference Attack

Gradients on Main Loss

$L(x, y; \theta)$

Main Task (Gender)

Layer N

Layer 2

Layer 1

Upload local updates

Server

Download joint model

Gradients on Joint Loss

$\alpha * L(x, y; \theta) + (1 - a) * L(x, p; \theta)$

Main Task (Gender)

Inference Task (Facial ID)

Layer N

Layer 2

Layer 1