Backdoor Attacks/Defenses

Can you backdoor federated learning?

Difficult to control the local model submitted by malicious participants

Defenses that require access to the training data or to invert the model violate privacy (ouch!)

Can you really backdoor federated learning?

Norm Bounding

Weak Differential Privacy

Work okay in most settings, but privacy?

48

Backdoor Attacks/Defenses

Can you backdoor federated learning?

Difficult to control the local model submitted by malicious participants

Defenses that require access to the training data or to invert the model violate privacy (ouch!)

Can you really backdoor federated learning?

Norm Bounding

Weak Differential Privacy

Work okay in most settings, but privacy?

Backdoor Defenses