Hardware fingerprint

$\mathcal{D}_{train}$

$\mathcal{D}_{auth}$ Correct label

$\mathcal{D}_{rand}$ Random label

Add trigger

Shuffle label

$\mathcal{L}_{total}$ Train

DNN

Model theft

with trigger

Authorized use

airplane

w/o trigger

Unauthorized use

cat