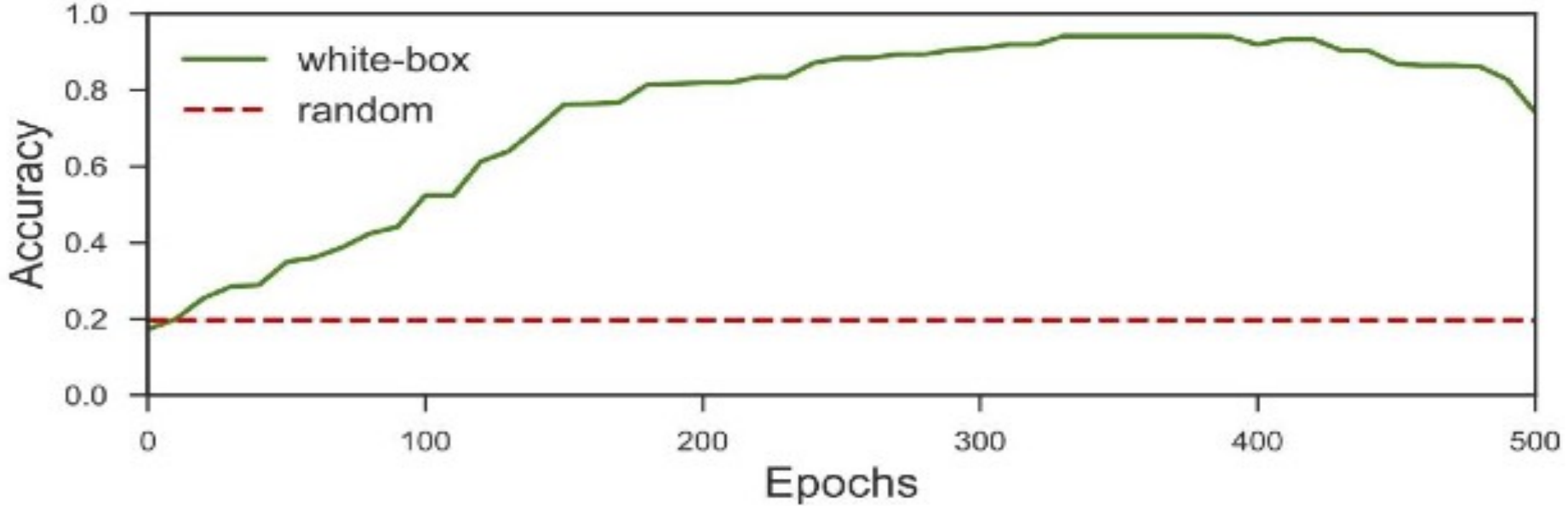
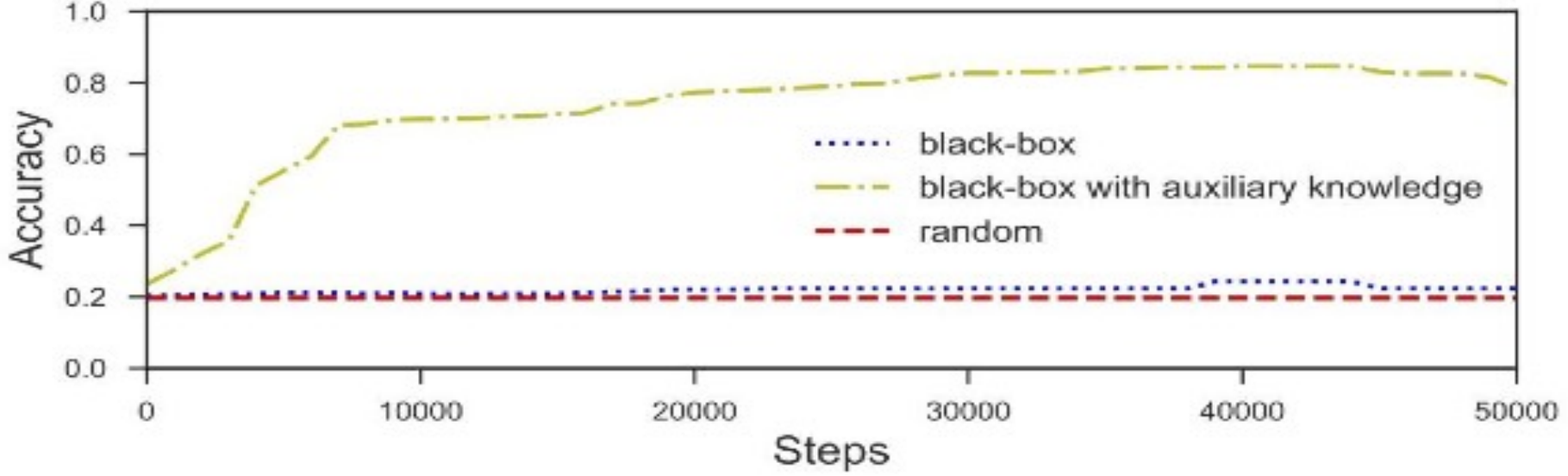
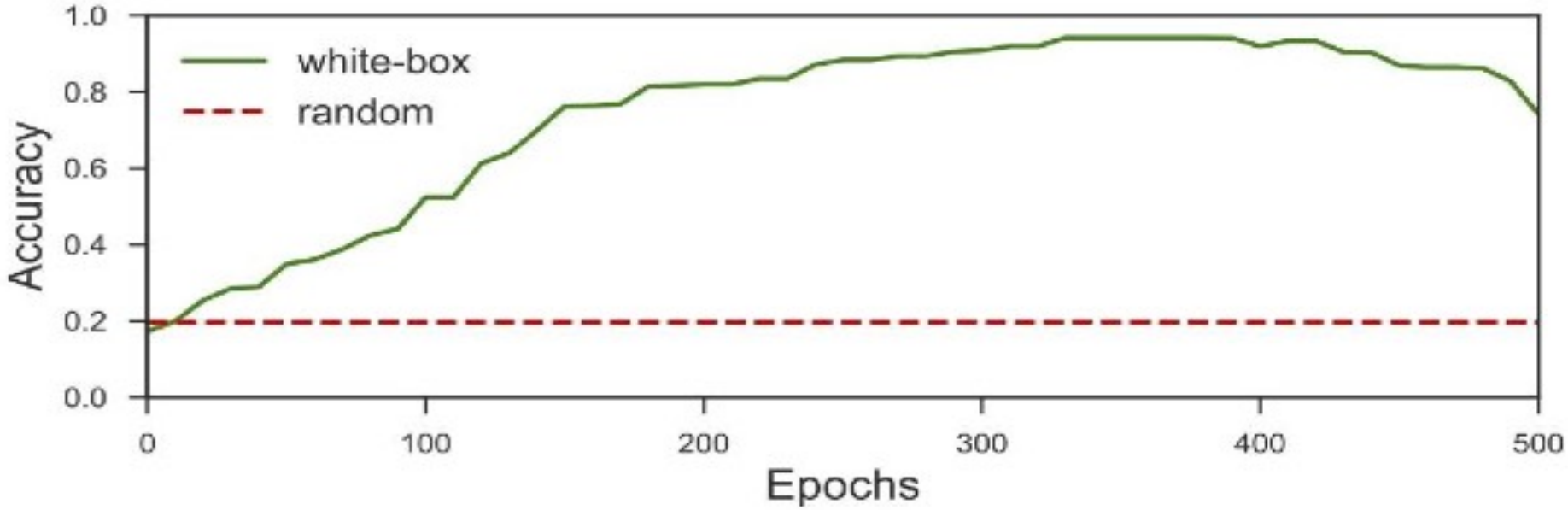
DR Dataset

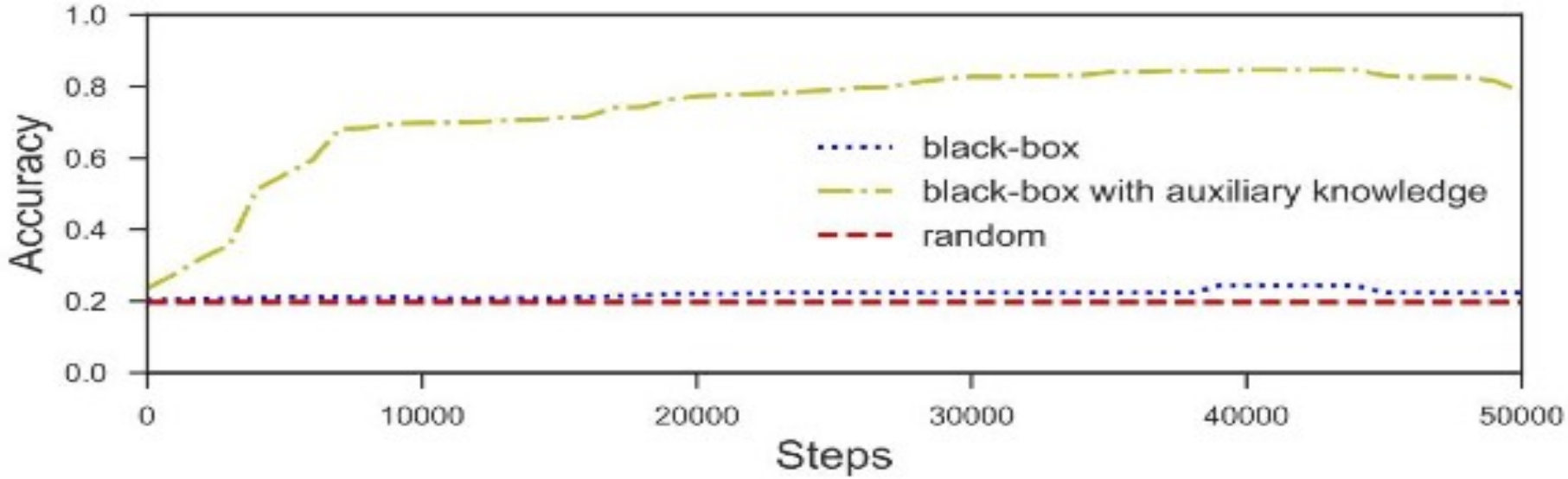

1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
white-box
random
0
100
200
300
400
500
Epochs


1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
black-box
black-box with auxiliary knowledge
random
0
10000
20000
30000
40000
50000
Steps

22

DR Dataset


1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
white-box
random
0
100
200
300
400
500
Epochs


1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
black-box
black-box with auxiliary knowledge
random
0
10000
20000
30000
40000
50000
Steps

Results

Attack	LFW	CIFAR-10	DR
White-box	100%	100%	95%
Black-box	40%	37%	22%
Black-box with aux knowledge	60%	58%	81%
Random guess	10%	10%	20%