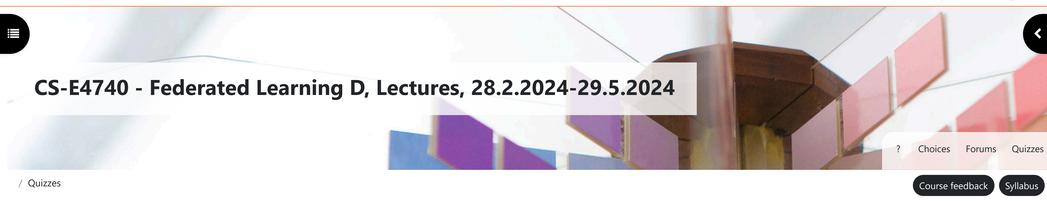

CS-E4740 - Federated Learning D, Lectures, 28.2.2024-29.5.2024

Started on	Friday, 26 April 2024, 7:35 PM
State	Finished
Completed on	Friday, 26 April 2024, 9:14 PM
Time taken	1 hour 38 mins
Grade	**11.00** out of 11.00 (**100**%)

Question 1

Flag question Mark 3.00 out of 3.00 Correct

Match the attack types with their correct descriptions.

Some private attributes of data points at a target node are inferred by exploring the learnt model parameters at this node. — Privacy Attack ✔

A target node within a FL system is forced to learn a hypothesis that is accurate on the local dataset. However, the learn hypothesis behaves very different outside the feature range of the data points in the local dataset. — Backdoor Attack ✔

A target node within a FL system is forced to learn, by manipulating the operation at other nodes, a hypothesis that is not accurate. — Denial-of-Service Attack ✔

Your answer is correct.

The correct answer is:
Some private attributes of data points at a target node are inferred by exploring the learnt model parameters at this node. → Privacy Attack,

A target node within a FL system is forced to learn a hypothesis that is accurate on the local dataset. However, the learn hypothesis behaves very different outside the feature range of the data points in the local dataset. → Backdoor Attack,

A target node within a FL system is forced to learn, by manipulating the operation at other nodes, a hypothesis that is not accurate. → Denial-of-Service Attack

Question 2

Flag question Mark 3.00 out of 3.00 Correct

Which of the following loss functions typically results in ERM being **least robust** against perturbations of data points in the training set.

- [x] a. The squared error loss. ✔
- [ ] b. The absolute error loss.
- [ ] c. The linear least squares function regularized by l2-norm.

Your answer is correct.

The correct answer is:
The squared error loss.

Question 3

Flag question Mark 3.00 out of 3.00 Correct

*This question refers to **the student task #1** in the "Data Poisoning in FL" assignment.*

The implemented Denial-of-Service attack affects the validation error of the attacked node's model parameters via adding noise to (randomly selected) other nodes in the empirical graph.

Match the random seed with the corresponding minimum required number of poisoned nodes to increase the validation error of the attacked node's model parameters by 20%. Attack the node indexed 1 (in the code: *attacked_node = 1*).

P.S. The intervals with the number of poisoned nodes are given to allow for variations caused by using different Python environments. If - for a specific seed value - you find that at least 3 poisoned nodes are required, then the intervals [1, 3], [2, 5], or [3, 10] are all correct.

Seed = 10001 [21, 23] ✔

Seed = 101 [4, 6] ✔

Seed = 4 [8, 10] ✔

Seed = 1 [4, 6] ✔

Seed = 4740 [17, 19] ✔

Your answer is correct.

The correct answer is:
Seed = 10001 → [21, 23],

Seed = 101 → [4, 6],

Seed = 4 → [8, 10],

Seed = 1 → [4, 6],

Seed = 4740 → [17, 19]

Question 4

Flag question Mark 2.00 out of 2.00 Correct

*This question refers to **the student task #2** in the "Data Poisoning in FL" assignment.*

How many data points of the attacked node have been poisoned to plant the backdoor into the trained linear model? Attack the node indexed 1 (in the code: *attacked_node = 1*). The backdoor trigger is 4 (in the code: *trigger = 4*).

P.S. Consider all data points of the attacked node (training + validation).

- [ ] a. 0
- [ ] b. 1
- [ ] c. 2
- [ ] d. 3
- [x] e. 4 ✔
- [ ] f. 5
- [ ] g. 6
- [ ] h. 7

Your answer is correct.

The correct answer is:
4

Finish review

Previous activity

◄ "Privacy in FL"