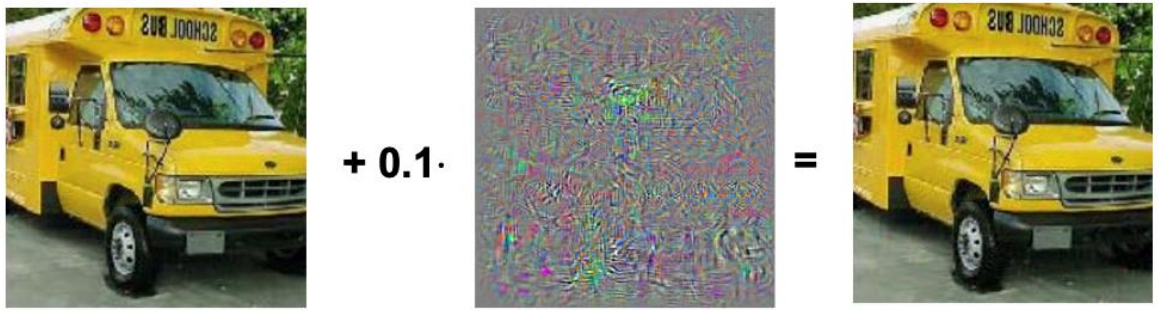
CS-E4001 - Research seminar on Security and Privacy of Machine Learning, 5 credits

When: Period I-II, Tue & Fri, 12:15-14

(Registration period: 12.8.-16.9.2019)



What:

- Read scientific papers on security threats/attacks/defences to ML systems
- Present and discuss papers in contact sessions (2 papers per session)

Topics of discussion:

- Model evasion with adversarial examples and defenses against them
- Model poisoning that modifies the decision boundary of ML models
- Protection of the intellectual property of ML models
- Privacy of training (data and ML models)
- Etc.

https://mycourses.aalto.fi/course/view.php?id=26474