EPFL-Inria
INTERNATIONAL LAB

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Workshop EPFL-Inria
January 30 and 31, 2019, Lausanne

***Carmela Tronsoco*,** EPFL

Title: « When foes are friends: adversarial examples as protective technologies »

Abstract:
The last decade advances in machine learning have made it a flagship technology for industry in order to optimize their operation and benefits. At the same time, these advances may have very negative effects on users. Machine learning algorithms can perform unprecedented inferences and can be used to make accurate predictions about individuals. Given the lack of explainability of machine learning decisions, an open research field, devising protections against these inferences is a hard task. In this talk we explore the potential of adversarial examples as a tool to systematically design protection against the threats introduced by the pervasiveness of machine learning in everyday online services.