Work on security evaluation of learning algorithms

Work on evasion attacks (a.k.a . adversarial examples)

…..in malware detection ( PDF / Android)

Work on poisoning attacks

Adversarial ML

2004 2005 : pioneering work

Dalivi et al,.KDD 2004

Lowd & Meek, KDD 2005

* Mimimum-distance evasion of linear classifiers
* Notion of adversary-aware classifiers