Adversarial machine learning

Abstrak

Written by leading researchers, this complete introduction brings together all the theory and tools needed for building robust machine learning in adversarial environments. Discover how machine learning systems can adapt when an adversary actively poisons data to manipulate statistical inference, learn the latest practical techniques for investigating system security and performing robust data analysis, and gain insight into new approaches for designing effective countermeasures against the latest wave of cyber-attacks. Privacy-preserving mechanisms and the near-optimal evasion of classifiers are discussed in detail, and in-depth case studies on email spam and network security highlight successful attacks on traditional machine learning algorithms. Providing a thorough overview of the current state of the art in the field, and possible future directions, this groundbreaking work is essential reading for researchers, practitioners and students in computer security and machine learning, and those wanting to learn about the next stage of the cybersecurity arms race.