Not that smart!
Security Vulnerabilities in Machine Learning

by Konrad Rieck (TU Braunschweig)

Machine learning is increasingly used in security-critical applications, such as autonomous driving, face recognition, and malware detection. However, most learning algorithms have not been designed with security in mind and thus are vulnerable to different types of attacks. These attacks may hinder the learning process (poisoning), induce false predictions (evasion), or extract sensitive data from the system (inference). This talk provides an overview of current research on adversarial machine learning and discusses relevant attack types. The talk closes with an outlook on the development of defenses for learning-based systems.