Computers » Cybernetics

Secure Learning and Learning for Security: Research in the Intersection

Authors: Benjamin I Rubinstein; CALIFORNIA UNIV DAVIS DEPT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

Abstract: Statistical Machine Learning is used in many real-world systems, such as web search, network and power management, online advertising, finance and health services, in which adversaries are incentivized to attack the learner, motivating the urgent need for a better understanding of the security vulnerabilities of adaptive systems. Conversely, research in Computer Security stands to reap great benefits by leveraging learning for building adaptive defenses and even designing intelligent attacks on existing systems. This dissertation contributes new results in the intersection of Machine Learning and Security, relating to both of these complementary research agendas. The first part of this dissertation considers Machine Learning under the lens of Computer Security, where the goal is to learn in the presence of an adversary. Two large case-studies on email spam filtering and network-wide anomaly detection explore adversaries that manipulate a learner by poisoning its training data. In the first study, the False Positive Rate (FPR) of an open-source spam filter is increased to 40% by feeding the filter a training set made up of 99% regular legitimate and spam messages, and 1% dictionary attack spam messages containing legitimate words. By increasing the FPR the adversary a defects a Denial of Service attack on the filter. In the second case-study, the False Negative Rate of a popular network-wide anomaly detector based on Principal Components Analysis is increased 7-fold (increasing the attacker's chance of subsequent evasion by the same amount) by a variance injection attack of **chaff** traffic inserted into the network at training time. This high-variance **chaff** traffic increases the traffic volume by only 10%.

Limitations:	APPROVED FOR PUBLIC RELEASE
Description:	Doctoral thesis
Pages:	208
Report Date:	13 May 2010
Report Number:	A243835

« Back to search