Security and Machine Learning

Professor David Wagner
University of California, Berkeley
daw@cs.berkeley.edu

ABSTRACT

Machine learning has seen increasing use for a wide range of practical applications. What are the security implications of relying upon machine learning in these settings? Recent research suggests that modern machine learning methods are fragile and easily attacked, which raises concerns about their use in security-critical settings. This talk will explore several attacks on machine learning and survey directions for making machine learning more robust against attack.

BIOGRAPHY

David Wagner is Professor of Computer Science at the University of California at Berkeley. He has published over 100 peer-reviewed papers in the scientific literature and has co-authored two books on encryption and computer security. His research has analyzed and contributed to the security of cellular networks, 802.11 wireless networks, electronic voting systems, and other widely deployed systems.

CCS'17, October 30-November 3, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-4946-8/17/10.
DOI: https://doi.org/10.1145/3133956.3134108