UCI Department of Computer Science

DISTINGUISHED LECTURE SERIES

SOMESH JHA

Lubar Professor, Computer Sciences Department
University of Wisconsin - Madison

"Towards Semantic Adversarial Examples"

Friday, January 18, 2019 • 11 a.m.
Donald Bren Hall, Room 6011

ABSTRACT

Fueled by massive amounts of data, models produced by machine-learning (ML) algorithms, especially deep neural networks, are being used in diverse domains where trustworthiness is a concern, including automotive systems, finance, health care, natural language processing, and malware detection. Of particular concern is the use of ML algorithms in cyber-physical systems (CPS), such as self-driving cars and aviation, where an adversary can cause serious consequences. However, existing approaches to generating adversarial examples and devising robust ML algorithms mostly ignore the semantics and context of the overall system containing the ML component. For example, in an autonomous vehicle using deep learning for perception, not every adversarial example for the neural network might lead to a harmful consequence. Moreover, one may want to prioritize the search for adversarial examples towards those that significantly modify the desired semantics of the overall system. Along the same lines, existing algorithms for constructing robust ML algorithms ignore the specification of the overall system. In this talk, we argue that the semantics and specification of the overall system has a crucial role to play in this line of research. We present preliminary research results that support this claim.

BIO

Somesh Jha received his B.Tech from Indian Institute of Technology, New Delhi in Electrical Engineering. He received his Ph.D. in Computer Science from Carnegie Mellon University in 1996 under the supervision of Prof. Edmund Clarke (a Turing award winner). Currently, Somesh Jha is the Lubar Professor in the Computer Sciences Department at the University of Wisconsin (Madison), which he joined in 2000. His work focuses on analysis of security protocols, survivability analysis, intrusion detection, formal methods for security, and analyzing malicious code. Recently, he has also worked on privacy-preserving protocols and adversarial ML. Somesh Jha has published over 150 articles in highly-refereed conferences and prominent journals. He has won numerous best-paper and distinguished-paper awards. Prof Jha also received the NSF career award. Prof. Jha is the fellow of the ACM and IEEE.

No cost to attend • Open to the public • Seating is on a first-come, first-served basis

For further information, please contact hbyrnes@ics.uci.edu or go to www.cs.uci.edu