ISTeC
The Information Science and Technology Center

COLORADO STATE UNIVERSITY

Distinguished Lectures
Spring 2019

Colorado State University's Information Science and Technology Center (ISTeC) presents two lectures by

Dr. Somesh Jha
Sheldon B. Lubar Professor
Computer Sciences Department
University of Wisconsin

ISTeC Distinguished Lecture

In conjunction with the Department of Computer Science and Department of Electrical and Computer Engineering Seminar Series

"Towards Semantic Adversarial Examples"

Monday, April 22, 2019
Reception with refreshments: 10:30 a.m.
Lecture: 11:00 a.m.-12:00 noon
Morgan Library Event Hall

Department of Computer Science and Department of Electrical and Computer Engineering Seminar Series Sponsored by ISTeC

"Balancing Security-Privacy and Functionality in Software Synthesis"

Tuesday, April 23, 2019
Lecture: 9:30-10:45 a.m.
Computer Science Bldg. Room 425

Abstracts

Towards Semantic Adversarial Examples

Fueled by massive amounts of data, models produced by machine-learning (ML) algorithms, especially deep neural networks, ar 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.

Balancing Security-Privacy and Functionality in Software Synthesis

The problem of implementing a secure program is an ideal problem domain for formal methods. In this talk, I will be using security as term that encompasses traditional security concepts and also privacy. Even a small error in the logic of a program can drastically weaken the security and privacy guarantees that it provides. Existing work on applying formal methods to security has focused primarily on applying verification techniques to determine if an existing program satisfies a desired security guarantee. However, the challenge is to synthesize correct software from the outset. However, the key issue here is to balance security and functionality (a secure software that does nothing is easy to synthesize. Just do nothing.)

In this work, I will describe some of the projects that I have worked on that balance the two competing requirements (i.e., security-privacy and functionality). I will then describe some interesting open problems along these lines.

Speaker Biography

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.

To arrange a meeting with the speaker, please contact Prof. Indrakshi Ray, Indrakshi.Ray@ColoState.EDU.

Upcoming Distinguished Lectures

April 29

Internet Beyond Packets: Network Neutrality, Rural Broadband, Spectrum and Access for People with Disabilities

11 a.m.-12 noon

Morgan Library Event Hall

Dr. Henning Schulzrinne

ISTeC (Information Science and Technology Center) is a university-wide organization for promoting, facilitating, and enhancing CSU's research, education, and outreach activities pertaining to the design and innovative application of computer, communication, and information systems. For more information please see ISTeC.ColoState.edu.