ISTeC

The Information Science and Technology Center

Colorado State University

Distinguished Lectures

Fall 2017

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

Dr. Patrick McDaniel

Distinguished Professor
Director, Institute for Network and Security Research
School of Electrical Engineering and Computer Science
The Pennsylvania State University

ISTeC Distinguished Lecture

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

"Tracing the Arc of Smartphone Application Security"

Monday, Oct. 16, 2017
Reception with refreshments: 10:30 a.m.
Lecture: 11:00 a.m.-12:00 noon
Morgan Library Event Hall

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

"The Limitations of Machine Learning in Adversarial Settings"

Monday, Oct. 16, 2017
Lecture: 2:00-3:00 p.m.
Computer Science Building 130

Abstracts

Tracing the Arc of Smartphone Application Security

The introduction of smart phones in the mid-2000s forever changed the way users interact with data and computation—and through it prompted a renaissance of digital innovation. Yet, at the same time, the architectures, applications and services that fostered this new reality fundamentally altered the relationship between users and security and privacy. In this talk I map the scientific community's evolving efforts over the last decade in evaluating smart phone application security and privacy. I consider several key scientific questions and explore the methods and tools used to answer them. Through this exposition, I show how our joint understanding of adversary and industry practices have matured over time, and briefly consider how these results have informed and shaped technical public policy in the United States. I conclude with a discussion of the open problems and opportunities in mobile device security and privacy.

The Limitations of Machine Learning in Adversarial Settings

Advances in machine learning have enabled to new applications and services to computationally process inputs in previously unthinkably complex environments. Autonomous cars, automated analytics, adaptive communication systems and self-aware software systems are now revolutionizing markets and blurring the lines between computer systems and real intelligence. In this talk, I consider whether the current use of machine learning in security-sensitive contexts is vulnerable to nonobvious and potentially dangerous manipulation. Here, we examine sensitivity in any application whose misuse might lead to harm—for instance, forcing adaptive network in an unstable state, crashing an autonomous vehicle or bypassing anadult content filter. I explore the use of machine learning in this area particularly in light of recent discoveries in the creation of adversarial samples, and posit on future attacks on machine learning. The talk is concluded with a discussion of the unavoidable vulnerabilities of systems built on probabilistic machine learning, and outline areas for defensive research in the future.

Speaker Biography

Patrick McDaniel is a Distinguished Professor in the School of Electrical Engineering and Computer Science at Pennsylvania State University, Fellow of the IEEE and ACM, and Director of the Institute for Networking and Security Research. Professor McDaniel is also the program manager and lead scientist for the Army Research Laboratory's Cyber-Security Collaborative Research Alliance. Patrick's research focuses on a wide range of topics in computer and network security and technical public policy. Prior to joining Penn State in 2004, he was a senior research staff member at AT&T Labs-Research.

To arrange a meeting with the speaker, please contact Prof. Dr. Indrakshi Ray (iray@cs.colostate.edu).

Upcoming Distinguished Lectures

Oct. 30

"Large-Scale Machine Learning and AI: A Cross-Industry Perspective"

11:00 a.m.-12:00 noon

Morgan Library Event Hall

Dr. Ashok Srivastava

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.