מכון ויצמן למדע

THE WEIZMANN INSTITUTE OF SCIENCE

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Computer Science Seminar

,The Wolfson Auditorium Building
on Thursday, Nov 01, 2018
at 11:30

Wolfson Auditorium

Adi Shamir
Weizmann Institute

Machine Learning in Security: Applications and Implications

Abstract:

In this talk I will survey the way machine learning research is affecting the field of security, and the way security research Is affecting the field of machine learning. After giving several examples of each type, I will discuss some of the latest developments In adversarial machine learning research, which are used by hackers to defeat security mechanisms based on regular machine learning techniques