THE UNIVERSITY OF CHICAGO
DEPARTMENT OF COMPUTER SCIENCE PRESENTS:

"COMPROMISING CYBER-RESILIENCE VIA SPATIAL & TEMPORAL DYNAMICS"

Thursday

October 24th

2:30 PM

JCL 298

PRATEEK MITTAL
Princeton University
Associate Professor, Department of EE
Associated Faculty, Department of CS

ABSTRACT

When reasoning about cyber-resilience, security analysts typically rely on simple abstractions of the system to make the analysis tractable. In this talk, I will highlight a key limitation of this approach: commonly used abstractions do not explicitly model the ability of an adversary to maliciously induce temporal or spatial changes in the system, which can then be used to compromise user security or privacy. I will illustrate this compromise of system security and privacy via two case studies of critical systems: public key infrastructure, and machine learning-based systems.