CPS: Breakthrough: Towards a Science of Attack Composition, Mitigation and Verification in Cyber Physical Systems: A Passivity Based Approach (CNS-1446866)
Principal Investigators: Radha Poovendran, Linda Bushnell
Network Security Lab, Department of Electrical Engineering
University of Washington, Seattle {rp3, lb2}@uw.edu

Need for Science of CPS Security
- CPS are inviting targets for intelligent, persistent attacks
- Composition of multiple attacks and development of mitigation strategies are open problems in cyber security
- Need to provide verifiable guarantees of CPS performance and security in the presence of cyber attacks

Scientific Questions Addressed
- How to model intelligent, persistent attacks and their impact on CPS?
- How to compose multiple attacks and develop efficient mitigation strategies against composed attacks?
- How to verify the mitigation strategies provide required performance, safety and security of CPS?

Our Passivity Based Approach
- Provides composition rules of multiple adversary models
- Enables identification of new attack primitives via decomposition of composed attacks
- Leads to seamless integration into dynamical models of CPS
- Adaptive incorporation of newly-discovered attacks into composed adversary mode
- Develop techniques for verification of passivity-based adversary models and mitigation via approximate bisimulation

Passivity Modeling of Individual Attacks and Mitigation
- Formulate passive dynamical models representing impact of attack on CPS
- Identify class of cyber-attacks that admit passive dynamical representation
- Model the time-varying mitigation strategy as passivity dynamical system
- Design mitigation strategy to guarantee security properties of CPS

Passivity-Based Composition of Adversary Models and Mitigation
- Compose attacks by non-colluding, colluding, and competing adversaries
- Compose attacks targeting distinct, interdependent CPS components
- Decompose a composed adversary model into attack primitives
- Develop efficient mitigation strategies against composed adversary model

Adaptive Patching Strategy Against Malware Propagation
Main idea:
Adaptively update the patching rate when an infection is detected

CoreMelt Attack
- Attacker sends high volume of data from compromised clients to compromised servers
- Overloads backbone Internet routers, resulting in denial of service for other network nodes

Passivity-Based Approach to CoreMelt
- Developed a Lyapunov-based framework for analyzing the adversary's attack strategy
- Characterized the optimal attack strategy for achieving a desired congestion level for the targeted link
- Proposed mitigation strategies for increasing the bandwidth allocated to legitimate users

References