



NC STATE UNIVERSITY Computer Science

# Research Challenges for Cyber Physical Systems Security

Peng Ning

## Cyber Physical Systems (CPS)

- What is a CPS?
  - A system of systems in which cyber components are embedded in, and work for/with, physical systems
  - Integration of computation and physical processes
- Examples
  - Intelligent power grids (Microgrid)
  - Process control systems
  - Defense systems
  - Smart highway

NC STATE UNIVERSITY Computer Science

2

## What Does Security Mean for CPS

- High-level security objective
  - A CPS should work as expected even when there are malicious attacks
- How about the classic security objectives
  - Confidentiality
    - Apply in certain applications (e.g., military)
  - Integrity
    - Necessary
  - Availability
    - Necessary, particularly in real-time CPS
- **But what do they exactly mean in CPS applications?**
  - Different applications have different interpretations
  - Need deeper understanding

## Research Challenges (1)

- Understand what security means for a CPS
  - Threat modeling
  - Understanding of application domains
    - Assumptions and constraints
- CPS applications are dynamic
  - Should be aware of, harness, and provide feedback to CPS R&D efforts
  - E.g., advanced power grid/microgrid

## Research Challenges (2)

- How to deal with real-time requirements in CPS under malicious attacks
  - Real-time is often a requirement in CPS to handle physical processes
  - We never know any general security mechanisms that can guarantee real-time requirements under attacks
  - Real-time community seldom considers malicious attacks
  - Beyond the traditional security and real-time research

## Research Challenges (3)

- How to handle the control loop in CPS
  - How to deal with malicious attacks that target the control loop?
  - Example:
    - Infrared-decoy target for missiles

## Research Challenges (4)

- How to guarantee availability in CPS
  - Cyber and physical components in a CPS may depend on each other
  - How to guarantee system availability?
  - We don't fully understand how to guarantee high availability for cyber systems yet
  - The integration with physical systems makes it more challenging

## Research Challenges (5)

- How to deal with the physical part in CPS
  - Physical attacks
    - Target the physical processes in a CPS
  - How to authenticate physical phenomenon
    - Security localization: don't know how to authenticate physical signals
  - Monitor of physical components
    - Better intrusion detection for physical components?
  - We have limited understanding
- Scalability
  - Some CPS could be large
    - Nation-wide power grids
  - Integration of many cyber and physical components makes it hard to guarantee security properties

## Research Challenges (6)

- How to deal with malicious attacks that target the concurrency aspects in CPS
  - CPS is concurrent in nature
    - Physical processes are intrinsically concurrent
    - Concurrently running cyber and physical processes
  - We are aware of this problem, but the current solutions seem insufficient
  - Example
    - Race condition: We are aware of this, but there are quite some attacks exploiting race condition vulnerabilities

## Research Challenges (7)

- How to provide isolation while keeping collaboration among cyber and physical components
  - Avoid cascading failures

## Research Challenges (8)

- Software security
  - Interconnection of individual computers brought tremendous risks to computer software
  - Does exposure to physical world bring more harms to software?
    - The problem exists in embedded systems
    - But the threats and risks are not well understood yet
  - Does complex interaction among CPS components bring more challenges to software?

- What else?
  
- Research agenda?