Collaborative Research: CPS: Medium: Timeliness vs. Trustworthiness: Balancing Predictability and Security in Time-Sensitive CPS Design

Thidapat (Tam) Chantem[†], Nathan Fisher[‡], Ning Zhang[*], Cong Liu[◇], and Ryan Gerdes[†]
[†]Virginia Tech, [‡]Wayne State University, [*]Washington University in St. Louis, [◇]U. of Texas at Dallas

Challenges

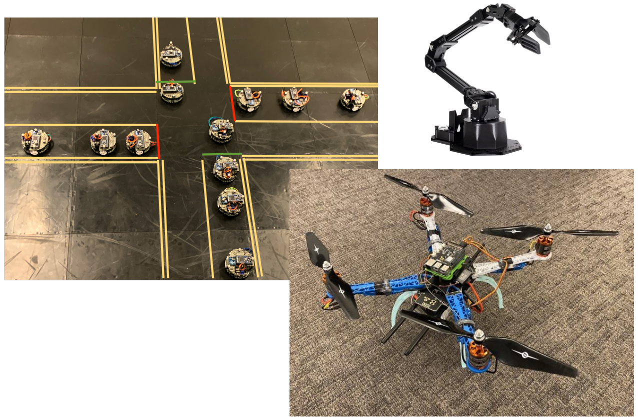
- The lack of a single system-level security metric to optimize for
- The difficulty in securing
  - The scheduling infrastructure
  - The real-time tasks
- Unknown/imprecise threat models at design time and/or unknown/unforeseen vulnerabilities

Solution

- Secure the fundamental real-time components from the ground up and to the extent possible on resource-constrained RT·CPS
- Quantify the cost of security and create a real-time scheduling/security co- design framework that determines, on-the-fly, when and how to use the secure real-time components and/or appropriate
- Enable incremental system recovery

Scientific Impact

- Enable secure RT·CPS that is
  - Less complex
  - Easier to analyze
  - Resilient in face of external and/or uncontrolled changes to the system and/or physical environment
- Proactively prevent attacks using moving target defense, as well as detect and recover from attacks that cannot be avoided.



Broader Impact on Society

- Research applicable to defense, medicine, transportation, manufacturing, agriculture domains, etc.
- Improved trust in automated systems by, and quality of life of, users

Broader Impact on Education and Outreach

- Course modules and red-teaming exercises for undergraduate students in all engineering disciplines
- Interactive learning modules and internship experience for K-12 students

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 2038726, 2038609, 2038995, 2038727