
Insup Lee (PI)
PRECISE Center
School of Engineering and Applied Science
University of Pennsylvania

Intel-NSF Project Meeting
Stanford University
July 12 & 13, 2018
Team Members

Insup Lee (PI, Penn)  Andreas Haeberlen (Penn)  Bill Hanson (UPHS)  Nadia Heninger (Penn)

Ross Koppel (Penn, Sociology)  Miroslav Pajic (Duke)  George Pappas (Penn)  Linh Phan (Penn)  Rita Powell (Penn)

Kang G. Shin (Michigan)  Oleg Sokolsky (Penn)  James Weimer (Penn)  Christopher Yoo (Penn, Law)
Outline

• Intro on CPS security
• What our team has done
• Lily’s Questions
Cyber-Physical Systems

We are heading towards (living in?) a sensor-driven world

need control systems capable of operating in malicious environments
Cyber-Physical Systems Security

Car hackers use laptop to control standard car
By Zoe Kleinman

National Security

Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing
By Greg Jaffe and Thomas Erdbrink, December 04, 2011
A secret U.S. surveillance drone that went missing last week in western Afghanistan appear have crashed in Iran, in what may be the first case of such an aircraft ending up in the hands of an adversary.

Obama Order Sped Up Wave of Cyberattacks Against Iran
By DAVID E. SANGER
Published: June 1, 2012
WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran’s main nuclear enrichment facilities, significantly expanding America’s first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program, accidentally

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Hackers Remotely Kill a Jeep on the Highway—With Me in It
Since Stuxnet, reports on cyber-physical attacks have multiplied. A history of publicly reported incidents illustrates a remarkable variety of motives and attack approaches in cyberspace with a direct impact in physical space. Public spending on security of critical national infrastructures against security threats has also increased globally and researchers have extended the breadth of potential targets by staging attacks against implantable medical devices, private cars, autonomous vehicles, building automation devices, and other cyber-physical systems. Causing physical damage or injury with a cyber attack is now seen as a reality, not merely a possibility.

Figure 2.3 shows a timeline of the publicly reported incidents that were discussed in this chapter. Notable incidents confirmed to have been the result of a cyber security breach, whether real-world ones or research experiments, are highlighted with a dark background.

— Siberian pipeline: June 1982:
  - Soviets stole control software from Canadian company.
  - US influence Canadian company to alter code such that pipeline pressures would build up.
  - Explosion could be seen from space.
CPS security incidents

Maroochi Shire sewage hacking, Spring 2000:

- Disgruntled employee hacked control system to release tons of raw sewage into the neighborhood
CPS security incidents

Since Stuxnet, reports on cyber-physical attacks have multiplied. A history of publicly reported incidents illustrates a remarkable variety of motives and attack approaches in cyberspace with a direct impact in physical space. Public spending on security of critical national infrastructures against security threats has also increased globally and researchers have extended the breadth of potential targets by staging attacks against implantable medical devices, private cars, autonomous vehicles, building automation devices, and other cyber-physical systems. Causing physical damage or injury with a cyber attack is now seen as a reality, not merely a possibility.

Figure 2.3 shows a timeline of the publicly reported incidents that were discussed in this chapter. Notable incidents confirmed to have been the result of a cyber security breach, whether real-world ones or research experiments, are highlighted with a dark background.

– Stuxnet: 2009:
  - Attack on Iranian nuclear facility
  - Used 4 undiscovered exploits targeting control
Since Stuxnet, reports on cyber-physical attacks have multiplied. A history of publicly reported incidents illustrates a remarkable variety of motives and attack approaches in cyberspace with a direct impact in physical space. Public spending on security of critical national infrastructures against security threats has also increased globally and researchers have extended the breadth of potential targets by staging attacks against implantable medical devices, private cars, autonomous vehicles, building automation devices, and other cyber-physical systems. Causing physical damage or injury with a cyber attack is now seen as a reality, not merely a possibility.

Figure 2.3 shows a timeline of the publicly reported incidents that were discussed in this chapter. Notable incidents confirmed to have been the result of a cyber security breach, whether real-world ones or research experiments, are highlighted with a dark background.

— US Drone captured: 2011:
  - Iran captured predator drone that landed in the wrong area.
  - GPS spoofing
  - “System” worked perfectly
    — sensor measurements were wrong
CPS security incidents

Since Stuxnet, reports on cyber-physical attacks have multiplied. A history of publicly reported incidents illustrates a remarkable variety of motives and attack approaches in cyberspace with a direct impact in physical space. Public spending on security of critical national infrastructures against security threats has also increased globally and researchers have extended the breadth of potential targets by staging attacks against implantable medical devices, private cars, autonomous vehicles, building automation devices, and other cyber-physical systems. Causing physical damage or injury with a cyber attack is now seen as a reality, not merely a possibility.

Figure 2.3 shows a timeline of the publicly reported incidents that were discussed in this chapter. Notable incidents confirmed to have been the result of a cyber security breach, whether real-world ones or research experiments, are highlighted with a dark background.

### IoT DDoS : October 21, 2016
- Thousands of devices overtaken using default passwords
- Organized into botnet to flood DNS provider
- Took down many major websites
  - $17 Billion cost to economy (0.1% of GDP)
CPS security incidents

Since Stuxnet, reports on cyber-physical attacks have multiplied. A history of publicly reported incidents illustrates a remarkable variety of motives and attack approaches in cyberspace with a direct impact in physical space. Public spending on security of critical national infrastructures against security threats has also increased globally and researchers have extended the breadth of potential targets by staging attacks against implantable medical devices, private cars, autonomous vehicles, building automation devices, and other cyber-physical systems. Causing physical damage or injury with a cyber attack is now seen as a reality, not merely a possibility.

Figure 2.3 shows a timeline of the publicly reported incidents that were discussed in this chapter. Notable incidents confirmed to have been the result of a cyber security breach, whether real-world ones or research experiments, are highlighted with a dark background.

Figure 2.3 Historical timeline of publicly reported cyber-physical security incidents. The upper half contains notable real-world incidents and the lower half contains notable research experiments. Confirmed cyber-physical attacks are highlighted with a dark background.

Common Vulnerabilities and Exposures (CVEs) (1988 – 2012)

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.
Typical CPS Architecture
Software as a Medical Device (SaMD)

- Medical device defined by software that interacts with existing FDA certified devices
- Benefits:
  - simplified pathway to certification
  - potential for formal safety guarantees
- Challenges:
  - tools to enable developers
    - lack of standardization makes development hard
  - IoMT infrastructure development
    - interfacing with devices
    - deployment hardware
    - real-time guarantees
    - EHR APIs

FDA release of clinical evaluation guidelines on Dec 8, 2017

Software as a Medical Device (SAMD): Clinical Evaluation

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 8, 2017.
The draft of this document was issued on October 14, 2016.
For questions about this document, contact the Office of the Center Director at 301-796-6900 or the Digital Health Program at digitalhealth@fda.hhs.gov.
Internet of Medical Things (IoMT)
What is CPS Security?

• A CPS attack whose goal is to (negatively) affect the interaction between a CPS and the physical world
  – Originates through any attack surface
    • cyber, physical, or any combination of cyber/physical

• CPS security concerns the development of technologies for defending against CPS attacks
  – e.g., discovering new vulnerabilities, techniques for detection/mitigation/recovery, ...
Cyber- vs. CPS security

• All cyber-security challenges are still there!
• New challenges
  – Larger attack surface
  – New kinds of attacks
  – Imperfect system models
• New opportunities
  – Laws of physics
  – Natural redundancy
  – Operational context
CPS Attack Surfaces

- **Cyber attack surfaces**
  - e.g., communication, networks, computers, databases, ...

- **Physical attack surfaces**
  - e.g., locks, casings, cables, ...

- **Environmental attack surfaces**
  - e.g., GPS signal, electro-magnetic interference, battery draining/cycling/heating, ...

- **Human attack surfaces**
  - e.g., phishing, bribing, blackmail, etc.
CPS Security Challenges

• Foundational Challenges
  – How to build an ideal resilient CPS?
  – Quantifying CPS attacks effectiveness
    • wide variability in metrics for CPS security
    • concerns depend on the CPS mission
  – System evolution
    • operate in many different physical environments
    • adapt to physical surroundings
  – Operating scenarios restrict defensive capabilities
    • patching and frequent updates, are not well suited for control systems
    • real-time availability provides a stricter operational environment than most traditional IT systems.
    • legacy systems may not be updated

• Social and Legal Challenges
  – What solutions will be accepted by practitioners?
  – Who/what is liable when such a system fails due to security and privacy attacks?
• Cyber physical systems are systems of components
  – Heterogeneous computation and interaction models
• Composition of components are about the *interactions* of systems
  – One of the Three Mile Island investigators
  – NRC Study “Software for Dependable Systems: Sufficient Evidence?”
• Posits that sufficiently complex systems can produce accidents without a simple cause due to interactive complexity and tight coupling
Unintended Feature Interactions

• A complex system exhibits complex interactions due to
  – Unexpected interferences that are not visible or not immediately comprehensible
  – Unfamiliar or unintended feedback loops
  – Limited isolation of failed components

• Examples of Security Vulnerabilities
  – Secure door lock and rollover
  – Meltdown/Spectra(?)
Improving CPS security

• Apply suitable best (cyber) security practices

• CPS can provide additional information
  – CPS architecture / physical-world interface
    • e.g., multiple sensors, actuators, controllers
  – Environmental context
    • e.g., operating conditions (rain/snow), geographic location
  – Physical constraints and guarantees
    • e.g., laws of physics, bounds on power, CPU speed, network bandwidth

• How to leverage additional information to improve CPS security?
Security and Privacy-Aware Cyber-Physical Systems

**Challenges:**
- How to build an ideal resilient CPS?
  - architecture, build blocks and capabilities, design requirements (technical, legal, social)
- What solutions will be accepted by practitioners?
- Who/what is liable when such a system fails due to security and privacy attacks?

**Solution:**
- Platform support for security
- Security-aware control design
- Differential privacy in CPS
- Privacy-related tradeoffs for CPS
- Human-in-the-loop security assurance

**Scientific Impact:**
- Foundational understanding
- Case studies from different CPS domains (transportation, medical) to ensure that results are generally applicable

**Broader Impact:**
- Safer and more trustworthy CPS and IoT systems
- Clarification of legal consequences
- Joint law/engineering workforce training
Two Complementary Approaches

• Robustness
  – Employ preventive measures
  – Tolerate small problems with acceptable loss of performance

• Detection and recovery
  – Attack/anomaly detection: redundant sensors, models, laws of physics, context
  – Recover: forward recovery/mitigation

• Complementary
  – Not every attack can be masked
  – Attacks can exceed system robustness
Overall technical approach

Task 1: Platform support for CPS security
- Timing Guarantees for Accountability
- Bounded-Time Recovery
- Secure Synchronous Provenance

Task 2: Security-Aware Control Design
- Robust Attack Detection and Identification
- Platform-Aware Attack-Resilient Control Systems
- Control-Aware Cryptography

Task 3: Working with sensitive data
- Homeomorphic encryption
- Differential Privacy in Distributed Systems
- Differential Privacy for Medical Data
- Security and Privacy Duality in Control of CPS

Task 4: CPS security assurance
- Human factors in CPS security assurance
- Policy-Aware Modeling of CPS
- Security Assurance Cases for CPS
Research Results Summary
Task 1. Platform Support

• Attack Detection using Sensor Fusion
  – Attack-resilient Sensor Fusion with Fault Models
  – Incorporate Context in Sensor Fusion

• Forensics: Diagnosing Timing Faults
  – Timing Provenance

• CPS Checkpointing and (Forward) Recovery

• Bounded-Time Recovery

• Vehicle Security and Data Collection

• Design and Implementation of Secure Platform for IoMT: OpenICE-lite and LogSafe
Task 2. Resilient Control Design

- Attack-resilient state estimation in the presence of noise
  - Formal robustness guarantees even for the computationally efficient convex-optimization based estimator
- Control-aware *intermittent* integrity enforcement
  - e.g., using Message Authentication Codes (MAC)
  - Physics-aware Intermittent Message Authentication for Secure Control
- Security-Aware Scheduling for CPS
- Secrecy in Wireless Control Systems
- Resilient Linear Classification: An Approach to Deal with Attacks on Training Data
Task 3. Preserving Privacy

• Preserving Privacy in CPS
• Approaches
  – Partially Homomorphic Encryption
  – Differential privacy
• Optimization and Control using Partially Homomorphic Encryption
• Control with secrecy against eavesdroppers
• Distributed Differential Privacy
  – Approach #1: Crypto (MPC, secret sharing)
  – Approach #2: Trusted hardware (SGX)
Task 4. Security and Safety Assurance

• Security-Aware Human-on-the-Loop Protocols

• Security in Healthcare
  – Perspective on Healthcare Security
  – Understanding Circumvention/Workarounds of Cyber-Security Authentication

• Legal View on MCPS liabilities and HIPAA Compliance

• Safety Assurance
  – Verification Challenge Problem based on Proposed Self-Driving Car Policy
Talks by Penn/Michigan/Duke Team

- Who Killed My Parked Car?, Kang Shin
- Security and Privacy-Aware Cyber-Physical Systems: Legal Considerations, Christopher Yoo
- Integrating Security in Resource Constrained CPS + demo on eBuggy (electric vehicle), Miroslav Pajic + Vuk Lesi
- CPS Checkpoint and Recovery, Fanxin Kong + Oleg Sokolsky
- Bounded-Time Recovery, Andreas Haeberlen + Brian Sandler
- Timing Provenance, Linh Phan
- Control with secrecy against eavesdroppers, Tasos Tsiamis + Konstantinos Gatsis
- Self-Driving Vehicle Verification Challenges/ Benchmark, Nima Roohi
Lily’s Questions

1. What have we achieved from the last 3 years against the original objective?
2. What are the most important things we discovered/learnt?
3. What surprised us, what new trends or changes emerged during the 3 years that we didn’t anticipate at the beginning but turns out to be important?
4. What research you think are important to continue (outside of this program) in the general theme of CPS security/privacy going forward?
5. What feedback you may have for Intel
Additional CPS Security Challenges

• Security in autonomous CPS
  – Data-driven CPS
  – Attacks on training data
  – Learning enabled components in safety-critical CPS
• Human-in-the-loop CPS
• How to retrofit legacy systems to be resilient to newly discovered attacks?
• Formal modeling and synthesis techniques for evaluating resiliency to attacks/vulnerabilities
• Systematic understanding of exploitable side channels/unexpected feature interaction
Acknowledgements

• Special thanks to
  – Lily Yang, Intel
  – Richard Chow, Intel
  – Alan Tatourian, Intel
  – Jesse Walker, retired from Intel
  – David Corman, NSF

• Funded by NSF CNS-1505799 and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy.
THANK YOU!

PRECISE

PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

http://precise.seas.upenn.edu