Security in transportation systems

Suhas Diggavi M. Srivastava P. Tabuada

Department of Elecrical Engineering
Laboratory for Information Theory and Systems (LICOS)
University of California, Los Angeles
Los Angeles, California
Email: suhas@ee.ucla.edu
URL: http://licos.ee.ucla.edu

January 24th 2014

Drivers for security needs

- Networked transportation systems.

Drivers for security needs

- Networked transportation systems.
- Automated transportation systems.

UCLA

Drivers for security needs

- Networked transportation systems.
- Automated transportation systems.
- Heterogeneous systems: co-existence with different traffic and human-operation.

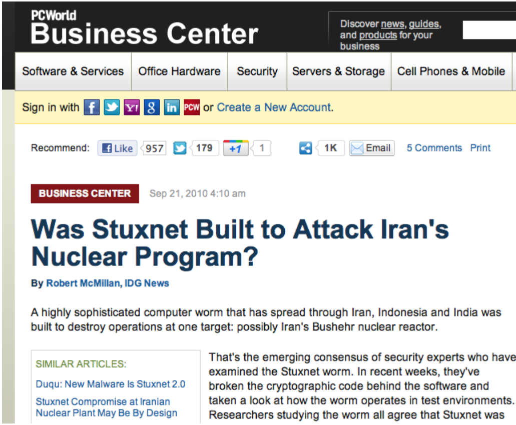
Drivers for security needs

- Networked transportation systems.
- Automated transportation systems.
- Heterogeneous systems: co-existence with different traffic and human-operation.

Implications: Creates multiple attack possibilities.

What makes CPS security different?

- Information security insufficient.



BUSINESS CENTER Sep 21, 2010 4:10 am

Was Stuxnet Built to Attack Iran's Nuclear Program?

By Robert McMillan, IDG News

A highly sophisticated computer worm that has spread through Iran, Indonesia and India was built to destroy operations at one target: possibly Iran's Bushehr nuclear reactor.

SIMILAR ARTICLES:

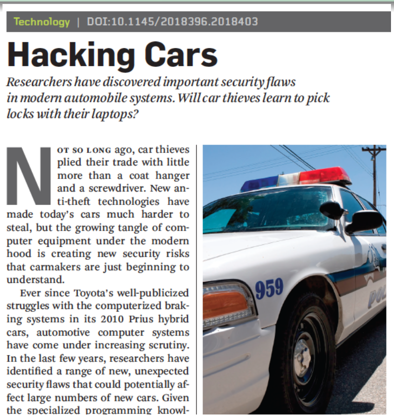
Duqu: New Malware Is Stuxnet 2.0

Stuxnet Compromise at Iranian Nuclear Plant May Be By Design

That's the emerging consensus of security experts who have examined the Stuxnet worm. In recent weeks, they've broken the cryptographic code behind the software and taken a look at how the worm operates in test environments. Researchers studying the worm all agree that Stuxnet was

What makes CPS security different?

- Information security insufficient.
- Exploit physical vulnerabilities.



Technology | DOI:10.1145/2018396.2018403

Hacking Cars

Researchers have discovered important security flaws in modern automobile systems. Will car thieves learn to pick locks with their laptops?

Not so long ago, car thieves plied their trade with little more than a coat hanger and a screwdriver. New anti-theft technologies have made today's cars much harder to steal, but the growing tangle of computer equipment under the modern hood is creating new security risks that carmakers are just beginning to understand.

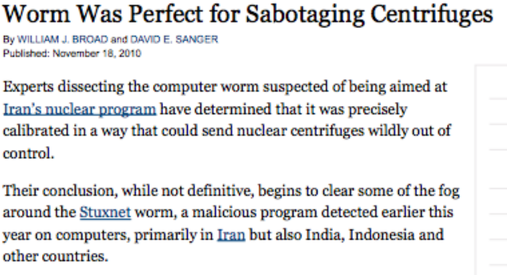
Ever since Toyota's well-publicized struggles with the computerized braking systems in its 2010 Prius hybrid cars, automotive computer systems have come under increasing scrutiny. In the last few years, researchers have identified a range of new, unexpected security flaws that could potentially affect large numbers of new cars. Given the specialized programming knowl-

What makes CPS security different?

- Information security insufficient.
- Exploit physical vulnerabilities.
- Real-time operation (latency important).

What makes CPS security different?

- Information security insufficient.
- Exploit physical vulnerabilities.
- Real-time operation (latency important).



Worm Was Perfect for Sabotaging Centrifuges

By WILLIAM J. BROAD and DAVID E. SANGER
Published: November 18, 2010

Experts dissecting the computer worm suspected of being aimed at Iran's nuclear program have determined that it was precisely calibrated in a way that could send nuclear centrifuges wildly out of control.

Their conclusion, while not definitive, begins to clear some of the fog around the Stuxnet worm, a malicious program detected earlier this year on computers, primarily in Iran but also India, Indonesia and other countries.

Attack vectors:

- Software/hardware attacks: implementation vulnerabilities.
- Communication attacks: Changing information bits, delays, impersonation etc.
- Physical attacks: Sensor/actuator attacks and spoofing.

Message: Vulnerability in both software/cyber and physical sides.

What is distinct about transportation CPS security?

- Humans-in-the-loop
  - Shared control.
  - Multiple time-scales.

UCLA

What is distinct about transportation CPS security?

- Humans-in-the-loop
  - Shared control.
  - Multiple time-scales.
- Heterogeneity of traffic.

What is distinct about transportation CPS security?

- Humans-in-the-loop
  - Shared control.
  - Multiple time-scales.
- Heterogeneity of traffic.
- Scale: lots of individual vehicles.

What is distinct about transportation CPS security?

- Humans-in-the-loop
  - Shared control.
  - Multiple time-scales.
- Heterogeneity of traffic.
- Scale: lots of individual vehicles.
- Social sensing: *e.g.,* crowdsourced traffic update.

What is distinct about transportation CPS security?

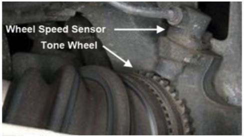
- Humans-in-the-loop
    - Shared control.
    - Multiple time-scales.
- Heterogeneity of traffic.
- Scale: lots of individual vehicles.
- Social sensing: *e.g.,* crowdsourced traffic update.

Message: Increased opportunities to attack.

Can we spoof sensors?

Fooling ABS sensors

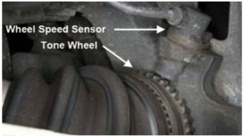
ABS sensor



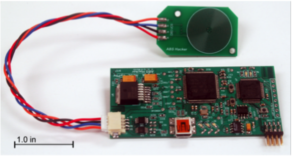
Can we spoof sensors?

Fooling ABS sensors

ABS sensor



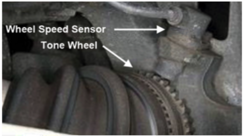
Spoofing device



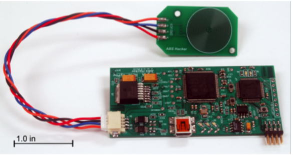
Can we spoof sensors?

Fooling ABS sensors

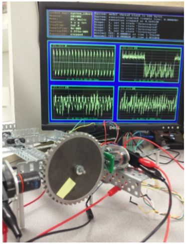
ABS sensor



Spoofing device



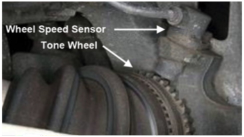
Spoofing ABS sensor



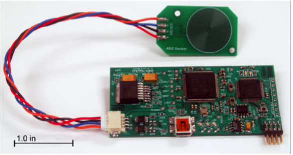
Can we spoof sensors?

Fooling ABS sensors

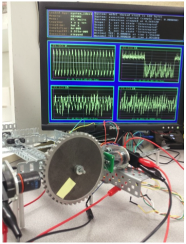
ABS sensor



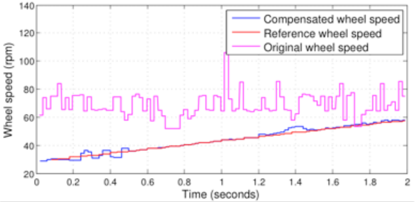
Spoofing device



Spoofing ABS sensor



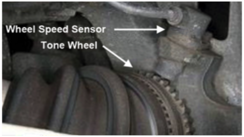
Result



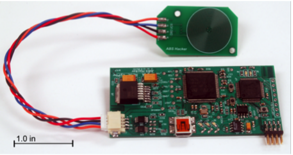
Can we spoof sensors?

Fooling ABS sensors

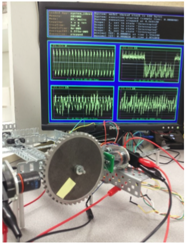
ABS sensor



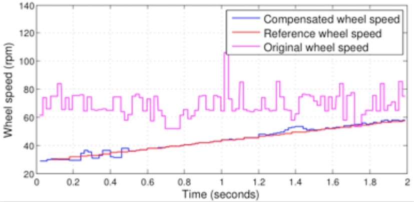
Spoofing device



Spoofing ABS sensor



Result



Implication: Cryptography cannot protect against (analog) sensed signal manipulation.

Shoukry etal CHES 2013.

Potential goals of attack

- Cause catastrophe.

Potential goals of attack

- Cause catastrophe.
- Change system behavior.

Potential goals of attack

- Cause catastrophe.
- Change system behavior.
- Move system to undesirable state.

Defense: Will depend on type of attack.

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.

Holistic approach

NSF CPS project "Foundations of secure CPS"

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.
- Distributed secure (private) control: no one has complete view.

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.
- Distributed secure (private) control: no one has complete view.
- Attack needs to be mounted in real time (before it being stale).

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.
- Distributed secure (private) control: no one has complete view.
- Attack needs to be mounted in real time (before it being stale).
- Use human-in-the-loop to aid security.

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.
- Distributed secure (private) control: no one has complete view.
- Attack needs to be mounted in real time (before it being stale).
- Use human-in-the-loop to aid security.

Project goal: To establish a systematic approach to security in cyber-physical systems and validate it.

Holistic approach

NSF CPS project “Foundations of secure CPS”

Idea: Secure CPS needs a holistic *cyber-physical* approach.

- Use physics with multiple sensing to create error-correction capability.
- Distributed secure (private) control: no one has complete view.
- Attack needs to be mounted in real time (before it being stale).
- Use human-in-the-loop to aid security.

Project goal: To establish a systematic approach to security in cyber-physical systems and validate it.

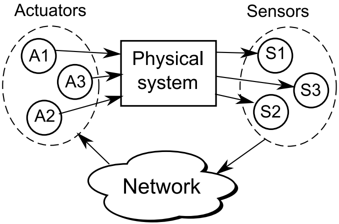
Illustrative idea: Use the redundancy inherent to physical system dynamics to provide “error-correction” capability.

Secure state estimation and control

Physical process modeled as a linear dynamical system:

$$x^{(t+1)} = Ax^{(t)} + Bu^{(t)}$$

$$\underbrace{y^{(t)}}_{\in\mathbb{R}^p} = Cx^{(t)}$$



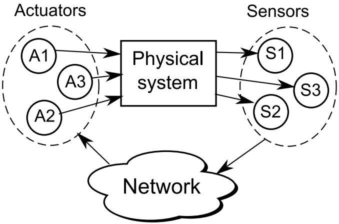
UCLA

Secure state estimation and control

Physical process modeled as a linear dynamical system:

$$x^{(t+1)} = Ax^{(t)} + Bu^{(t)}$$

$$\underbrace{y^{(t)}}_{\in\mathbb{R}^p} = Cx^{(t)} + \underbrace{e^{(t)}}_{\substack{\textit{attack}\\ \textit{vector}}}$$

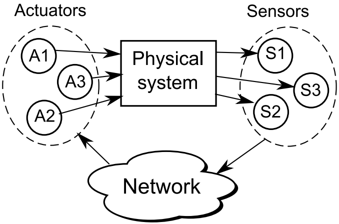


Secure state estimation and control

Physical process modeled as a linear dynamical system:

$$x^{(t+1)} = Ax^{(t)} + Bu^{(t)}$$

$$\underbrace{y^{(t)}}_{\in\mathbb{R}^p} = Cx^{(t)} + \underbrace{e^{(t)}}_{\text{attack vector}}$$



Results:

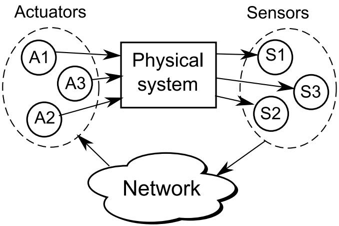
- If $q = \mathrm{supp}(e) < \frac{p}{2}$ then can estimate state (a.e. system) $\longrightarrow$ real error correction.
- Separation principle: with secure feedback can separate secure state estimation and control.
- Convex relaxation $\longrightarrow$ computationally efficient secure state estimation (compressed sensing).
- Can handle some actuator attacks.

Secure state estimation and control

Physical process modeled as a linear dynamical system:

$$x^{(t+1)} = Ax^{(t)} + Bu^{(t)}$$

$$\underbrace{y^{(t)}}_{\in\mathbb{R}^p} = Cx^{(t)} + \underbrace{e^{(t)}}_{\substack{\text{attack}\\ \text{vector}}}$$



Results:

- If $q = \mathrm{supp}(e) < \frac{p}{2}$ then can estimate state (a.e. system) $\longrightarrow$ real error correction.
- Separation principle: with secure feedback can separate secure state estimation and control.
- Convex relaxation $\longrightarrow$ computationally efficient secure state estimation (compressed sensing).
- Can handle some actuator attacks.

Bottomline: Using physical dynamical model we can defend against (some) sensor/actuator attacks.

Fawzi, Tabuada and Diggavi, Trans. Aut. Control.

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?
- What networked topologies are more resilient?

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?
- What networked topologies are more resilient?
- Limit extent of undefendable attacks?

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?
- What networked topologies are more resilient?
- Limit extent of undefendable attacks?
- Time-scales of automation versus human reaction time.

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?
- What networked topologies are more resilient?
- Limit extent of undefendable attacks?
- Time-scales of automation versus human reaction time.
- Utility/cost versus security.
- ...

Ideas and challenges

Idea: Physics (through models) gives opportunity to create CPS security.

Challenges:

- How to model complex transportation systems?
- How to model humans-in-the-loop?
- What networked topologies are more resilient?
- Limit extent of undefendable attacks?
- Time-scales of automation versus human reaction time.
- Utility/cost versus security.
- ...

New ideas needed: Mix of security, control, networking, error correction and human/social behavior.

Specific research directions

- **Modeling:** Critically used for security.

Specific research directions

- **Modeling:** Critically used for security.
  - How accurate should model be?
  - Can data-driven approach work? What guarantees?
  - Aggregates models better than individual? Useful at scale?

Specific research directions

- **Modeling:** Critically used for security.
  - How accurate should model be?
  - Can data-driven approach work? What guarantees?
  - Aggregates models better than individual? Useful at scale?
- **Shared control:**
  - When and how to use human control? Time-scales?
  - How to present choices for decision support? Training/adaptation?
  - How to localize damage?
  - Incentive mechanisms (*e.g.*, social sensing)?

Specific research directions

- **Modeling:** Critically used for security.
  - How accurate should model be?
  - Can data-driven approach work? What guarantees?
  - Aggregates models better than individual? Useful at scale?
- **Shared control:**
  - When and how to use human control? Time-scales?
  - How to present choices for decision support? Training/adaptation?
  - How to localize damage?
  - Incentive mechanisms (*e.g.*, social sensing)?
- **Secure networked control:**
  - Overlay monitoring system?
  - No single point of failure: no one with complete view.
  - Secure sensing/actuation (analog domain).
  - Offline design: added security around points of vulnerability.