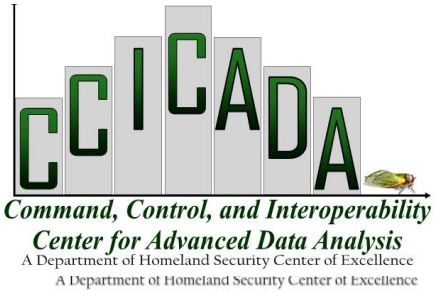
The Trend Toward Convergence of Physical and Logical (Cyber) Security

Fred S. Roberts
Director
Command, Control, and Interoperability Center
for Advanced Data Analysis (CCICADA)*
Rutgers University

*A Department of Homeland Security
University Center of Excellence



Super Bowl 47, New Orleans

- Was it terrorism?
- Was it cyber-terrorism?
- (Luckily just a relay device failing at Entergy Orleans)

Credit: businessinsider.com

A Department of Homeland Security Center of Excellence

Super Bowl 48, New Jersey

Credit:
new.mta.info

NJ State Police Regional Operations Intelligence Center assessment:

- ***Cyber attacks by "ideologically motivated and malicious" hackers, exploiting wireless systems, on stadium infrastructure or Super Bowl websites, is a serious possibility.***

A Department of Homeland Security Center of Excellence

CCICADA Project: Best Practices for Stadium Security & Analyses of Security Processes

Supported by DHS Office of SAFETY Act Implementation

Lambeau Field – Mike Roemer/AP

CCICADA

Command, Control, and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security Center of Excellence

It's not Just Sports Stadiums

- It's any places where large crowds gather
  - Airports
  - Train stations, bus terminals
  - Concert halls
  - Amusement parks
  - Political conventions

Port Authority Bus Terminal, NYC
Credit: nj1015.com

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

A Department of Homeland Security Center of Excellence

Cyber-physical Systems in Stadiums

- Access control systems
  - For patrons
  - For employees
- HVAC
- Communication systems
  - Electronic message boards
  - Public address systems
- Security cameras
- Elevators, escalators
- Lighting systems
- Power systems
- Traffic control in the parking lots

A Department of Homeland Security Center of Excellence

Cyber-physical Systems in Stadiums

- Recent report by CNBC (Nov. 2013) names five large sports stadiums running a particular industrial control system software with known vulnerabilities.
- Include Bryant-Denny Stadium (University of Alabama) and Marlins Park (home of the Miami Marlins baseball team)
- Vulnerabilities supposedly addressed.

Bryant-Denny Stadium
Credit: wikipedia.org

Cyber-physical Systems in Stadiums

- DHS has an Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Works directly with software manufacturers and potentially affected facilities
  - Develops and implement mitigation strategies as necessary

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

So Why So Many Vulnerabilities?

- Building management systems have many parties involved
  - Selling
  - Implementing
  - Maintaining
- Need systems for large, complex facilities
- CPS are of great complexity and are often engineered for environments not engineered from scratch (as in the power grid)
- Cyber security neglected
- Management doesn't want to pay for cyber security (security in general)
- Public/private communication needs improvement

Another Scenario: Car Hacking in the Stadium Parking Lot

- Car hacking: criminals remotely take control of your car
- Imagine the damage a hacker could do in a stadium parking lot.

Credit: ctvnews.ca

CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Another Scenario: Car Hacking in the Stadium Parking Lot

- Car hacking: criminals remotely take control of your car
- A serious challenge as in-car technology becomes more sophisticated
- Already thousands of semi-autonomous cars
  - In-car computer systems
  - Electronic control units
- Coming: fully autonomous cars
  - Self-driving cars

Credit: wikipedia.org

Another Scenario: Car Hacking in the Stadium Parking Lot

- 2013: Miller (Twitter) and Valasek (IOActive) demonstrated take control of Toyota Prius and Ford Escape from a laptop.
- They were able to remotely control:
  - Smart steering
  - Braking
  - Displays
  - Acceleration
  - Engines
  - Horns
  - Lights

Credit: npr.org

Why Vulnerabilities in Cars?

Baheti and Gill (2011):

- Vehicle control system depends on system components manufactured by different vendors
- Each vendor uses their own software and hardware
- Manufacturers like to develop components that will work for different kinds of vehicles (cheaper) – spreading the vulnerabilities
- Increasing complexity of components like sensors, actuators, wireless communication, multicore processors

Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Why Vulnerabilities in Cars?

Baheti and Gill (2011):

- Development of control system may be independent of system implementation
- Challenge of integrating various subsystems while keeping them functional
- Research missing on understanding interactions between vehicle control systems and other subsystems:
  - Engine, transmission, steering, wheel, brake, suspension

A Department of Homeland Security Center of Excellence

Important Issues in Security of Cyber-physical Systems

NSF CPS solicitation 2013:

- Develop the fundamental science needed to engineer systems of the complexity of cyber-physical systems that you can have high confidence in.
- Find ways to conceptualize and design for the deep interdependencies among engineered systems and the natural world

A Department of Homeland Security Center of Excellence

Important Issues in Security of Cyber-physical Systems

- Need methods of verification and validation
- How can you certify performance of such highly complex systems?
- Right now, overdesign may be only route to system certification

Credit: collegepals.org

A Department of Homeland Security Center of Excellence

Important Issues in Security of Cyber-physical Systems: Data

- Huge amounts of data available to describe CPS
- Challenge: Find ways to utilize data to enhance safety and security of CPS
- Data about state of the system can come to us so fast humans can't process it.
- Need tools for rapid system understanding.
- Need tools for rapid anomaly detection.