RUTGERS
School of Arts and Sciences

Rutgers College *Class of 1961* presents

Big Questions: Rutgers Faculty and Alumni in Conversation

Agenda

- Welcome - Tom Calamia; President, RC Class of 1961
- Moderator - Peter March, Executive Dean
- Speakers:
  - Rachel Somerville
  - David Greenberg
  - Fred S. Roberts
- Closing Remarks - Tom Calamia

RUTGERS
School of Arts and Sciences

Professor Rachel Somerville

George A. and Margaret M. Downsbrough Chair in Astrophysics

Distinguished Professor of Physics and Astronomy

2013 Dannie Heineman Prize in Astrophysics "for providing fundamental insights into galaxy formation and evolution using semi-analytic modeling, simulations and observations"

Big Question: What are black holes and what is their role in the formation and evolution of galaxies?

RUTGERS
School of Arts and Sciences

Professor David Greenberg

Associate Professor of History & Journalism and Media Studies

Author of "Republic of Spin: An Inside History of the American Presidency" (W. W. Norton 2016)

2008 Hiett Prize "to a single junior scholar in the humanities whose work has had a public influence"

Big Question: How will this presidential campaign be similar to or different from pas campaigns?

RUTGERS
School of Arts and Sciences

Fred S. Roberts

Distinguished Professor of Mathematics

Director; Command, Control and Interoperability Center for Advanced Data Analysis (DHS University Center of Excellence)

2013 Docteur Honoris Causa, University of Paris - Dauphine

Big Question: What Role are Data Mining and Computer Science Playing in Support of Homeland Security?

Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs

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

Image credits: wikipedia.org

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

RUTGERS
School of Arts and Sciences

CCICADA Center

- Founded 2009 as a ***Dept. of Homeland Security University Center of Excellence***
- Based at Rutgers - *Rutgers selected by DHS after nationwide competition for a data science center.*
- Today's decision makers in fields ranging from engineering to medicine to the maritime environment have available to them:
  - Remarkable new technologies
  - Huge amounts of information
  - Ability to share information at unprecedented speeds and quantities

Super Bowl 47, New Orleans

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

Credit: businessinsider.com

RUTGERS
School of Arts and Sciences

CCICADA & Stadium Security

- Numerous projects on patron inspection, employee credentialing, safety and security of infrastructure, etc.
- Working with all major sports leagues (MLB, NFL, NBA, NHL, MLS, etc.) + NCAA and minor leagues

Lambeau Field – Mike Roemer/AP

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

RUTGERS
School of Arts and Sciences

CCICADA & Stadium Security

- Workshop on Stadium Security
- Highpoint Solutions Stadium, Rutgers, Feb. 2013
- Panel on an Effective Security/Counter-terrorism Plan
  - Senior VP Security, NBA
  - Exec VP Security, NHL
  - Director Strategic Security Programs, NFL
  - Senior Manager Security, NASCAR
  - Director of Security, USTA
  - Director Security Operations, MLB
  - Safety & Security Consultant, MLS
  - Moderator: DHS Office of Infrastructure Protection

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

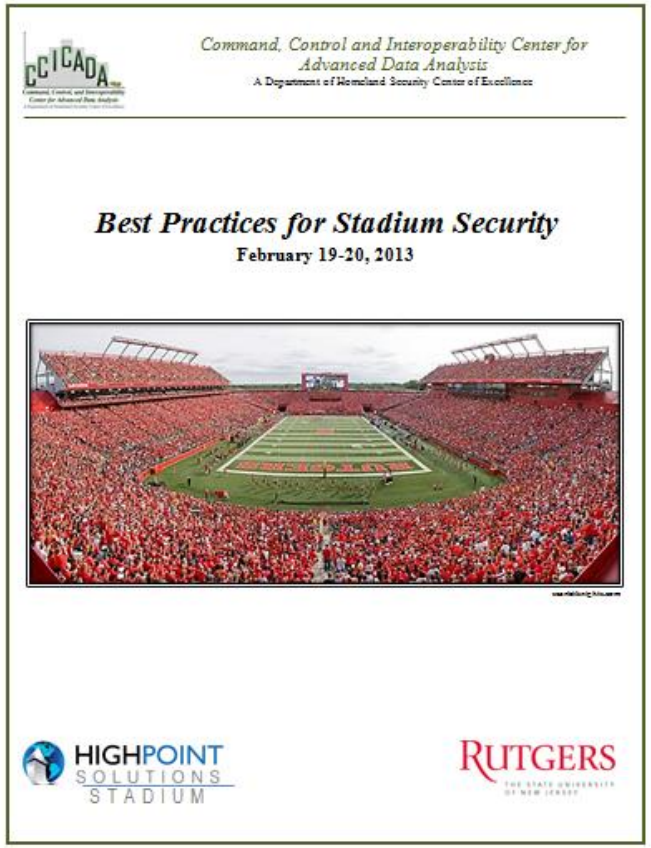
RUTGERS
School of Arts and Sciences

Best Practices for Stadium Security

CCICADA project supported by DHS Office of SAFETY Act Implementation (OSAI)

CCICADA's Best Practices for Stadium Security Resource Guide can be found on the OSAI website

Widely used by all major sports leagues

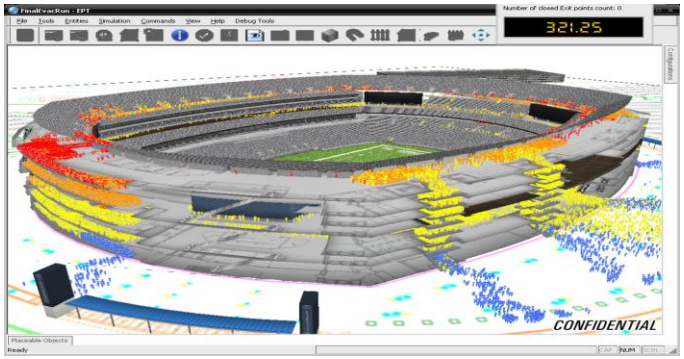


CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

RUTGERS
School of Arts and Sciences

Special Partnership: MetLife Stadium

- CCICADA's evacuation models helped MetLife during lightning storm just after it opened.
- CCICADA's "inspection simulator" helped MetLife determine how many walkthrough metal detectors to buy
- After Paris attacks, MetLife hosted CCICADA's "Conversation on Venue Security after Paris"



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
- CCICADA project at Port Authority Bus Terminal, NYC

Port Authority Bus Terminal, NYC
Credit: nj1015.com

A Department of Homeland Security Center of Excellence

Vulnerabilities of Cyber-Physical Systems

- Some of our nation's most important critical infrastructure is increasingly controlled by computer networks.
  - Power systems ("smart grid")
  - Transportation systems ("smart transportation")
  - Water supply systems
  - Air traffic control
  - Building control systems ("smart buildings")
- This infrastructure is potentially vulnerable to failures of computer systems or deliberate cyber attacks

Source: www.leesburgva.gov

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

Cyber-Physical Systems

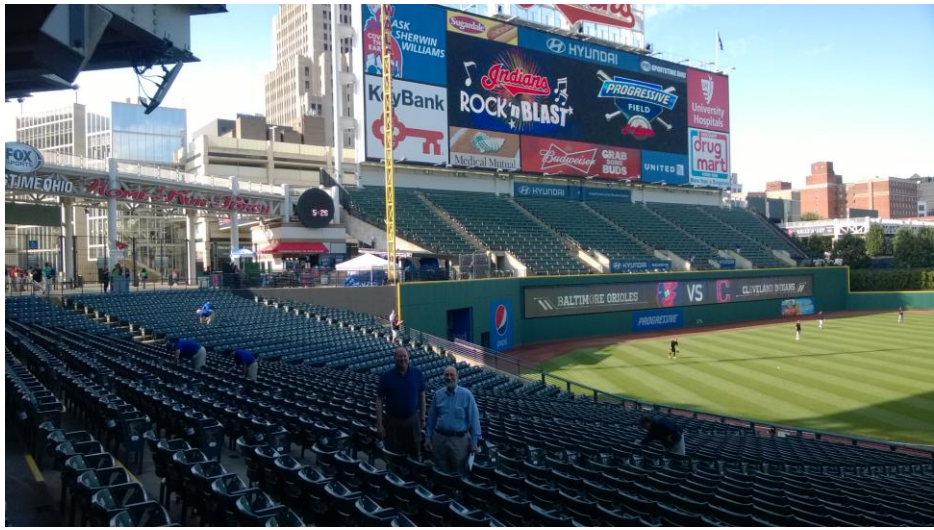
- ***Cyber-physical systems (CPS)***: Engineered systems that are built from and depend upon the synergy of computational and physical components.
- National Science Foundation (2013): "The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability."

A Department of Homeland Security Center of Excellence

RUTGERS
School of Arts and Sciences

Cyber-physical Systems in Stadiums

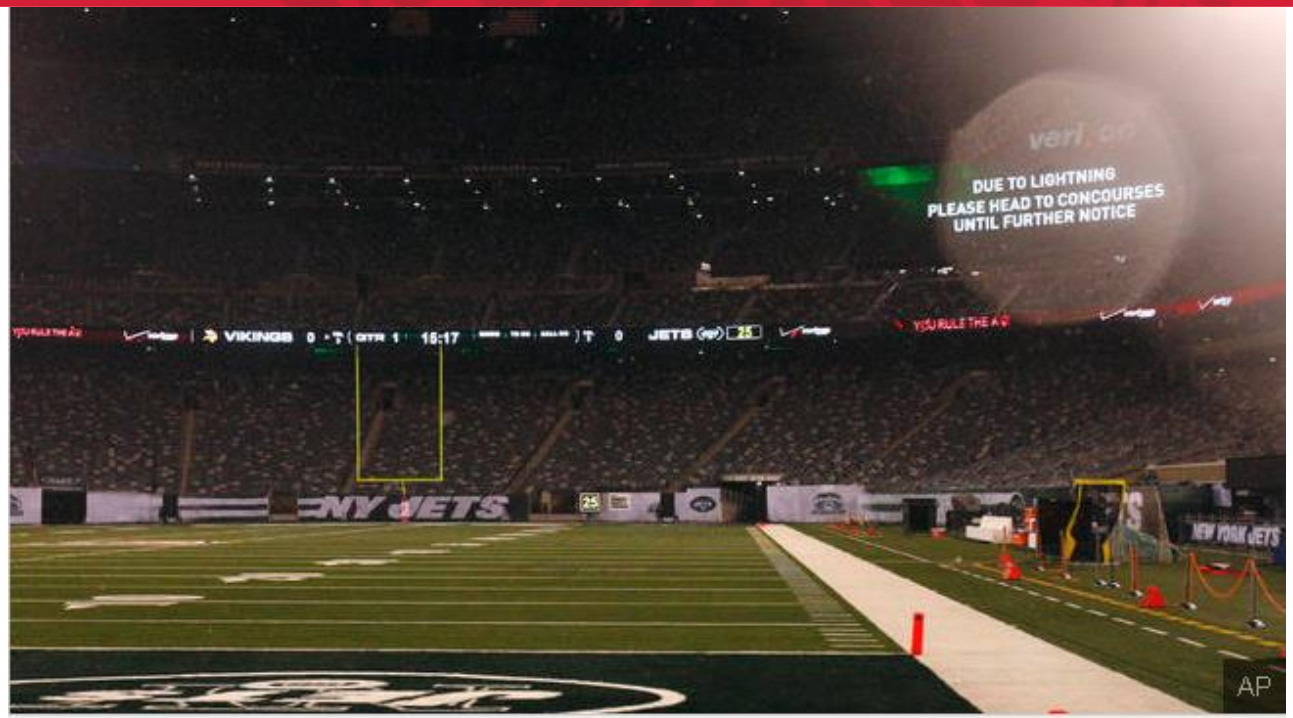
- Access control systems
  - For patrons
  - For employees
- HVAC
- Communication systems
  - Electronic message boards
  - Public address systems
- Security cameras
- Elevators, escalators
- Lighting systems
- Power systems
- Traffic control in the parking lots



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

Hacking into the Communications System

- This was a real emergency and a real message.
- But imagine what chaos a hacker could cause with a fake emergency message.



Stands are empty before an NFL football game between the Minnesota Vikings and the New York Jets on Monday, Oct. 11, 2010, in East Rutherford, N.J. The start of the game was delayed because of lightning and heavy rain; fans were cleared from the stands.

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

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

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

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

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?

- 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
- Challenge of integrating various subsystems while keeping them functional

Credit: Baheti and Gill (2011)

Hacking into a Ship

- Much less well known than cars: vulnerabilities in CPS of the maritime transportation system.
- A recent demonstration by a UT Austin team showed how a potential adversary could remotely take control of a vessel by manipulating its GPS.
- The yacht "White Rose of Drax" was successfully spoofed while sailing on the Mediterranean.
- The team's counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship's navigation system.
- "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line."

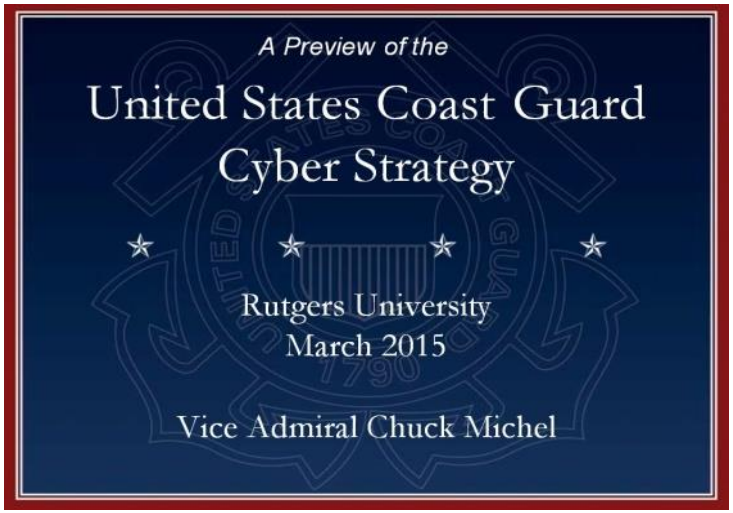
Source: UT Austin "Know"

Hacking into a Ship

- The maritime transportation system is critical to the world's economy.
- 95% of goods in international trade are still transported by sea.
- Disruption of global supply chain for commodities such as oil or food could cause dramatic problems for the world-wide economy.
- Disruption of the maritime transportation system could cause billions of dollars in damage to the economy.
- During January 2015, ports on US West Coast were closed due to a labor stoppage – with dramatic impact on the economy.

Maritime Cyber Security

- March 2-3, 2015: Rutgers organized the first-ever tutorial and symposium on Maritime Cyber Security
- Keynote by Vice Admiral Chuck Michel, US Coast Guard Deputy Commandant
- VADM Michel used the occasion to roll out the USCG's cyber security strategy.



CCICADA and USCG

- CCICADA works closely with the USCG
  - Fisheries law enforcement
  - Boat and aircraft placement and allocation – saved USCG $120M
  - Hoax calls
  - Oil spill response
  - Maritime risk
- In recognition of this, Admiral Paul Zukunft, Commandant of the USCG, visited Rutgers in October 2014.

CCICADA and USCG

- This has led to remarkable educational experiences for Rutgers students (and faculty).

RUTGERS
School of Arts and Sciences

CCICADA and USCG

RDC Project Spotlight

Maritime Cyber Security University Research

PROJECT BACKGROUND

In March 2015, the Rutgers University Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) DHS Center of Excellence hosted the Maritime Cyber Security Symposium for the US Coast Guard's key cyber challenges. VADM Chuck Michel issued six research challenges to Academia. In June 2015 the USCG released the Cyber Strategy, a document that identifies three distinct strategic priorities that are critical to the Coast Guard's overall mission success - defending cyberspace, enabling operations, and protecting infrastructure.

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
RUTGERS

Rutgers University Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA)

PROJECT TEAM

Research Chairman : Dr. Fred Roberts, Rutgers University Director of CCICADA

RDC Members: LTJG Shanda Harper, Dr. Joe DiRenzo, Judi Connelly

Acquisition Directorate
Research & Development Center

Rutgers-CCICADA has led the USCG-university research effort in maritime cyber security

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

RUTGERS
School of Arts and Sciences

Maritime Cyber: Modern Ship CPS

- For modern ships: dependence on a proliferation of sophisticated technology – that is subject to cyber attack
  - ECDIS (Electronic Chart Display and Information System)
  - AIS (Automatic Identification System)
  - Radar/ARPA (Radio Direction and Ranging) (Au
    Plotting Aid)
  - Compass (Gyro, Fluxgate, GPS and others)
  - Steering (Computerized Automatic
    Steering System)
  - VDR (Voyage Data Recorder –"Black Box")
  - GMDSS (Global Maritime Distress and Safety System)
  - Numerous other advanced units and systems

Thanks to Capt David Moskoff, US Merchant Marine Academy, for many of the following examples. Also thanks to Dana Goward and Joe DiRenzo.

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

Electronic Chart Display & Info System

- Electronic Chart Display & Information System (ECDIS):
  - Computer-based navigation system
  - Can be used as an alternative to paper navigation charts
  - Integrates a variety of real-time information
  - Automated decision aid - continuously determining ship's position in relation to land, charted objects, navigation aids and unseen hazards
  - Includes electronic navigational charts and integrates position information from the Global Positioning System (GPS) and other navigational sensors, such as radar, fathometer and automatic identification systems (AIS).
  - May also display additional navigation-related information, such as sailing directions.

RUTGERS
School of Arts and Sciences

Electronic Chart Display & Info System

- Electronic Chart Display and Information System enables solo watchstanding

Electronic Chart Display & Info System

- World's largest container ship: Triple E Maersk under construction
  - 18,000 containers
  - 400 meters long!
  - Crew size: Can operate with 13 crew members!!
    - ➢Thanks to ECDIS & other such systems.

Credit: http://www.worldslargestship.com/

Electronic Chart Display & Info System

- The Royal Caribbean's Allure of the Seas cruise ship, launched in 2010, is not far behind in size.
- 360 meters long
- Capacity of 6360 passengers

Credit: royalcaribbean.com/

Electronic Chart Display & Info System

- ECDIS flaws might allow attacker to access & modify files & charts on board or on shore; could cause serious environmental and financial damage, even loss of life.
- In Jan. 2014, the NCC Group tried to penetrate an ECDIS product from a major manufacturer.
- Several security weaknesses were found: ability to read, download, replace or delete any file stored on the machine hosting ECDIS, etc.
- Once such unauthorized access is obtained, attackers could be able to interact with the shipboard network and everything to which it is connected.
- Attack could be made through something as basic as insertion of USB key or download from Internet.

Sources: templarexecs.com 2014, CyberKeel 2014

Automatic Identification System

- Automatic Identification System (AIS) transceivers on over 400,000 ships (2013 estimate).
- Estimated that the number will soon reach a million.
- Installation is mandatory for all passenger ships and commercial (non-fishing) ships over 300 metric tons per International Maritime Union agreement.
- Tracks ships automatically by electronically exchanging data with other ships, AIS base stations, and satellites.

Source: Help Net Security

Credit: wikipedia.org

Automatic Identification System

- AIS enables ships to communicate with other ships, plot a course and follow it, and avoid collisions with other ships, reefs, floating objects, etc.
- An attacker with a $100 VHF radio could exploit weaknesses in Automatic Identification System which transmits data (e.g. vessels' identity, type, position, heading and speed to shore stations).
- The attacker could also tamper with the data, impersonate port authorities, communicate with the ship or effectively shut down communications between ships and with ports.

Source: templarexecs.com 2014,
Help Net Security net-security.org

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Plausible scenarios (CyberKeel 2014):
  - Modification of all ship details, position, course, cargo, speed, name
  - Creation of "ghost" vessels at any global location, which would be recognized by receivers as genuine vessels
  - Trigger a false collision warning alert, resulting in a course adjustment

Dr. Marco Balduzzi of Trend Micro discussing potential scenario
Credit: Help Net Security

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Plausible scenarios continued (CyberKeel 2014):
  - Send false weather information to a vessel to have them divert around a non-existent storm
  - The ability to impersonate marine authorities to trick the vessel crew into disabling their AIS transmitter, rendering them invisible to anyone but the attackers themselves
  - Cause vessels to increase the frequency with which they transmit AIS data, resulting in all vessels and marine authorities being flooded by data. Essentially a "denial-of-service attack"

Automatic Identification System

- Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they're somewhere else. (Reuters 4/23/14)

Credit: wikipedia.org

Oil Rigs

- Not just ships – ***vulnerabilities extend to the entire maritime transportation system.***
- Hackers recently shut down a floating oil rig off the coast of Africa by tilting it. It took a week to identify and fix the problem. (Reuters 4/23/14)
- In 2010: drilling rig being moved at sea from South Korea to South America was infected by malicious software so its critical control systems couldn't operate. Took 19 days to fix matters. (Reuters 4/23/14)
- Large cost: Oil rigs are contracted for at close to $1M a day.

Credit: www.peakoil.net

Oil Rigs

- In the Korean example: the computers controlling the blowout preventer were infected.
- If this had happened while the rig was engaged in drilling operations, there could have been a well blowout with possible explosion and oil spill.
- The blowout preventer failed during the Deepwater Horizon oil spill in the Gulf of Mexico in 2010.
- The malware involved might not have caused a problem for a smartphone, but that has much better security than an oil rig.

Credit: wikipedia.org, Shauk 2013

Cargo

- Cargo is also affected.
- Modern port operations are heavily dependent on complex, networked logistics
- Management systems track maritime cargo from overseas until it reaches a retailer
- Yet, these systems are subject to cyber attacks that can cause significant problems.

Credit: VADM Chuck Michel

Cargo

- Port of Antwerp is one of the world's biggest.
- 2011-2013: Hackers infiltrated computers connected to the Port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records.
- Attackers obtained remote access to the terminal systems; released containers to their own truckers without knowledge of the port or the shipping line.
- Access to port systems was used to delete information as to the existence of the container after the fact.

Source: Reuters 4/23/14, CyberKeel

Credit: wikipedia.org

Cargo

- The hackers began by emailing malware to the port authorities and/or shipping companies.
- After the infection was discovered and a firewall installed to prevent further infections, the criminals broke into the facility housing cargo-handling computers and fitted devices allowing wireless access to keystrokes and screen shots of computer screens.

Source: Bell 2013, Mulrenan 2014, Woodland Group

Cargo

- In 2012 it was revealed that crime syndicates had penetrated the cargo systems operated by the Australian Customs and Border protection.
- The penetration of the systems allowed the criminals to check whether their shipping containers were regarded as suspicious by the police or customs authorities.
- The consequence was that containers with contraband were abandoned whenever such attention was identified by the criminals.
- Others could be handled without worrying about the police.

Credit: commons.wikipedia.org

Source: CyberKeel

Cargo

- The FBI has advised private industry that GPS jammers are a common tool for cargo theft by organized crime.
- July 2014 FBI Advisory: report 46 instances of jammer use transporting stolen cars to China, and one instance of theft of a trailer of refrigerated pharmaceuticals.

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

Port Operations

- Today, ports rely as much on computer networks as on human stevedores.
- Networked logistics management systems track cargo from overseas until reaching a U.S. retailer.
- Networked control systems are also often involved in the loading and unloading of these goods.
- Modern gantry cranes and other systems use optical recognition and other technologies to locate, scan, and manage all facets of port terminal operations.
- Automated container terminal systems use GPS to facilitate the automatic placement and movement of containers.

Source: CDR Joe Kramek, Brookings Report 2013

Port Operations

- Trucks that haul cargo away from the port are also heavily dependent on GPS.
- This modern port operating system makes the entire port vulnerable.
- In 2014, to give just one example, two cranes at a major East Coast port in the US were idled for 76 hours when they were unable to received GPS signals.

Sources: CDR Joe Kramek, Brookings Report 2013, Resilient Navigation and Timing Foundation

Michael @ NW Lens via Flickr

Fred Roberts

Port Operations

- The entire port is vulnerable – from cargo handling to truck and crane movement.
- Easily available GPS jammers could close down a port at cost of more than $1B per day (more counting effect on GDP regionally and nationally).
- GPS jamming is possible with low cost jammers available over the Internet (though illegal).
- Many devices are battery-operated or can be plugged into a cigarette lighter and cost as little as $20.

RUTGERS
School of Arts and Sciences

Maritime Cyber Security: Research Continues

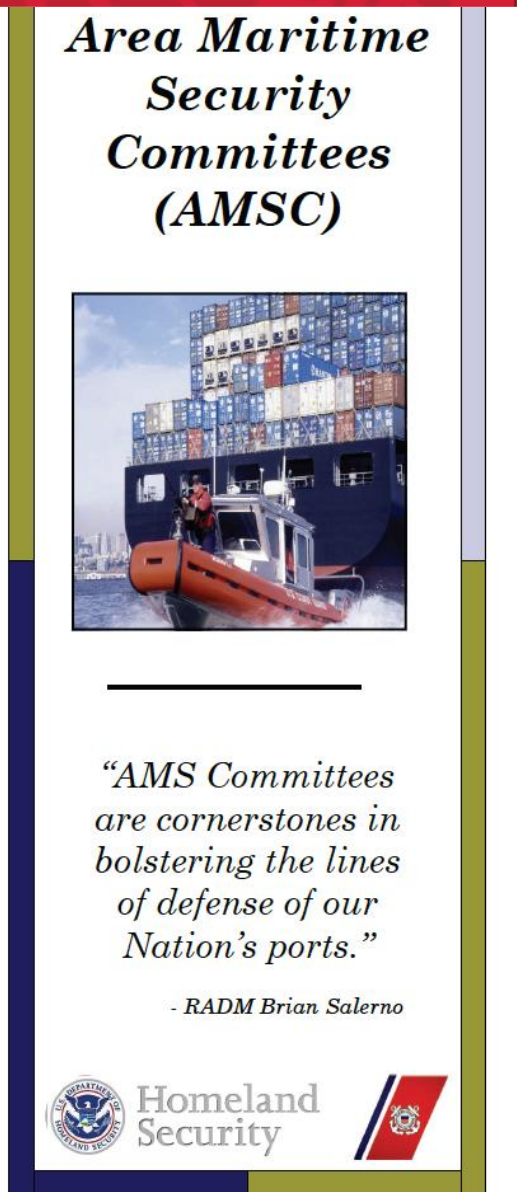
- Information sharing is key: but what are the incentives for sharing information?
  - In some domains (auto, aviation, financial services) there is a great deal of sharing
  - Maritime transportation system is harder
- How do we assess the cyber readiness of your company? Will you let us into your network to do it?
- What about coordinated cyber & physical attacks?
- What are the single points of failure in the maritime cyber system?
- What are the best ways to educate/train the workforce on proper cyber behavior – A CCICADA Report for DHS

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

RUTGERS
School of Arts and Sciences

Maritime Cyber Security: Research Continues

- CCICADA is pioneering in maritime cyber information sharing.
  - For example, through co-chairmanship of USCG Area Maritime Security Committee Cyber Security Subcommittee – Port of NY/NJ
  - Co-chaired with NYPD
  - Leading private sector firms involved:
    - American Express, Goldman Sachs
    - Maher Terminals
    - PSE&G, Con Edison
    - AT&T
    - Phillips 66
- Admiral Zukunft returning to NYC in May to learn about our efforts.



Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs

For More Information:

Dr. Fred Roberts
froberts@dimacs.rutgers.edu

CCICADA Center
www.ccicada.org

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