The Little-known Challenge of Maritime Cyber Security

Joseph DiRenzo, US Coast Guard

Dana Goward, Resilient Navigation and Timing Foundation

Fred S. Roberts, CCICADA Center, Rutgers University

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

Hacking into a Ship

- 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”

CCICADA

Command, Control, and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security Center of Excellence

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.

Modern Ship Cyber-Physical Systems

- 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) (Automatic Radar 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.

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 and 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.

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/

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

Electronic Chart Display & Info System

- ECDIS flaws might would allow an attacker to access and modify files and 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, share positional data, 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

Attack 3: CPA Alerting [1/2]

- Fake a CPA alert (Closest Point of Approach) and trigger a collision warning alert.

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

Automatic Identification System

- How it could work: “Frequency Hopping Attack” (Balduzzi & Pasta)
  - Every vessel is tuned in on a range of frequencies where they can interact with port authorities, as well as other vessels.
  - There is a specific set of instructions that only port authorities can issue that make the vessel's automatic information system transponder work on a specific frequency.
  - A malicious attacker can spoof this type of "command" and practically switch the target's frequency to another one which will be blank. This will cause the vessel to stop transmitting and receiving messages on the right frequency, effectively making it "disappear" and unable to communicate.
- How it could work: Timing Attack (Replay Attack):
  - Attacker spoofs command to delay transmission time and repeat this over and over
  - Effectively causes vessel to disappear.

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Why? (CyberKeel 2014):
  - The key problem with AIS is that it has no built-in security. All information is automatically assumed as being genuine and hence treated as correct piece of information.
  - Additionally, AIS messages are not encrypted and therefore very easy for outsiders to tap into and manipulate.

Automatic Identification System

- Potential Countermeasures to AIS Vulnerability:
  - Addition of authentication in order to ensure that the transmitter is the owner of the vessel
  - Creating a way to check AIS messages for tampering
  - Making it impossible to enact replay attacks by adding time checking
  - Adding a validity check for the data contained in the messages (e.g. geographical information)

Source: Help Net Security

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

GPS Jamming

- GPS Jamming can wreak havoc with modern ships.
- This was demonstrated by the attack on the White Rose of Drax.
- Civil GNSS (global navigation satellite systems) in use are much more vulnerable to attack than military GPS.
- Such systems are unencrypted and unathenticated.
- Loran-C had been a widespread backup to GNSS but was "abandoned" in the US in 2010.

Source: Bhatti and Humphreys

GPS Jamming

- In 2008, the UK & Irish General Lighthouse Authority directed GPS jamming equipment at a specific patch of ocean to demonstrate the effect of jamming.
- When the MN Pole Star entered the jamming zone, a range of services failed: the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system.
- ECDIS was not updated due to GPS failure, so the screen remained static.

Source: CyberKeel 2014

GPS Jamming

- In this case, because the crew was expecting this, it was able to cope with multiple alarms as they had been expecting this.
- However, on a modern vessel the bridge might in some cases be single-manned at night, causing significant problems should such a situation occur – imagine this if it were the Emma Maersk.
- A similar problem could arise if jamming attack took place during a highly complex maneuver requiring high concentration, such as docking under very low visibility.

Source: CyberKeel 2014; Grant, Williams, Ward, Basker

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

GPS Jamming

- 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.

Credit: CAPT David Moskoff

GPS Jamming

- One goal of the UK and Irish General Lighthouse Authority study: Investigate effectiveness of alternative sources of position, navigation, and timing for ships that are complementary to GPS.
- Especially important in light of the decision to not maintain formal support of Loran-C in the US.
- Enhanced Loran (eLoran) has different failure modes than GPS, so could serve as backup.
- This was demonstrated in this study.
- Justifies effort to introduce eLoran in the UK.

Source: Grant, Williams, Ward, Basker

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)

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

Oil Rigs

- The system that keeps an oil rig in position also has vulnerabilities.
- Dynamic positioning (DP) is a computer-controlled system to automatically maintain the position (and heading) of a vessel, in particular an oil rig.
- In DP, knowledge of the oil rig’s position and angle, sensor information, wind direction, and speed feed into a computer program that contributes to the oil rig’s stability.
- Disabling the DP of an oil rig by jamming its GPS could conceivably have a serious effect on the rig.
- In addition to safety and environmental impacts, large cost: Oil rigs are contracted for at close to $1M a day.

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: CyberKeel

Credit: commons.wikipedia.org

Cargo

- The Iranian shipping line IRISL suffered from a successful cyber attack in 2011.
- The attacks damaged all the data related to rates, loading, cargo number, date and place.
- This meant that no one knew where containers were, whether they had been loaded or not, which boxes were onboard the ships or onshore.
- Even though the data was eventually recovered, it led to significant disruptions in operations and resulted in sending cargo to wrong destinations causing severe financial losses.
- Additionally, a considerable amount of cargo was lost.

Credit: CyberKeel

Cargo

- In the US, 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 in transporting stolen cars to China, and one instance of theft of a trailer of refrigerated pharmaceuticals.

Port Operations

- Today, ports rely as much on computer networks as on human stevedores.
- Complex networked logistics management systems track maritime cargo from overseas until reaching a 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

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

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. (source: Resilient Navigation and Timing Foundation)

Source: CDR Joe Kramek, Brookings Report 2013

Port Operations

- The entire port is vulnerable – from cargo handling to truck and crane movement.
- Easily available jammers could close down a port at cost of more than $1B per day (more counting effect on GDP regionally and nationally).

Maritime Cyber Security

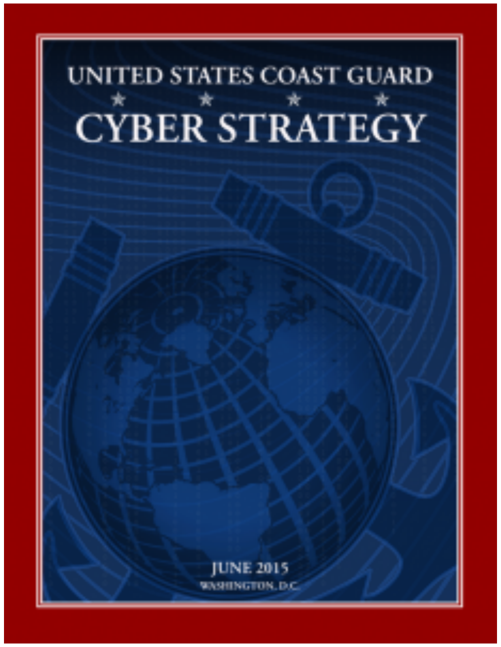
- The cyber threats to the maritime domain are serious.
- These threats not well known.
- In November 2011, the European Network and Information Security Agency (ENISA) reported that, “[t]he awareness on cybersecurity needs in the maritime sector is currently low to non-existent.”
- ENISA recommends:
  - maritime cyber security awareness training, cyber security training of shipping companies, port authorities, and national cyber security offices.
  - Updating regulations/policies from emphasis on physical security to cyber aspects

Maritime Cyber Security

- 2013 Brookings Report found that of the six ports studied, only one had conducted a cyber security vulnerability assessment and not a single one had a cyber incident response plan
- 2014 US General Accounting Office (GAO) report found that Dept. of Homeland Security needs to better address maritime cyber security (in particular port cyber security)
- GAO recommended that:
  - US Coast Guard assess cyber-related risks & use the assessment to inform maritime security guidance;
  - Federal Emergency Management Agency use the cyber risk assessment to inform its grant guidance

Maritime Cyber Security

- June 2015: US Coast Guard officially unveiled its Cyber Security Strategy.
- Previous emphasis was on prevention, response to, and recovery from physical attacks.
- First emphasis on prevention, response to, and recovery from cyber attacks.



UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

Maritime Cyber Security

- Is the maritime transportation system “special” in its cyber threats?
- In some ways, e.g.:
  - Dependence on long range communications systems due to distance from land, dependence on specialized instruments for position, navigation, and timing.
- But mostly the issues involve lack of awareness by management, lack of information about attacks and vulnerabilities, emphasis on physical security, lack of cyber security training of personnel – similar to many other sectors.
- The industry can and should learn from other industries.
- We need to spread awareness of the maritime cyber threat.

Research Issues in Security of Cyber-Physical Systems

US National Science Foundation 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.

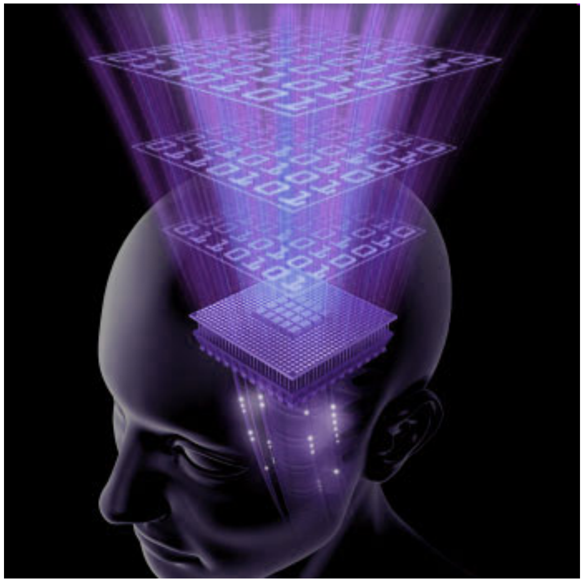
Research Issues in Security of Cyber-Physical Systems

- 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

Research 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.



Specific Research Issues for Maritime Cyber Security

- Understand the possibilities for eLoran as a promising solution to problems arising from GPS jamming
- Explore methods of proper authentication and validation as part of the solution to problems arising from vulnerability of Automatic Identification Systems
- What are some incentives for players in the Maritime Transportation System to share information about cyber threats and attacks and responses?

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

Specific Research Issues for Maritime Cyber Security

- Develop notions of cyber vulnerability in the maritime context and tools for assessing cyber vulnerability
- Find ways to estimate the probability of different types of cyber attacks on the Maritime Transportation System and the risk reduction of different counter-measures
- Find ways to estimate the cascading costs of a successful cyber attack on a component of the Maritime Transportation System

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

The Little-known Challenge of Maritime Cyber Security

For More Information:

Fred Roberts
froberts@dimacs.rutgers.edu

CCICADA Center
www.ccicada.org

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