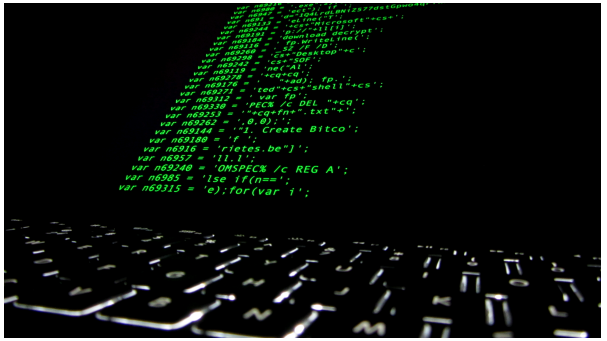
Combined Cyber and Physical Attacks on the Maritime Transportation System

Fred S. Roberts

Director

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



Source for all images: wikimedia commons

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

Combined Cyber and Physical Attacks

- A great deal of discussion about physical security in the maritime transportation system (MTS).
  - Leads to standards, regulations, etc.
- Increasing interest in cyber security in the MTS.
  - Leading to discussion of best practices.
- ***But more sophisticated attacks will be multi-modal.***
- Could lead to more harm.
- Simple example: hacking into security cameras at a port increases vulnerability to a physical intrusion.
- Special case: cyber attack as precursor to physical attack, or vice versa.
- Will present scenarios and discuss their likelihood.

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

Combined Cyber and Physical Attacks

- Our examples derive from input from a variety of subject matter experts (SMEs):
  - CAPT Michael Dickey, USCG
  - Mark Dubina, Port of Tampa Bay
  - Casey Hehr, Port of Long Beach (USCG – ret)
  - CAPT David Moskoff, SUNY Maritime
  - VADM Rob Parker, USCG-ret
  - Randy Parsons, Port of Long Beach
  - Daniel Searforce, Pennsylvania Public Utilities Commission
  - Drew Schneider, Port of Long Beach
  - CAPT Andrew Tucci, USCG-ret
  - CDR Nick Wong, USCG
  - Michael Young, TSA and Secret Service – ret

A Simple Example: Fake News

- Fake news could be spread via social media.
- Something is happening at Pier F in the port.
- Draws first responders to Pier F.
- Actual intent is to attack Pier L, which now may have less protection.
- Another version: hack into a company's or agency's email system and generate an official-looking report about Pier F.

Tina Jones
@tinajones
People shot at Pier F
2:22 PM 6 Dec 2017

John Smith
@johnsmith
There is a shooter at Pier F
2:23 PM 6 Dec 2017

A Simple Example: Fake News

- Another version: Spread news that a celebrity is at Pier F; draw a crowd; then attack the crowd.
  - "Justin Bieber is at Pier F"

Source: wikimedia commons

More Sophisticated Attacks on a Port

- Cyber attack on operating systems in the port making a following physical attack more likely to succeed:
  - **Shut the gates** so people are trapped inside and first responders are trapped outside.
  - **Turn off the lights** – make it easier for physical attackers.
  - **Turn off the alarms** – make it easier for physical attackers to avoid detection.
  - **Disable the cameras** – make it easier to avoid detection.
  - **Interrupt the power supply**.
  - **Disable cyber-enabled traffic lights** to create traffic jams - emergency vehicles unable to respond to a physical attack.
  - **Hack into emergency communication system** and tell first responders to go to a different place.
  - **Spoof TWIC cards or other access control systems** to let the "bad guys' in.

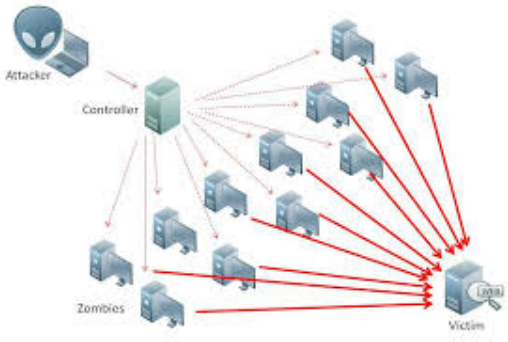
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

More Sophisticated Attacks on a Port

- Many of these seem feasible.
- But an adversary with this level of sophistication might find it is easier to do a more intrusive physical break-in.
- *Likelihood of a given scenario needs to be taken into consideration.*
- *More generally, consider threat, vulnerability, and consequence in determining the risk of a given attack scenario.*
- *There are virtually no useful tools for quantitative risk assessment for combined attacks.*
- Not surprisingly, the SMEs we talked to didn't always agree as to likelihood or risk.

More Sophisticated Attacks on a Port

- Disabling cameras may have a high level of risk because they are often add-ons.
- Hacking into the emergency communications system depends upon how it is configured.
  - If connected to the Internet, certainly possible.
  - Jamming communications might be easier.
  - One SME felt that port security would quickly determine that this was a hack and limit first responders going to the wrong place.
- A Denial of Service Attack could turn off the lights or the alarms.
- A cyber attack on the power supply could have significant consequences since many terminal operations do not have backup generators.



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

Credit for both images: commons.wikimedia.org

Port Security can Create Vulnerabilities

- Large sports and entertainment venues use walkthrough metal detectors or other systems to screen patrons
- The long lines waiting to be screened create vulnerabilities.
  - After the Boston Marathon attacks, sports stadiums sought to minimize vulnerabilities by creating an outer perimeter with initial screening.

Lambeau Field –
Mike Roemer/AP

Port Security can Create Vulnerabilities

- At a cruise ship terminal with many ships leaving at roughly the same time, lines form outside the building.
  - Passengers are initially vetted to see if they have a valid ID and are at the right terminal. An attacker should not get past the screener.
  - Unless they bought a cheap ticket …

Credit : commons.wikimedia.org

Port Security can Create Vulnerabilities

- The 2017 attack at the Ariana Grande concert in the Manchester Arena showed that patrons leaving an arena could be vulnerable.
  - What if they were "drawn out" in a group by hacking into the arena's emergency communication system or "message board"?
- In general, debarking at cruise ship terminals does not have as many vulnerabilities as embarking.
  - Passengers are released in groups to avoid standing in line at customs.
  - There is good departing security.
  - Operators think you are ok once you leave the dock.
  - *But what if a hacker could manipulate an alarm system to get them all to debark at the same time?*
  - There is still an under-appreciation of debarking vulnerabilities.

Manchester arena after attack
Credit: en.wikipedia.org BBC picture

Port Security can Create Vulnerabilities

- Could a hacker manipulate an alarm system (e.g., fire alarm) and perhaps a communication system to get passengers to debark at the same time?
- That might depend upon whether the alarm system and communication system were online.
- Port fire alarm systems are not too sophisticated
  - They are designed to operate over a network and push a signal out to a monitoring agency.
  - It might be a challenging hack to get into this system.
- Physically setting off the fire alarm might be more likely to succeed.

Autonomous Vehicles in Ports

- Terror attacks using vehicles on the rise:
  - Berlin, Nice, London, New York
- The lines of passengers lining up to embark on cruise ships could be vulnerable to this type of attack.
- But terrorists ended up dying in the process.
- What if they could control a vehicle remotely and not risk dying?
- Semi-autonomous cars are already here.
- 2013: Miller (Twitter) and Valasek (IOActive) demonstrated take control of Toyota Prius and Ford Escape from a laptop.

Christmas Market Vehicle Attack, Berlin, Dec. 2016
Credit: wikipedia.org

Autonomous Vehicles in Ports

- Already, many ports are operating with autonomous vehicles.
- At the Long Beach container terminal:
  - Gantry crane operator brings container to truck.
  - Computer lowers container to autonomous truck.
  - Truck takes it to storage area or non-autonomous truck.
  - Autonomous trucks even monitor their battery life and drive themselves to charging station for a recharge – operated by a robot.

Credit: Wikimedia commons

Credit: Daimler

Autonomous Vehicles in Ports

- The Hampton Roads container terminal is completely automated, robotic, and intermodal (rails, cars, trucks).
- Cranes are run from an office.
- All vehicles are autonomous.

Source: virginiaplaces.org

Autonomous Vehicles in Ports

- Could an autonomous truck be used as a weapon in a port scenario?
- Technically possible. An adversary could use low-cost jammers to jam the GPS that makes the autonomous vehicle work.
- 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

Autonomous Vehicles in Ports

- The hacking might seem harder to do than hijacking a truck and driving it into the port to create havoc.
- Also, where autonomous trucks operate in a port, they are blocked from people, so would more likely damage infrastructure.
- This suggests risk of this scenario is not so high.
- But automated vehicles in ports create other problems: could a "bad guy" hack into the control system and arrange to put the "wrong" box on the wrong train, or take it to the storage facility and open it?

Credit: commons.wikimedia.org

LNG Ships

- Gigantic LNG ships enter directly into the city of Boston to dock at the LNG terminals in Boston Harbor.
  - One of the few ports in the world (and only one in US) where this happens.
- Could a cyber attack on an LNG ship cause it to careen off course and create an explosion?
- Not likely – there are tugs on it and and Coast Guard keeps other vessels away.

Credit: commons.wikimedia.org

LNG Ships

- However, once the ship is in the terminal, if an adversary could access its industrial control systems, they could cause a serious problem.
- There are pumps, valves, etc. (operational technology – OT) run by software/computers (IT systems).
- Hacking into those systems could conceivably lead to an explosion in light of the hazards from LNG.
- How likely is this scenario?
- At least one of our sources had this as his nightmare scenario.

Credit: en.wikipedia.org

LNG Ships

- Maybe this isn't so far-fetched.
- The Stuxnet is a malicious computer worm that targets industrial computer systems.
- It put a virus into a controller running centrifuges and damaged them – causing substantial damage to Iran's nuclear program.
- Similarly, an adversary could hack into a sensor system, e.g., affecting tank level indicators, pressure sensors, temperature sensors, hazardous gas sensors.
- A leak or build-up of pressure or a fire might not be detected, thus possibly leading to an explosion.

What about Vessels?

- Today's vessels are highly dependent on cyber-physical systems
- Example: Electronic Chart Display & Information System (ECDIS).
- ECDIS flaws might allow an attacker to access and modify files and charts on board or on shore.
- 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.
- An adversary doesn't need physical access to cause damage; they can get in via cellphones or satellite.

Credit: commons.wikimedia.org

ECDIS

- Recent demonstration by Naval Dome (Israeli company) showed what could be accomplished by an attack on ECDIS.
- Designed an attack to change the vessel's position during a "night-time passage through a narrow canal."
- Attack left ECDIS display looking completely normal.
- If fully implemented, would have sent the vessel aground.
- The position, heading, depth and speed all looked different from what they really were.
- Attack took place through the captain's computer, which was regularly connected to the internet through a satellite link, which is used for chart updates and regular logistic updates.

Credit: commons.wikimedia.org

Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Automatic Identification System

- In Oct. 2013 Trend Micro demonstrated how easy it is to penetrate a ship's AIS.
- Recently: Coast Guard Academy team used commercially available software to hack into AIS and turn it off.
- Per Cyberkeel, 2014, such a hack could allow an attacker to impersonate marine authorities to trick the vessel crew into disabling their AIS transmitter.
- This would render the vessel invisible to anyone but the attackers themselves.
- 2017: suspected mass spoofing of AIS on 20 ships in Black Sea; GPS gave false locations.

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

Monitoring Vessels from Elsewhere

- There is increasing interest in being able to monitor the behavior of shipboard systems from elsewhere, e.g., company HQ.
- Now, engine manufacturers can monitor their engines for reliability, but also to make sure they are not being abused - which would void a warranty.
  - They might be watching sensors that give advance notice that something isn't working right.
  - E.g., you might detect vibrations before a bearing goes bad.
- Bottom line: many outsiders have access to vessel systems.
- A bad actor could hack into your system from outside, especially if your shipboard systems are networked.

Credit: En.wikipedia.org
Corroded bearing

Monitoring Vessels from Elsewhere

- For HQ or engine manufacturer to monitor your vessel systems, you might send telemetry from the ship.
- As soon as you create the network connection, there could be a problem.
  - You could try to completely separate a sensor network.
  - But it is easier to put everything on the same network – thus causing potential problems.
- This opens you up to ransomware attacks
- Monitoring from elsewhere also leads to a different combined attack scenario: Start with a physical attack on the remote monitoring facility that allows the adversary to take over the facility and send malicious code to your vessel.
- What about autonomous vessels: Could you hack into HQ computer and direct vessel to go to place it could be boarded by attackers?

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

Cruise Ships: Hacking into the Navigation System

- A 2012 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."
- Something like this happened to a container vessel from Cyprus to Djibouti in 2017: Pirates gained full control of the navigation system. (Fairplay, 2017)

Source: UT Austin "Know"

Cruise Ships: Hacking into the Navigation System

- A bad actor could hack into cruise ship navigation system and cause it to change direction imperceptibly, eventually running it aground.
- This could be the precursor for a physical attack on the ship.
- Is this scenario feasible?
  - Jamming a ship's navigation system takes almost no sophistication.
  - Spoofing it takes more.
  - They would need intimate knowledge of where the vessel is and reasonably close access and would need to transmit false data.
- Each time they told it it was off course to the left (though not true), it would compensate by moving to the right.
- One SME pointed out that with modern ECDIS, the radar overlay would show your GPS is off.
- Another SME said that a physical attack is unlikely to be very successful since first responders would be there quickly.

Credit: commons.wikimedia.org

Fire Alarm on a Cruise Ship

- Could a "bad guy" hack into the fire alarm system on a cruise ship, leading passengers to gather at mustering boat stations as a prelude to a physical attack there?
  - Through a planted explosive or attack by group arriving by boat or a suicide bomber on board cruise ship.
- Is this a plausible scenario?
- It seems feasible to hack into a fire alarm system on a ship, at least in some cases.
- But wouldn't it be easier to let an inside actor attack a large group of passengers already in one place – e.g., dining room?
- Or easier for a group of attackers to come alongside by boat and just start shooting at miscellaneous passengers?
- One SME doubted this kind of combined attack would work because security on cruise ships is so good.

Credit: royalcaribbean.com/

Fire Alarm on a Cruise Ship

- Side comment: To maximize impact, an attacker would not have to follow the fake fire alarm with a physical attack.
- Simply fake a fire alarm, announce they were responsible and say they could do it again.
- This could create psychological impact and potential economic damage to the cruise industry.
- Doing it multiple times would create an even bigger impact.

Credit: en.wikipedia.org

Pirates and Cargo

- Pirates have been reported to have hacked into a cargo management system and identified where on a vessel valuable cargo is located.
- This enabled them to make a very fast and efficient raid on a vessel, going right to the container of interest.
- Is this feasible?
- One of our SMEs felt that it was feasible to hack into the cargo system and identify containers of interest and their location, but wondered how this would help the pirates since it is only the topmost containers they could access.

Credit: wikipedia.org

Pirates and Cargo

- Another of our SMEs pointed out that the USCG had gotten quite good at getting into containers upon boarding a ship.
- Still another SME pointed out that the adversary could influence the loading of containers so that those of interest were placed to be accessible.

Credit both images: commons.wikimedia.org

Closing Comments

- Ultimately, the weak link in defense against combined cyber-physical attacks is still the human being.
- A successful attacker tries to influence behavior, leading to bad decisions.
  - Introduce doubt.
  - E.g. through false aids to navigation showing up on an electronic chart. Spoofing a vessel track that may not correlate with radar.
  - Creating a chain of things initiated by influencing the thinking of the bridge operator.

Credit: commons.wikimedia.org

Closing Comments

- Examples of other areas to discuss include combined attacks on:
  - Ferries
  - Locks
  - Drawbridges
  - Barges
  - Oil rigs
  - Inter-modal landside connections

Source for both:
wikimedia commons

Thanks to my Collaborators from CCICADA

Dr. Dennis Egan

Dr. Christie Nelson

Mr. Ryan Whytlaw

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

Thanks to AEGIS for financial support

aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

- AEGIS is a Horizon 2020 project focusing on EU-US cybersecurity and privacy dialogue. http://aegis-project.org
- Goal: Strengthen international dialogues on cybersecurity and privacy with the objective to facilitate exchange of views, policies and best practices to accelerate EU-US cooperation in cybersecurity and privacy research and innovation.
- Partners: Inmark Europa, Waterford Institute of Technology, The Italian National Research Council (CNR), Hewlett Packard Enterprise, Rutgers University, European American Chamber of Commerce – New Jersey, The Providence Group

aegis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647

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

Combined Cyber and Physical Attacks on the Maritime Transportation System

For More Information:

Dr. 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