# Track 1: Hack the Machine – Maritime Electronics System Test Bed

## Overview

Modern maritime vessels heavily rely upon electronic systems for safe passage through our nation’s waterways and harbors.  Electronic systems include various sensors distributed throughout the vessel to monitor and report status, satellite weather imagery and GNSS receivers, vessel to vessel anti-collision radios, RADAR and internet services such as software and mapping updates via Wi-Fi or cell service.  Pilots increasingly rely upon electronic systems to make safe navigation decisions as maritime vessels grow bigger, become more integrated and carry smaller crews.

Recent events have made it clear that such systems are vulnerable to attack.  On December 4, 2011 Iran captured an American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle by high jacking the UAV’s PNT system and commanding it to land.  On July 29, 2013 students from the University of Texas successfully piloted an 80-million-dollar super yacht 30 miles offshore in the Mediterranean Sea by overriding the ship’s PNT electronic system without alarming the pilot or crew. Remote hacking of electronic systems is currently in its infancy, though growing.

## Challenge

The objective of this challenge is to hack into the machine’s infrastructure causing disruptions to various systems. Some examples of possible scenarios are:

* Hack in the Wi-Fi/LTE Router:
  + Jam the WiFi Router
  + Listen to and record data flowing through the router
  + Modify the data flowing through the router
* Hack the Auto-Pilot System
  + From a NMEA2000 drop, listen and record the output from the Auto-Pilot device.
  + From a NMEA2000 drop, command and control the Auto-Pilot system
  + From either Ethernet or W-iFi, navigate to the Auto-Pilot System and alter the commands
* Hack the Depth, Speed and Temperature Sensor
  + Listen and Record the information transmitted on the sensor.
  + Disable the DST Sensor.
  + From a NMEA2000 drop, modify the information transmitted from the sensor.
* Hack the AIS
  + Listen and Record the boat's AIS messages.
  + Jam the AIS.
  + Spoof AIS messages and get them to show up on TZTouch
* Hack the GPS
  + Jam the GPS.
  + Change the GPS coordinates to report an alternate location.
  + Slowly drift the position of the vessel to an alternate location.
* Hack the RADAR
  + Jam the RADAR
  + Record and recreate a broadcasted RADAR image
  + Create and broadcast a fake RADAR image that includes your team name
* Hack the NavNet TZtouch2
  + Identify the TZtouch2's OS, open TCP/UDP ports, Ethernet messages, or NMEA2000 messages.
  + Spoof a message and have it show up on the TZtouch2.
  + Use the TZtouch2 to send messages from the NMEA2000 network to the Ethernet network or vice versa.
* Hack the machine
  + Be Creative!

## Scoring

When a team feels they have completed a successful hack of the system, the hack will need to be verified and scored by a judge. The judges will score each successful hack based on the scoring system below.

Additionally, the team will have to fill out a Hack Description Template and send a copy of it to HackTheMachineAustin@gmail.com in order for their hack to be counted to their score.

### Scoring Criteria

#### Attack Vector (AV)

This judges the “remoteness” of the attacker relative to the vulnerable component. The more remote an attacker is, the larger the score. This component is a multiplying factor.

|  |  |  |
| --- | --- | --- |
| Metric Value | Description | Numerical Score |
| Remote | Attack is executed beyond the line-of-sight of the boat, including attacking the internet through the Cradlepoint. | 4x |
| Adjacent | Attack is executed within line-of-sight of the boat including attacking the AIS, WiFi, GPS. | 2x |
| Physical | Attack is executed by physically plugging into devices or networks including Ethernet, CAN/NMEA2000, USB. | 1x |

#### Attack Requirements (AR)

This takes into consideration software, hardware or networking conditions required for the vulnerability to be successfully exploited.

|  |  |  |
| --- | --- | --- |
| Metric Value | Description | Numerical Score |
| Low | Attack satisfies the following criteria:   * Exploit requires no outside user interaction. * Exploit does not require inside knowledge such as WiFi password, root access, special permissions, etc… * This is black-box testing. | 3 |
| Medium | Attack satisfies the following criteria:   * Exploit requires minimal outside user interaction such as opening an email, acknowledging alerts, etc... * Exploit requires minimal inside knowledge such as WiFi password, low-level scan data, etc… * This is gray-box testing. | 2 |
| High | Attack satisfies the following criteria:   * Exploit requires significant outside user interaction such as downloading a patch, altering configuration files, etc... * Exploit does requires inside knowledge such as root access, high-level scan data, special permissions, etc… * This is white-box testing. | 1 |

#### Mission Impact (MI)

Judges the attack’s ability to keep the vessel’s crew from executing their intended commands.

|  |  |  |
| --- | --- | --- |
| Metric Value | Description | Numerical Score |
| High | Attack affects the mission in a majority of the following ways:   * Exploit changes the crew’s ability to navigate including routing, guidance and current position information. * Exploit does not allow crew to access critical component information due to availability issues, such as signal jamming, etc… * Exploit changes information that causes system failure or alters the mission. * Exploit affects two or three of the following networks: IT Network, Engineering Network, Voyage Network | 4 |
| Medium | Attack affects the mission in a majority of the following ways:   * Exploit reveals critical information to the attacker such as position, personnel or route information. This does not alter the crew’s actions. * Exploit causes intermittent access to component information due to availability issues, such as partial signal jamming, etc… * Exploit changes information that alters a random set of non-mission-critical data. * Exploit affects one or two of the following networks: IT Network, Engineering Network, Voyage Network | 2 |
| Low | Attack affects the mission in a majority of the following ways:   * Exploit does not change or reveal mission critical information. * Exploit does not cause availability issues to the vessel. * Exploit does not alter data within the system. * Exploit affects one of the following networks: IT Network, Engineering Network, Voyage Network | 1 |

Team Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Scoring Rubric**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hack Description | AV | AR | MI | Score |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Total Score: \_\_\_\_\_\_\_\_

Hack Description Template

|  |
| --- |
| Team Name |

|  |
| --- |
| Type of Hack/Brief Description: |

|  |
| --- |
| Steps taken: |