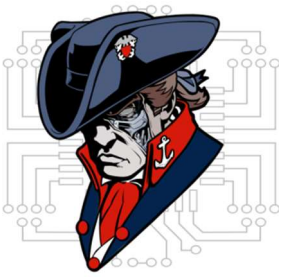
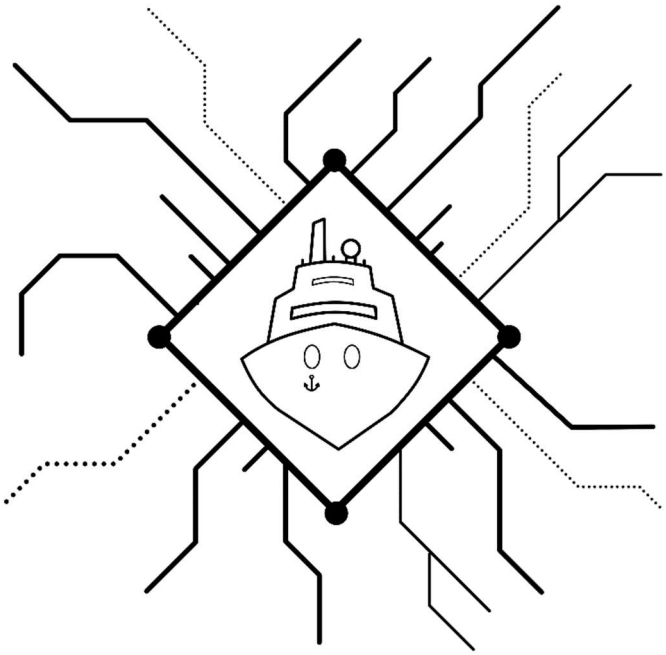


# HACKtheMACHINE
## BOSTON 2017



2017

# HACKtheMACHINE:

# TRUDI

TECHNICAL DOCUMENTATION

"Don't give up the ship!"-James Lawrence, Commander, *US Navy*, 1813

"Don't brick the ship!"-Zachary Staples, Commander, *US Navy*, 2017

# HACK THE MACHINE
## BOSTON 2017

# TABLE OF CONTENTS

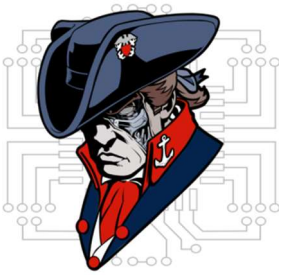
# TABLE OF FIGURES

# HACK THE MACHINE
## BOSTON 2017

# TECHNICAL SPECIFICATIONS

### HARDWARE AND INTERFACING

| Hardware | Network | Connection Type |
|---|---|---|
| **NavNet TZtouch2** | Voyage, IT | Ethernet, NMEA2000,WiFi |
| **Furuno AIS Transponder FA50** | Voyage | Ethernet, Coaxial |
| **Furuno VHF Antenna FAB151D** | Voyage | Coaxial |
| **Furuno Radar DRS4D** | Voyage | Ethernet |
| **Furuno GPS Antenna GPA017** | Voyage | Coaxial |
| **Furuno GPS Receiver GP330B** | Voyage | NMEA2000 |
| **Furuno Integrated Heading Sensor PG700** | Voyage | NMEA2000 |
| **Furuno Satellite Weather Receiver BBWX3** | Voyage | Ethernet |
| **Furuno Satellite Weather Antenna WX1** | Voyage | Ethernet |
| **AirMax Weather Station 220WX** | Voyage | NMEA2000 |
| **Furuno NMEA Junction FI5002** | Engineering | NMEA2000 |
| **Furuno Autopilot Control FAP7011** | Engineering | Serial (Proprietary) |
| **Furuno Autopilot Processor FAP7002** | Engineering | NMEA2000 |
| **Furuno Rudder Reference FAP6112** | Engineering | Serial (Proprietary) |
| **Furuno DST-800MSF** | Engineering | NMEA2000 |
| **Furuno HUB101** | IT | Ethernet |
| **Cradlepoint 1BR1100 Modem/Router** | IT | WiFi |
| **Email Server** | IT | WiFi, Ethernet |



# HACKTHEMACHINE
## BOSTON 2017

### FREQUENCY CHART

Frequency ranges are non-inclusive.

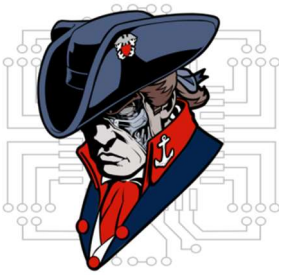
| Standard/Protocol | Devices | Frequency (MHz) |
|---|---|---|
| WiFi | TZTouch2, Email Server, 1BR1100 | 2400, 5000 |
| Sirius | WX1, BBWX3 | 2320-2332.5 |
| XM | Wx1, BBWX3 | 2332.5-2345 |
| AIS | FA50 | 162.025 |
| GPS | GPA017, GP330B, FA50, 220WX, TZTouch2 | 1575.42 (L1) |
| LTE | 1BR1100 | 2500-2690 |
| RADAR | DRS4d-NXT | 9380, 9400, 9420, 9440 |

### IT NETWORK

The following lists the IPV4 addresses, hardware addresses, and open ports for the IT Network

| Hardware | IPV4 Address | Hardware Address | Open Ports (TCP) |
|---|---|---|---|
| 1BR1100 | 192.168.0.1 | 00:30:44:26:25:96 | 22, 53, 80, 443 |
| TZTouch2 | 192.168.0.100 | 00:40:9d:7f:67:70 | 10010, 10023, 10112-10116, 10128, 10129, 10131, 10132, 20010, 20045, 20101 |
| Windows Server 2012 Exchange Server | 10.0.0.4 | 08:00:27:05:41:14 | 25, 80, 81, 135, 389, 443, 444,445, 465, 475, 587, 593, 636, 717, 808, 890, 1801, 2103, 2105, 2107, 2525,5060 |
| Email Server Host Laptop | 10.0.0.3 | 58:fb:84:57:41:26 | 1316, 1925, 826, 1298, 31893 |





# HACKTHEMACHINE
## BOSTON 2017

### VOYAGE NETWORK

| Hardware | IPV4 Address | Hardware Address | Open Ports (TCP) |
|---|---|---|---|
| TZTouch2 | 172.31.252.1 | 00:40:9d:7f:67:70 | 10010, 10023, 10112-10116, 10128, 10129, 10131, 10132, 20010, 20045, 20101 |
| DRS4D | 172.31.3.18 | 00:d0:1d:17:47:fb | 10010, 10100 |
| FA50 | 172.31.24.3 | 00:d0:1d:17:77:3a | 80, 10010 |
| BBWX3 | 172.31.200.20 | 00:18:9d:86:9c:f5 | 23, 9001, 9002, 9010, 9090, 20005 |

# RECOMMENDED MATERIALS

## HARDWARE

**Provided Hardware**

The following hardware will be available in limited quantities at the event:

| Hardware | Interface Type | Useful Against |
|---|---|---|
| Ettus Research USRP N210 | RF (Wireless) | Voyage, IT |
| WBX69-2200 MHz Daughterboard | RF (Wireless) | Voyage, IT |
| RTL-SDR | RF (Wireless) | Voyage, IT |
| NGT1USB NMEA2000 Converter | NMEA2000, USB A | Engineering |

**Recommended Hardware**

It is recommended you bring the following hardware with you:

| Hardware | Interface Type | Notes |
|---|---|---|
| Laptop | Varies by manufacturer | See software list below |
| Cat5 Ethernet Cable | Ethernet | Recommended 30feet or more |



The following optional hardware will support connections to the TRUDI CAN bus and various wireless navigation and networking sensors.

| Hardware | Interface Type | Notes |
|---|---|---|
| NMEA2000 to USB Converter | NMEA2000, USB A | Recommended NGT1USB |
| CAN BUS Analyzer | Serial | Recommended Ginkgo |
| SDR and Antennae | RF (Wireless) | Recommended N210 |
| External Network Interface Card | RF (Wireless) | Packet Injection Capable |

## SOFTWARE

The following list of recommended additional software can be tailored to your skill level and approach to interacting with TRUDI.

| Software Name | Type |
|---|---|
| Kali Linux | Penetration Testing Operating System |
| Wireshark | Network traffic sniffer, analyzer |
| Cain & Abel | Password Recovery Tool |
| NMAP | Network Mapping Tool |
| GNU Radio | Software Defined Radio Development Kit |
| Open Skipper | NMEA2000 Message Decoder |
| Aircrack | Wi-Fi Network Security Tool Suite |
| Metasploit | Penetration Testing Tool Suite |
| Docker | Software Development Containerization Tool |
| OpenCPN | Chart Plotter Navigation Software |
| GRASSMARLIN | ICS, SCADA Network Mapping Tool |

# TRUDI

Every ship must have a name, and the name of this ship is TRUDI. TRUDI, or the Tactical Reconfigurable Underway Demonstration Interface, is a specially built hackable test bed configured to mimic the network onboard a maritime vessel. Just as there are archetypal nicknames within aviation (such as George, for autopilot), there are nicknames within the field of cryptography as well. In cryptography, Trudy is the traditional malicious adversary in a classic Man in the Middle (MitM) attack on a network communication between Alice and Bob. TRUDI is a slight modification to this idea that takes away the malicious intent while still providing insight into the communication patterns of underway cyber physical systems.

# MARITIME SYSTEMS

## OVERVIEW

Modern maritime vessels are *cyber physical systems* (CPSs), meaning they synergize computational and physical components. While CPSs provide greater usability and functionality, they also allow for more points of failure and as a result are vulnerable to attack. Technologies currently used in modern vessels include: ECDIS, AIS, Radar/ARPA, Compass (Electronic), Computerized Automatic Steering System, among many others. Vessels have both an internal network for intra-ship communication, and a network infrastructure for communicating inter-ship and with shore installations. A commercial ship's network includes the Voyage, Engineering, and Information Technology (IT) Networks.

## VOYAGE NETWORK

The purpose of the voyage network is to help navigate the vessel. It includes systems such as the ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), Radar/Automatic Radar Plotting Aid, Compass, Voyage Data Recorder, and others. The voyage network gathers information from sensors and communications equipment, which are processed and then transmitted to a device that the crew can interface with. A ship's bridge will contain many of the interface devices for the voyage network.

Hardware in test bed: GPS, Radar, AIS, ECDIS (Navigation touch panel), Weather Station

### ECDIS (ELECTRONIC CHART DISPLAY AND INFORMATION SYSTEM)

The ECDIS is part of the voyage network and is a computer based navigation system. It collects, transmits, and integrates real-time information that allows the ship to be manned and controlled. ECDIS accomplishes this by continuously determining the vessel's position relative to land, charted objects, navigation aids, and unseen hazards. It utilizes information from a variety of other systems to include the Global Positioning System (GPS), radar, fathometer (which is depth meter) and Automatic identification systems (AIS). While ECDIS helps a boat be manned with fewer crew, it is as vulnerable as its host machine. Attackers can potentially read, download, replace or delete any file on the machine hosting the ECDIS to include crucial navigational charts. The ECDIS system can also be used to pivot, or gain access to other shipboard networks once it is compromised. The ECDIS in the test bed system is part of the Furuno NavNet display.

### AIS (AUTOMATIC IDENTIFICATION SYSTEM)

AIS is an automated tracking system that must be fitted aboard international voyaging ships over a certain size, and to all passenger ships regardless of size. A 2013 estimate of the number of AIS equipped vessels was over 400,000, and that number is increasing annually. The AIS tracks the ship by exchanging data with other ships' AIS systems, with AIS base stations, and with satellite data. This information can then be displayed on the ship's ECDIS system. This data can include the vessel's identity, type, position, heading, and speed to shore stations. This system will be explored further in a separate document. The AIS in the test bed system is a FA50 Class B transponder.

### RADAR/ARPA

While now a colloquial term, radar was actually coined by the U.S. Navy as an acronym, standing for Radio Detection and Ranging. Marine radars provide bearing (or direction) and distance of ships. Radars are vital for navigation and for avoiding collisions. An ARPA (Automatic Radar Plotting Aid) is a system that can automatically create tracks of objects to provide the crew with a visual representation of a tracked object's path. The radar and ECDIS system in the test bed are ARPA capable.

## INFORMATION TECHNOLOGY NETWORK

The IT network is administrative and allows crew to conduct IT tasks. These tasks include but are not limited to: communication with shore installations for weather, scheduling, logistics, and maintenance; web surfing; email; and running client-server applications. This network typically allows users wireless access utilizing personal devices. The hardware in this network includes both wired (such as Ethernet) devices and wireless devices, which include personal electronics.

Hardware in test bed: Junction boxes, Ethernet hubs, Wi-Fi modem/router, processor units, etc.

**Hub**: A network hub is a device that repeats information. It will broadcast information it receives to all open ports and thus to any device connected to those ports. The HUB101 device in the test bed can act as a hub. For more information, see the Ethernet/Lightweight Ethernet overview document.

**Switch**: A network switch will also keep MAC address records in a MAC table. This allows for the maximization of bandwidth for devices within the network. The HUB101 device in the test bed can also act as a switch. For more information, see the Ethernet/Lightweight Ethernet overview document.

**Wi-Fi Modem/router:** Most commonly referred to as just a "modem" or a "router" due to the ubiquity of Wi-Fi, these devices are *wireless access points* that are typically connected to a wired or cellular network. A typical device can service up to 30 clients within a range of approximately 100 meters. In the case of the Cradlepoint COR IBR1100 device in the test bed, it is a wireless access point that connects to a 4G cellular network to provide internet access.

**Email Server:** A typical server is simply a specially configured computer that stores and exchanges information. The email server onboard TRUDI consists of a laptop configured to run a Microsoft Exchange Windows Server

2012 email server. The server itself is run through a Virtual Machine (VM) hosted on a Ubuntu laptop and connects to the network via Wi-Fi.

## ENGINEERING NETWORK

The engineering network connects crew members to the ICS (Industrial Control Systems) onboard that actuate the ship's propulsion, steering, and auxiliary systems. While the voyage network provides the information, the engineering network provides the infrastructure link between the crew and the ship. It can include systems such as the Computerized Automatic Steering System.

Hardware in test bed: Auto pilot, linear actuators, depth, speed & temperature sensors, etc.

### COMPUTERIZED AUTOMATIC STEERING SYSTEM (AUTOPILOT)

The purpose of the simplest autopilot is to lock the heading of a boat towards a predefined course. However, this simple task requires the autopilot system to be connected to and able to control many of the systems onboard the ship. To provide steering, the autopilot has to be connected via the Control Area Network (CAN) to the ICS that controls rudder position. The autopilot also draws navigation and GPS information via the CAN network in order to provide course correction as the ship travels along its predefined course.

### GPS (GLOBAL POSITIONING SYSTEM)

Most modern vessels use a GPS receiver for position and heading information (i.e. as a compass). GPS uses information from a constellation of satellites to determine the receiver's location. A receiver utilizing two separate antennae and an internal gyroscope can combine location and motion information and act as an accurate compass. GPS can also effectively measure the vessel's pitch and roll, which are measurements of the vessel's rotational motions. However, GPS requires movement to act as an effective heading indicator. As with any receiver, GPS operates at certain frequencies and can be intentionally blocked, jammed, or interfered through specially configured radio frequency transmitters. While illegal, jamming devices are easily accessible and are low-cost. It is also possible for attackers to build their own.

### COMPASS

Magnetic compasses have been used for bearing and heading information for millennia. They provide a reliable source of heading information that is not reliant on signal reception. Magnetic compasses align to the Earth's natural magnetic field, and also any other external magnetic fields or large metal bodies such as ships. Digital compasses use the same concept to determine direction, except a magnetometer is utilized instead of a magnetized needle. These devices are cheap, efficient, and decently reliable. Shipboard digital compasses are commonly referred to as *fluxgate* compasses. Instead of a magnetic needle pointing to a heading, variations in an electronically generated magnetic field are measured and processed digitally to provide a heading. The Furuno PG700 Integrated Heading Sensor is a fluxgate magnetic compass that also provides angular velocity data. It is connected to the navigation system via the NMEA2000 network. A technical specification sheet for compasses is provided in your resources.

# IT NETWORK OVERVIEW

## IT NETWORK

The IT Network is for the crewmembers and passengers to conduct all manner of conventional information technology (IT) tasks. Crewmembers use the IT network on the ships communications such as weather, scheduling, logistics and maintenance. Both crew and passengers also conduct morale related IT tasks that include surfing the web, sending email, and client-server applications. This network most often allows its users wireless access. The Maritime test bed is equipped with various devices that comprise its IT Network, which are: the Cradlepoint router, the NavNet TZTouch2, and the Windows Server 2012 email server.

## CRADLEPOINT

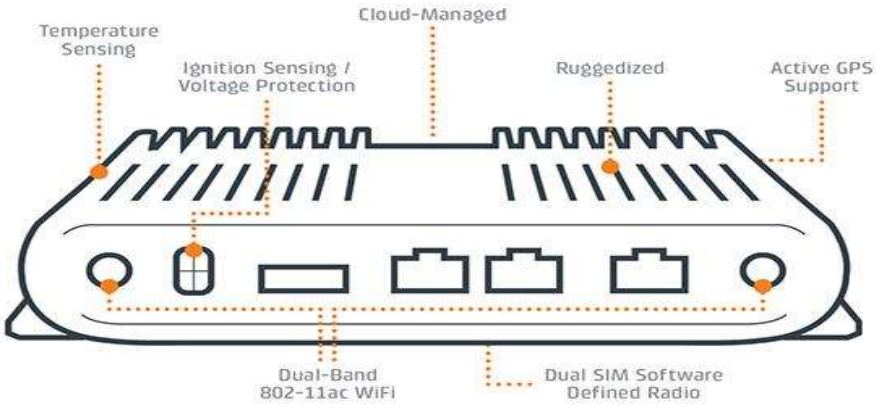



**Figure 1:Cradlepoint IBR1100**

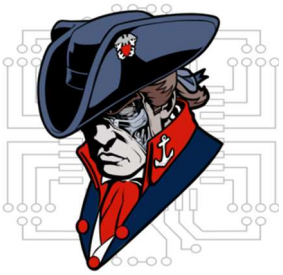
The Maritime test bed uses a Cradlepoint IBR1100 Series router. The router is a compact, ruggedized 3G/4G/LTE networking device designed for connectivity in the most challenging environments. This particular series has advanced its security, added Virtual Private Network (VPN) and stateful firewall features to protect sensitive data. The router provides internet connectivity to both crewmembers and passengers. It also provides internet functionality for the NAVnet TZ touch 2 and email server.

## NAVNET TZ TOUCH 2

Furuno uses the NAVnet TZ touch 2 to merge various technologies and devices into one robust product. The TZ touch is a Multi-Function Display (MFD) unit that integrates both hardware and software to make it a much more intuitive device. Furuno takes the liberty of integrating an internal fish finder, chart plotter, radar, wireless and apps. Giving the TZ Touch 2 multi-functionality makes it the central device in the Maritime Test Bed.

## EMAIL SERVER

The email server is hosted on a standalone Linux-based laptop. A virtual machine will run be running a Microsoft Server 2012 Exchange server. The host laptop will connect to the IT network via Wi-Fi through the 1BR1100. The virtual machine utilizes a bridge adapter to then connect the email server to the rest of the IT network. The server is set up to simulate the crewmembers of our large civilian leisure craft.



# HACKTHEMACHINE
## BOSTON 2017

# ETHERNET/LIGHTWEIGHT ETHERNET

## OVERVIEW

A LAN (Local Area Network) is generally confined to a limited geographic area such as a home, school, or small office building. Ethernet refers to the suite of technologies that are commonly utilized in LANs. Ethernet connections maintain backwards compatibility. The hardware connected via Ethernet within the test bed includes: FA50 AIS Transponder, Ethernet Hub101, Satellite Weather Receiver BBWX3, and the radar system.

### HUBS/REPEATERS

A hub within a LAN acts as a repeater. While you may see the terms hub, switch, and router used interchangeably, they have different functionalities. A hub is a simple repeater that will *broadcast* to all of its ports. Essentially, all information that passes through the hub will go to every device connected to the hub. The HUB101 device within the test bed can act as a hub for all the devices connected via Ethernet.

### SWITCHES

A switch is a device that also keeps a record of MAC (Media Access Control) address of devices connected to it organized into a MAC table; it can identify the specific port information is being sent to, allowing greater bandwidth allocation relative to a hub. The HUB101 device within the test bed can act as a switch, but will be configured as a hub.

### LIGHTWEIGHT ETHERNET

IEC 61162, or Lightweight Ethernet is a set of standards for network communication aboard a ship via Ethernet capable devices. IEC 61162 Part 3 utilizes the NMEA2000 standard. For more information on the NMEA2000 network aboard the test bed, see the CAN overview document. Lightweight Ethernet has *fixed addressing* built in, meaning each device on the network is identified by a preconfigured numbering system.

## VULNERABILITIES

### PHYSICAL ACCESS/CABLING

Most LANs are wired using Category 5 or 6 copper cabling with a maximum segment length of 100 meters. With a maximum segment length of 100 meters, larger networks require additional hardware like hubs and repeaters, which will then receive all the broadcast information. You will be given physical access to the switch. A malicious user could access a switch in a telecom closet as the basis of a maritime cyber-attack.

### MAC FLOODING



In a MAC flooding attack, an attacker feeds many unique MAC addresses to the switch in an attempt to use up the limited memory used to store the MAC table. The intended effect of this being that once the legitimate MAC table is unusable, the switch will then broadcast incoming data to all ports, including the attacker's. Data capture utilizing packet analyzing software can then occur.

## ARP SPOOFING

ARP spoofing involves sending a spoofed message in an attempt to associate the attacker's MAC address with a different IP address, causing the intentional misrouting of network traffic.

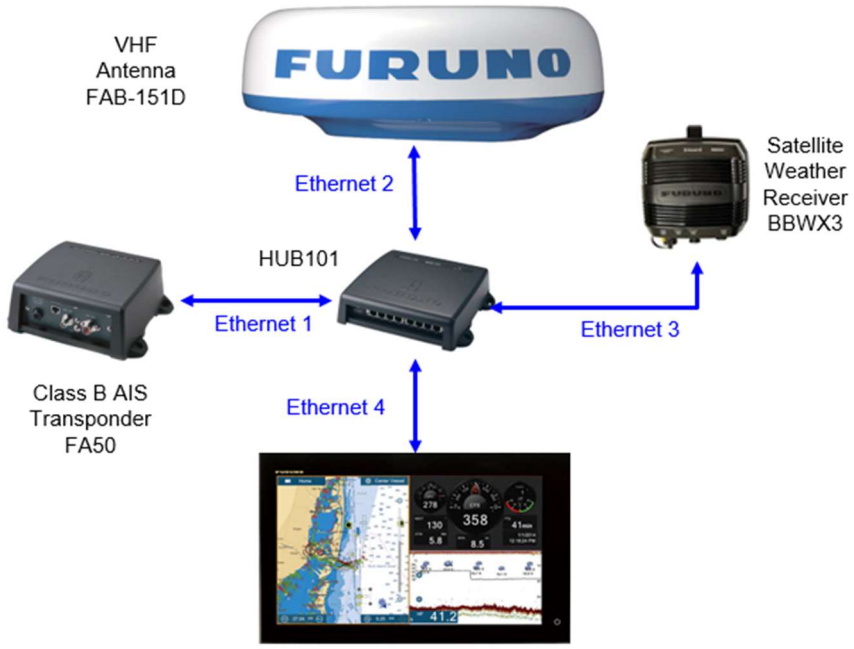



**Figure 2: Maritime Ethernet Network**

# CONTROLLER AREA NETWORK (CAN)

## OVERVIEW

The Controller Area Network (CAN) bus standard was initially developed for the automotive industry. Unlike serial communication protocols which provide one to one communication, the CAN bus allows for high data rate point-to-point transfers.

The Furuno FI5002 junction box in the test bed allows for access to the CAN bus. Devices on the CAN bus utilize the NMEA2000 proprietary communication standard for connecting marine devices and display units.

Examples of devices that can be connected to the NMEA2000 network onboard a ship include: GPS receivers; auto-pilot systems; depth, temperature and speed sensors; navigation devices; weather stations; and radars. This interconnectivity effectively allows the GPS and navigation systems to correct the course the auto-pilot is steering by bridging the voyage and engineering networks.

CAN was designed without security or message authentication. With many modern vehicles containing more and more electronics, many critical systems are connected to the CAN network to reduce the amount of wiring required and allow for distributed feedback. For instance, the now infamous hack of a popular SUV via a zero-day exploit involved compromising the vehicle through the CAN bus. Through the wireless entertainment system, the hackers were able to send commands to compromise the dashboard, steering, brakes, and transmission. Most CAN hacking requires one to be directly plugged into the network hackers can pivot from wireless devices connected the CAN bus to critical systems. The laptop used to compromise the SUV was located in a basement while the vehicle was driving on a highway quite some distance away.

CAN hardware and software analytical tools can be utilized onboard the NMEA2000 network. A NMEA2000 to USB converter cable is recommended, but not required. Some NMEA2000 tools are included in your resources folder.

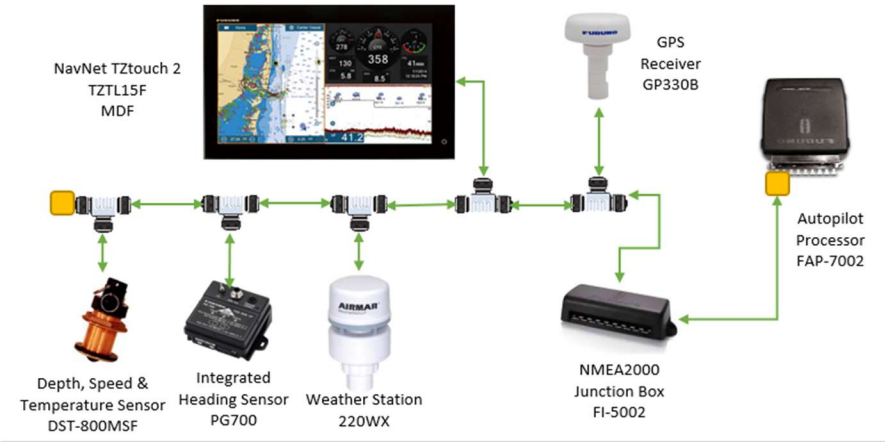



Figure 3: NMEA2000 Maritime Network

# AUTOMATED IDENTIFICATION SYSTEM

## OVERVIEW

The Automated Identification System (AIS) is an automated system used on ships to identify and locate other vessels.

### HARDWARE

AIS transceivers periodically broadcast information about their position, speed, navigational status (anchored, underway, etc.) at regular intervals via VHF. The AIS transceiver is programmed with information about the vessels characteristics and the location of the AIS's GPS receiver used to broadcast its location. Some information, such as the vessel's Maritime Mobile Service Identity (MMSI) identifier, is programmed into the transceiver upon installation. AIS base stations are shored based transceivers capable of controlling an any AIS device. Buoy-based Aids to Navigation (AtoN) can act as relays to extend network coverage. Class A AIS devices are vessel mounted systems used mainly by large commercial vessels, have integrated displays and can receive all types of AIS messages. Class B AIS devices are also vessel mounted but are targeted at commercial or leisure markets, being smaller and without an integrated display. The FA50 Transponder in this test bed is a Class B device. The VHF transmission power of a Class B is restricted to between 2-5 watts, giving it a 5-10 mile range. The FA50 uses a built-in GPS receiver for position fixing.

### BROADCAST INFORMATION

Class A transponders transmit messages at set intervals. See appendix for acronym list and attached AIS reference sheet from the U.S. Coast Guard.

- Message 1 (Every 2, 3, or 6 seconds if moving, 3 min if anchored): MMSI, UTC Time-Stamp, Position, Position Accuracy Flag, RAIM flag, COG, SOG, HDG, ROT, Navigation Status, Communication State
- Message 5 (Every 6 min): MMSI, IMO#, Call-sign, Name, Ship Type, Dimensions, Static Draft, Destination, ETA, EPFS type, Data Terminal availability, AIS version
  Class B transponders transmit a similar set of messages.

- Message 18 (Every 30s, 3 min if anchored): MMSI, UTC Time-Stamp, Position, Position Accuracy Flag, RAIM flag, COG, SOG, HDG, Communication State, Type(SO/CS), Operating Mode, Availability of a Display, DSC Receiver, Full/Limited Bandwidth, Channel Management
- Message 24A&B (Every 6 min): MMSI, Call-Sign, Name, Ship Type, Dimensions, EPFS type, AIS version, Vendor ID

Additionally, the information can be classified as static or dynamic (Information is FA50 specific)

- Static:
  - MMSI
  - Call Sign & Ship's Name
  - Type of Ship
  - Location of antenna on ship
- Dynamic:
  - Ship Position with accuracy indication and integrity status (from GPS)
  - UTC
  - COG
  - SOG
  - Heading

## VULNERABILITIES

*Hardware required*: Marine VHF Radio (156.0-162.025 MHz)

**Possible Exploit Scenarios:**

- Modify ship details: position, course, cargo, speed, name
- Spoof "ghost" vessels recognizable as genuine vessels by receivers
- Trigger false collision warning alerts
- Falsify weather information
- Impersonation of marine authorities
- DOS attack

## ACRONYM LIST

MMSI-Maritime Mobile Service Identity

RAIM-Receiver Autonomous Integrity Monitoring

COG-Course over ground

SOG-Speed over ground

HDG-Heading

CS-Carrier Sense (Type of Class B transceiver)

SO-Self-Organizing (Type of Class B transceiver)

EPFS-Electronic Position Fixing System

ID-Identification

UTC-Coordinated Universal Time

# GLOBAL POSITIONING SYSTEM (GPS)

## OVERVIEW

GPS is an accurate and crucial positioning system whose capabilities are offered to anyone with a GPS receiver. There are four systems onboard the test bed with GPS receivers: The Furuno TZTouch2, the GP330B GPS Receiver, the FA50 AIS Transponder, and the 220WX Weather Station. The TZTouch2 is configured to use position data from the GP330B receiver.

GPS determines your location via the geometric concept known as triangulation. Triangulation involves knowing your distance from three established reference points. In terms of cell tower triangulation, the three established reference points would be three cell towers with the receiver being your cell phone. This provides an accuracy to about .75 km, with more reference points (such as a high density urban area) providing even greater accuracy. GPS on the other hand, utilizes satellites zipping around the Earth at roughly 14,000 km/hr. GPS receivers actually require connection to four satellites to provide latitude, longitude, altitude, and timing information due to the fact that GPS satellites are moving reference points. With a little bit of math, your GPS receiver can then give you your three-dimensional position within about 10 meters.

## VULNERABILITIES

### JAMMING

As with any kind of receiver, GPS operates at certain frequencies and can be intentionally blocked, jammed or interfered with through specially configured radio frequency transmitters. While illegal, jamming devices are easily accessible and low-cost. It is also possible for attackers to build their own. Remember, there are four GPS enabled devices in the test bed. The TZTouch2 defaults to using information from the GP330B.

### SPOOFING

By its very nature, the L1 (civilian) frequency is unencrypted due to the large user base. It contains no authentication or authorization. Thus, most commercial GPS receivers are subject to spoofing attacks. A spoofed GPS signal is recognized by the (unencrypted) GPS receiver as legitimate yet it may contain altered or potentially dangerous information. With the right signal and timing, an attacker can change the GPS coordinates to report a different location, causing confusion and loss of bearing. An attacker can also slowly drift the position of the vessel to an alternate location, which could be potentially disastrous to an inattentive crew.

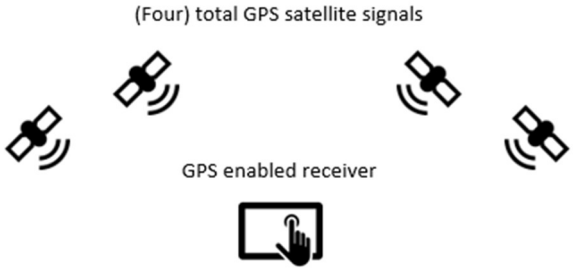


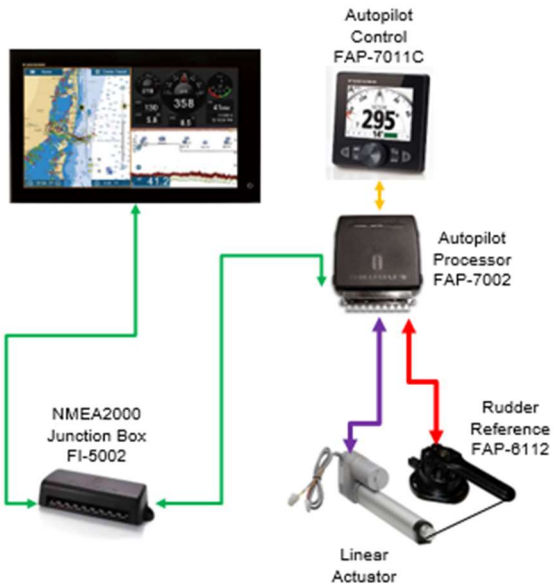

**Figure : GPS System**

# AUTOPILOT

## OVERVIEW

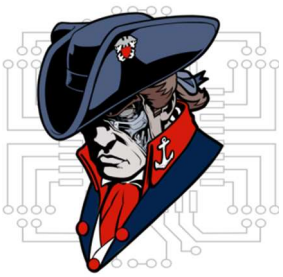
Autopilot can also be useful in maritime applications. Modern vessels can be simple like a sailboat or incredibly sophisticated like aircraft carriers. Our test bed is to simulate a large civilian craft, and in turn it contains an autopilot system that will help the captain focus on other, more important tasks. Marine autopilot systems perform the same function as airborne systems in that it will activate the ICS in control of the rudder to keep the vessel on a predetermined course. A complete autopilot system involves three separate systems: a heading sensor, a central processing unit, and a drive unit.

Marine autopilot systems adjust the rudder orientation to steer the vessel towards the heading or waypoint set by the autopilot system. More sophisticated systems will integrate with GPS and other course plotting software or devices to provide more advanced autopilot features. The Furuno FAP7011C control unit in the test bed is the user interface of the autopilot system. The Furuno FAP7002 autopilot processor is the central processing unit. It takes user input from the FAP7011C and will activate the rudder system (drive unit). Both the control display and processor are connected via the NMEA2000 network to the NavNet TZTouch2, which provides both heading and course plotting functionality.




The FAP7011C control unit has a graphic display and will automatically adjust parameters such as speed, trim, draught and tide along your course. A user can input a reference heading for the autopilot to follow, or it can also be configured to perform port and starboard turns and to follow a course plotted by the navigation system on the TZTouch2. Please note, the FAP7011C and FAP7002 do not have inherent GPS capabilities. The FAP7011C has dual NMEA2000 and NMEA0183 bus interfaces. The TZTouch2 utilizes a combination of GPS data and a digital compass for heading and navigation information. The FAP7002 processor utilizes the NMEA2000 interface to connect to the TZTouch2. The FAP-7011C, FAP-6112, and Linear Actuator are connected via Furuno proprietary (serial) cables.

**Figure 5: Maritime Autopilot System**



# HACKTHEMACHINE
## BOSTON 2017

# HACKING WI-FI

## OVERVIEW

Virtually any shop, airport, hotel, library, etc… offers Wi-Fi to its patrons. It is hard to go anywhere these days without being able to connect to a public or private wireless network. Having access to the internet at all times has become a necessity in modern day society. Wi-Fi utilizes the IEEE (Institute of Electrical and Electronics Engineers) 802.11 network standard that comes in a variety of forms. The most common one used is 802.11n and is backwards compatible with 802.11a & b.

You will find that most places house a router, which both provides the internet services and access to the network. The router comes in varying sizes and capabilities as determined by the manufacturer. As a single device the router also contains a port for cable or DSL modem connection, a firewall, Ethernet hub and a wireless access point. Some people give access to their network to the public, which means that anybody can logon and off. However, it is common practice to protect your private wireless network by setting up a password.

Wi-Fi encryption has evolved over the years. Wired Equivalency Privacy (WEP) was once the standard for WAN security, but hackers exploited the vulnerabilities of this approach, rendering it unsecure to use. Systems that still employ WEP are susceptible to cyber-attacks and easily compromised. Most current devices use, Wi-Fi Protected Access Version 2 – Pre-Shared Key (WPA2-PSK), which is the successor to WEP and WPA. It has become the security standard for WAN security.

As with any sort of network, there are vulnerabilities that can be exploited in order to gain access and control of a system. Wi-Fi hacking has become increasingly popular over the last few years. Some vulnerabilities include:

**Eavesdropping:** A type of electronic attack where digital communications are intercepted by an individual whom they are not intended.

**Media Access Control (MAC) Address Spoofing:** Copying a known MAC address to fool the network that the device that is being used belongs on the network.

**Address Resolution Protocol (ARP) Spoofing:** Sending false ARP messages over a network, which links the hackers MAC address with the Internet Protocol (IP) address of a legitimate device on the network.

**Denial of Service (DoS):** Any form of attack where hackers attempt to prevent legitimate users from accessing the service.

**Wireless Phishing:** Any technique used by a hacker to convince wireless network users to divulge sensitive information.



## WIRELESS HACKING TOOLS

The aforementioned vulnerabilities are some of the most popular attacks used by hackers to infiltrate and compromise Wireless Local Area Networks (WLANs). Successful attacks can lead to stolen data, compromising and degradation of a system. Hackers are utilizing a wide range of tools in order to successfully exploit the vulnerabilities of Wi-Fi. Some of the current and most popular tools are:

- Aircrack
- AirSnort
- Cain & Able
- Wi-Fi Pineapple
- LAN Turtle
- USB Rubber Ducky

## TEST BED

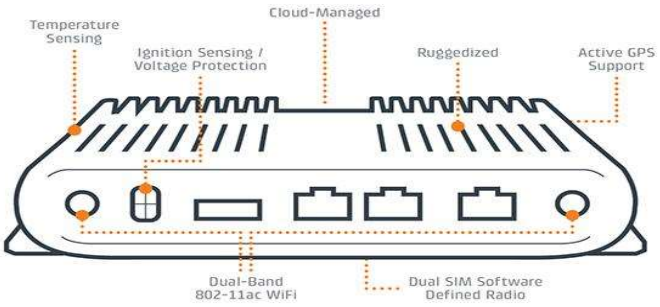



**Figure 6: Cradlepoint IBR1100**

The Maritime test bed uses a Cradlepoint IBR1100 Series router. The router is a compact, ruggedized 3G/4G/LTE networking device designed for connectivity in the most challenging environments. This particular series has advanced its security, added Virtual Private Network (VPN) and stateful firewall features to protect sensitive data.


Figure 7: Maritime Wireless Network

# WEATHER SYSTEMS

## OVERVIEW

Navigating the oceans is highly dependent on the weather. While modern powered vessels are more weather independent than the sailboats of yore, weather is a valid safety concern for crews and must be properly planned for. Maritime weather systems will display some of this relevant information: radar and precipitation type, current conditions, storm attributes, lightning, weather warnings, tropical storm tracks, weather map, marine zone forecasts, sea surface temperatures, wind and wave forecasts, and cloud cover. Storms, high winds, low visibility, and other weather phenomena could potentially cause a captain to reroute the vessel for safety.

Connectivity is an important issue while at sea. The weather system aboard the test bed is made up of a Furuno WX1-005-003 Satellite Weather Antenna, a Furuno BBWX3 Satellite Weather Receiver, the Furuno TZTouch2, and an AIRMAR WX220 Weather Station. The BBWX3 is a SiruisXM capable receiver that will display information via the TZTouch2. The WX220 Weather Station is a pole-mounted real-time weather monitor connected to the TZTouch2 via the NMEA2000 network.

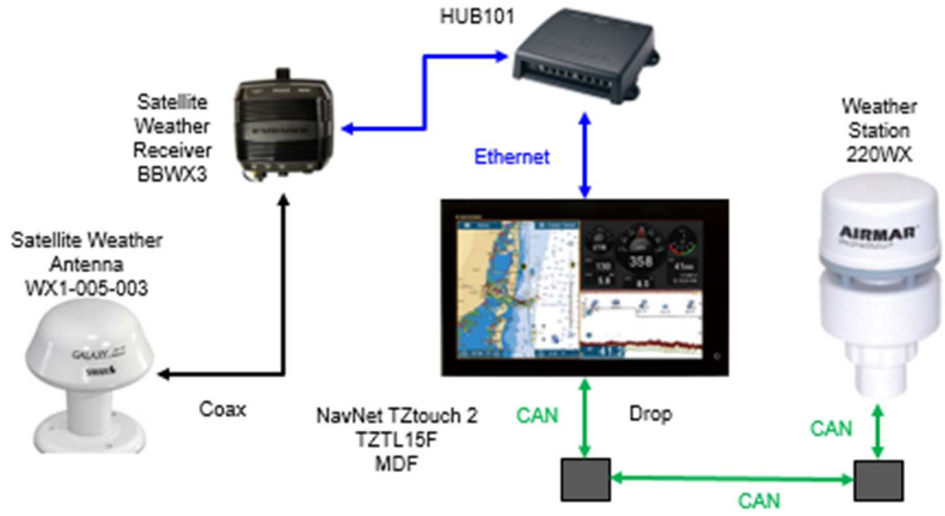



**Figure 8: Maritime Weather System**

Weather information from the receiver is delivered through the commercial SiriusXM Marine Weather services. SiriusXM is a satellite-based radio service commonly found in vehicles. The Sirius XM constellation consists of 9 operational satellites that operate in the S Band range of frequencies. There is also an expansive network of terrestrial repeaters. It is worth noting that SiriusXM does not operate any weather satellites. Their weather information is obtained from a contractor, Baron Services. Baron Services aggregates data information from several sources including the Department of Defense and National Weather Service.

The AIRMAR 220WX is an on-site sensor bed that relays real-time information to the TZtouch2 via the NMEA2000 network. It has sensors for the following information: apparent wind speed and angle, true wind speed and direction, barometric pressure, air temperature and wind chill, internal GPS position, speed over ground, course over ground, compass, pitch and roll accelerometer, rate of turn gyro, and humidity data.

## VULNERABILITIES

Like any radio frequency receiver, the satellite weather receiver is susceptible to jamming and spoofing attacks. While most satellite based hacks have only involved intercepting traffic, recent demonstrations have shown that man in the middle attacks are possible and have occurred. The most common form of attack is a broadcast signal intrusion, frequently affecting devices that simply rebroadcast information received from another source, such as many radios. The S Band range of frequencies is well within the range of most commercial receivers and antennas. However, SiriusXM is naturally very secretive about its proprietary encryption method for all of its traffic.

The AIRMAR WX220 weather station is part of the NMEA2000 (CAN bus interface) network onboard the test bed. While all of its sensors are internal to the system, the WX220 also contains a GPS receiver. A full list of the NMEA2000 sentence structure can be found in your resources.