DEFCON: Hack the Sea Personal Experiences

John Zage

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

What is Defcon?

- One of the world's most notable hacker conventions
- Includes:
  - Computer Security Professionals
  - Journalists
  - Lawers
  - Federal Government Employees
  - Security Researchers
  - Hackers

2019 Hack the Sea Village

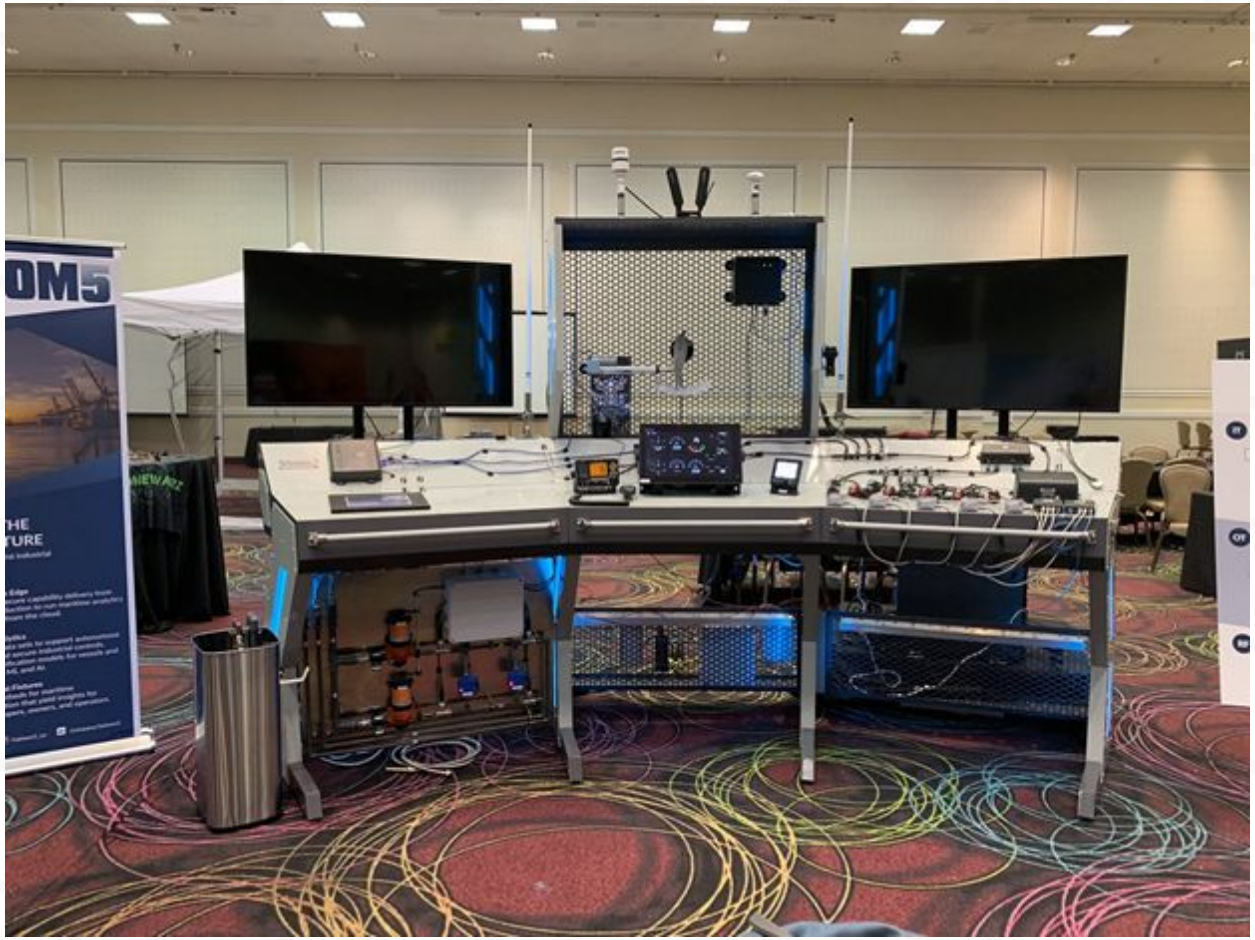
- Members of the maritime community at DEFCON faced similar issues; they seek to solve them through collaboration
- Participants included:
  - American Bureau of Shipping
  - Coastguard
  - ABS Security
  - Fathom5 Security
  - Maritime and Port Security ISAO
  - Hackers
- Some of the challenges are too large to solve individually, EG Operational Technology (OT) Security

Why Collaborate?

- Too many facets to consider, too many vulnerabilities for one individual or organization to solve
- Sharing cybersecurity intelligence can prevent additional victims being hit by the same attack
- Additional minds on a problem can lead to improved solutions

2019 Hack the Sea Village

- Villages are dedicated spaces arranged around a specific topic in DEFCON
- Held Hack the Sea CTF
  - Fathom5 security provided GRACE, a maritime infosec lab for hackers to learn on
  - Originally designed for US Navy



2019 Hack the Sea Village

- Topics discussed included:
  - Policy Talks
  - Cargo Management, smart cargo & EDIFACT
  - GDMSS, including AIS (Automated Identification System)
  - Navigation, including ECDIS, GPS, and radar
  - Propulsion
  - Communications, including Satcom and NMEA protocols

Personal Experiences

- Firmware Analysis
- Propulsion talk

State of Operational Technology Security

- Cybersecurity of OT discussed during various talks
- Issue with OT: layers of binary files
  - Fundamental Supply Line Issue: components of OT software are created by different manufacturers
  - Each manufacturer compiles binary, passes it onto the next manufacturer up the chain
  - Ends up with no one manufacturer having access to the source code of the OT device
  - Cybersecurity Researcher would have immense difficulty performing a security review of the OT device

Firmware Analysis – Presented by Kyle O'Meara

- Workaround for not having source code of OT:
  - Open source tools that decompile
- OT systems on the ships have Images of their standard configuration stored online by the system vendors, as a binary files
  - Accessible with serial and device numbers from the ship OT
- TROMMEL CERTCC was showcased (https://github.com/CERTCC/trommel)
  - Python script used to search through imbedded files for vulnerability indicators, such as:
    - Unsecure system calls, SSH Key Files, IP Addresses, Specific Binary Files

Propulsion- Presented by REdoubt

- Focused on vulnerabilities in engine propulsion firmware
- Tested on B&W 12S90ME-C Mark 9.2 and Wartsila-Sulzer RTA96-C Flex
- Engines use unsafe unencrypted communications between engine and control system (old version of ModBus)
- There is a new version of ModBus that is encrypted
- Old version can have replay attacks and spoofed messages
- Hacker was able to cause engine to shut down, fooling the engine to think it was not getting the correct power

Resources

- Visit https://hackthesea.org/ for more info or contact info@hackthesea.org for DEFCON 2020 plans

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Questions?