Maritime Cyber Security Risks

Attack surface

- IT data providers
- Maritime authorities
- Customs & Border protecitons
- ports
- terminals
- logistic companies
- shipping lines
  - Cargo tracking software
  - websites
    - CyberKeel
    - Email query forms
    - Schedule lookup

- Vessels, oil platforms, rigs
  - AIS transponders
    - attacks
      - AIS spoofing, frequency hopping etc.
        - TrendMicro
  - Satelite links
    - attacks
      - against the SATCOM device
        - malicious text messages (SMS, ship to ship message)
        - backdoors
        - default creds
          - IOACTIVE
    - GMDSS Global Maritime Distress and Safety System
    - SSAS Ship Security Alert System
    - Broadband communications
  - dependent on GPS
    - attacks
      - malware - localy introduced
      - GPS manipulation jamming, injection
        - University of Texas Performed audit
    - automated container terminal systems
    - Navigation systems
      - DGPS receivers
      - dynamic positioning system
      - digital selective calling
      - gyrocalibration system
  - ECDIS
    - connected with
      - attacks
        - interconnected system
          - NCC group
        - malware - localy introduced
      - NAVTEX
      - radar
      - AIS
      - Sailing directions
      - navigation charts (loaded via CD/DVD or USB not over network)
      - Position fixing
      - Speed log
      - anemometer
      - fathometer
      - Echo sounder
  - SCADA
    - standard systems with LAN connectivity
      - attacks
    - attacks
      - standarad vectors
      - malware - localy introduced
      - interconnected system ???

Root causes

- diversity of vessels
- Slow product adoption process
  - diversity of HW & SW maniferturers
  - wide range of regulatory framwroks to comply with (SOLAS, COLREG, FAL, SUA etc)
  - Little provision of the frameworks towards infosec and data privacy issues
- Contributers to status quo
- Insecure HW & SW implementations
  - SATCOM devices
  - ECDIS
- Insecure protocols
  - GPS
  - Protocols used in SATCOM
  - other
  - AIS
- IT staff not trained with focus on security
- Insecure network configuration
  - Lack of crew awareness

attacks against vessels

- Operations disruption
  - SATCOM attacks
    - malicious messages
      - DCS/VHF
    - interconnected devices
  - Navigation attacks
    - GPS manipulation
      - special data channels and protocols attacks
        - NMEA, SIRF, MTK
    - AIS manipulation
      - special data channels and protocols attacks
        - SOTDMA / VHF, USB, RS232, NMEA
    - ECDIS attacks
      - mallware - removable devices
      - standard network attacks
  - SCADA attacks
    - malware locally introduced
      - compromised firmware
      - removable devices
    - interconnected systema
      - special data channels
      - standard network attacks
- Data exfiltration
  - local copy
    - removable devices
  - network attack
    - standard network attack vector
  - Side channel intelligence
    - crew (for example social network behaviour monitoring)

Legend

- Companies/Researchers
- attack vectors

25 - 11 - 2014 ePs