Maritime Cyber Security

Threats and Opportunities

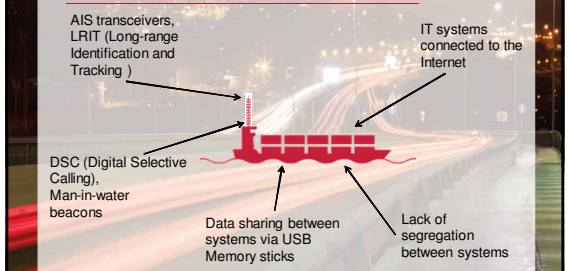
Agenda

- Maritime Cyber Threats
- Attack Surface Overview
- Potential Impact
- Reported Incidents
- Solutions
- Guidance
- The NCC Group Approach

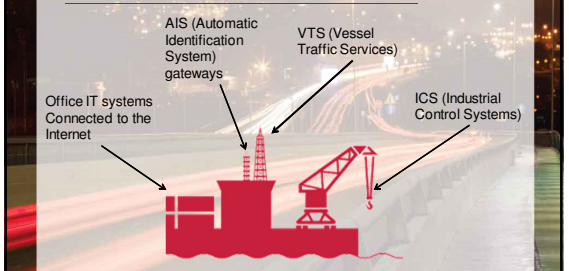
Maritime Cyber Threats

- Increasing connectivity of ships
- Ever-greater integration of ICS into onboard networks
- Pre-Internet systems and protocols wrapped in IP
- Widespread use of USB memory devices for data sharing
- Greater use of remote access capability
- Attackers increasing targeting non-conventional IT

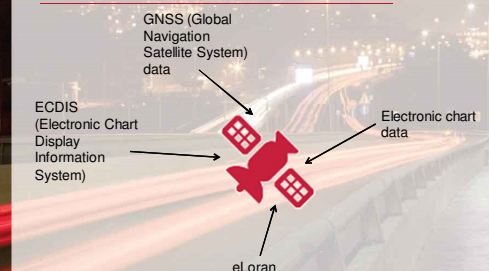
Attack Surface Overview: Ships



Attack Surface Overview: Harbour



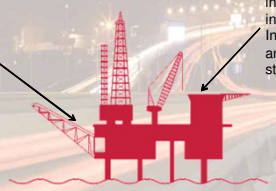
Attack Surface Overview: Navigation



Attack Surface Overview: Rigs

DP (Dynamic Positioning) systems

Malware inadvertently introduced via Internet browsing and USB memory sticks



Potential Impact

- Technical safety controls in ICS systems and procedural controls make 'catastrophic' scenarios unlikely, but possible.
- More likely: Failure of a critical system (e.g. Engine Management or ECDIS) leaving a ship 'quarantined' in harbour losing $$$ every day

Impact: Some Reported Incidents

- In 2012 criminals penetrated the cargo systems operated by the Australian Customs and Border protection, allowing them to check whether their shipping containers were regarded as suspicious by the police or customs authorities.
- Drug traffickers reportedly hacked into the computer controlling the location and movement of shipping containers at the port of Antwerp
- In 2012, North Korea uses lorry-mounted devices to block GPS signals in South Korea for 16 days, causing 1,016 aircraft and 254 ships to report disruption
- In 2016, pirates worked together with hackers to identify high-value cargo on ships in order to target their attacks.

Short-Term Solutions

- The active threats to marine systems should be identified through threat modelling
- If software/firmware can easily be fixed to mitigate vulnerabilities this should be done
- More complex design-related vulnerabilities need to be contained using segregation technologies

Medium-Term Solutions

- Standards Documentation:
  - IEC Standards and Guidance development 61162-450:2011 in particular provides good guidelines on how to implement security into shipboard network infrastructure.
  - DNV Classification society documentation and DNV Nautical Safety (Network Based Integration of Navigation Systems (ICS)).
  - IEC TC80 standard contributions (61162-460)
- Policy and Strategy Best-Practice Development
  - Further Development of Industry Best-practice guidance for process and technical activities

Long-Term Solutions

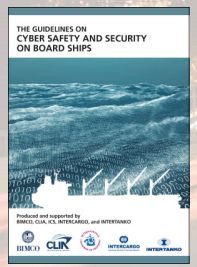
- Marine systems developers need to implement an SDL (Secure Development Lifecycle)

- System components and fully integrated solutions should be subject to regular security assessment.
- Remote connectivity solutions should be tailored to the specific environment and the risks fully evaluated.

Raising Security Awareness

- Effective cyber security starts with Security Awareness
- Understanding the fundamentals can make a huge difference: You don't need to be an expert to spot potential security risks
- Processes need to be implemented to enable people to raise potential security issues/risks from systems development through to operations.

Guidance



- NCC Group were a key contributor to the BIMCO *Guidelines on Safety and Security On Board Ships.*
- Guidelines include:
  - Understanding Cyber Threats
  - Risk Assessment
  - Cyber Security Controls
  - Incident Response and Recovery Plans

NCC Group Approach

- The NCC Group Approach to Maritime Cyber Security tackles the challenges facing maritime businesses at three levels.
- **Strategic:** At the Strategic level, NCC Group leverages years of experience in developing information security strategy and a broad understanding of the maritime environment to help businesses develop strategies and policies.
- **Technical:** NCC Group is well-known as a centre of excellence for security assessment and research. We have a highly-skilled technical consulting team holding many UK Government security testing accreditations.
- **Operational:** NCC Group provides real-time and rolling monitoring to detect security incidents and provide rapid Incident Response.

Strategic
Technical
Operational

15

Conclusions

- The potential impact of marine cyber attacks includes potential revenue loss, environmental damage and loss of life
- Development and implementation of agreed standards and guidelines is required
- More security testing of marine systems, networks, hardware devices and any associated software is required
- The ultimate solution is to embed security into the development lifecycle of products and systems
- The most important step is to ensure staff are aware of cyber security threats through appropriate training so that they can be identified and reported

Questions?

17

Contact us

+44 161 209 5200
maritimesecurity@nccgroup.trust
www.nccgroup.trust

North America
- Atlanta
- Austin
- Chicago
- New York
- San Francisco
- Seattle
- Sunnyvale

Canada
- Waterloo

Europe
- Manchester - Head Office
- Amsterdam
- Basingstoke
- Cambridge
- Cheltenham
- Copenhagen
- Edinburgh
- Glasgow
- Leatherhead
- Leeds
- London
- Luxembourg
- Madrid
- Malmö
- Milton Keynes
- Munich
- Vilnius
- Wetherby
- Zurich

Australia
- Sydney

18