nccgroup
freedom from doubt

An NCC Group Publication

Preparing for Cyber Battleships – Electronic Chart Display and Information System Security

Prepared by:
Yevgen Dyryavyy

Contents

1 Introduction

In an increasingly connected world, cyber security is more important than ever. NCC Group, one of the world's leading cyber security research companies, regularly investigates the susceptibility of non-traditional systems to attack in order to help raise awareness of the risks to these systems,

In this paper, we discuss the results of a research project looking at the security risks and weaknesses within Electronic Chart Display and Information Systems (ECDIS) [1], an information technology product used by the maritime industry.

ECDIS is a computer-based navigation information system used as an alternative to paper nautical charts. These systems are usually installed on the bridge of the ship and used by navigation officers as an aid to traditional paper chart navigation.

The International Maritime Organization (IMO) is currently implementing regulations which require these systems to be installed on all commercial vessels, with the aim of completely replacing the use of paper nautical charts in the near future. This paper presents and reviews the security issues found in one well-known ECDIS software product during research conducted by NCC Group.

2 Preparing for Cyber Battleships

2.1 Information Technology and Cyber Security in Maritime

Information technology proliferation with in the maritime and shipping industry is usually very slow. There are several contributory factors to this; for example the adoption of a new software product could take months, if not years, due to diversity and geographic spread of the vessels across the globe. Another factor is that manufacturers, vendors, and software development companies have to comply with a range of regulation frameworks and certification programs, such as the International Convention for the Safety of Life at Sea (SOLAS) [7], the Convention on the International Regulations for Preventing Collisions at Sea (COLREG), the Convention on Facilitation of International Maritime Traffic (FAL), and the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA), among others, all of which take time to achieve. Such compliance programs and frameworks were established decades ago and tend to cover product usability, general safety, and conformance to standards. When compared to the current and future threat landscape, there is very little provision on information security and data privacy within the standards.

Although guidelines and frameworks such as Security Development Lifecycle (SDL) do exist, vendors are not obliged to follow them. Crew members and management companies often also install software such as control systems, Microsoft Office, and email clients on shipboard systems, and these programs can also contain vulnerabilities.

Typically the following systems, as shown in the diagrams below, are found to be interconnected via shipboard LAN:

- SCADA for power plant control and machinery monitoring
- Just-in-time spare part ordering
- CCTV systems
- Bridge Navigation Watch Alarm System (BNWAS)
- Track history and electronic logbook
- Remote monitoring
- Onboard Wi-Fi and Internet access (to be used by crew and guests)
- VoIP Telephony

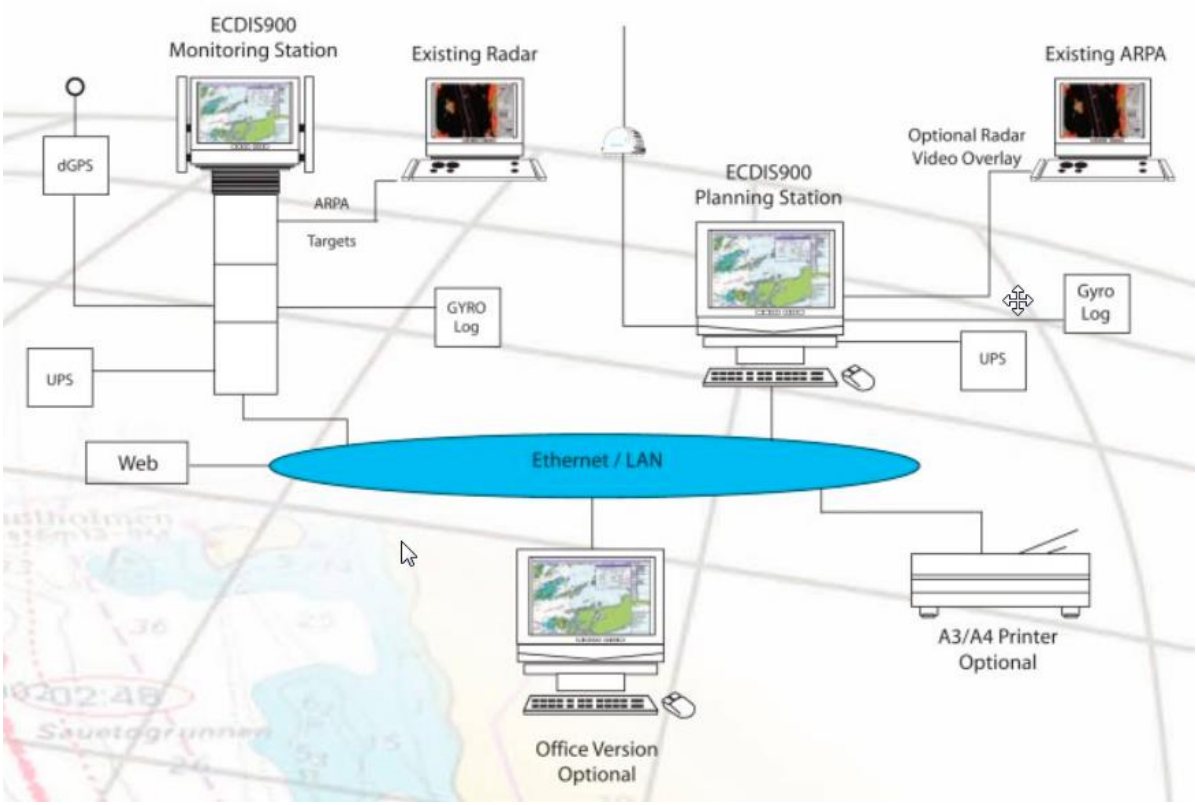

Figure 1: Diagram of systems typically connected to a ship's LAN
[source http://pdf.nauticexpo.com/pdf/maritime-information-systems/ecdis-900/31325-42061-_9.html]

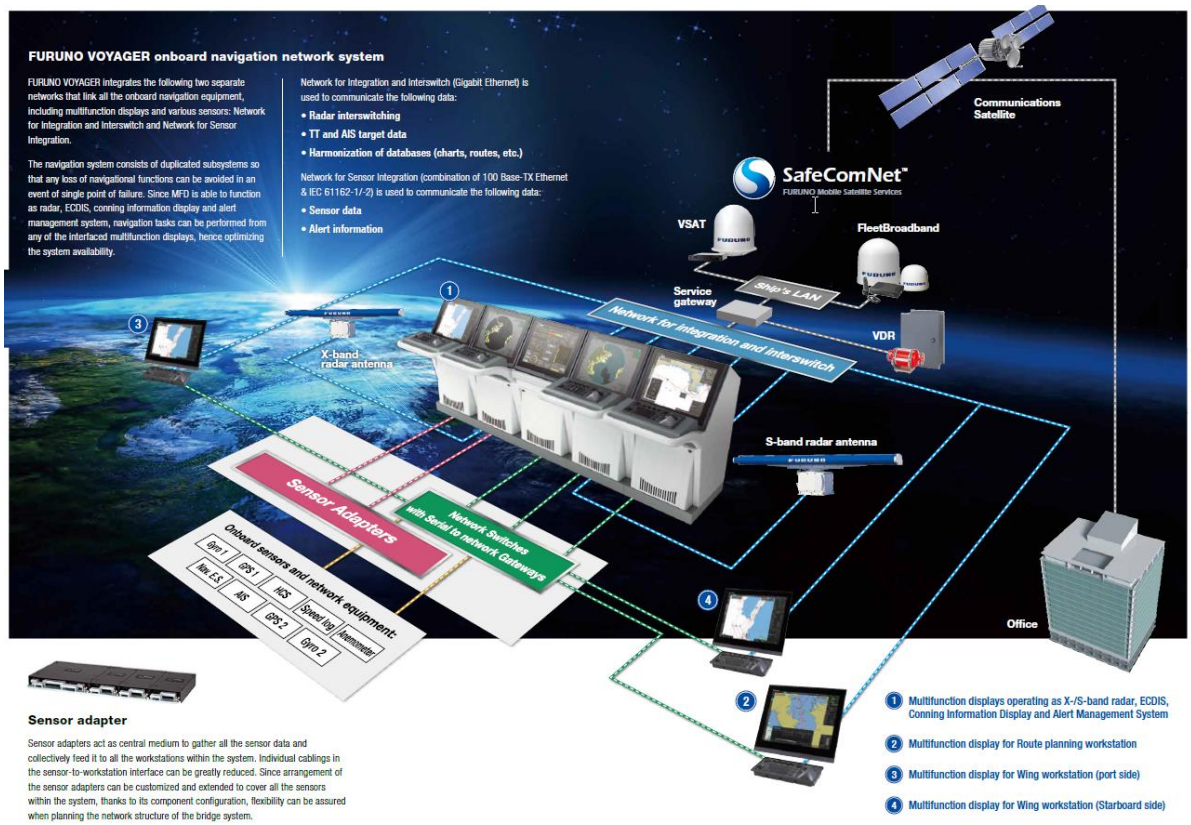

Figure 2: Onboard navigation network system
[source http://www.furuno.com/en/business_product/merchant/product/voyager/]

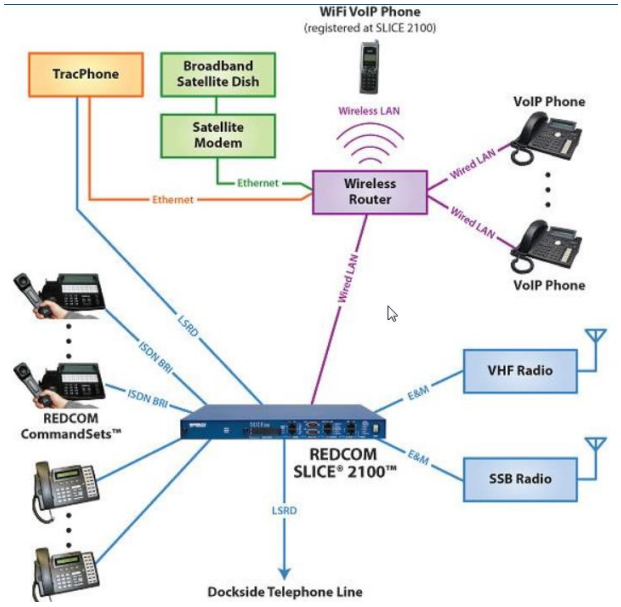

Figure 3: Typical onboard VoIP system
[source http://www.redcom.com/markets/shipboard-communications/]

The cyber security research community has now turned its eye on the maritime industry, and research is being conducted against the software and hardware that forms a crucial part of vessels' systems. The recent exposure of several vulnerabilities found in Automatic Identification Systems (AIS), and methods for attacking them [2], is an indication that general interest is growing. Such interest will inevitably attract those with malicious intent.

These vulnerabilities are of great concern as increasing satellite connectivity such as the roll out of Ka Band [3] offering high-speed broadband services around the world at speeds of up to 50Mbps. at sea, is resulting in ubiquitous, fast, and cheaper connectivity. These stable and fast connections make compromise of vessel systems easier than ever before.

The increasing threat to maritime security and integrity has been recognised by the community, and the United Kingdom Hydrographic Office (UKHO) has released information security standards (S-63) concerning Electronic Navigational Charts (ENC) distribution systems, with which chart distributors now have to comply. These have subsequently been implemented in their ADMIRALTY Vector Chart Service (AVCS).

S-63 is an industry standard cryptographic system which provides hydrographic offices and ECDIS manufacturers with the tools to protect ENCs, and which authenticates the originator of the charts so that end users can be assured of the source of their data [4][5].

These are first steps to address the integrity of one particular aspect of shipboard systems, however much more needs to be done to improve information and cyber security within the maritime industry.

2.2 ECDIS Software Connectivity

ENCs form a crucial part of the system that is used by navigation officers to steer and plot the course of vessels. Due to recent regulation changes, all vessels are now required to carry and use ECDIS. Although ECDIS brings many benefits and provides great assistance with navigation, it also represents an increasing attack surface and thus introduces risks that shipping companies, navigation officers, and the maritime community in general should be aware of.

An ECDIS system is, in NCC Group's experience, typically a workstation PC, usually running Windows XP, which is installed on the bridge of a vessel. There are sensor feeds connected, typically including radar, Navigational Telex (NAVTEX), Automatic Identification Systems (AIS), Sailing Directions, Position Fixing, Speed Log, Echo Sounder, anemometer, and fathometer. These sensor feeds are often connected to the shipboard LAN (via special serial/NMEA to LAN adaptors), which in turn has a gateway to the Internet.

ENCs are loaded in to ECDIS and used by the navigation officers to plot the course, navigate, and monitor the voyage progress, speed of the vessel, and many other crucial indicators. These charts are either downloaded on to ECDIS directly via the Internet or loaded from CD/DVD or USB memory disk manually by the personnel.

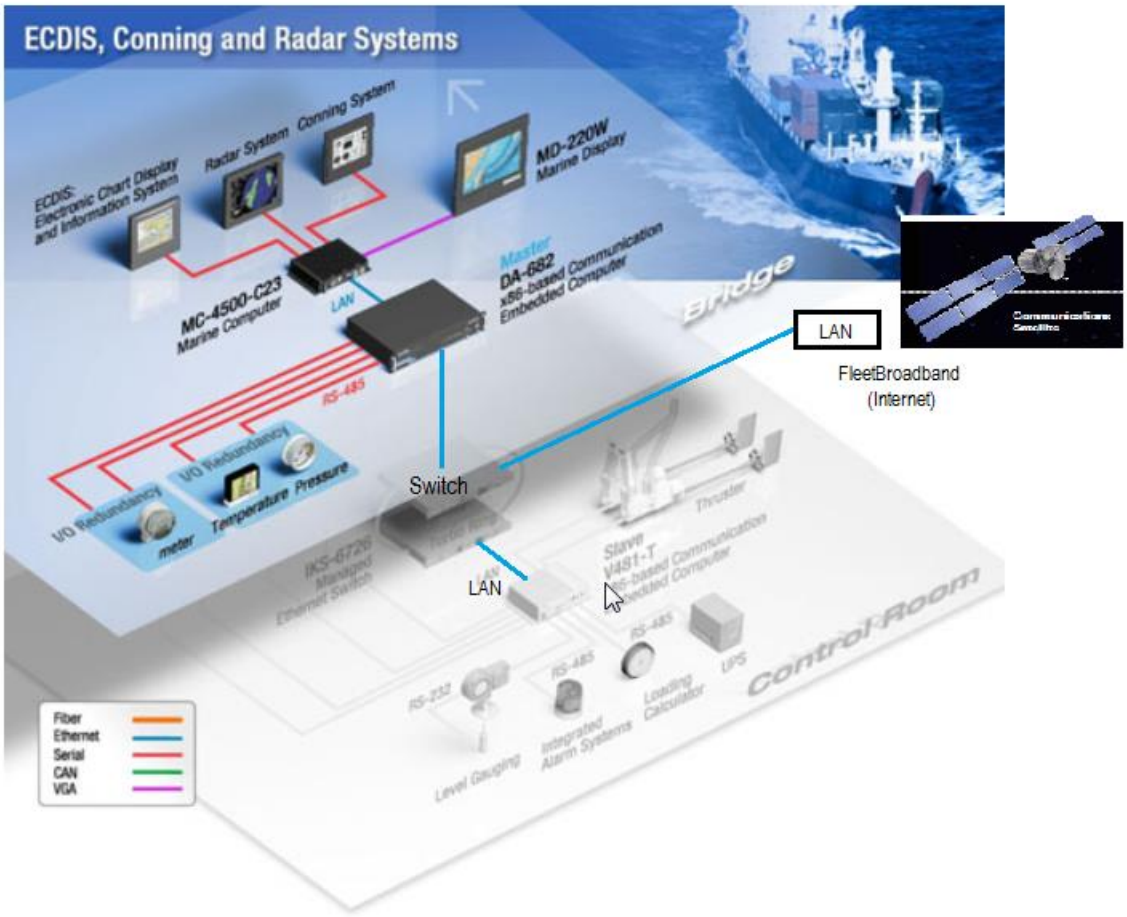

Figure 4: ECDIS, Conning and Radar systems
[source http://www.moxa.com/applications/Integration_of_Maritime_Systems_with_Industrial_Computers_on_the_Bridge.htm]

As a result of the connections to external systems and sensors, the ECDIS workstation becomes a highly connected convergence point for navigation. These data sources not only provide valuable information but also are conceivably viable attack vectors.

2.3 Effect of an ECDIS Compromise

Ultimately, ECDIS compromise could lead to the loss of life, environmental pollution and big financial losses[6]. The connectivity between the critical systems and the office and communication platforms (Microsoft Office, email, VoIP and Wi-Fi access), combined with the access to the Internet, could allow attackers to gain unauthorised access. This access could be achieved by various means, such as the introduction of a virus via portable USB disk by a crew member, or the exploitation of an unpatched vulnerability via the Internet. Once such unauthorised access is gained, attackers could be able to interact with the shipboard network and everything to which it is connected.

Once access has achieved, it might be possible to:

- Subvert sensor data and misrepresent it to ECDIS. This could influence the decision-making process of navigation personnel, and possibly lead to collision or the ship running aground.
- Steal ENCs.
- Compromise local area network and gain access to other data.

2.4 ECDIS Software Vulnerabilities

Research that NCC Group conducted against the available ECDIS demo product of one the major ECDIS manufacturers has revealed several serious trivial security shortcomings, weaknesses, and vulnerabilities.

Research has been conducted using stand alone, up to date Windows 7 (x32) machine with the basic default configuration and no antivirus or firewall protection.

During this research project several serious vulnerabilities were identified:

- **Directory Traversal**

ECDIS was found to be running a local Apache Web server which was vulnerable to directory traversal attack. This weakness allowed NCC to browse, list and download any of the files stored on the Windows 7 machine.
An example of opening win.ini file would be using following URL to access files:

```
http://10.0.0.1:50000/apps/sailor/..\..\..\..\..\..\..\win.ini
```

Where 10.0.0.1 IP address of the ECDIS machine.

- **Dangerous HTTP Methods Allowed**

ECDIS Apache Web server that was running on TCP port 50000 allowed `PUT` and `DELETE` HTTP Methods. This vulnerability allowed NCC to upload, delete or replace any file located on the ECDIS Windows 7 system.

Using a tool called Curl NCC was able to upload the file as shown below:

```
curl –i –X PUT –T /upload.file http://10.0.0.1:50000/apps/sailor/
```

- **Outdated Apache Web server software**

ECDIS system was running outdated Apache Web Server software which had multiple vulnerabilities and weaknesses associated with it such as directory traversal vulnerability (described earlier) and Denial of Service. Also, Apache Xerces version 2.0 was found to be in use which suffers to numerous vulnerabilities too.

- **HTTP Header Injection.**

Apache Web Server that was used by ECDIS system was found to be vulnerable to HTTP Header injection attacks. NCC was able to inject malicious content in to the “host=” parameter within the HTTP headers using the following POST request:

```
POST /config/ HTTP/1.1
Host: 10.0.0.1:50000
User-Agent: Mozilla/5.0 (X11;Linux)Gecko/2010010 Firefox/22.0
Accept: text/html, application/xhtml+xml,application/xml;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```



```
Referer: http://10.0.0.1:50000/config
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

Host=<malicious payload here>&service=service&section=1&type=int&value=1
```

3 General Remediation Recommendations

General recommendations for minimising or mitigating the risks highlighted in this paper are:

- ECDIS developers should look to adopt Security Development Lifecycles.
- Processes and procedures should be put in place to document, monitor, and patch the ECDIS software and its underlying system on a regular basis. Build reviews should be conducted periodically to establish a secure baseline, and when using any third-party software, processes should include the installation of security patches as they become available from the vendor.
- The update process for ECDIS charts should be monitored and logged, especially where manual updates are performed via CD or Flash USB disk. All update files should be scanned using antivirus software at the very minimum.
- The internal network infrastructure to which ECDIS is connected should be reviewed to establish if the ECDIS system could be completely segregated or otherwise firewalled.
- Physical access to ECDIS and its underlying components should be limited to the appropriate personnel only.

4 Future Areas of Research

It is evident that steps are already been taken to address the existing risks however in ever evolving technology world these steps need to be re-assessed and re-tested on the regular basis. All technology that is currently in use by the industry be it ENCs distribution system or types of Wi-Fi Access points installed on board of a vessels should be assessed and tested from the security point of view. In particular following areas of research should bring interesting results:

- Research in to wider network & hardware configurations and deployment of a variety of shipboard networks and interconnectivity from cyber security point of view.

This will include:

- Security assessments of a shipboard networks.
- Security assessment of all the associated devices such as Satellite Routers, Switches and Firewalls are connected to ECDIS in one way or another
- Security review of all other devices such as “Serial-to-Lan” adaptors used to feed the sensor data to ECDIS.

Research the possible development and introduction of certification processes for cyber security in relation to maritime systems.

- Applicability of existing accepted certification processes.
- Development of industry specific standards and certification processes.

5 Conclusions

The security vulnerabilities discovered during this research should not come as a surprise given the little prior research attention. Manufacturers are currently relying on the fact that access to ECDIS systems on vessels is somewhat restricted as their major method of risk mitigation. This is inadvisable; however, as viable attack entry points still exist to the system – be it USB memory stick, sensor compromise, or via other systems connected to the vessel's local area network.

In NCC Group's experience it is common for ECDIS to be connected to the internal network while also being connected to the Internet (thus creating a bridge between internal and external systems) in order to download data such as ENCs and other software updates via the satellite link. These methods of connectivity, which introduce significant risks, are preferred by some manufacturers. For example, in the case of a flat LAN, other PCs, servers, or Wi-Fi access points could exist on the same network segment with no firewall in place, providing entry points and increasing the attack surface.

It is reasonable to expect that such systems will be targeted in the near term by more sophisticated threat actors, if indeed they have not already been targeted. Therefore NCC Group recommends that more attention should be drawn to the security of such software products and the systems they are deployed upon.

6 References and Further Reading

1. Electronic Chart Display and Information System
   http://en.wikipedia.org/wiki/Electronic_Chart_Display_and_Information_System
2. Attacking Vessel Tracking Systems for Fun and Profit
   http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf
3. Ka Band Satellite Connectivity
   http://blog.admiralty.co.uk/2013/06/24/meeting-the-latest-data-protection-standard-for-digital-charts-2/
4. ENC Encryption
   http://en.wikipedia.org/wiki/S-63_%28encryption_standard%29
5. Meeting the latest data protection standard for digital charts
   http://blog.admiralty.co.uk/2013/06/24/meeting-the-latest-data-protection-standard-for-digital-charts-2/
6. Grounding of a US warship
   http://www.pilotmag.co.uk/2013/02/24/ecdis-update-kevin-vallance/#more-6557
7. IMO SOLAS
   http://www.imo.org/About/Conventions/ListOfConventions/Pages/Default.aspx

