nccgroup
freedom from doubt

RESEARCH INSIGHTS

Sector Focus: Maritime Industry

Author: Yevgen Dyryavyy

CONTENTS

All Rights Reserved. © NCC Group 2015

AUTHOR

YEVGEN DYRYAVYY

Yevgen is a security consultant at NCC Group with more than ten years technical IT experience. For the past six years he has held a number of positions in the information security industry. Yevgen participated in the development of information technology risk assessment software which is being used by blue chip companies, and is a committee member at the British Standards Institute (BSI), covering all technical aspects of maritime navigation and radio communication equipment and systems (EPL/80 Work Group 6).

All Rights Reserved. © NCC Group 2015

INTRODUCTION

In an increasingly connected world, cyber security is more important than ever. NCC Group, a world leading information security assurance company, regularly investigates the susceptibility of non-traditional systems to attack, in order to help raise awareness of the risks to these systems and to provide guidance on how they may be secured. Computerised systems that are present on board a vessel suffer from many of the same vulnerabilities as traditional systems, but these shipboard systems also require a non-traditional approach to security testing and risk assessment. Some of the security issues that specifically affect offshore maritime technology environments include:

- Insufficiently protected and maintained software on board a vessel.
- Misconfigured shipboard communication and navigation networks.
- Navigation software and software that is used to control other devices and hardware, that is not developed in line with best security practices and as part of a secure development lifecycle (SDLC).
- Computerised vessel systems (propulsion and others), legacy industrial control systems (ICS) and SCADA systems with well-known weaknesses and vulnerabilities.
- Computerised vessel access control systems such as CCTV, bridge navigational watch alarm systems (BNWAS), shipboard security alarm systems (SSAS), electronic “personnel-on-board” systems.
- Cargo control systems in which computer networks are interconnected with sensor switching networks.
- The apparent widespread use of USB storage devices to share data between different, unconnected systems on a ship.

Due to the great diversity of maritime systems and their presence in various configurations onboard a vessel, and the fact that the ownership and maintenance contracts for these systems vary significantly, the potential for cyber security weaknesses is high. This document aims to illustrate some of the possible security issues that the maritime industry currently faces.

All Rights Reserved. © NCC Group 2015

MARITIME CYBER SECURITY

The cyber security research community has started to investigate [1] systems within the maritime industry and research is being conducted against the software and hardware used within critical components of vessels' systems. While it has been known for some time that automatic identification systems contain vulnerabilities, and these are being addressed by the industry, it is only recently that they have been successfully exploited [2] using easily available software defined radio technology and open source software. This is an indication that general interest is growing; such interest will inevitably attract those with malicious intent.

Insufficiently protected and maintained software on board a vessel

Electronic Chart Display and Information System (ECDIS) is one of the critical components used in navigation to augment paper-based 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 Organisation (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.

"General interest in exploits is growing; such interest will inevitably attract those with malicious intent."

It is understood that the majority of ECDIS installations are on Microsoft Windows-based systems running on conventional hardware; sometimes even off-the-shelf personal computers are used and interconnected using Ethernet LAN technology. This means that all the traditional risks associated with software and network security are present. Research performed by NCC Group [3] suggests that popular ECDIS software, if the version installed is the same as the demonstration version available to the public, is vulnerable to attack via services exposed to the network.

Misconfigured shipboard communication and navigation networks

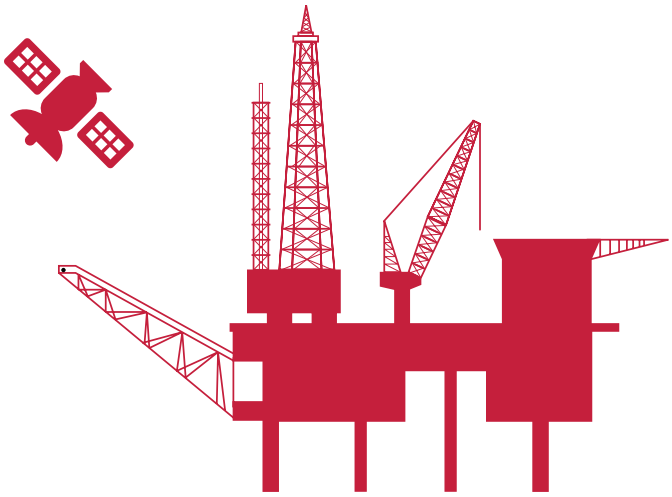
Where on-board systems and networks are installed or retrofitted, maintained and supported by different parties, there is always a risk of vulnerabilities being introduced either intentionally or otherwise. Networks could be bridged and new attack vectors introduced to a network that is otherwise secure.

Software development best practices and SDLC

In scenarios where outsourcing software development is a common business practice, new risks are introduced through inadequate quality assurance testing or by not adopting best practices with respect to secure design and development. Software that is not developed in line with a secure development lifecycle (SDLC) is more likely to be vulnerable to cyber attack, and because security has not been considered throughout the development process, any security-related design flaws are often very costly to fix retrospectively.

[1] http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/
[2] 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] https://www.nccgroup.trust/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

All Rights Reserved. © NCC Group 2015



Industrial control systems with well-known software vulnerabilities

Ships that were built many years or decades ago using the technology that was available at the time are still in use. While that technology was considered secure when it was installed (to the extent that security was not considered at all), much of it is vulnerable to more recent threats. This represents a serious risk to outdated systems which are difficult to replace, such as ICS/SCADA systems used for the engine and propulsion control. These security challenges are starting to be addressed by other industries that use similar technologies, such as power generation and oil & gas, using segregation and protocol-aware filtering techniques.

Computerised vessel's access control systems

Physical access controls on vessels are often well implemented and audited. However, the introduction of computerised systems such as CCTV, bridge navigational watch alarm systems (BNWAS), shipboard security alarm systems (SSAS), electronic "personnel-on-board" systems, has resulted in new risks and new attack vectors.

The impact of exploiting any identified weaknesses within these systems could be wide-ranging. Such weaknesses are of great concern due to the increasing speeds of satellite connectivity, with technologies such as Ka-Band [4] now offering high-speed broadband services at sea.

These fast, stable, Internet connections make exploitation of vulnerabilities and compromise of vessel systems easier than ever before. Any interconnected shipboard system will be viewed by remote attackers as an attractive target either to expand their botnets or for conducting a targeted attack against specific vessel systems.

Cargo control systems

If the sensor networks associated with cargo control systems are not properly segregated from other networks and systems onboard vessels then a cyber attack mounted via the Internet against something seemingly innocuous, such as an email terminal, could become more serious.

If sensor data, for example, was manipulated by an attacker, this could result in damage and ultimately financial loss.

"Any interconnected shipboard system will be viewed by remote attackers as an attractive target."

Data sharing with USB storage devices

There is currently widespread use of USB storage devices to share data between different systems onboard vessels. As a result there have been a number of documented [5] and anecdotal cases of malware infection on ships and rigs which have resulted in significant financial loss. The potential dangers of the use of USB storage devices within the corporate IT world have been known for some time and here the maritime industry is behind the curve with respect to employee cyber security awareness and best practice.

[4] http://www.inmarsat.com/service/global-xpress/
[5] http://www.aiche.org/chenected/2013/03/malware-infects-gulf-mexico-offshore-rigs

All Rights Reserved. © NCC Group 2015

Current status and conclusions

The increasing threat to maritime cyber security and integrity has been recognised by the community and various initiatives are underway. The US Coast Guard "Guidance on Maritime Cybersecurity Standards" [6] represents an attempt to collate and analyse all the information security-related material which will be used in production of possible maritime cyber security standards.

Existing International Electrotechncial Commission (IEC) published standards (61162-450) provide some guidance on the security of navigational networks. The IEC is also working on the 61162-460 standard which will provide detailed guidance on building and interconnecting bridge navigation networks and equipment in a secure manner.

NCC Group has recently become a member of the Comité International Radio-Maritime (CIRM) in order to assist the maritime industry by offering cyber security assessment services, best practice guidance and awareness training.

These are the initial steps to address the cyber security risks associated with shipboard systems; however, much more needs to be done to improve information and cyber security within the maritime industry. Significant work still needs to be done to assess the cyber security posture of those systems on board vessels that are already in service.

NCC Group has also seen new features of mobile platforms open up categories of issues which developers are failing to defend against. With mobile devices storing an ever increasing amount of sensitive data about our lives and work, it is more important than ever to ensure this data is being adequately protected.

"The increasing threat to maritime cyber security and integrity has been recognised by the community, and various initiatives are underway."

[6] https://www.federalregister.gov/articles/2014/12/18/2014-29658/guidance-on-maritime-cybersecurity-standards

All Rights Reserved. © NCC Group 2015

CONTACT US

0161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Cheltenham

Edinburgh

Glasgow

Leatherhead

London

Manchester - Head office

Milton Keynes

Europe

Denmark

Germany

The Netherlands

Switzerland

North America

Atlanta

Austin

Chicago

New York

San Francisco

Seattle

Sunnyvale

Asia Pacific

Sydney

www.nccgroup.trust
@nccgroupplc

All Rights Reserved. © NCC Group 2015