Proceedings of the 18th International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2016
September 18-23, 2016, Kobe, Japan

Paper No. 4033

Cyber Security in Transport

Author: Mr Rakesh Burgul

Chief Information Security Officer
International Nuclear Services
Risley, Warrington
Cheshire
United Kingdom

Abstract

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Whilst the layman's view of cyber security tends to involve purely technical disciplines, in actual fact, it is everything that contributes to the protection of systems and data. For example, security culture is a key security control in cyber security and relates to the proper behaviour of individuals in protecting systems and data.

This paper will focus on the relatively new specialism of Maritime Cyber Security (MCS) and will discuss whether cyber security is an issue that nuclear transporters should be worried about. In doing so, it will be necessary to discuss potential consequences of successful or even unsuccessful cyber-attacks.

It will also discuss the potential threats to the maritime industry and will opine on the probability of such threats manifesting.

The paper will detail potential vulnerabilities for ships systems and illustrate these through the use of examples of maritime cyber-attacks that have already occurred. Research work that has already been carried out will be referred to which demonstrates clear vulnerabilities in various ships systems such as GPS, SatCom and AIS. In addition, novel and asymmetric attack possibilities such as the hacking of ships WiFi systems, USB malware attacks and Supply Chain attacks will be discussed. In principle, all these attack vectors are already known about within the context of conventional IT networks and Industrial Control Systems and there is nothing particularly different from a technical perspective where transports are concerned. However, cyber-attacks on transport mechanisms or mechanisms which support transport may require some lateral thinking on the part of the defender due to the changing nature of, for example, a ships surroundings.

This paper will propose a four-phased approach to resolving such issues in non-conventional networks and industrial settings.

Whilst this paper deals primarily with Maritime Cyber Security, it will finish by establishing that the attack vectors, security principles and mitigations discussed may be equally applicable to other modes of transport such as land and air.

Introduction

International Nuclear Services (INS) has over 40 years' experience of safely and securely delivering Category I transports and other nuclear materials with pride[1]. INS must comply with multiple requirements from multiple stakeholders but in addition must service moral and ethical duties in a manner that exhibits diligence, integrity and engagement with the global community.

The global context of INS's works mean that INS cannot work in isolation and therefore engages with its stakeholders to provide safe and secure services. This necessarily requires INS to communicate and interact and in common with all organisations, INS uses computer systems to help enable service provision and communication. In doing so, INS relies on the Confidentiality, Integrity and Availability (CIA) of information. These concepts are introduced below.

Before introducing the CIA concepts, it will be useful to note that classically, cyber security is applied to IT systems and networks however, over the last few years, there has been a growing threat vector against Operational Technology (OT) systems. These are systems such as industrial and plant control systems. This is important in the context of INS and this will be discussed later in this paper. You are invited to note that this paper will not discuss any specific threats and vulnerabilities to INS marine vessels.

It will not escape readers that the use of computer systems has benefits but comes with risks. There is not a day that goes by that we do not hear about the latest hack of a computer system by adversaries and the subsequent compromise of information. Information is at the heart of what INS does and INS recognises that the compromise of its sensitive information could have serious consequences. For example, the compromise of dates, times and routes for nuclear shipments will be of interest to our adversaries. INS therefore takes every effort to protect the confidentiality of its information from its adversaries in order to fulfil its duties securely and safely.

However, confidentiality is not the only property of information that INS wishes to manage. If INS acts on information that it cannot rely on because it doesn't trust the information, then the provision of assurance to stakeholders such as Regulators becomes difficult if not impossible. We therefore introduce the concept of integrity of information. That is, assuring ourselves that we maintain the accuracy and completeness of information. The compromise of integrity of information can also have serious consequences. If we cannot rely on the information and data related to safety cases, then we cannot for example demonstrate adequate safety cases for nuclear packages to regulators and therefore operations will stop.

The final property of information that INS manages is availability. This is defined as the ability to access the information when it is needed. If an adversary were able to affect our ability to access our information, we would be unable to provide certain services such as emergency response.

[1] http://www.innuserv.com/2016/03/ins-plays-another-key-role-in-international-non-proliferation-mission/

Different organisations will rely on these different properties to different extents depending on their business. A company providing web services such as Amazon or eBay will require their information and services to be accessible to a very high degree and therefore these companies implement high-availability systems. Governmental security organisations will operate systems that require very high confidentiality. Organisations that rely on their data to demonstrate compliance will require high integrity systems.

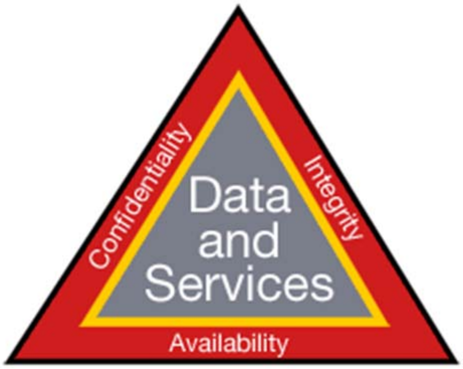

Figure 1 – The CIA triad of cyber security

This balance between the three properties has to be understood by organisations and by cyber security professionals who base their work on it.

The CIA triad is one foundation for cyber security. Another is risk appetite. Risk appetite is defined as the risk that is tolerable before embarking on a course of action or organisational objective. Generally speaking, low risk appetites result in systems with high levels of security control. For example, INS has a very low risk appetite when it comes to a class of information known in the UK as Sensitive Nuclear Information (SNI) and which is regulated by the Office for Nuclear Regulation (ONR) under the Nuclear Industries Security Regulation (NISR)[2]. In other words, INS is not willing to take risks which might compromise SNI and therefore builds many security controls around SNI to protect mainly its confidentiality but also its integrity and to some degree, its availability.

By introducing the concepts of confidentiality, integrity, availability and risk appetite, we have the foundations for a cyber security programme.

The author commends readers to think about these concepts and decide where the CIA balance is for their organisation. In conjunction with risk appetite, readers may be able to understand why their organisation implements certain security controls.

Cyber Security Threat

The cyber security threat can broadly be summarised in table 1

[2] http://www.legislation.gov.uk/uksi/2003/403/contents/made

Threat	Intent	Capability
Script Kiddies – amateurs who use publicly available hacking tools	HIGH	LOW
Hactivists – individuals with a social or political motivation	HIGH	MEDIUM
Competitors	MEDIUM	HIGH
Criminals	HIGH	MEDIUM to HIGH
Terrorists	HIGH	LOW
Insiders	HIGH	HIGH
Foreign Intelligence Services	HIGH	HIGH

Table 1 – Cyber Threat Landscape

We can debate the categorisation but there are two important points to note here. Firstly, and ironically, the table suggests that one of the first places to look for your highest cyber threat is within your own company. Logically this is reasonable since these individuals have already penetrated some of your security controls (they were given legitimate access) and their motivations change, usually unpredictably and sometimes against the organisation. Here we introduce the concept of Insider Threat. In some cases, insiders may be technically proficient (for example, IT staff) and the potential for these individuals to harm your organisation is extremely high. Usual security controls around this threat are security vetting, separation of duties and the “two-man-rule”.

Secondly, there is an ongoing discussion around capability. It is the author’s view that since expert computer hackers are selling their services and hacking is now commoditised, then by default, the capability of all adversaries is high since they would simply buy hacking services. This is especially true if the adversary has a high intent and is also highly motivated. The only thing stopping these individuals is access to funds and traceability.

Cyber Security Risk

An organisation cannot and should not address all cyber risks, all of the time, uniformly. This would cost huge amounts of money for little return and does not represent a good value proposition. It is better to rank cyber risks and treat them against a risk appetite. Cyber risk is defined as the probability that a cyber threat will exploit a vulnerability resulting in an unintended consequence. It has been variously represented thus:

$$\text{Risk} = \text{likelihood} \times \text{susceptibility} \times \text{consequence}$$

Using this formula, it is possible to prioritise cyber improvements and obtain a better return on investment.

Fundamental Tenets of Security

It is useful to state some basic truths in the world of security. These help to frame ones risk approach to security. These rules are:

- *There is no such thing as 100 per cent security.* We must accept that if an authorised individual can access an asset, then given enough time, money, resource, skill, motivation and intelligence, then others who are unauthorised will be able to as well.

- *In order to get security, you must give something up.* This alludes to the fact that increasing the security within a system generally requires some combination of; investment, effort, resource, loss of liberty, loss of time. For example, when Richard Reid (the shoe bomber) tried to set off a bomb on an aircraft by hiding it in his footwear, the world of security reacted by requiring passengers to remove their footwear or otherwise have them searched. We lost time and freedom standing in security queues so that we had extra security assurance around passenger's footwear.

- *Build Defence in Depth.* Security works when it is built in layers. In the same way that safety is built in layers for transport packages (fuel is sheathed, placed in an assembly, which is placed in a container, which is sealed in a flask and so on), security is much more effective when layered similarly. If intelligence fails, the fence will pick up the threat. If the fence fails, the security guard will face the threat. If the security guard fails, the full-height turnstile will provide protection. If the turnstile fails, staff will challenge and so on.

- *Put yourself in the mind of the adversary.* Security solutions are easier to devise when you "think like the bad guy". Asking yourself "how would I get in if I didn't need to follow the rules and if I didn't want to get caught?" generally exposes vulnerabilities much easier and it is therefore easier to devise security countermeasures. This is sometimes referred to as the security mindset. Rather than thinking about how a system works, think about how it could fail. Thieves walk into shops and think about how they could shop lift. Hackers look at systems and programs and wonder how they could break them. Engineers do this using Failure Mode and Effects Analysis (FMEA). Security professionals must therefore think similarly in order to build more secure systems.

- *Security is very different to safety.* In the safety world, we deal almost exclusively with "accident" scenarios. The controls that are implemented are therefore designed to prevent accidents from occurring. In the context of nuclear shipments, our threat is almost exclusively an adversary's "deliberate" attempt to cause harm and our controls are designed against an adversary who is actively looking to make something go wrong.

Thus far, I have very generally addressed threat, vulnerabilities, risks and risk appetite. Whilst it's useful to talk about these and address them organisationally, one should only do so in the context of consequences.

Consequences

If your risk analysis points out a high risk, it does not necessarily mean that mitigation is required. As an example, Global Positioning Satellites (GPS) provide members of the public (through their personal devices) and corporations (through their corporate systems), highly accurate geographical location information. INS vessels use GPS to help locate themselves globally. It would be reasonable to assume that if the GPS system was attacked by an adversary (and there is evidence that this has already happened to other organisations), then this could have serious consequences for anyone relying on the technology. However, if the primary means of navigation is physical charts, then there is no reliance on electronics and GPS and therefore little or no requirement to mitigate the risk of GPS systems failing. In actual fact, a mitigation for corrupted GPS is navigational charts. The consequence part of the equation is therefore very important in confirming or discounting mitigations to postulated threats.

Threats to the Maritime sector

Somali pirates regularly use marine tracking systems such as Marine Traffic[3] or Vessel Finder[4]. In fact, specific apps exist that allow anyone to follow the course, speed and other details of marine vessels. In the face of such a threat, the only counter is to either avoid the area, or switch off the locational system or spoof the system so that your vessel appears in a different location than it actually is. Military vessels usually switch off such systems. INS vessels are also authorised to switch off such systems when on the high seas.

In 2011 and over a 2 year period, drug traffickers recruited hackers to infiltrate the Port of Antwerp’s IT systems. The hackers were able to access the location of specific shipping containers allegedly containing drugs. The traffickers were then able to remove the containers using lorries and the hackers deleted the existence of the containers from the IT system[5].

In 2013, hackers infiltrated the control systems of an oil rig and disabled it by tilting it[6].

In 2013, the University of Texas demonstrated that they could get a 210-foot super-yacht in the Mediterranean Sea to change course by using a spoofed GPS signal.

Researchers have found various vulnerabilities in key marine technologies; GPS, marine Automatic Identification System (AIS), and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS).

The cyber security company Rapid7 found more than 100,000 devices which were connected to the internet using serial ports with poor security.

[3] http://www.marinetraffic.com
[4] https://www.vesselfinder.com/
[5] http://www.bbc.co.uk/news/world-europe-24539417
[6] http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424

One commonality that all these systems share is connectivity. It is generally true that the greater the connectivity to the internet, the greater the threat to the system. Conversely, systems that are not connected to the internet face a much reduced threat although even these systems are still vulnerable. This was starkly illustrated by the discovery of Stuxnet[7]. Discovered in 2010 by a cyber security company, the Stuxnet malware was so complex that it was thought to be the world's first cyber weapon. Close analysis by various experts led to the conclusion that Stuxnet had only one solitary purpose; to damage and delay the Iranian nuclear enrichment programme. Interestingly, the Industrial Control System running the Iranian enrichment facility was not connected to the internet. Successful implementation of Stuxnet therefore required the malware to cross the "air gap" between the internet and ICS. This was achieved by using a human being and an infected USB stick. Not even physical separation will protect you.

The website *shodan.io* provides its users (anyone can register) with lists of vulnerable devices that are connected to the internet. These could include every day technology such as internet connected fridges, washing machines and other home technology to Industrial Control Systems, traffic lights and other transport systems such as trains, cars and marine vessels.

Direct cyber-attacks are of course a concern but by using the security mindset, it is also possible to see how attackers can use "blended attacks" or indirect methods to achieve their aim. For example, even if there is physical segregation between a corporate IT network and an industrial control system, it could be possible for an attacker to attack and compromise the corporate network, identify the location of operating procedures and change the procedures such that for example "Close valve A" reads "Open valve A".

It is the authors assertion that a cyber-attack on an INS vessel, whether successful or unsuccessful, would have significant reputational impact on INS which could range from insignificant to major with a range of stakeholders taking an interest not least of which are members of the public, governments and global media. We have already seen that such attention in the world of nuclear can affect global nuclear policy and therefore INS has set a very low risk appetite for cyber-attacks.

In the face of such threats & vulnerabilities and publically available intelligence and in the light of the potential consequences of successful exploitation, INS has completed a cyber security review of its marine environment. We cannot detail the results of this review but it is useful to talk about the methodology used.

Cyber Risk Reviews

The physical security methodology of understanding and analysing threats, vulnerabilities, motivations, capabilities and consequences works just as well in the virtual world. There are many standards and methodologies available some of which rely on baseline compliance and some of which rely on risk management. These are illustrated in table 2.

[7] https://en.wikipedia.org/wiki/Stuxnet

Cyber Security Methodologies	
Compliance Based	Risk Based
Cyber Essentials/Cyber Essential+ (5 critical controls)	ISO 27001 and 27002 (International)
UK 10 Steps to Cyber Security (10 critical controls)	The Information Security Forum Standard of Good Practice (International)
SANS 20 Critical Controls	National Institute for Standards and Technology Cyber Security Framework (US)
Many others	Information Security Manual (Australia)
	ETSI Cyber Security Technical Committee

Table 2 – Cyber Security Methodologies

The decision on which methodology to use can be determined based on many factors:

- Am I mandated to comply with a standard?
- Is my system a corporate network or an Industrial Control system?
- Is it simple or complex?
- Is my system a high Confidentiality, Integrity or Availability system?
- Is it connected to the internet?
- Who are my threats and how capable are they?
- What are the consequences if I get it wrong?

In short, if your system is complex, connected to the internet and its threats are nation state actors with high capability where successful exploitation of your network would result in very serious national or international consequences, then it is unlikely that simple security controls on the upper left hand side of table 2 will be sufficient. Different nations take different approaches. In the United States, the Department of Energy depending on the answers to questions like the ones above, requires operators to comply with different sets of cyber security controls. In the United Kingdom, the Office of Nuclear Regulation has taken a different approach which is risk-based. As long as civil nuclear operators in the United Kingdom (including INS) can demonstrate that they have taken a thorough and demonstrable risk-based approach and have implemented cyber security controls that perform as expected, then operators are free to use any methodology they chose.

INS has chosen an ISO 27001 based methodology which essentially consists implementing an Information Security Management System, some elements of which are:

- Identify your assets
- Show the threats, vulnerabilities and consequences against these assets
- Quantify the cyber risks
- Mitigate the risk using appropriate security controls
- Show that controls are working
- Review
- Improve

Strategically and generically, a four-phased approach to the issue of cyber security is posited by this paper that is suitable for all organisations of any size. It is the author's view that successful implementation of a cyber programme must include:

1. **Leadership** – No organisational initiative will be successful without senior understanding and sponsorship but in addition, the appropriate competence
2. **Discovery** – Organisations must have a full and managed inventory of networked and non-networked IT and OT assets and in particular, must understand their connectivity especially to the internet
3. **Risk Management** – Organisations must understand their business, regulatory and stakeholder environment and in particular, must understand and agree their appetite for risk at the highest level of the organisation in order to decide on cyber security standards and controls
4. **Culture** – At the heart of most cyber incidents globally, is the failure of a human being to either understand that a credible risk exists (thereby behaving incorrectly) OR a failure to comply with procedure. It is therefore vitally important that the organisation builds a cyber security aware culture. Preferably, this should be aligned to other cultural initiatives in order to fully exploit any synergies

Relevance to PATRAM

Much of the information that INS processes has a high confidentiality requirement. However, in the example of safety cases for transport packages or engineering and financial modelling data, this information requires very high integrity. Failure to implement integrity controls will result in a failure of engineering conclusions or safety cases. For PATRAM organisations reliant on such properties of their data, failure to deliver on them could result in very serious consequences to the business due to loss of confidence or worse, physical manifestations of, for example, package failure. As has already been discussed, these manifestations could have a global impact.

Conclusions

Businesses with an online presence and even those who are physically segregated from the internet are vulnerable to cyber attack.

The skills to carry out complex cyber-attacks are becoming increasingly widely available or commoditised. Therefore, their severity and frequency is increasing.

The complexity of attacks is increasing to such a degree that cyber professionals now assume that if an attacker is motivated enough, capable enough, intent enough and has enough resource, then their attack is likely to be successful. This therefore moves the focus from cyber-risk management to incident management. Increasingly, cyber professional are concentrating on identifying compromises and acting swiftly to manage an incident forensically in order to identify and cleanse the system of an attacker. Some organisations are going a step further and are implementing false or ghost networks called "honeypots" in which attackers think they have penetrated a corporate network but they have actually only penetrated a honeypot. Sophisticated organisations are using a technique that is known as "threat hunting" and are essentially counter attacking in order to try to identify attackers and certainly to deny them further access to corporate networks.

The consequences of cyber-attack will be different for different businesses but in the nuclear transport world, they may be particularly serious to the degree that global nuclear policy is affected.

Businesses must acknowledge that they will be affected by cyber-attacks whether or not they are connected to the internet and they must therefore adopt a structured approach to resolving it which is appropriate to their organisation.

Other nuclear transport platforms such as rail and road may also be susceptible and organisations must ensure that their cyber security programme includes all IT equipment in all situations.

Ignore your staff at your peril. One of the keys to successful cyber security is the correct behaviour of staff. Therefore a good (appropriate) security culture is paramount.

An air gap will not protect you.

Acknowledgments

INS would like to thank the Office for Nuclear Regulation (ONR) and the Nuclear Decommissioning Authority (NDA) for their expertise and support in striving for the appropriate standards of safety and security. The author would also like to thank the INS Executive as without their active support, INS cyber risk programme would not have been completed.

References

ISO/IEC 27001:2013, *Information Technology – Security Techniques – Information Security Management Systems - requirements*

Cabinet Office (2011), *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*

Department of Business, Energy and Industrial Strategy (formerly Department for Energy and Climate Change) 2016, *Civil Nuclear Cyber Security Strategy*

The Office for Nuclear Regulation (2016), *Cyber Security Objectives and Regulatory Expectations*

The Information Security Forum (2016), *Standard of Good Practice*