eng.vessel_informational_security

Alexandr Kirilov (https://github.com/alexandrkirilov)

Vessel Informational Security

Before describing informational security issues need to be noticed few points:

- there are no nay security system that will make any warranty of 100% of being no-hacked, the technology stack is improving and there are always risk that someone smart and experienced enough will jump over
- you always should keep eyes opened for monitoring the system, any security precaution is only buying for you more time before being hacked
- in addition to defence system you should have the fence system and the system of avoiding of being hacked

All of written bellow based on this 3 points, for example:

- VPN - making difficult the process of monitoring network activity and as result making longer the process of attack preparation (if the time for preparing attack longer then the time of information being valid - no attack reasons at all)
- Encrypting messages between modules - making difficult to make an attack and buying some time for reaction against attacker
- Organised and defined procedures in real world by real company staff - the fence resources against attack and attackers, every involved in security procedures should know their own part at time of defending, like any drill on vessel.
- etc

All of problems described below related to the informational security on level of software and devices that using software. All of issues related to the physical principles level of informational security outside of this article.

0.1. Absence of vessel informational model, where vessel is the source of information

At time of writing this article author hasn't found any information about informational modelling vessel. There are nothing about testing the vessels systems for being hacked or theirs vulnerabilities. As a result there might be very surprised situation related to informational security.

To solve this issue possible by developing universal platform that is based reliable Operational System (if there need additional consultation about architecture solution - contact the author), that will allow to use vessel like informational

source or carrier of information. The informational security procedures should be looped like endless process that including kind of R&D issues for every device located on vessel.

0.1. Base Operational System

Almost every informational device on any vessel based on transistors and all of this devices has own Operational System. Based on rule - "the chain not stronger then weakest element of the chain", if Operational System on your devices vulnerable - you will never develop well secured application on it. The Operational System - THE KEY POINT FOR INFORMATIONAL SECURITY!!!

You might to check the Operation System that used onboard on this site www.cvedetails.com. This site specialised on vulnerabilities.

```
The author notice.
At time of contract in 2015 been very surprised by fact of
using Windows XP like background for the last and modern
generation of navigational system that is uniting all of
navigational resources in one. Beside all of it there was
totally opened data transferring over network between parts
of this navigational system.
For the question "Why this?" got reply: "Because there are huge
code inheritance and no-one will rebuild it". This reply very
illustrious for understanding when this kind of systems been
planing for developing. The informational technology moved
far far forward.
After this dialog between author and vendor support there were
more same OS discovering in modern vessels.
```

Partly this problem might be solved by organising vessel VPN but never the less if your operational system vulnerable the vessel system vulnerable too.

This kind of problems - the reason why been mentioning about developing platform based on secured operational system from begin.

And now again about FreeBSD and Linux-family, the point - LICENSE. All of matter described in article "Why FreeBSD?" and if you want to use the system of blockchain signals via TCP ports (example described in this article "Blockchain example. Connected servers, client-server implementation.") you will need to

implement code into existed, in case of FreeBSD you will do it freely, but in case of Linux you required to publish it openly. The code related to the private security should be published?

0.1. The messages between modules

Any vessel contain huge list of systems that using digital messages or signals for interaction between each other. Every system has own standard and interface. Every system is working separately and this is really good practise for being sure if something goes wrong in one system it shouldn't start chain of actions for crashing whole vessel. But from the point of informational security - worst scenario, and if there plans of remote vessel handling there will be required to unite this systems in one for the purpose of delivering remote handling. If nothing changed, it going to be almost impossible to be sure about security at all.

This kind of issues possible to solve by developing vessel informational model and analysing every link and every source of information. After this kind of modelling implement this architecture to the platform that is providing solution for vessel handling where the ability of remote access and distributed applications vessel-office from begin.

0.1. Document management between vessel and onshore facilities.

For the current time MOST DIFFICULT problem in case of informational security. If risks of hacking navigational system is relatively rare, but risks of getting malware or virus onboard - huge.

For example just look on situation: the vessel carrying collected general cargo from few owners and the Port Authority require provide document for every kind of cargo in different format and in different documents and make numbers of copies for each. There are legends about amount of paperwork through the mariners and of course mariners will try to reduce this amount.

And now about how this situation might be solved: the vessel agent provide crew with templates of required documents, if not agent then crew getting it by own and fill it and print. If vessel been arriving to this particular port their getting templates from archive that might be stored on any private computer of any crew member. This kind of templates always in MS Word or MS Excel file format and transferring by copying it on Flash-drive.

Everything looking good, but now questions about informational security:

- Who said that in small African Port Authority well enough precaution of

informational security and there are nothing about included malware or virus?
- The basis OS for document management MS Windows, this historical fact because of absence any alternative. It is as it is, but never the less, just visit www.cvedetails.com.
- Who said that the personal laptop where been storing templates secured enough?
- etc

The list of questions might be prolonged further and endlessly. In case of separate using navigational system and the computer where document management - nothing dangerous. No physical connection - no troubles. But in case of increasing automatisation onboard you will be required to solve this problem. The antivirus application - not the solution because of how often you need to prepare documents for ports and how often updating antivirus database application and who often new viruses appearing?

The solution for this problem mostly outside the vessel and mostly based on real world procedures that is making sure of security, for example: the onshore part of company getting this templates, at least checking it and sending it to the vessel. The best solution to develop document management system that looks like distributed application where templates is in library and all of documents printing based on templates from the system. The side effect is if you done it for one vessel, you don't need to do it for every vessel in the company you only delivering template for every vessel.

Some futurology. Just imagine that there are universal and international standard of cargo documentation management and you don't need the papers at all. In every port one standard and you only downloading data to the server of the Port Authority.

0.1. Conclusion

This article contain only few main problems describing. There are much more problems but most of them related to the global informational technology gap for vessels. Without solving this gap might be not possible to solve new problems at all.