rus.vessel_informational_security

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

Информационная безопасность на судне.

Прежде чем описывать множество проблем и их решения нужно отметить несколько пунктов:

- не существует систем безопасности дающих 100% гарантию что вас не взломают, технологии развиваются и всегда есть шанс что найдется кто-то кто окажется лучше
- всегда "держите руку на пульсе", любое средство безопасности только дает вам немного времени для распознания опасности, много средств безопасности не бывает и у всего есть срок годности, иногда атака не происходит только потому что очень долго взламывать и ценность ради которой нужно было взламывать потеряла свою ценность
- помимо средств защиты у вас всегда должны быть средства нападения или ухода от угрозы

Все описанное ниже основывается на этих пунктах, например:

- VPN - усложняет процесс мониторинга и сбора сетевого трафика тем самым давая вам время определить что кто-то посторонний в сети
- Шифрованные межмодульные сообщения - усложняют анализ собранных данных, тем самым давая вам время на определение что что-то не так
- Организованные и прописанные процедуры в случае DoS атаки - это ваше средство нападения, и это зачастую не имеет никакого отношения к ПО, в большинстве случаев это менеджмент и человечески фактор.
- и т.д.

Все описанные проблемы имеют отношение к информационной безопасности на уровне устройств и программного обеспечения к ним. Проблемы информационной безопасности на уровне физических принципов передачи информации или носителей не рассматриваются.

0.1. Отсутствие моделирование судна с точки зрения когда судно - источник информации.

В данный момент автору статье не встречались материалы на предмет моделирования информационных потоков на судне. Не проводилось тестирование информационных систем на взлом и проникновение. Как

результат крайне сложно сказать на данный момент какая из судовых систем может оказаться "слабым звеном" в судовой информационной безопасности.

Решить данную проблему можно только разработкой единой платформы основанной на заведомо надежной операционной системе (если нужны консультации на тему возможной архитектуры платформы - свяжитесь с автором статьи), которая будет позволять воспринимать судно как источник информации и шаг за шагом проверять каждую судовую систему на предмет возможности взлома и проникновения.

0.1. Базовая операционная система

Практически все устройства на судне тем или иным образом основаны на транзисторах и интегральных схемах. У всех этих устройств есть Операционная Система - И ЭТО ОТПРАВНАЯ ТОЧКА ДЛЯ АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ!!! Если операционная система, которая используется в качестве базовой изначально уязвима, то о какой информационной безопасности вы собираетесь говорить? Проверить операционную систему на предмет безопасности и наличия уязвимостей можно на специализированном сайте www.cvedetails.com

```
Примечание автора.
Во время контракта в 2015 году было огромным удивлением
обнаружить Windows XP как базовую для навигационной системы
последнего поколения на судне 2014 года постройки. В дополнение
к этому использует методы открытой передачи данных (не используя
никакого шифрования) между устройствами и терминалами. Система
которая уже не поддерживается Microsoft и не получает нужного
количества обновлений безопасности используется как базовая
для навигационной системы.
На вопрос - почему так? Ответ был дан простой: "Наследие
прошлого, огромное количество кода написанного под Windows XP
и никто не хочет писать новое. И лицензия на Windows XP дешевле." А
самое страшное то, что этот ответ четко иллюстрирует
время в которое ставились задачи на проектировку данных систем.
Информационные технологии ушли сильно дальше тех которые
используются на судах и взламывать будут суда новыми
технологиями. Никто не будет играть в рыцарей и снимать шлем
если вы оказались без шлема.
В последующем, к большому сожалению, было обнаружено что
это далеко не единичный случай и на более новых судах.
```

Частично решить эту проблему можно организацией судового VPN и принудительным шифрованием на уровне сети. Но это только частичное решение потому как по прежнему это одна из самых уязвимых операционных систем.

Данная проблема - одна из причин почему было упомянуто про разработку единой платформы которая будет основана на гораздо более надежной с точки зрения безопасности системы и учитывать все описанное выше.

Теперь почему было упомянуто про FreeBSD а не Linux-семейство, ответ - ЛИЦЕНЗИЯ. Как это было описано в статье "Почему FreeBSD?" и если вы хотите использовать систему blockchain-сигналов через порты TCP для обеспечения безопасности (пример описан в статье "Blockchain пример для серверных решений") вам придется изменять исходный код операционной системы. В случае с FreeBSD вы можете это делать свободно, в случае с Linux-семейством вы будете обязаны опубликовать это. А про какую безопасность вы собираетесь разговаривать если вы обязаны открыто рассказать о том как вы собираетесь защищаться?

0.1. Межмодульные сообщения

На судне существует огромное количество электронных сообщений (сигналов) между системами и датчиками. У каждой системы свой стандарт, у каждой системы свой интерфейс. Каждая из систем работает независимо, и так и должно быть потому что если выходит одна из систем из строя, то это не должно повлечь за собой цепную реакцию выхода из строя других систем. Но с точки зрения информационной безопасности - это одна из самых страшных ситуаций, критичность которой усилится в случае беспилотного судовождения и предоставления интерфейса удаленного управления. Обеспечивать безопасность "технологического зоопарка" крайне сложно потому что у каждой технологии свои тонкости и нет гарантии что производитель тестировал эти устройства с точки зрения информационной безопасности.

Данную проблему можно будет решить путем создания модели информационного обмена на судне и на основании этой модели разрабатывать информационную систему состояния судна на основании которой происходит разработка системы удаленного управления судном. Эта система не должна заменять существующие, она должна быть информационной, которая информирует оператора судна и предоставляет возможность судну быть контролируемым оператором (эта формулировка

написана специально именно так как она написана, потому как это отражает политику безопасности судна по отношению к оператору). Опять же вопрос о платформе на основании которой это будет разрабатываться.

0.1. Экипаж, документооборот с береговыми службами и компанией

На данный момент это самая главная проблема в информационной безопасности судна. Если риски взлома системы навигации еще относительно редки, то риск загрузить вредоносное ПО которое обрушит что-то на судне очень велик.

Рассмотрим ситуацию для примера: судно везет сборный груз от нескольких десятков грузоотправителей, а портовые власти требуют мало того, что для каждого типа груза свою форму документа так еще много копий каждого из них. Про объемы судовых документов на приход и на отход ходят легенды среди моряков.

А теперь о том как эта проблема обычно решается. Судовой агент присылает шаблоны документов на судно, судовые документы заполняются и распечатываются. Как правило это шаблоны созданные в Microsoft Word или Excel. Если судно уже заходило в этот порт и заполняло документы то файлы берутся из архива предшественника которые хранились у него на его личном компьютере путем переноса для примера на Flash-drive.

А теперь вопросы касающиеся этой ситуации с точки зрения информационной безопасности:

- Кто сказал что в маленьком порту где-то в Африке должный уровень информационной безопасности и файлы присланные на судно не заражены вредоносным ПО?
- Базовая система для документоборота - Windows по исторически сложившимся обстоятельствам, но тем не менее, визит на сайт https://www.cvedetails.com для выяснения уязвимостей позволит задать вопрос о том на сколько эта система уязвима.
- Кто сказал что сменщик должным образом обеспечивает безопасность своего компьютера и что при копировании шаблонов документов он вам не скопирует вредоносное ПО?
- и т.д.

Этот список может быть продолжен бесконечно. В случае если системы разделены физически и компьютер на котором происходит работа с документами не подключен физически к сети в которой находится системы управления судном - то ничего страшного, максимум что произойдет, вы потеряете шаблоны документов, но не потеряете возможность управлять судном. Но в случае увеличения уровня автоматизации вы будете вынуждены объединять системы и тогда придется решать эту проблему. Антивирусы установленные на судовых компьютерах не защитят по одной причине - как частно обновляется база данных антивируса на судах? Как часто появляются новые вирусы и как быстро они распространяются на берегу?

Решение данной проблемы в большинстве случаев лежит за пределами судна. Это организация процедуры документооборота таким образом что на судно не попадают непроверенные данные. Один из примеров этого решения - система документооброта разработанная таким образом, что все документы сначала попадают в офис компании проверяются или еще лучше всего осмысленно переводятся в формат шаблонов своей собственной системы (только осмысленная трансформация информации является наиболее сильным средством против скрытых инъекций, и это действует как для физических законов передачи информации и для аппаратных средств) которые становятся доступны в системе на судне удаленно и только потом заполняются и распечатываются на судне. Заплатить за передачу маленького архива с шаблонном может оказаться дешевле чем потерять контроль над судном, это делается только один раз, в случае с большими компаниями эти шаблоны могут храниться в виде справочников и распространяться на все суда, что в свою очередь обеспечит безопасность на всех судах компании сразу.

0.1. Заключение

В этой статье были описаны только некоторые, основные проблемы сетевой безопасности. По факту их больше. Но все эти проблемы тем или иным образом относятся к проблеме общей отсталости судовых технологий и без глобального решения проблем платформы для судов может оказаться не возможным решение многих проблем в будущем, а процесс обеспечения информационной безопасности судов может оказаться простым залатыванием дыр.

Следите за обновлениями автора в **Linkedin**.

Следите за AR|BO|RE|US обновлениями в **Twitter** в **Linkedin**.