УДК 004.056.55

РАЗРАБОТКА АЛГОРИТМА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПРОЦЕДУРЫ ОБМЕНА СООБЩЕНИЯМИ МЕЖДУ СУДНОМ И БЕРЕГОВЫМИ ОБЪЕКТАМИ

Веселова М.Д.. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.в.н., доцент Юрин И.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данной работе рассмотрен алгоритм передачи информации между судном и береговыми объектами, выявлены уязвимые места текущего алгоритма, на которые может воздействовать нарушитель, и возможные атаки. Предложен механизм, позволяющий повысить безопасность процедуры обмена сообщениями, основанный на применении постквантовой криптосистемы. В заключении указаны плюсы и возможные недостатки практического использования предложенного алгоритма.

Введение. IT-технологии в мореплавании – это новое направление судостроении. На данный момент существует множество научных исследований в области автоматизации процессов управления судами, их навигации, отслеживания состояния судов, обмена сообщениями между судами и береговыми объектами. В данной сфере важно отслеживание состояния судна в реальном времени как на мостике капитана, так и в автоматизированных системах береговых объектов, например, в системах управления движением судов (далее - СУДС) или системах, которыми пользуются компании-владельцы судов. Отслеживание состояния выполняется за счет обмена информацией между различными датчиками и информационной системой судна (далее - ИНС). Так же береговые объекты должны быть осведомлены о планах навигации судна, кроме того СУДС может отправлять на судно сообщения о навигационных опасностях или присылать рекомендованный маршрут для судна, так как в прибрежной области именно СУДС утверждает все движения судов. Помимо фиксированных сообщений, таких как отправка маршрутов, предупреждений и тревог, состояния судна, между береговыми объектами и судами, а также между судами существует отправка текстовых сообщений.
С появлением информационных технологий в данной сфере всё большее внимание стал занимать вопрос обеспечения информационной безопасности, которая крайне важна, поскольку потеря судна и экипажа или возникновение нештатных ситуаций, которые потенциально могут привести к катастрофе, недопустимы и являются серьезной трагедией как на государственном, так и на мировом уровне. Особенно слабым местом в данной сфере является обмен сообщениями, поскольку при отсутствии необходимых средств защиты информации передача может быть перехвачена третьей стороной, что может привести к получению несанкционированного доступа к данным судна, экипажа, к отправке третьей стороной недостоверных данных на судно, к удаленному доступу к системе.

Основная часть. В настоящее время для защиты передаваемых данных используется протокол TLS и сертификация X.509. Таким образом, чтобы начать взаимодействие между двумя сторонами, необходимо сначала получить сертификат, который содержит данные о его владельце, сведения об удостоверяющем центре и электронную цифровую подпись, что позволяет однозначно идентифицировать сторону обмена данных. После чего можно начать взаимодействие с другой стороной, имеющей сертификат, выполнив TLS-рукопожатие. Протокол рукопожатия используется для согласования и установки безопасного канала между сторонами. При успешном завершении процесса TLS-рукопожатия начинается обмен данными, зашифрованными сессионным ключом, полученным в момент TLS-рукопожатия.
Основной уязвимостью в процессе передачи информации является ассиметричные криптосистемы в TLS, которые используются при аутентификации сторон и получении общего симметричного секрета. Взлом криптосистемы позволяет подменить узлы и

произвести атаку с возможностью перехвата сессии, а также возможна реализация атаки, позволяющей читать трафик сессий в пассивном режиме. Ввиду большой вероятности возникновения угроз необходимо реализовать первоочередные меры для защиты TLS – внедрение постквантовых криптосистем. Стойкость, которая достигается за счет их применения, основана на использовании математических конструкций, не содержащих структур, для которых известны возможные квантовые реализации атак.
Постквантовую криптосистему предлагается внедрить на этапе формирования секрета, а именно, в момент TLS-рукопожатия, в результате чего общий секрет будет генерироваться при помощи постквантового алгоритма, что позволит увеличить эффективную разрядность полного секрета, так как к определенной разрядности секрета дополнительно будет добавлена еще часть постквантового секрета с такой же разрядностью. Таким образом, TLS будет не полностью заменен, а лишь дополнительно усовершенствован.

Выводы. Постквантовая криптография как мера защиты была предложена сравнительно недавно, однако, NIST уже запустил проект по её стандартизации и даже презентовал несколько лидирующий алгоритмов.
За счет применения данного способа при обмене сообщениями между судном и береговыми объектами значительно увеличивается вероятность того, что атака не будет реализована, благодаря использованию в алгоритме защиты классического подхода в сочетании с постквантовой криптографией. Такая мера исключает раскрытие сразу двух секретов, поскольку атаковать можно лишь одним способом, чтобы была уязвима либо посквантовая криптосистема, либо ассиметричная криптосистема.

Веселова М.Д. (автор) Подпись

Юрин И.В. (научный руководитель) Подпись