УДК 004.942

РАЗРАБОТКА МЕТОДИКИ ОБЕСПЕЧЕНИЯ АУТЕНТИЧНОСТИ СООБЩЕНИЙ ПРОТОКОЛА CRISP ДЛЯ ЗАЩИТЫ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ МАЛОМОЩНЫХ IOT УСТРОЙСТВ

Лемаев А. О. (Университет ИТМО)

Научный руководитель – к.т.н. Таранов С. В.

(Университет ИТМО)

В данной работе предложены методы по обеспечению аутентичности сообщений для протокола CRISP для защиты межмашинного взаимодействия маломощных IoT устройств. На основе методов разработаны формальные модели описания.

Введение.

Число кибератак на IoT (internet of things, интернет вещей) и IIoT (Industrial IoT, промышленный интернет вещей) растет. Если недавно эта проблема носила умозрительный характер, сейчас она приобрела реальные очертания. Причем нарушение промышленной безопасности чревато последствиями, далеко выходящими за рамки финансового ущерба и потери репутации. Необходимость разработки протокола CRISP была вызвана общей тенденцией и обсуждением вопросов безопасности КИИ (критическая информационная инфраструктура) и АСУ ТП (автоматизированная система управления технологическим процессом), в частности защиты каналов передачи данных и данных, предаваемых по разным сетям. Не все индустриальные и промышленные сети можно защитить с помощью VPN и TLS.

В ходе исследования МР 26.4.001-2019 «Протокол защищенного обмена для индустриальных систем (CRISP 1.0)» были выявлены существенные недостатки протокола CRISP, которые необходимо решить. Во-первых, в пункте 5 «ограничения» описано, что отправитель и получатель имеют общий базовый ключ. Данный ключ участвует в выработке ключей шифрования и имитозащиты. Для базового ключа не предусмотрены никакие действия по оценке криптостойкости данного ключа, также нету никаких гарантий, что данный ключ не был скомпрометирован третьими лицами, получается, что обе стороны доверяют друг другу, также отсутствует механизмы по оценке актуальности и времени жизни ключа (не отслеживаются и не фиксируется информация кем был сгенерирован ключ). Во-вторых, описано, что отправитель и получатель имеют общие криптографические наборы, которые никак не согласуются между узлами. В случае ошибок в наборе протокол может сработать некорректно, что может привести в дальнейшим к компрометации сообщения CRISP либо к ошибке при дешифровании в случае попытки восстановление исходного сообщения получателем. В-третьих, для CRISP-собщения вычисляется имитовставка. Хэш-сумма не является изящным решением для обеспечения целостности сообщения, она обнаруживает с высокой вероятностью ошибки даже те ошибки который внедряются злоумышленником, но она их не исправляет.

Основная часть.

Предлагается рассмотреть современный протокол для аутентификации маломощных узлов и установки общего базового ключа для протокола CRISP, внедрить дополнительное поле с CRC (циклически избыточным кодом) для CRISP-сообщения, реализовать модифицированный протокол на формальном языке с целью тестирования на различных моделях нарушителей.

Выводы.

Для тестирования предлагается построить модели нарушителей на формальном языке в целях определения актуальности угроз из составленного перечня. Таким образом, в результате

научной работы проведенные испытания позволят оценить эффективность модифицированного протокола CRISP.

Лемаев А. О. (автор) Подпись

Таранов С. В. (научный руководитель) Подпись