УДК 004.056.52

Е.А. Кушко, Д.А. Грачёв, Н.Ю. Паротькин, В.В. Золотарёв

О вопросах безопасности киберфизических систем

Киберфизические системы находят все более широкое применение во всех отраслях. С ростом распространения этих систем увеличивается и число атак на них. Рассмотрены основные технологии, используемые для построения киберфизических систем, меры безопасности, реализуемые в них, их преимущества, недостатки и уязвимости. Также авторами приведен общий подход к обеспечению безопасности киберфизических систем.
Ключевые слова: киберфизические системы, сенсорные сети, интернет вещей, уязвимость.
DOI: 10.21293/1818-0442-2022-25-4-101-109

Киберфизическая система – это комплексная система, состоящая из вычислительных и физических элементов, которая постоянно получает данные из окружающей среды и использует их для дальнейшей оптимизации процессов управления [1]. Примерами такой системы могут являться: «умный» дом, «умный» город и другие «умные» автоматизированные системы управления. Ключевой особенностью киберфизических систем является связывание физических процессов производства или других процессов, которые требуют непрерывного управления в реальном времени с программно-аппаратными системами [2].

Интернет вещей (Internet of things, IoT) – это динамичная распределенная среда, которая связывает множество интеллектуальных устройств, способных воспринимать окружающую среду и выполнять соответствующие действия [3]. Такие устройства позволяют отслеживать состояние внешней среды, собирать информацию о реальном мире и создавать системы повсеместных вычислений, в которых каждое устройство может взаимодействовать с любым другим устройством в мире, где бы оно ни находилось. IoT-технологии обеспечивают совместную работу устройств – как отдельных датчиков или как совокупности различных датчиков, образующих конечную макросистему и действующих как единое целое.

Понятие киберфизических систем часто рассматривают совместно с понятием интернета вещей. Оба типа систем имеют схожие элементы, однако киберфизические системы являются более широким понятием и имеют более сложную архитектуру. Главная схожесть архитектур заключается в том, что на нижнем уровне киберфизических систем и систем интернета вещей лежит сенсорная сеть. Сенсорная сеть представляет собой динамическую, самоорганизующуюся и распределенную сеть датчиков и исполнительных устройств. Она предназначена для решения задач автоматизации, диагностики, телеметрии и межмашинного взаимодействия. Сенсорная сеть должна быть проста в создании и эксплуатации, нетребовательна к частому техническому обслуживанию, обладать высокой отказоустойчивостью и надежностью, а также быть легко масштабируемой [4].

Технологии передачи данных

Технология передачи данных сенсорной сети выбирается в зависимости от требований по дальности и энергопотреблению, уровня шума и производительности устройств. На первый взгляд, многие беспроводные стандарты, применяющиеся в сенсорных сетях, имеют схожие свойства, однако эти стандарты разработаны для решения разных задач и, соответственно, функционируют по-разному. В табл. 1 приведена сравнительная таблица популярных стандартов.

Таблица 1

Сравнительная характеристика стандартов беспроводной связи сенсорных сетей

Технология беспроводной передачи данных (стандарт)	Bluetooth (IEEE 802.15.1)	Wi-Fi (IEEE 802.11b)	ZigBee (IEEE 802.15.4)	LoRa	Z-Wave
Частотный диапазон, ГГц	2,4–2,483	2,4–2,483	2,4–2,483	2,4–2,483	0,8–0,9
Пропускная способность, кбит/с	723,1	11 000	250	до 50	до 100
Размер стека протокола, Кбайт	Более 250	Более 1000	32–64	64	64
Время непрерывной автономной работы от батареи, дни	1–100	0,5–5	100–1000	365–1000	90–700
Максимальное количество узлов в сети	7	10	65 536	1000	232
Диапазон действия, м (усредненные значения)	10–100	20–300	10–100	500	40–100
Область применения	Создание персональных сетей	Создание локальных сетей	Удаленный мониторинг и управление	Удаленная передача информации	Удаленный мониторинг и управление

Из-за того, что устройства сенсорной сети должны функционировать достаточно длительное время в сложных условиях, это накладывает ограничения на их размер, дальность передачи данных, энергопотребление. Кроме того, устройств требуется вплоть до несколько тысяч в зависимости от решаемых за-

дач. Поэтому такие устройства имеют низкую стоимость, низкую производительность и функционируют в условиях низкой пропускной способности [4].

На безопасности сенсорных сетей сказывается отсутствие механизмов обнаружения вторжений, аутентификации и шифрования. В силу низкой производительности и стоимости устройств средства и механизмы защиты, как правило, сильно упрощены, что делает эти устройства уязвимыми. Все вышеперечисленные факторы влияют на то, что злоумышленник может с минимальными затратами проникнуть в сенсорную сеть [5].

Задачи, которые решает сенсорная сеть, требуют от неё соответствия следующим характеристикам: автономность, надежность, отказоустойчивость и масштабируемость. В некоторых случаях может стоять задача сбора и анализа данных в режиме реального времени, что дополнительно накладывает требования к задержкам. Поэтому и меры защиты, реализуемые в сенсорных сетях, направлены на обеспечение высокой доступности: обеспечения устойчивых каналов связи, построение оптимальных маршрутов, защита от внешних воздействий и т.д.

Bluetooth

Сеть Bluetooth имеет топологию типа «звезда» или ячеистой сети и использует высоконагруженный диапазон 2,4 ГГц, что вносит помехи при организации связи. Поддержка стандартом Bluetooth небольшого числа узлов в сети ограничивает разработчиков систем в построении систем со сложной структурой. Сенсорная сеть на базе Bluetooth не является надежным решением. Однако широкая распространенность данного стандарта позволяет достаточно легко взаимодействовать с конечными устройствами сенсорной сети при помощи персональных мобильных устройств. Стандарт Bluetooth охватывает все уровни модели OSI. Данный стандарт поддерживает механизмы аутентификации и шифрования сообщений как на уровне сети, так и на прикладном уровне, однако имеет ряд существенных уязвимостей [6].

Wi-Fi

Сеть Wi-Fi имеет централизованную структуру, а соответственно единую точку отказа, так как типичная топология сети Wi-Fi – это «звезда» или «дерево». Выход из строя одного маршрутизатора нарушает нормальное функционирование всей сети. Механизм добавления новых узлов не позволяет гибко наращивать масштаб сенсорной сети. Высокая пропускная способность сети Wi-Fi связана с высоким энергопотреблением. Скорости, предлагаемые стандартом Wi-Fi, избыточны для сенсорной сети, для неё гораздо важнее низкое энергопотребление. Несмотря на широкую распространённость данного беспроводного стандарта, существуют более дешевые решения, которые лишены указанных недостатков. Но у сети Wi-Fi есть значительное преимущество – это возможность применения средств защиты информации, которые используются для защиты обычных локальных сетей. Wi-Fi охватывает только физический и канальный уровни модели OSI, соответственно, у разработчиков системы есть возможность гибкого конфигурирования и использования протоколов других уровней. Однако это и снижает совместимость устройств разных производителей между собой.

ZigBee

Сеть ZigBee имеет ячеистую топологию. В сети ZigBee существует две модели безопасности: распределенная модель и централизованная модель [7]. В обоих моделях безопасности используется шифрование AES-128 как на сетевом уровне, так и на уровне приложений. ZigBee также предусматривает проверку целостности при помощи механизма Message Integrity Check (MIC). Однако для подключения к сети ZigBee используется глобальный заранее сгенерированный ключ для подключения к сети (pre-configured global link key), который имеет значение по умолчанию. Этот ключ используется для обеспечения совместимости устройств ZigBee от различных производителей. Для повышения уровня защищенности необходимо прописывать во все устройства в сети ZigBee нестандартный ключ, иначе сеть будет уязвима для проникновения злоумышленником. Также злоумышленник может перехватить ключ сетевого уровня [8] или физически извлечь его из прошивки устройства [9]. Шифрование на уровне приложений также является уязвимым, так как этот ключ тоже может быть скомпрометирован [10].

LoRa

LoRa образует сеть с топологией «звезда из звезд» и охватывает все уровни модели OSI. LoRa обеспечивает конфиденциальность передаваемых данных средствами шифрования AES на нескольких уровнях: на сетевом уровне с использованием уникального ключа сети (Unique Network key, EUI64); сквозную безопасность на уровне приложений с помощью уникального ключа приложения (Unique Application key, EUI64); специального ключа устройства (Device specific key, EUI128). Однако технология LoRa также имеет уязвимости [11].

Z-Wave

Сеть Z-Wave реализует тополгию ячеистой сети. Данный факт в совокупности с использованием гораздо менее нагруженного диапазона 0,8–0,9 ГГц, наличия механизмов самовосстановления (процедура Explorer Frame) и построения оптимальных маршрутов доставки делает Z-Wave одним из самых надежных решений для сенсорной сети. Z-Wave также охватывает все уровни модели OSI. Z-Wave использует собственный стандарт безопасности Security 2 [12], который также поддерживает шифрование AES-128 и использует механизмы подключения новых устройств в сети при помощи PIN-кодов и QR-кодов для того, чтобы злоумышленник не мог осуществить перехват подключения и проникнуть в сеть. Использование протокола Диффи–Хеллмана на эллиптических кривых для обмена ключами также значительно повышает уровень защищенности сети Z-Wave. Однако, как и любая другая технология, она имеет уязвимости [13].

Протоколы прикладного уровня

Наиболее широко распространенными протоколами прикладного уровня, используемыми в киберфизических системах, являются MQTT, CoAP, AMQP, DDS и XMPP (рис. 1). MQTT и CoAP особенно подходят для сервисов, требующих сбора данных (например, обновления датчиков) в условиях систем с ограниченными возможностями. Напротив, AMQP, DDS и XMPP отвечают специфическим требованиям к услугам, а именно: обмен деловыми сообщениями, обмен мгновенными сообщениями и обнаружение присутствия в сети и обмен сообщениями в реальном времени соответственно.

Прикладной уровень	MQTT	CoAP	AMQP	DDS	XMPP
Транспортный уровень	TCP			UDP	
Интернет-уровень	IPv4 и IPv6 + 6LoWPAN				
Уровень сетевых интерфейсов	IEEE 802.3	IEEE 802.11	IEEE 802.15	IEEE 802.16	Другие

Рис. 1. Протоколы прикладного уровня

Что касается служб безопасности, то решения, обеспечивающие целостность и конфиденциальность обмена данными и предоставляющие механизмы аутентификации и авторизации, весьма разнообразны. Протоколы обмена сообщениями обычно поддерживают как стандартные, так и собственные службы безопасности. Исходя из этого, реализация соответствующих решений по обеспечению безопасности возлагается на разработчиков. Ниже приведена табл. 2, в которой отражены возможности рассмотренных ранее протоколов в области шифрования, авторизации и обеспечения конфиденциальности [14].

Таблица 2

Сводка служб безопасности, поддерживаемых протоколами обмена сообщениями

Протокол	Аутентификация		Авторизация	Конфиденциальность	
	SASL	Sp*	Sp*	TLS	DTLS
MQTT		+		+	
CoAP					+
AMQP	+			+	
DDS		+	+	+	
XMPP	+		+	+	

* Sp (special) – специфичная реализация.

Из приведенных данных видно, что механизмы шифрования имеются во всех протоколах обмена сообщениями. Например, конфиденциальность обеспечивается стандартными службами, такими как TLS и DTLS, а механизмы аутентификации и авторизации основаны на стандартных (т.е. SASL) или пользовательских решениях.

Важно отметить отсутствие некоторых механизмов обеспечения безопасности при разработке протокола. Более того, использование служб обеспечения безопасности носит рекомендательный характер, и в целях снижения нагрузки на вычислительные мощности IoT-сетей разработчики склонны пренебрегать этими службами при разработке, настройке и использовании своих приложений. В связи с этим, устройства часто подвергаются рискам безопасности, характерным для рассматриваемых протоколов.

Уязвимости протокола MQTT

На основе анализа возможных угроз безопасности устройств с поддержкой MQTT были определены следующие потенциально уязвимые процессы:

• аутентификация: брокер MQTT не проверяет должным образом личность издателя/подписчика и не блокирует повторные попытки аутентификации. Эти уязвимости могут предоставить злоумышленнику доступ к MQTT-устройствам или, что еще хуже, к брокеру, что может иметь плачевные последствия для функционирования всей сети;

• авторизация: брокер MQTT неправильно устанавливает разрешения на публикацию/подписку. Эта уязвимость может предоставить злоумышленнику контроль над данными или функциями MQTT-устройств;

• доставка сообщений: издатель отправляет сообщения, которые не могут быть доставлены из-за отсутствия подписчиков. Эта уязвимость может привести к значительному снижению производительности брокера;

• проверка сообщений: издатель отправляет сообщения, содержащие запрещенные символы, которые неправильно интерпретируются брокерами и подписчиками. не исключено, что эта уязвимость может быть использована для осуществления различных вредоносных атак;

• шифрование сообщений: клиенты и серверы обмениваются сообщениями в открытом виде, что позволяет злоумышленнику подслушивать и подменять сообщения во время их передачи. Эта уязвимость может быть использована для проведения атак типа «человек посередине» (MITM).

Анализ CVE, затрагивающих продукты и услуги на базе MQTT, показал, что существует около 60 уязвимостей CVE. В частности, поддельные MQTT-сообщения могут легко заставить брокеров не реагировать на запросы. Например, вредоносный MQTT-клиент может вызвать переполнение стека, просто отправив пакет SUBSCRIBE, содержащий не менее 65 400 символов «/» (CVE-2019-11779). Аналогично пакет CONNECT в сочетании с неправильно сформированным пакетом запроса UNSUBSCRIBE может быть использован для атаки типа «отказ в обслуживании» (DoS) на брокера (CVE-2019-6241).

Другие проблемы безопасности относятся к категориям аутентификации и авторизации, как в случае с клиентами, которые устанавливают свое имя пользователя на «#», тем самым обходя механизмы контроля доступа и подписываясь на все темы MQTT (CVE-2017-7650).

Помимо этого, актуальная атака «отказ в обслуживании», направленная на то, чтобы сделать брокер невосприимчивым или даже аварийным, может быть осуществлена путем отправки больших сообщений или сообщений с высоким уровнем QoS. Кроме того, несанкционированная публикация, направленная на физическое повреждение или отключение IoT-устройств, может быть осуществлена с помощью привилегированных сообщений, которые предоставляют злоумышленнику удаленный контроль над этими устройствами. Таким образом, рассмотренные угрозы безопасности могут серьезно повлиять на сеть на базе протокола MQTT и поставить под угрозу доступность и конфиденциальность циркулирующих в ней данных.

В качестве ответных мер угрозам безопасности в стандарте MQTT перечислены механизмы, которые должны быть включены в реализацию MQTT, а именно:

• аутентификация пользователей и устройств;

• авторизация доступа к ресурсам сервера;

• целостность управляющих пакетов MQTT и данных приложения;

• конфиденциальность управляющих пакетов MQTT и данных приложения.

Для каждого из этих механизмов стандарт дает некоторые общие рекомендации (например, повторная аутентификация длительных сессий, предотвращение подписки на все темы, использование VPN). Однако данные контрмеры относятся к простым сценариям, т.е. в отношении более сложных атак эти меры могут быть недостаточными или попросту бесполезными.

Несмотря на то, что использование протокола TLS настоятельно рекомендуется стандартом MQTT для обеспечения безопасной связи, TLS не решает всех проблем безопасности. Как известно, старые версии TLS, его неправильная конфигурация и использование слабых наборов шифров делают протоколы подверженными атакам безопасности. Кроме того, для реализации TLS требуется значительная вычислительная мощность и пропускная способность сети, которые могут быть попросту недоступны в сетях IoT с ограниченными вычислительными возможностями.

Уязвимости протокола CoAP

CoAP поддерживает использование протокола Datagram Transport Layer Security (DTLS), UDP-реализации протокола TLS, который обеспечивает эквивалентные гарантии безопасности. Привязка DTLS для протокола CoAP определена в терминах четырех режимов безопасности, которые отличаются механизмами аутентификации и согласования ключей и варьируются от отсутствия безопасности до безопасности на основе сертификатов. То есть при их использовании стоит задача найти оптимальный компромисс между ограничениями производительности/энергии и требованиями безопасности. Конечно, отсутствие соответствующих служб безопасности может позволить злоумышленнику легко скомпрометировать среды CoAP.

На основе анализа возможных угроз безопасности устройств с поддержкой CoAP были определены следующие потенциально уязвимые процессы:

• разбор сообщений: использование парсеров, т.е. программ (сервисов или скриптов), собирающих данные с определенных источников информации и выдающих в нужном формате, может послужить источником угроз из-за некорректной обработки. Эта уязвимость может повлиять на доступность узла CoAP и даже открыть возможность удаленного выполнения произвольного кода на атакуемом узле;

• проксирование и кэширование: механизмы контроля доступа к прокси и кэшам не реализованы должным образом. Эта уязвимость может скомпрометировать их содержимое, тем самым нарушив конфиденциальность и целостность сообщений CoAP;

• bootstrapping: установка новых узлов CoAP реализована неправильно. Эта уязвимость может предоставить неавторизованным узлам доступ к среде CoAP;

• генерация ключей: генерация криптографических ключей недостаточно надежна. Использование этих ключей может скомпрометировать узлы CoAP;

• подделка IP-адресов: подделывая IP-адреса узлов CoAP, злоумышленник может осуществлять атаки, связанные с генерацией поддельных сообщений и подтверждений, а также повлиять на межпротокольные обмены: сообщение с поддельным IP-адресом и фальшивым номером порта источника, отправленное на CoAP-узел, может заставить его интерпретировать полученное сообщение в соответствии с правилами целевого протокола.

Анализ нескольких CVE, затрагивающих продукты и услуги на базе CoAP, показывает, что наиболее распространенная проблема безопасности связана с неправильным разбором сообщений. Например, некоторые библиотеки CoAP неправильно обрабатывают недопустимые параметры или определенные исключения при получении специально созданных сообщений (например, CVE-2018-12679, CVE-2018-12680). Другие библиотеки подвержены уязвимостям переполнения при обработке входящего сообщения (например, CVE-2019-17212). Эксплуатация этих уязвимостей может иметь различные последствия, такие как утечка памяти, отказ в обслуживании, а также удаленное выполнение кода, что приводит к серьезным последствиям для всей системы, функционирующей на базе протокола CoAP.

Протокол UDP также является вектором, используемым для атаки на узлы с поддержкой CoAP. Например, определенные интерфейсы сервера CoAP могут быть использованы для атаки распределенного отказа в обслуживании с использованием подмены IP-адреса источника и усиления трафика. Эта уязвимость является следствием неправильной обработки определенного сообщения ответа (например, CVE-2019-9750).

Стандарт CoAP предусматривает некоторые общие меры по смягчению последствий, чтобы справиться с типами угроз и атак, рассмотренных в

предыдущем разделе. В частности, стандарт настоятельно рекомендует использовать DTLS для защиты узлов CoAP.

В рамках механизма контроля доступа существует угроза, связанная с возможностями узла по сбору информации, необходимой для внедрения в сеть с поддержкой CoAP в качестве аутентифицированного узла. В данном вопросе был предложен трехэтапный процесс загрузки нового узла. Процесс начинается с фазы обнаружения, на которой обнаруживается новый узел. Затем этому узлу предоставляются ключи для установления безопасного канала связи. Наконец, эти ключи используются для выполнения фактической конфигурации самого узла [15].

Улучшения протокола DTLS также изучались с точки зрения криптографического алгоритма. В частности, интеграция DTLS в CoAP на основе криптографии эллиптических кривых помогает минимизировать вычислительные затраты и использование ПЗУ [16].

Уязвимости протокола AMQP

Что касается безопасности, AMQP поддерживает фреймворк Simple Authentication and Security Layer (SASL) для аутентификации клиента и TLS для обеспечения целостности и конфиденциальности связи. Отметим, что в отличие от MQTT и CoAP, эти службы безопасности обычно включены по умолчанию, что снижает потенциальные риски безопасности. Тем не менее, согласно базе данных NVD, за последние шесть лет в продуктах и сервисах на базе AMQP было обнаружено множество уязвимостей. Эти уязвимости в основном затрагивают центральный компонент сети – брокер. Они влияют на такие процессы, как управление доступом, проверка сообщений и идентификации, управление очередью сообщений.

Последствия этих уязвимостей включают повышение привилегий, раскрытие информации, атаки типа «отказ в обслуживании», обход аутентификации и авторизации, удаленное выполнение кода, перехват трафика. Более конкретно, несколько уязвимостей связаны с отсутствием проверки имен хостов и сертификатов, эксплуатация которых позволяет злоумышленникам подделывать идентификаторы и перехватывать трафик для MiTM-атак (например, CVE-2018-11087, CVE-2018-8119, CVE-2016-4467). Аналогично отсутствие контроля доступа в очередях сообщений позволяет злоумышленникам выполнять привилегированные команды (CVE-2019-3845). Кроме того, несколько CVE указывают на то, что использование специально созданных сообщений AMQP и открытых команд отключения позволяет осуществить атаку типа «отказ в обслуживании» (CVE-2015-7559, CVE-2017-15699, CVE-2015-0224, CVE-2015-1499).

Другие риски безопасности, влияющие на AMQP-среды, связаны с конфигурацией брокеров. Несмотря на наличие веб-интерфейса пользователя, их настройка может быть очень сложной. Неправильный выбор при настройке очередей сообщений, обменов, производителей и потребителей может привести к серьезным уязвимостям. Кроме того, пользовательские интерфейсы могут быть подвержены уязвимостям, обычно встречающимся в вебсфере (например, CVE-2015-0862, CVE-2016-0734, CVE-2017-4965).

Одна из наиболее распространенных ошибок конфигурации связана с применением стандартных учетных данных для входа в систему, которые могут быть использованы злоумышленником для получения контроля над интерфейсом администратора брокера и, следовательно, над всей средой AMQP.

Уязвимости протокола DDS

Что касается безопасности, протокол DDS предлагает богатое разнообразие механизмов. Как и другие протоколы обмена сообщениями, DDS поддерживает TLS и DTLS. Более того, для обеспечения конфиденциальности, целостности и подлинности обменов новейшая спецификация безопасности OMG DDS определяет архитектуру, основанную на наборе встроенных плагинов. Например, плагины предлагают механизмы аутентификации и авторизации DataWriters и DataReaders, что позволяет избежать несанкционированной публикации и подписки. Тем не менее, и спецификация, и плагины подвержены уязвимостям. В частности, протокол рукопожатия, используемый для подтверждения разрешений, передает открытым текстом информацию о возможностях участников, что позволяет злоумышленникам обнаружить потенциально важную информацию о достижимости в сети DDS (CVE-2019-15135).

Продолжая тему уязвимостей предлагаемых плагинов, стоит отметить две уязвимости, обнаруженные для плагина Access Control, способные привести к несанкционированным или непреднамеренным соединениям между участниками (CVE-2019-15136, CVE-2019-15137).

Уязвимости протокола XMPP

Протокол XMPP предоставляет надежные услуги безопасности, поддерживая SASL для процесса аутентификации и TLS для обеспечения конфиденциальности и целостности данных. Эти службы встроены в основные спецификации протокола, поэтому они включены по умолчанию. Тем не менее отсутствие поддержки сквозного шифрования делает протокол уязвимым для различных типов угроз. Например, злоумышленник может изменить, удалить или воспроизвести строфы или получить несанкционированный вход на сервер. В дополнение к проблемам безопасности протокола стоит отметить, что частые проблемы связаны с недостаточным контролем операций с памятью и ненадлежащей проверкой сертификатов (CVE-2019-1845, CVE-2019-12855, CVE-2014-3451, CVE-2018-15720, CVE-2016-1307).

Эти уязвимости позволяют осуществлять широкий спектр атак с различными последствиями, например, сделать сервисы недоступными, получить конфиденциальную информацию или получить доступ к XMPP-серверам.

Несколько методов снижения угроз безопасности были разработаны в качестве расширений XMPP в серии XEP. В частности, в XEP-0205 представлены меры, направленные на предотвращение DoS-атак, а XEP-0178 посвящен правильному использованию сертификатов для аутентификации SASL. Тем не менее несколько XEP содержат уязвимости, связанные с неправильной реализацией самих XEP (например, CVE-2016-10376, CVE-2017-5602, CVE-2019-1000021). Используя эти уязвимости, злоумышленники могут получить доступ к частным данным или выдать себя за пользователя и осуществить атаки социальной инженерии.

Атаки на протоколы прикладного уровня

Частые источники рисков связаны с отсутствием соответствующих служб безопасности или их неправильной конфигурацией. Хотя протоколы обмена сообщениями и предлагают различные службы безопасности, они уязвимы с точки зрения неправильной конфигурации этих служб. Кроме того, отсутствие встроенных механизмов аутентификации / авторизации или использование слабых механизмов делает устройства уязвимыми для несанкционированного доступа. Аналогично неправильная настройка TLS или использование слабых наборов шифров делают устройства уязвимыми к раскрытию данных, циркулирующих в киберфизической системе.

Эти выводы были подтверждены анализом CVE продуктов и услуг, основанных на рассмотренных протоколах. Более точно, многие уязвимости связаны с неправильной проверкой/разбором сообщений (например, переполнение буфера, проверка опций/исключений) и слабыми механизмами аутентификации/авторизации (например, проверка имени пользователя/имени хоста, проверка сертификата).

Важно также отметить, что риски и уязвимости безопасности подвергают устройства широкому спектру угроз и атак, представленных в табл. 3, которые могут иметь очень серьезные последствия.

Таблица 3

Подверженность прикладных протоколов типам атак

Протокол	Атаки типа «IP-спуфинг»	Атаки типа DoS/DDoS	Атаки типа MITM
MQTT		+	+
CoAP	+	+	+
AMQP		+	
DDS		+	
XMPP		+	+

Обеспечение безопасности киберфизических систем

Доступность, надежность и целостность приоритетнее конфиденциальности из-за потенциального воздействия на физический мир. Надежные системы шифрования и аутентификации могут привести к недопустимым задержкам. Необходимо реализовывать меры безопасности не на отдельных устройствах, а на всей инфраструктуре системы.

Традиционные средства защиты, такие как межсетевые экраны, средства антивирусной защиты, средства обнаружения и предотвращения вторжений и др., очень часто неэффективны для защиты IoT-инфраструктуры из-за того, что трафик генерируемый системой специфичен и сложен в анализе и устройства взаимодействуют напрямую друг с другом по беспроводному соединению [17].

При этом киберфизическая система должна быть устойчива к помехам, иметь резервные пути доставки информации, иметь механизмы обнаружения и противодействия действиям злоумышленников: проникновение в сеть, искажение кадров, подмена узлов и т.д.

Устойчивость к помехам реализуется использованием помехозащищенной передачи. Ячеистая топология сети предполагает несколько путей доставки, однако необходимо строить топологию таким образом, при котором существуют резервные пути доставки для каждого узла.

В общем виде система обнаружения вторжений для киберфизических систем осуществляет сбор трафика или его статистики и сравнение собранных данных с эталоном. Любое отклонение от эталона может свидетельствовать об атаке:

• Изменение количества узлов в сети. Это напрямую указывает на наличие нелегитимного узла.

• Изменение уровня мощности сигнала узла. Резкое изменение уровня принимаемого сигнала может свидетельствовать о подмене передающего узла.

• Изменение маршрутов доставки данных. Большинство киберфизических систем имеют ячеистую топологию, а одним из критериев выбора маршрута доставки является качество сигнала. Поэтому изменение маршрута может быть вызвано добавлением нового узла или подменой существующего, а соответственно, и влиянием на качество передачи.

• Увеличение или уменьшение числа кадров, изменение типа трафика. В киберфизических системах узлы генерируют, как правило, однотипный трафик, поэтому изменение количества трафика и его типа, например рост числа служебных пакетов, может указывать на присутствие злоумышленника.

• Ухудшение характеристик производительности сети. Снижение пропускной способности, увеличение задержек также может указывать на присутствие злоумышленника в системе.

• Уменьшение или увеличение времени реакции на запросы. Данный факт может указывать на подмену легитимного узла, например, более производительным устройством, в случае более быстрой реакции на запросы.

• Изменение временных периодов отправки данных. Узлы в киберфизических системах функционируют, как правило, по определенным временным циклам, большинство времени находясь в режиме низкого энергопотребления. Соответственно, и активность в периоды, не свойственные узлу, является аномальной.

Очевидно, что каждый параметр отклонения в отдельности может давать ложный результат, поэтому их следует использовать в совокупности.

Для обеспечения конфиденциальности сообщений и их подлинности необходимо использовать

такие алгоритмы шифрования (например, блочные: CLEFIA, PRESENT [18] и потоковые: MICKEY 2.0, Trivium [19]) и схемы аутентификации (например, μTESLA [20], схема Wenbo [21]), которые будут учитывать требования к задержкам в системе, а также требования к энергоэффективности и низкую производительность конечных устройств.

Разработка таких решений является одним из востребованных направлений исследований на текущий момент.

Защита от исследования

При применении такой схемы построения системы защиты вынуждены постоянно собирать, анализировать трафик и состояние киберфизической системы в целом. Поэтому существует другой подход к повышению защищенности – это технология защиты движущейся цели. Данный подход предполагает, что без собранной информации о системе злоумышленник не может эффективно осуществить свою атаку.

Киберфизические системы, как правило, статичны: данные передаются самыми эффективными маршрутами между конкретными узлами по заданным протоколам. Злоумышленник, в случае проникновения в систему, имеет неограниченные временные ресурсы для сбора информации для планирования своей атаки. Технология защиты движущейся цели предполагает реконфигурирование защищаемой системы через интервалы времени таким образом, при котором злоумышленник не может обладать долгосрочной информацией о системе. Злоумышленник при этом никак не ограничивается в своих действиях.

Авторами предложено новое решение [22, 23], которое основано на принципах технологии движущейся цели и децентрализованных анонимных сетей. Узлы в сенсорной сети передают данные таким образом, при котором защищены шифрованием передаваемые данные и скрыты стороны взаимодействия, т.е. скрыт сам факт передачи информации. Протокол передачи данных не использует явную адресацию, а информационный поток скрыт среди множества идентичных потоков. Передача данных предусмотрена таким образом, чтобы затруднить анализ данных.

Заключение

По причине того, что киберфизические системы функционируют на базе устройств низкой производительности в условиях низкой пропускной способности, такие системы имеют недостаточный уровень защищенности. В силу особенности задач, решаемых системами такого рода, реализуемые меры защиты в них направлены прежде всего на обеспечение высокой доступности и надежности.

Беспроводная связь, ячеистая топология, низкая производительность, высокие требования к энергопотреблению – все это приводит к тому, что традиционные средства защиты невозможно применить в киберфизических системах. Однако использование помехозащищенных технологий передачи, резервирование путей доставки данных, анализ системы на предмет аномалий, использование алгоритмов шифрования из класса «легковесной» криптографии, а также использование схем аутентификаций для слабопроизводительных систем позволяют значительно повысить уровень защищенности киберфизической системы.

Также существует и другой подход к защите – технология защиты движущейся цели. Данная технология не ограничивает в действиях злоумышленника, а лишь не позволяет ему обладать долгосрочной информацией о системе, на основе которой он может эффективно планировать свою атаку.

Исследование выполнено при финансовой поддержке Минцифры РФ (грант ИБ). Проект № 40469-07/2021-К.

Литература

1. Киберфизические системы в современном мире. Блог компании Toshiba [Электронный ресурс]. – Режим доступа: http://habr.com/ru/company/toshibarus/blog/438262, свободный (дата обращения: 15.08.2022).

2. Куприяновский В.П. Киберфизические системы как основа цифровой экономики / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies. – 2016. – Т. 4, № 2. – С. 18–25.

3. Чеклецов В.В. Чувство планеты. Интернет вещей и следующая технологическая революция. – М.: Изд-во Российского исследовательского центра по интернету вещей, 2013. – 130 с.

4. Русанов П.И. Особенности работы беспроводных сенсорных сетей / П.И. Русанов, А.Г. Юрочкин // Вестник Воронежского института высоких технологий. – 2019. – № 4 (31). – С. 79–81.

5. Десницкий В.А. Анализ защищенности программно-аппаратных компонентов в беспроводных сенсорных сетях / В.А. Десницкий, А.В. Мелешко // Информационные технологии и телекоммуникации. – 2019. – Т. 7, № 1. – С. 75–83.

6. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey / A. Barua, A. Al Alamin, S. Hossain, E. Hossain // IEEE Open Journal of the Communications Society. – 2022. – Vol. 3. – P. 251–281.

7. Security analysis of ZigBee / X. Fan, F. Susan, W. Long, S. Li // MWR InfoSecurity. – 2017. – P. 1–18.

8. ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys / P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, S. Carlsen // 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. – 2010. – P. 465–470.

9. Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned / O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen // 2014 14th International Conference on Hybrid Intelligent Systems. – 2014. – P. 199–206.

10. Ďurech J. Security attacks to ZigBee technology and their practical realization / J. Ďurech, M. Franeková // 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI). – 2014. – P. 345–349.

11. Chacko S. Security mechanisms and Vulnerabilities in LPWAN / S. Chacko, M.D. Job // IOP conference series: materials science and engineering. – IOP Publishing, 2018. – Vol. 396, No. 1. – P. 012027.

12. Lilli M. Formal Proof of a Vulnerability in Z-Wave IoT Protocol / M. Lilli, C. Braghin, E. Riccobene // SECRYPT. – 2021. – P. 198–209.

13. Crushing the Wave--new Z-Wave vulnerabilities exposed / N. Boucif, F. Golchert, A. Siemer, P. Felke, F. Gosewehr // arXiv preprint arXiv:2001.08497. – 2020.

14. Nebbione G. Security of IoT application layer protocols: Challenges and findings / G. Nebbione, M.C. Calzarossa // Future Internet. – 2020. – Vol. 12, No. 3. – P. 55–75.

15. Secure bootstrapping of nodes in a CoAP network / O. Bergmann, S. Gerdes, S. Schafer, F. Junge, C. Bormann // 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). – 2012. – P. 220–225.

16. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography / F. Albalas, M. Al-Soud, O. Almomani, A. Almomani // Power (mw). – 2018. – Vol. 1333. – P. 550–558.

17. NTT Security - GTIR 2017 [Электронный ресурс]. – Режим доступа: https://www.nttsecurity.com/en-us/gtir-2017, свободный (дата обращения: 15.08.2022).

18. Jangra M. Performance analysis of CLEFIA and PRESENT lightweight block ciphers / M. Jangra, B. Singh // Journal of Discrete Mathematical Sciences and Cryptography. – 2019. – Vol. 22, No. 8. – P. 1489–1499.

19. Ertaul L. IoT security: Performance evaluation of grain, mickey, and trivium-lightweight stream ciphers / L. Ertaul, A. Woodall // Proceedings of the International Conference on Security and Management (SAM). – 2017. – P. 32–38.

20. Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA / X. Li, N. Ruan, F. Wu, J. Li, M. Li // 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). – 2014. – P. 1–8.

21. A secure user authentication protocol for sensor network in data capturing / Z. Quan, T. Chunming, Z. Xianghan, R. Chunming // Journal of Cloud Computing. – 2015. – Vol. 4, No. 1. – P. 1–12.

22. Кушко Е.А. Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. – 2020. – № 4. – С. 39–52.

23. Kushko E.A. Concealment of sensor network node interaction / E.A. Kushko, N.Y. Parotkin // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1155, No. 1. – P. 012058.

Кушко Евгений Александрович
Аспирант каф. безопасности информационных технологий (БИТ) Сибирского государственного ун-та науки и технологий (СибГУ) им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, д. 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: evgeny.kushko@gmail.com

Грачёв Дмитрий Александрович
Студент каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: ostromir28@gmail.com

Паротькин Николай Юрьевич
Канд. техн. наук, доцент каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: nyparotkin@yandex.ru

Золотарёв Вячеслав Владимирович
Канд. техн. наук, доцент, зав. каф. БИТ СибГУ им. акад. М.Ф. Решетнёва
Имени газеты «Красноярский рабочий» пр-т, 31,
г. Красноярск, Россия, 660037
Тел.: +7 (391-2) 22-76-39
Эл. почта: amida.2@yandex.ru

Kushko E.A., Grachyov D.A., Parotkin N.Y., Zolotaryov V.V.

Security issues of cyber-physical systems

Cyber-physical systems are increasingly being used in all industries. However, as the distribution of these systems grows, the number of attacks on them increases. The paper covers main cyber-physical systems building technologies, implemented security measures, advantages, disadvantages and vulnerabilities of such systems. The authors also provide a general approach to ensuring cyber-physical systems security.

Keywords: cyber-physical systems, sensor networks, internet of things, vulnerability.
DOI: 10.21293/1818-0442-2022-25-4-101-109

References

1. *Kiber-fizicheskie sistemy v sovremennom mire. Blog kompanii Toshiba* [Cyber-physical systems in the modern world. Toshiba Blog]. Available at: http://habr.com/ru/company/toshibarus/blog/438262, free (Accessed: August 15, 2022) (in Russ.).

2. Kupriyanovsky V.P., Namiot D.E., Sinyagov S.A. [Cyber-physical systems as a base for digital economy]. *International Journal of Open Information Technologies*, 2016, vol. 4, no. 2, pp. 18–25 (in Russ.).

3. Cheklecov V.V. *Chuvstvo planety. Internet veshchej i sleduyushchaya tekhnologicheskaya revolyuciya* [Feeling the planet. Internet of Things and the next technological revolution]. Moscow: Russian Research Center Internet of Things Publ., 2013. 130 p. (in Russ.).

4. Rusanov P.I. Yurochin A.G. [Wireless features touch networks]. *Bulletin of Voronezh Institute of High Technologies*, 2019, no. 4 (31), pp. 79–81 (in Russ.).

5. Desnitsky V.A., Meleshko A.V. [Security analysis of software and hardware components in wireless sensor networks]. *Telecom IT*, 2019, vol. 7, no. 1, pp. 75–83 (in Russ.).

6. Barua A., Al Alamin A., Hossain S., Hossain E. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. *IEEE Open Journal of the Communications Society*, 2022, vol. 3, pp. 251–281.

7. Fan X., Susan F., Long W., Li S. Security analysis of ZigBee. *MWR InfoSecurity*, 2017, pp. 1–18.

8. Radmand P., Domingo M., Singh J., Arnedo J., Talevski A., Petersen S., Carlsen S. ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys. *Proceedings of 2010 International Conference on P2P*, Parallel, Grid, Cloud and Internet Computing. IEEE Publ., 2010, pp. 465–470.

9. Olawumi O., Haataja K., Asikainen M., Vidgren N., Toivanen P. Three practical attacks against ZigBee security:

Attack scenario definitions, practical experiments, countermeasures, and lessons learned. *Proceedings of 14th International Conference on Hybrid Intelligent Systems*. IEEE Publ., 2014, pp. 199–206.

10. Ďurech J., Franeková M. Security attacks to ZigBee technology and their practical realization. *Proceedings of 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, 2014, pp. 345–349.

11. Chacko S., Job M.D. Security mechanisms and Vulnerabilities in LPWAN. *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 396, no. 1, p. 012027.

12. Lilli M., Braghin C., Riccobene E. Formal Proof of a Vulnerability in Z-Wave IoT Protocol. *SECRYPT*, 2021, pp. 198–209.

13. Boucif N., Golchert F., Siemer A., Felke P., Gosewehr F. Crushing the Wave--new Z-Wave vulnerabilities exposed. *arXiv preprint arXiv:2001.08497*, 2020. Available at: https://arxiv.org/abs/2001.08497 (Accessed: August 15, 2022).

14. Nebbione G., Calzarossa M.C. Security of IoT application layer protocols: Challenges and findings. *Future Internet*, 2020, vol. 12, no. 3, pp. 55–75.

15. Bergmann O., Gerdes S., Schafer S., Junge F., Bormann C. Secure bootstrapping of nodes in a CoAP network. *Proceedings of Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE Publ., 2012, pp. 220–225.

16. Albalas F., Al-Soud M., Almomani O., Almomani A. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. *Power (mw)*, 2018, vol. 1333, pp. 550–558.

17. NTT Security - GTIR 2017. Available at: https://nttsecurity.com/en-us/gtir-2017, free (Accessed: August 15, 2022).

18. Jangra M., Singh B. Performance analysis of CLEFIA and PRESENT lightweight block ciphers. *Journal of Discrete Mathematical Sciences and Cryptography*, 2019, vol. 22, no. 8, pp. 1489–1499.

19. Ertaul L., Woodall A. IoT security: Performance evaluation of grain, mickey, and trivium-lightweight stream ciphers. *Proceeding of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science Computer Engineering and Applied Computing WorldComp Publ., 2017, pp. 32–38.

20. Li X., Ruan N., Wu F., Li J., Li M. Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA. *Proceedings of 33rd International Performance Computing and Communications Conference (IPCCC)*. IEEE Publ., 2014, pp. 1–8.

21. Quan Z., Chunming T., Xianghan Z., Chunming R. A secure user authentication protocol for sensor network in data capturing. *Journal of Cloud Computing*, 2015, vol. 4, no. 1, pp. 1–12.

22. Kushko E.A. [Secure data communication implementing method based on dynamic network topology]. *Herald of the Siberian State University of Telecommunications and Informatics*, 2020, no. 4, pp. 39–52 (in Russ.).

23. Kushko E.A., Parotkin N.Y. Concealment of sensor network node interaction. *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1155, no. 1, p. 012058.

Evgenij A. Kushko
Postgraduate student, Department of Information Technologies Security, Reshetnev Siberian State University of Science and Technology (SibSU)
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: evgeny.kushko@gmail.com

Dmitrij A. Grachyov
Student, Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: ostromir28@gmail.com

Nikolaj Y. Parotkin
Candidate of Science in Engineering, Assistant Professor, Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: nyparotkin@yandex.ru

Vyacheslav V. Zolotaryov
Candidate of Science in Engineering, Head of Department of Information Technologies Security, SibSU
31, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
Phone: +7 (391-2) 22-76-39
Email: amida.2@yandex.ru