Денисов Н.А. Методика разработки и внедрения защитных протоколов для IoT устройств с учетом распространенных уязвимостей // Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 4(42) С. 107–114

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.052

МЕТОДИКА РАЗРАБОТКИ И ВНЕДРЕНИЯ ЗАЩИТНЫХ ПРОТОКОЛОВ ДЛЯ IOT УСТРОЙСТВ С УЧЕТОМ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ

Денисов Н.А.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: ndenisoff@icloud.com

По мере того как устройства интернета вещей (IoT) становятся неотъемлемой частью повседневной жизни людей, важными элементами промышленности, медицины и других ключевых секторов экономики, они также начинают выступать целью для кибератак. Уязвимости в этих устройствах могут привести к серьезным последствиям, в том числе, утечке конфиденциальной информации, нарушению работы ключевых систем и даже физическим угрозам. Более того, характер и сложность уязвимостей в IoT устройствах часто отличаются от традиционных вычислительных систем. Недостатки в безопасности могут возникать на различных уровнях – аппаратном и прикладном обеспечении, сетевых протоколах и других элементах. Это означает, что подходы к защите, применяемые в традиционных ИТ-системах, не всегда применимы к IoT и создает потребность в разработке специализированных защитных протоколов для IoT. В связи с вышеизложенным, автором настоящей статьи, была предпринята попытка исследования методики разработки и внедрения защитных протоколов для iot устройств с учетом распространенных уязвимостей

Ключевые слова: Устройства интернета вещей (IoT), кибератаки, разработка и внедрение защитных протоколов, IoT устройства, распространенные уязвимости, разработка специализированных защитных протоколов для IoT.

METHODOLOGY FOR DEVELOPMENT AND IMPLEMENTATION OF SECURITY PROTOCOLS FOR IOT DEVICES, CONSIDERING COMMON VULNERABILITIES

Denisov N.A.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ndenisoff@icloud.com

As Internet of Things (IoT) devices become an integral part of people's daily lives, important elements of industry, medicine and other key sectors of the economy, they also become a target for cyber attacks. Vulnerabilities in these devices can lead to serious consequences, including leakage of confidential information, disruption of key systems, and even physical threats. Moreover, the nature and complexity of vulnerabilities in IoT devices often differ from traditional computing systems. Security flaws can occur at various levels - hardware and application software, network protocols and other elements. This means that security approaches used in traditional IT systems are not always applicable to IoT and creates a need for the development of specialized security protocols for IoT. In connection with the above, the author of this article made an attempt to study the methodology for the development and implementation of security protocols for iot devices, taking into account common vulnerabilities.

Keywords: Internet of Things (IoT) devices, cyber attacks, development and implementation of security protocols, IoT devices, common vulnerabilities, development of specialized security protocols for IoT.

Введение

Интернет вещей (IoT) представляет собой растущую сеть физических объектов, оснащенных встроенными сенсорами, программным обеспечением и другими технологиями для подключения и обмена данными с другими устройствами и системами через Интернет. Данная концепция революционизирует способ взаимодействия людей с окружающим миром, предоставляя новые возможности для интеграции физического и цифрового пространств.

Традиционно Интернет использовался для соединения компьютеров и мобильных устройств. Однако, с появлением IoT, практически любой объект может быть оснащен способностью отправлять и получать данные. IoT способствует созданию "умных" домов и предприятий, где все устройства могут быть связаны и автоматически управляться. К возможностям IoT относят автоматизацию процессов (например, регулирование температуры, освещения и безопасности), предоставление пользователю возможности контролировать эти процессы удаленно через смартфоны или другие устройства и т.д.

В современную эпоху, когда технологии интернета вещей (IoT) стремительно интегрируются в повседневную жизнь, обеспечение безопасности этих устройств становится насущной необходимостью. Растущая зависимость от IoT в различных сферах (бытовая автоматизация, промышленное производство, здравоохранение и т.д.), подчеркивает значимость разработки и внедрения эффективных защитных протоколов. Особенно это актуально с учетом увеличения числа кибератак и уязвимостей, которые способны кардинально нарушить приватность, безопасность данных и функциональную надежность систем на основе IoT. Проблема обеспечения безопасности IoT устройств усугубляется многообразием существующих устройств и разнообразием способов их применения. Таким образом, разработка универсальных и одновременно специфических защитных протоколов, способных учитывать широкий спектр уязвимостей и атак, является важной и востребованной задачей.

Характеристика методики

Целью методики разработки и внедрения защитных протоколов для IoT устройств является предотвращение различных уязвимостей и обеспечение высокого уровня безопасности данных и функционирования устройств.

Основные задачи методики: анализ уязвимостей, разработка стратегии защиты, минимизация поверхности атаки, протоколирование и мониторинг, соблюдение нормативных требований.

Центральным элементом методики является комплексный подход к безопасности, который включает в себя технические аспекты защиты, а также управленческие, нормативные и процедурные меры. Методика учитывает не только непосредственно угрозы безопасности и уязвимости самих устройств, но и широкий спектр внешних и внутренних факторов, способных повлиять на безопасность системы в целом. Стратегия защиты, реализованная в рамках данной методики, определяет оптимальные способы защиты устройств и данных от различных видов атак путем выбора подходящих методов шифрования, управления доступом, аутентификации и других мер безопасности.

Методика также направлена на минимизацию поверхности атаки, что подразумевает ограничение возможностей для несанкционированного доступа и вмешательства в работу устройств и систем путем оптимизации конфигураций устройств и сетей, а также ограничения

доступа к некритичным функциям и сервисам. Для обеспечения возможности отслеживания и анализа безопасности в реальном времени, своевременного обнаружения и реагирования на инциденты безопасности, аудита и проверки соответствия систем безопасности установленным требованиям и стандартам, предусмотрено протоколирование и мониторинг.

С целью юридической защиты и повышения доверия пользователей и партнеров к системе IoT, предлагаемая методика предусматривает соблюдение нормативных требований в части соответствия законодательству и стандартам в области защиты данных и информационной безопасности.

Предлагаемая методика подразумевает интеграцию на четырех уровнях IoT устройств:

1. Уровень приложений занимает центральное место во взаимодействии пользователя с IoT-системой и включает в себя все программное обеспечение и приложения, которые позволяют пользователям управлять IoT-устройствами, а также собирать, анализировать и визуализировать данные, полученные от этих устройств. На уровне приложений обеспечивается защита пользовательского интерфейса и приложений, которые взаимодействуют с IoT устройствами. Предлагается использование SSL/TLS для защиты данных, передаваемых между приложениями и IoT устройствами; реализация многофакторной аутентификации и контроля доступа к приложениям; автоматизация процесса обновления приложений для устранения уязвимостей и поддержания актуальности защиты; отслеживание активности пользователей и запись событий безопасности.

2. Уровень служб касается сервисов и программного обеспечения, которое управляет IoT устройствами. На данном уровне планируется обеспечение безопасности API, через который приложения взаимодействуют с устройствами; разделение систем на разные сегменты для снижения рисков распространения угроз; реализация надежных процедур бэкапа и восстановления данных для предотвращения потерь информации.

3. Сетевой уровень в архитектуре Интернета вещей обеспечивает связь между IoT-устройствами и другими компонентами системы (серверы обработки данных или приложения уровня пользователя). Сетевой уровень отвечает за передачу данных, собранных устройствами, и является ключевым для обеспечения эффективности и безопасности всей IoT-системы. На сетевом уровне акцент сделан на обеспечении безопасности передачи данных между устройствами и через сетевые узлы. Будет реализовано использование VPN и шифрование сетевого трафика для защиты данных в процессе передачи; создание сетевых сегментов для изоляции критически важных устройств и данных; развертывание IDS/IPS для мониторинга и реагирования на подозрительную активность в сети.

4. Уровень элементов относится к физическим устройствам и компонентам, которые непосредственно выполняют сбор данных и взаимодействуют с внешней средой. На уровне элементов рассматривается защита физических устройств и компонентов. Будет организована защита устройств от несанкционированного физического доступа и повреждений; регулярное обновление прошивок, использование надежного аппаратного обеспечения; ограничение функционала устройств до необходимого минимума для уменьшения рисков.

Алгоритм реализации методики: [4, с. 725]

1. Оценка существующей инфраструктуры IoT, выявление и анализ уязвимостей на всех уровнях (аппаратное обеспечение, программное обеспечение, сетевые компоненты).

2. Анализ уязвимостей и выбор инструментов для тестирования безопасности.

3. Проектирование и разработка защитных протоколов, адаптированных под специфику IoT устройств:

- создание системы защиты, предусматривающей шифрование данных, управление доступом и аутентификации, авторизацию и обнаружение инцидентов;
- устранение ненужных функций, ограничение доступа, применение принципа наименьших привилегий;
- разработка процесса обновления программного обеспечения и прошивок, включая патчи безопасности.

4. Пилотное внедрение протоколов с последующим тестированием и оптимизацией: [1, с. 69]

- установка систем протоколирования и мониторинга для обнаружения и реагирования на инциденты;
- проведение тестов на проникновение и оценка рисков, связанных с уязвимостями.

5. Развертывание защитных протоколов на все IoT устройства, интеграция с существующими системами безопасности и настройка систем мониторинга и реагирования на инциденты.

6. Разработка программ обучения для разработчиков, администраторов и пользователей, проведение обучающих семинаров для сотрудников.

Основными программными модулями предлагаемого решения будут являться: [6, с. 59]

1. Модуль анализа уязвимостей. Отвечает за автоматическое сканирование уязвимостей в рамках интеграции с инструментами для обнаружения известных уязвимостей в аппаратном и программном обеспечении IoT, а также за ручную оценку уязвимостей в виде интерфейса для проведения экспертных аудитов и анализа сложных уязвимостей, которые не могут быть обнаружены автоматически.

2. Модуль шифрования и защиты данных. Обеспечивает за реализацию современных алгоритмов шифрования для защиты данных, передаваемых и хранимых на IoT устройствах, а также за безопасное хранение и обновление ключей шифрования.

3. Модуль управления доступом и аутентификации. Основные функции - управление доступом пользователей и устройств к IoT системам и возможность применения дополнительных мер аутентификации для повышения уровня безопасности.

4. Модуль минимизации поверхности атаки. Обеспечивает анализ текущей конфигурации с точки зрения ее оптимизации и управление настройками сети и устройств для ограничения доступа к неиспользуемым функциям и сервисам.

5. Модуль обновления и патчинга. Основные функции - автоматизация процесса обновления программного обеспечения, прошивок устройств и информирование администраторов о новых обновлениях безопасности.

6. Модуль мониторинга и протоколирования. Отвечает за обнаружение и предотвращение вторжений (IDS/IPS) путем мониторинга сетевого трафика на предмет подозрительной активности. Осуществляет запись важных событий безопасности для последующего анализа и расследования инцидентов (логирование и аудит).

7. Модуль тестирования на проникновение и оценки рисков. Обеспечивает интеграцию с инструментами для проведения тестов на проникновение и оценки уязвимостей и оценки и приоритизацию рисков, связанных с уязвимостями

Ожидаемые результаты: [3, с. 78]

- уменьшение количества уязвимостей и инцидентов безопасности в среде IoT;
- повышение уровня безопасности данных и надежности работы IoT устройств;
- соответствие современным стандартам и требованиям в области кибербезопасности.

Использование защитных протоколов для IoT устройств целесообразно в рамках системы Умный Дом и промышленных IoT систем.

В рамках системы Умный Дом внедрение защитных протоколов актуально для таких IoT устройств, как умные замки, системы безопасности, термостаты, и устройства для управления освещением и бытовой техникой.

Умные замки обеспечивают физическую безопасность дома; защитные протоколы здесь необходимы для предотвращения несанкционированного доступа, что важно для обеспечения безопасности жильцов. Системы безопасности включают в себя камеры видеонаблюдения, датчики движения и другие средства мониторинга; защита данных, передаваемых этими устройствами, минимизирует риски утечки информации о домашнем хозяйстве. Умные термостаты, контролирующие климат в доме, должны быть защищены от несанкционированного управления, поскольку это может привести к неэффективному использованию энергии или даже повреждению системы отопления и охлаждения. Защита устройств для управления освещением и бытовой техникой обеспечивает удобство и экономию энергии, а также предотвращает потенциальные риски, связанные с перегрузкой электросети или неожиданным включением техники.

Таким образом, основная цель внедрения предлагаемой методики в системе Умный Дом - повышение безопасности и защиты личной информации, снижение риска несанкционированного доступа. Особенности реализации защитных протоколов: [7, с. 124]

- анализ уязвимостей каждого устройства в системе, особенно умных замков и систем безопасности;
- внедрение защитных протоколов, включающих двухфакторную аутентификацию для доступа к умному замку и шифрование данных между устройствами и центральным управляющим хабом;
- отключение неиспользуемых сетевых интерфейсов и сервисов для обеспечения минимизации поверхности атаки.
- установление процесса автоматического обновления программного обеспечения для всех устройств.

Промышленные IoT системы используются для мониторинга и управления производственными процессами. В данном случае, внедрение защитных протоколов актуально для сенсоров по измерению температуры, давления и других параметров.

Так, защита сенсоров и устройств от несанкционированного доступа и манипуляций обеспечивает получение более точных и надежных данных для производственных процессов. Предотвращение вмешательства в работу систем позволяет поддерживать стабильность и эффективность производства. С учетом того, что промышленные IoT системы часто связаны с интернетом, они могут стать целью для хакеров. Предлагаемая методика помогает предотвратить атаки, направленные на парализацию производственных процессов или кражу конфиденциальной информации, а внедрение комплексных мер безопасности (шифрование

данных, сетевая безопасность) защищает системы от внешних и внутренних угроз. Надежная защита IoT устройств снижает риск непредвиденных остановок в производственных процессах, что может быть вызвано как техническими сбоями, так и кибератаками, обеспечивая более высокую производственную эффективность и снижая потенциальные финансовые потери от простоев. Кроме того, использование предложенной методики дает возможность предприятиям соответствовать стандартам и нормативным требованиям в области кибербезопасности и защиты данных, повышая их репутацию и доверие со стороны клиентов и партнеров.

Таким образом, основная цель внедрения предлагаемой методики в управлении производственными процессами - повышение надежности и безопасности промышленных систем, защита от потенциальных кибератак и снижение риска простоев на производстве.

Особенности реализации защитных протоколов:

- оценка уязвимостей промышленных IoT устройств, особенно в области защиты данных от внешних атак;
- реализация защитных механизмов, в частности шифрование всех передаваемых данных и строгие процедуры аутентификации для доступа к управлению системами;
- удаление всех ненужных функций и ограничение сетевых подключений только до необходимых узлов;
- настройка автоматизированной системы для обновления программного обеспечения и прошивок.

Таким образом, разработка и внедрение защитных протоколов для устройств интернета вещей (IoT) – это процесс создания и применения комплекса мер безопасности, предназначенных для защиты IoT устройств от различных угроз кибербезопасности.

Данный процесс осуществляется через комплексный анализ уязвимостей IoT устройств, последующую разработку стратегии защиты, адаптированной к специфике этих устройств, и реализацию предложенных защитных мер. Целью разработки и внедрения защитных протоколов является обеспечение безопасности и конфиденциальности данных, передаваемых и обрабатываемых IoT устройствами, защита устройств от несанкционированного доступа и снижение риска кибератак. [2, с. 49]

Реализация данных мер обусловлена растущим использованием IoT устройств и их интеграцией в критически важные области жизни и экономики. Предлагаемая методика предназначена для производителей и разработчиков IoT устройств, а также для специалистов по кибербезопасности и ИТ-администраторов, работающих в компаниях и организациях, использующих IoT технологии. Кроме того, она актуальна для конечных пользователей этих устройств, поскольку повышает уровень их безопасности и надежности.

Данный процесс предполагает максимально оперативную реализацию, учитывая текущую динамику роста использования IoT и соответствующих угроз кибербезопасности, а также требует регулярного пересмотра и обновления в соответствии с появлением новых технологий, угроз и стандартов безопасности. [5, с. 26]

В заключение можно отметить, что в современную эпоху цифровизации разработка и внедрение защитных протоколов для IoT устройств является важным элементом стратегии кибербезопасности, и ее значимость будет только повышаться по мере дальнейшего развития и распространения технологий интернета вещей.

Список литературы

1. Бармин, С. Протоколы прикладного уровня для функций M2M и IoT / С. Бармин // Электронные компоненты. – 2021. – № 10. – С. 66-71.
2. Кычкин, А. В. Разработка программной системы для управления IoT-устройствами с использованием структурных и поведенческих паттернов / А. В. Кычкин, О. В. Горшков // Прикладная информатика. – 2020. – Т. 15, № 4(88). – С. 44-53.
3. Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения / М. М. Ковцур, Д. И. Кириллов, А. В. Михайлова, П. А. Потемкин // Техника средств связи. – 2020. – № 4(152). – С. 74-86.
4. Корзухин, С. В. Конфигурируемые IoT-устройства на основе SoC-систем ESP8266 и протокола MQTT / С. В. Корзухин, Р. Р. Хайдарова, В. Н. Шматков // Научно-технический вестник информационных технологий, механики и оптики. – 2020. – Т. 20, № 5. – С. 722-728.
5. Кумалатов, Р. Ш. Разнообразие устройств и протоколов в решении безопасности iot / Р. Ш. Кумалатов // Студенческий. – 2022. – № 34-1(204). – С. 25-26.
6. Харламов, М. А. Использование уязвимостей IOT-устройств при DDOS-атаках / М. А. Харламов, Е. Д. Никитин // Молодежная научная школа кафедры "Защищенные системы связи". – 2021. – Т. 1, № 2(4). – С. 57-60.
7. Горбенко, А. К. Анализ методов обнаружения уязвимостей в IoT-устройствах / А. К. Горбенко, А. А. Маринов // Научный альманах Центрального Черноземья. – 2022. – № 1-6. – С. 117-128.

References

1. Barmin, S. Application layer protocols for M2M and IoT functions / S. Barmin // Electronic components. - 2021. – No. 10. – pp. 66-71.
2. Kychkin, A.V. Development of a software system for controlling IoT devices using structural and behavioral patterns / A.V. Kychkin, O. V. Gorshkov // Applied Informatics. - 2020. – vol. 15, No. 4(88). – pp. 44-53.
3. Development of a methodology for implementing machine learning to improve the information security of a web application / M. M. Kovtsur, D. I. Kirillov, A.V. Mikhailova, P. A. Potemkin // Communication equipment. – 2020. – № 4(152). – pp. 74-86.
4. Korzukhin, S. V. Configurable IoT devices based on the ESP8266 SoC systems and the MQTT protocol / S. V. Korzukhin, R. R. Khaidarova, V. N. Shmatkov // Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. - 2020. – Vol. 20, No. 5. – pp. 722-728.
5. Kumalatov, R. S. A variety of devices and protocols in the iot security solution / R. S. Kumalatov // Studentskiy. – 2022. – № 34-1(204). – pp. 25-26.
6. Kharlamov, M. A. The use of vulnerabilities of IOT devices in DDOS attacks / M. A. Kharlamov, E. D. Nikitin // Youth Scientific School of the department "Secure communication systems". - 2021. – Vol. 1, No. 2(4). – pp. 57-60.

7. Gorbenko, A. K. Analysis of vulnerability detection methods in IoT devices / A. K. Gorbenko, A. A. Marinov // Scientific Almanac of the Central Chernozem region. - 2022. – No. 1-6. – pp. 117-128.