Б. Я. СОВЕТОВ, Т. М. ТАТАРНИКОВА
Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СИСТЕМЫ УМНОГО ДОМА

Обсуждается проблема обеспечения информационной безопасности «умного дома», перечисляются основные уязвимости и последствия, к которым они могут привести. Предложены механизмы защиты информации в системе «умного дома» исходя из характеристик потребляемых ресурсов: энергии, времени, вычислительной мощности. Представлено описание собранного макета системы «умного дома», на котором выполнялось измерение характеристик потребляемых ресурсов с целью обоснованного выбора метода защиты информации, передаваемой устройствами по открытым каналам.

Введение. Подключение «умных» устройств к всемирной паутине требует обеспечения безопасности данных, передаваемых по каналам «устройство-устройство», «устройство-сервер», «устройство-пользователь». Злоумышленники могут не только похитить конфиденциальную информацию, но и перехватить контроль над устройством.

Основными уязвимостями безопасности системы «умного дома» являются [1]:

- Использование производителями систем умного дома собственного программного обеспечения, что усложняет взаимодействие между устройствами разных производителей. Кроме того, часто программное обеспечение имеет закрытый код, что в свою очередь затрудняет поиск уязвимостей.
- Незащищенность трафика, что может привести к получению злоумышленниками данных, передаваемых устройствами.
- Отсутствие механизма аутентификации, что позволяет злоумышленникам перехватить контроль над устройством.

Перечисленные угрозы могут привести к следующим последствиям:

- Нарушение работы устройства.
- Нарушение конфиденциальности, целостности и доступности информации.
- Перехват управления устройством злоумышленником.

Большая часть этих последствий объясняется малой производительностью устройств, что не позволяет реализовать защиту информации в полной мере [2,3].

Существует несколько подходов к обеспечению защиты устройств умного дома. Все они различаются алгоритмами, моделями угроз, но что более значимо для систем подобного рода – значениями потребляемых ресурсов: энергии, времени, вычислительной мощности.

В данной работе предложены методы защиты информации, передаваемой устройствами по открытым каналам в системе умного дома, выбор которых обоснован экспериментальным путем. Во-первых, собран макет системы умного дома, во-вторых, выполнены замеры потребляемых ресурсов.

Предлагаемый доклад посвящен особенностям реализации макета и выполнению на нем экспериментов для обоснования методов защиты информации.

Особенности реализации макета системы умного дома. В рамках макета системы умный дом реализованы следующие программные и программно-аппаратные модули (рисунок):

- Контроллер и подключенные к нему датчики температуры и давления.
- Сервер.
- База данных.
- Интерфейс пользователя.

В качестве контроллера для взаимодействия с датчиками используется Arduino uno [4]. Работа контроллера организована в бесконечном цикле – постоянно опрашиваются датчики и проверяются подключения пользователей. Для управления отключением/включением внешними устройствами используется реле.

Сервер реализован на языке php по шаблону MVC модель-представление-контроллер, что позволяет логически разделить взаимодействие с базой данных, интерфейс пользователя и логику приложения [5, 6].

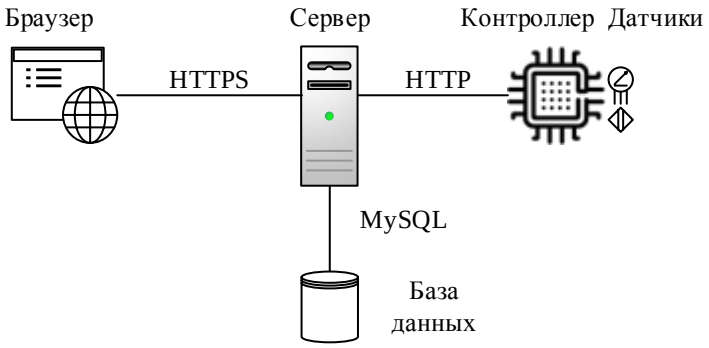

Рисунок. Схема взаимодействия модулей в макете системы «умный дом»

Для решения задачи хранения данных и контроля доступа используется база данных. База включает следующие таблицы: данные пользователя, уровни доступа, действия, которые поддерживаются приложением, показания и история их изменений.

Интерфейс пользователя представляет собой веб-приложение, которое содержит страницу регистрации, авторизации и главную страницу, на которой происходит отображение данных с контроллера. Приложение встречает пользователя окном авторизации, в котором пользователь может ввести свои данные для входа в систему или зарегистрироваться для начала работы. После входа пользователь попадает на главную страницу приложения. Здесь ему доступны данные с датчиков, которые обновляются раз в несколько секунд. Запросы для обновления данных происходят с помощью запросов на сервер. Также на этой странице возможно задать температуру, которая будет поддерживаться включением прибора через реле на контроллере. Еще одна возможность – просматривать историю изменения показаний температуры и влажности.

Рекомендуемые механизмы защиты системы «умный дом». В системе передаются два типа пакетов: управляющие пакеты (команды на изменение параметров) и информационные пакеты (информация с датчиков).

Поскольку контроллер является маломощным устройством, то не способен поддерживать https соединение. Поэтому для передачи данных от сервера к контроллеру используем протокол http с дополнительным решением задач шифрования и проверки целостности данных, передаваемых по сети интернет. Для шифрования рекомендуются симметричные алгоритмы. Для обеспечения целостности передаваемых данных решение принято в пользу имитозащиты, что в сравнении с электронной цифровой подписью требует меньшей вычислительной мощности и объема памяти.

Аутентификация пользователя (доступ к системе умного дома) реализуется на сервере с использованием https протокола, что позволит защитить пользовательские данные при передаче по открытым каналам. Также сервер будет запрашивать данные с контроллера и передавать их пользователю, что позволяет снять часть нагрузки с контроллера. Такой подход широко распространен при использовании маломощных устройств.

Для разделения доступа каждое действие, например получение главной страницы или запрос на обновление данных с датчиков, имеет свой уровень доступа. Так, все действия выше уровня 1 могут выполняться только зарегистрированными пользователями. Если же незарегистрированный пользователь, например, запросит данные с датчиков, то он будет переведен на страницу ошибки доступа.

Таким образом, обеспечение информационной безопасности системы умного дома включает следующие механизмы:

- Взаимодействие между клиентом и сервером осуществляется посредством протокола HTTPS, который за счет использования криптографических протоколов SSL/TLS, обеспечивает 3 уровня защиты:
  1. шифрование данных, что позволяет избежать их перехвата;
  2. фиксацию любых изменений данных, что что обеспечивает их целостность и сохранность;
  3. аутентификация, что защищает от перенаправления пользователя.

- Взаимодействие между контроллером и сервером осуществляется посредством протокола HTTP, но данные шифруются и защищаются от изменения имитовставкой.
- Шифрование/дешифрование данных, передаваемых между контроллером и сервером реализуется симметричной криптографической схемой.

Для управляющих пакетов важно использовать наиболее стойкие шифры, а также имитозащиту. Для информационных пакетов требования к защищенности ниже, но требования к скорости обработки и размеры выше.

Описание эксперимента на макете «умного дома» по замеру потребляемых ресурсов. Ресурсы, потребляемые системой, оцениваются следующими характеристиками:

1. Время отклика системы, в мс – показывает ожидаемое время ответа от системы на запрос пользователя.
2. Потребление энергии при единичном запросе, в Вт – показывает значение мощности, которую затрачивает система на обработку одного запроса.
3. Нагрузка на систему, в байтах – показывает, сколько данных передается по сети при единичном запросе.

Отклик системы оценивался посредством измерения времени от момента отправки пользовательского запроса до получения ответа в браузере клиентского компьютера [7]. Для этого использовалась стандартная панель разработчика, позволяющая просматривать время запроса.

Для оценки энергопотребления использовался мультиметр – измерялся ток, потребляемый Arduino в период выполнения запроса с вычислением потребляемой мощности.

Загрузка сети оценивалась через размеры пакетов, отправляемых с сервера на контроллер и обратно. Эта характеристика строго зависит от выбранных алгоритмов шифрования и имитовставки.

Таблица

Результаты измерений, выполненных на макете

Алгоритм шифрования	Время отклика, мс	Потребление энергии, Вт	Нагрузка на систему, байт
AES 128	126	0,059	72
AES 192	129	0,062	88
AES 256	134	0,064	104
DES	163	0,104	64
TDES	305	0,264	64
XTEA	89	0,040	64

Результаты экспериментов, проведенных на макете системы умного дома, показали, что наиболее подходящим алгоритмом для маломощных устройств является XTEA. Он обеспечивают наиболее быстрое шифрование с использованием минимальных затрат энергии. Но XTEA имеет не самую высокую криптостойкость, что ограничивает его применение для важных данных. Применение алгоритмов семейства AES также оправдано, так как они показали результаты, не сильно уступающие XTEA, но AES характеризуется высокой криптостойкостью. Таким образом, для информационных пакетов можно рекомендовать XTEA, для управляющих – AES.

Заключение. Предложенные в работе механизмы обеспечения информационной безопасности умного дома учитывают ресурсы, потребляемые системой, такие как время отклика, потребление энергии и нагрузка на систему. Выбор механизмов защиты основывается на результатах экспериментов, выполненных на макете системы умного дома.

ЛИТЕРАТУРА

1. Перспективные рынки и технологии интернета вещей: публичный аналитический доклад. М.: ООО «Лайм», 2019. 272 с.
2. **Sovetov B.Y., Tatarnikova T.M., Cehanovsky V.V.** Detection System for Threats of the Presence of Hazardous Substance in the Environment. *2019 XXII International Conference on Soft Computing and Measurements (SCM))*, St. Petersburg, Russia, 2019. P. 121-124. doi: 10.1109/SCM.2019.8903771.
3. **Doo-Soon Park**. Fault Tolerance and Energy Consumption Scheme of a Wireless Sensor Network. *International Journal of Distributed Sensor Networks*. 2013. Vol. 3. 7 p. doi: 10.1155/2013/396850.
4. **Chin R.** Arduino and Raspberry Pi Sensor Projects for the Evil Genius. McGraw-Hill Education TAB, 2017. 237 p.
5. **Bogatyrev V.A., Vinokurova M.S.** Control and Safety of Operation of Duplicated Computer Systems. *Communications in Computer and Information Science, IET – 2017*. 2017. Vol. 700. P. 331-342.

6. **Bogatyrev V.A., Bogatyrev S.V., Bogatyrev A.V.** Model and Interaction Efficiency of Computer Nodes Based on Transfer Reservation at Multipath Routing. *2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*. 2019. P. 8840647. doi: 10.1109/WECONF.2019.8840647
7. **Татарникова Т.М., Елизаров М.А.** Модель оценки временных характеристик при взаимодействии в сети интернета вещей. *Информационно-управляющие системы*. 2017. № 2 (87). С. 44-50.

B.Ya. Sovetov, T.M. Tatarnikova (Saint Petersburg Electrotechnical University “LETI”, St. Petersburg)

Smart Home Security Management

The problem of ensuring the information security of the “smart home” is discussed, the main vulnerabilities and the consequences to which they can lead are listed. The mechanisms of information protection in the “smart home” system are proposed based on the characteristics of consumed resources: energy, time, computing power. The description of the assembled model of the “smart home” system is presented, on which the characteristics of the consumed resources were measured in order to make a reasonable choice of the method of protecting information transmitted by devices over open channels.