Костюченко Владислав Владимирович
магистрант
Алефиренко Виктор Михайлович
канд. техн. наук, доцент
Белорусский государственный университет
информатики и радиоэлектроники
г. Минск, Республика Беларусь

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ И КОНТРОЛЯ ДОСТУПА В СИСТЕМАХ «УМНЫЙ ДОМ»

Аннотация*: в данной статье рассмотрены проблемы, встречающиеся при использовании системы «Умный дом». Постоянные изменения и дополнения в конструкции и архитектуре данной системы могут существенно отразиться на проблеме безопасности. Проанализированы характерные особенности существующих протоколов, выявлены их уязвимости, обоснована необходимость работы над безопасностью всей системы в целом. На основе изложенных фактов предлагаются способы повышения безопасности и контроля доступа в автоматизированной системе «Умный дом».*

Ключевые слова*: система «Умный дом», безопасность, протокол беспроводной связи, аутентификация, контроль доступа.*

В мире последнее время начала получать распространение так называемая система «Умный дом» (англ. Smart Home), которая позволяет автоматизировать и упростить управление собственным жилым помещением. Систему «Умный дом» можно рассматривать как экосистему, имеющую в своей основе программный комплекс, который тесно связан с датчиками, контроллером и облачными сервисами. Каждая компания-производитель предлагает свое видение построения систем «Умный дом» для потребителей, хотя и старается использовать один из готовых протоколов, предложенных на рынке. Но из-за высокой стоимости такого протокола, многие компании предпочитают использовать свои разработки, считая их, как минимум, не хуже существующих и уже

протестированных. К сожалению, пока нет сводных данных от исследователей безопасности о том, насколько хорошо защищено программное обеспечение (ПО) различных разработчиков, так как они не проводят открытый аудит безопасности.

Система «Умный дом» используется для облегчения и обеспечения более комфортного проживания в здании либо в офисе. Первое, что необходимо человеку, который подходит к зданию, управляемому электронной системой, – попасть внутрь при помощи ключа. Он хочет легко и комфортно открыть дверь, не доставая ключи, электронные карты или другие подобные устройства. В современных реалиях гораздо удобнее использовать смартфон, чем подобные устройства, которые нужно носить с собой. Смартфон всегда находится в кармане пользователя, так как является основным инструментом связи и неотъемлемой частью работы, и предоставляет огромный спектр вариантов для управления умным домом. Смартфон является по сути одним из ключевых пунктов контроля, настройки и управления системой умного дома. Таким образом, не требуется больше иметь набор отдельных устройств аутентификации, которые неудобно носить с собой все время.

Практически все современные мобильные устройства оснащены биометрическими сканерами. Биометрические технологии основаны на биометрии – измерении уникальных характеристик отдельно взятого человека. Это могут быть как уникальные признаки, полученные им с рождения (ДНК, отпечатки пальцев, радужная оболочка глаза), так и характеристики, приобретённые со временем или же способные меняться с возрастом или внешним воздействием (почерк, голос или походка). Обычно при классификации биометрических технологий выделяют две группы систем по типу используемых биометрических параметров [1]:

– первая группа систем использует статические биометрические параметры (отпечатки пальцев, геометрия руки, сетчатка глаза и т. п.);

– вторая группа систем использует для аутентификации динамические параметры (динамика воспроизведения подписи или рукописного ключевого слова, голос и т. п.)

Но сейчас мало кто пользуется биометрическими сканерами в системах умного дома, так как это достаточно дорого, сложно в установке и настройке, а также не всегда практично, когда домом пользуются более одного человека. Поэтому в настоящее время весьма удобно использовать смартфон как главный ключ входа в жилище либо в офис, так как он имеет набор персонализированных датчиков, которые находятся всегда с собой. Смартфон имеет записанную метку, например, NFC (Near Field Communication, «коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной передачи данных малого радиуса действия, которая передает ключ доступа к дому. Здесь кроется одна из ошибок безопасности, так как все наши смартфоны не так хорошо защищены, как принято считать. Подойдя к зданию, человек прикладывает смартфон к сканеру, затем электроника и ПО обрабатывают полученный результат, а ключ, переданный смартфоном, определяет, имеет ли он доступ в дом. После чего двери открываются, и человек может пройти в внутрь, если результат всех операций даст разрешающий ответ. Данная система весьма удобна и проста в использовании, но имеет целый ряд проблем безопасности, которые были показаны на различных конференциях по взлому и поискам ошибок системы умного дома [2].

В связи с этим весьма полезно для безопасности иметь двойную систему аутентификации пользователя. Например, при входе в здание необходимо не только приложить смартфон, но и требуется ввести пароль, либо приложить палец к сканеру отпечатка пальца, либо провести сканирование радужки глаза или лица. Сканирование лица произвести проще всего, так как почти все умные дома оборудованы системой видеонаблюдения и видеоглазком. При настройке системы умного дома видеоглазок вполне способен распознавать человеческое лицо и вкупе с правильным ключом добавит гораздо больше безопасности при входе.

Ниже на примере одного из протоколов рассмотрим, с какими проблемами безопасности чаще всего сталкивается пользователь системы умного дома. В качестве примера рассмотрим самые распространенные на данный момент

протоколы связи, которые используются по всему миру в сотнях различных сборок умных домов.

Если в здании есть система умного дома, то, очень вероятно, что используется протокол ZigBee. ZigBee – это беспроводной стандарт, используемый для подключения к устройствам управления IoT. Он используется в десятках миллионов интеллектуальных датчиков [3], и существует 1088 различных продуктах [4], перечисленных, как сертифицированные продукты ZigBee. Тем не менее, ZigBee является большой угрозой Интернету вещей из-за критических недостатков безопасности беспроводной сети, которые могут быть использованы для компрометации интеллектуальных источников света, дверных замков, датчиков движения, интеллектуальных коммутаторов, датчиков температуры, систем HVAC и других «умных» домашних устройств.

Существуют и другие возможности для подключения к устройствам IoT, например протокол Z-Wave. Однако несколько лет назад он был взломан специалистами по безопасности на конференции хакеров «Vegas Black Hat USA 2013» и «Def Con 21» [2]. Посредством этого протокола они смогли осуществлять атаки на автоматизированные дома.

Протоколы беспроводной связи ZigBee и Z-wave являются наиболее распространенной радиочастотной технологией в системах домашней автоматизации. Z-Wave – это собственный протокол беспроводной связи, который работает в промышленном, научном и медицинском радиодиапазонах (ISM). Он работает на частотах 868,42 МГц (Европа) и 908,42 МГц (США), предназначенных для передачи данных с низкой пропускной способностью во встроенных устройствах, таких как датчики безопасности, аварийные сигнальные системы, панели управления домашней автоматикой и т. д. Z-Wave микросхемы имеют 128-битный AES, которые используются системами контроля доступа, такими как дверные замки, аутентифицированное шифрование пакетов [5]. Доступна версия с открытым исходным кодом для стека протоколов Z-Wave Open ZWave, но пока она еще не поддерживает часть официально реализованного разработчиками шифрования для внешних устройств [6].

Основные проблемы безопасности выявляются преимущественно на различных конференциях, где исследователи по безопасности тестируют в том числе системы умных домов от различных производителей, взламывают протоколы и показывают системные ошибки и слабости в защите всех узлов и агрегатов умного дома, доступных для исследования, таких как контроллеры, программное обеспечение, протоколы, системы шифрования, системы связи и даже датчики.

Конференции хакеров «Vegas Black Hat USA 2013» и «Def Con 21» – не единственный случай, продемонстрировавший уязвимость протокола ZigBee. Так, например, Тобиас Зиллнер, старший аудитор IS в фирме по безопасности IT Cognosec, также предупредил, что хакеры могут скомпрометировать сети ZigBee, а затем взять на себя управление всеми подключенными устройствами в сети [7]. Сама система работает довольно по простому алгоритму, давно известному общественности. Ключи сетевого шифрования кратко передаются при очистке, когда новое устройство присоединяется к сети. Некоторые устройства используют стандартный ключ по умолчанию, то есть это то, что передается при добавлении нового устройства в сеть. Ключ может быть захвачен злоумышленником или вором, который мог бы, например, скопировать открытый ключ для умного замка двери. Научное сообщество по безопасности и этичному взлому не единожды продемонстрировала данную проблему на различных конференциях и в частных экспериментах.

Для простого примера возьмем умные лампы Philips Hue. Еще в 2013 году лампы Philips Hue были названы «легко взламываемыми» после того, как исследователь ввел вредоносное ПО в мост Hue и погасил свет [8]. По словам исследователей «Cognosec», интеллектуальные лампы постоянно ищут новые устройства для связи, что упрощает их возврат к заводским настройкам. Злоумышленник может захватить незашифрованный ключ, передаваемый лампой Hue при перезагрузке.

Если следовать логике и заявлениям исследователей «Cognosec», можно прийти к выводу, что злоумышленник может обследовать устройство и

присоединиться к нему, используя ключ по умолчанию. Тогда активный сетевой ключ будет скомпрометирован и конфиденциальность всей сетевой связи может считаться скомпрометированной. Следовательно, секретность ключей не должна быть основой архитектуры безопасности продуктов ZigBee. Это не значит, что следует избегать устройств с поддержкой ZigBee. Функции безопасности, предоставляемые стандартом ZigBee, могут считаться высококлассными и надежными [9]. Шифрование ZigBee основано на хорошо известном алгоритме AES для шифрования и аутентификации данных. Безопасность зависит от секретности ключей шифрования, а также от их безопасной инициализации и распространения ключей шифрования.

Основная проблема протокола ZigBee заключается в том, что он реализован неэффективным способом. Некоторые поставщики не думают о безопасности и реализуют минимум функций, требуемых для сертификации. Это может помочь снизить затраты, но для безопасности важно выполнить следующие предварительные условия реализации [9]:

– подделка устройства: «уязвимость, обеспечивающая защиту от несанкционированного доступа, может удалить конфиденциальную информацию, включая ключи безопасности, если обнаружен фальсификатор»;

– транспортировка ключей: «ключ ссылки по умолчанию не должен использоваться, поскольку этот ключ считается общедоступным и, следовательно, обеспечивает тот же уровень безопасности, что и незашифрованный транспорт ключей»;

– установка ключа: «основные ключи, используемые при создании ключа, должны быть распределены по внеполосным каналам». Это может быть достигнуто с помощью чего-то такого же простого, как наклейка с основным ключом, прикрепленным к устройству для входа пользователя во время установки оборудования;

– смена ключа: «безопасность связи зависит от секретности сетевого ключа и ключей связи» Сетевой ключ должен периодически меняться. Управление ключами в форме изменения сетевого ключа в рабочий период времени или после

ввода определенного количества сообщений. В противном случае может быть обнаружен известный открытый ключ или другие атаки на безопасность AES.

Существуют серьезные требования к конфиденциальности, когда речь заходит о домашней автоматизации, поскольку она генерирует огромное количество персонализированных данных. Пользователи платят высокую цену за смарт-устройства, но тогда им нужно передавать множество разрешений тем же поставщикам, чтобы использовать приложение для смартфонов для управления уже оплаченным устройством. Это само по себе неверно, потому что пользователи приобрели это устройство за высокую цену, но разработчики устройства небрежно хранят все полученные от них данные. По прогнозам Gartner, к 2022 году в домохозяйстве будет задействовано более 500 смарт-устройств для каждого домохозяйства [10], поэтому поставщикам необходимо серьезно относиться к конфиденциальности и безопасности данных пользователей.

Подводя итог вышесказанного, необходимо отметить, что системы умного дома год от года становятся безопасней и дружелюбней к пользователям, но производители упускают из виду тот факт, что простые изменения и дополнения в конструкции и архитектуре кардинально могут поменять проблему безопасности. Например, в каждом современном смартфоне уже есть дактилоскопический сенсор, часто встроены сканеры сетчатки глаза и лица. А значит, это можно использовать для дополнения к стандартной аутентификации пользователя, что сильно усложнит взлом в целом системы контроля доступа, но при этом не будет удорожать конструкцию всего умного дома, так как монтаж и установка датчика не потребуется. Так же, производителям стоило бы задуматься об использовании технологии подобной RSA ключам доступа, когда вначале требуется ввести приватный пароль, и только потом человек получает доступ к настоящему коду, ожидаемому системой, после ввода которого можно приложить смартфон с NFC меткой к сканеру. Эти простые меры позволят повысить безопасность доступа к жилищу, не делая более дорогой конструкцию, но сильно осложняя взлом и компрометацию данных пользователей.

Список литературы

1. Биометрические технологии // Свободная энциклопедия Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Биометрические_технологии (дата обращения: 21.03.2018).

2. Jun Li. I'm A Newbie Yet I Can Hack ZigBee – Take Unauthorized Control Over ZigBee Devices // DEF CON® Hacking Conference [Электронный ресурс]. – Режим доступа: https://www.defcon.org/html/defcon-23/dc-23-speakers.html#Li (дата обращения: 21.03.2018).

3. Ramon S. Zigbee Press Release: ZigBee Certified Products Surpass 1,000 // Zigbee Alliance. – 2014 [Электронный ресурс]. – Режим доступа: http://www.zigbee.org/zigbee-press-release-zigbee-certified-products-surpass-1000/ (дата обращения: 21.03.2018).

4. ZigBee Certified Products // Zigbee Alliance. – 2016 [Электронный ресурс]. – Режим доступа: http://www.zigbee.org/zigbee-products-2/ (дата обращения: 21.03.2018).

5. Introduction to the Z-Wave Security Ecosystem // Z-Wave – 2016 [Электронный ресурс]. – Режим доступа: https://z-wave.sigmadesigns.com/wp-content/uploads/2016/08/Z-Wave-Security-White-Paper.pdf (дата обращения: 21.03.2018).

6. Z-Wave Devices // Home Assistant. – 2018 [Электронный ресурс]. – Режим доступа: URL: https://home-assistant.io/docs/z-wave/devices/ (дата обращения: 21.03.2018).

7. Zillner T., Strobl S. Zigbee exploited – The good, the Bad and the ugly // Black Hat – 2015 [Электронный ресурс]. – Режим доступа: https://www.black-hat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf (дата обращения: 21.03.2018).

8. Condliffe J. Philips Hue Light Bulbs Are Highly Hackable // Gizmodo. – 2013 [Электронный ресурс]. – Режим доступа: https://gizmodo.com/how-philips-hue-light-bulbs-are-highly-hackable-1133092324 (дата обращения: 21.03.2018).

9. Zillner T. Zigbee exploited – The good, the bad and the ugly // Black Hat – 2015 [Электронный ресурс]. – Режим доступа: https://www.blackhat.com/docs/us-

15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf (дата обращения: 21.03.2018).

10. Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022 // Gartner. – 2014 [Электронный ресурс]. – Режим доступа: https://www.gartner.com/newsroom/id/2839717 (дата обращения: 21.03.2018).