УДК 681.518.5:004.896

Алефиренко Виктор Михайлович, Костюченко Владислав Владимирович
Белорусский государственный университет информатики и радиоэлектроники
(Минск, Беларусь)

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ В СИСТЕМАХ «УМНЫЙ ДОМ»

Аннотация. *Умные дома становятся все более популярными, и проблемы защищённости личных данных в них имеют первостепенную важность. Современные умные системы собирают о пользователе все большее количество информации и часто пользователи не осознают, как эта информация будет использована и куда передана, а также не представляют возможные риски при взломе или перехвате личных данных. В этой статье предоставлен обзор проблем конфиденциальности и безопасности систем современного умного дома.*

Ключевые слова: *умный дом, безопасность, приватность, IoT, сетевая безопасность.*

Alefirenko Viktor Mihajlovich, Kostuchenko Vladislav Uladimirovich
Belarus State University of Informatics and Radioelectronics
(Minsk, Belarus)

PROBLEMS OF CONFIDENTIALITY AND SECURITY IN THE SYSTEMS OF "SMART HOUSE"

Abstract*. Smart homes are becoming more popular, and the problems of protecting personal data are of great importance. Modern smart systems collect more and more information about the user and often users do not realize how this information will be used and where transferred, and also do not represent possible risks when hacking or intercepting personal data. This article provides an overview of the problems of privacy and security of modern smart home systems.*

Keywords*: smart home; security; privacy; IoT; network security.*

Проблема подключения умных домов к интернету гораздо более обширна, чем это может показаться на первый взгляд. Все дело в том, что производители не могут достаточно корректно защитить все передаваемые данные и создать надежное программное обеспечение для гаджетов пользователя и одновременно умного дома. Критически важно защитить связь между устройством пользователя и его домом, а также зашифрованный передаваемый контент. Помимо этого, большая часть данных обрабатывается удаленно, для этого чаще всего используется центральный сервер, который стоит в компании производителя системы. Его защищенность чаще всего мы проверить не можем. Также мы не знаем насколько хорошо защищено серверное помещение, где хранятся пользовательские данные. Держать же серверную комнату у себя дома достаточно дорого и не имеет особого смысла для стандартного небольшого здания. Иметь собственную серверную для

обработки данных, запросов систем, хранения информации и прочих пользовательских данных полезно только для больших офисных зданий, где находятся сотни человек и специальный персонал для обслуживания этих систем.

Современные умные дома собирают о пользователе большое количество информации, которая может иметь различный характер. Система умного дома может осуществлять следующие операции:

- интеллектуальное видеонаблюдение;
- запись голоса;
- обнаружение положения пользователя в пространстве;
- открытие, закрытие дверей и окон;
- управление домашним оборудованием;
- синхронизация со смартфоном, который может передавать данные о геолокации и копировать фотографии;
- запись аудио с телефона и в помещениях;
- получение доступа к номерам банковских карт и документам;
- синхронизация с домашними тренажерами;
- синхронизация с датчиками контроля физического состояния человека (например, с датчиком сердечного ритма, датчиками трекеров активности на руках пользователей, умными часами и т.д.).

Всё это привлекает интерес злоумышленников. А так как системы умного дома гораздо более слабо защищены, чем современные смартфоны, то такой способ взлома и получения секретных данных становится всё более актуальным. Контроль злоумышленника над такой информацией несет множество проблем и угроз конфиденциальности для пользователя.

Как правило, умный дом включает множество подключенных устройств, относящихся к различным областям применения. Обычно, области приложений делятся на четыре группы: развлечения, энергия, безопасность и здравоохранение [1].

Приложения для развлечения нацелены на максимальное удобство и комфорт и предоставляют персонализированный контент для развлечения, а также услуги социальной связи. «Энергетические» приложения предназначены для эффективного потребления энергии и управления ею. Приложения для безопасности домена предлагают услуги, предназначенные для мониторинга, обнаружения и контролирования угроз. Приложения для здравоохранения ориентированы на предоставление услуг мобильной медицинской помощи и поддержки фитнеса. Можно утверждать, что область здравоохранения имеет самое большое количество уязвимостей, от перехвата данных до фатального взлома.

По существу, систему умный дом можно рассматривать как систему устройств, коммуникаций и услуг.

1. Устройства.

Умные домашние устройства – это аппаратные блоки, обычно включающие датчики, приводы, шлюзы и умные объекты.

Типы устройств:

- Датчики – измеряют физические свойства окружающей среды или физические параметры. Виды датчиков могут варьироваться от носимых

(например, браслетов) до стационарных (например, IP-камерам). Видеокамеры считаются наиболее уязвимыми датчиками [3] наряду с микрофонами.

- Приводы и микросхемы – выполняют такие действия, как включение/выключение или затемнение света, закрывание окон, срабатывание сигналов тревоги и т. д.
- Шлюз – служит точкой доступа к дому, обычно позволяя владельцу контролировать объекты, контролировать и управлять домашними приборами или датчиками удаленно. Кроме того, он служит точкой агрегирования для отправки измеренных данных во внешнюю сеть, такую как коммунальные предприятия.
- Умные объекты – это устройства, состоящие из датчиков и/или исполнительных механизмов, которые подключены к Home Area Network. Некоторые из них включают интеллектуальные устройства, такие как интеллектуальные блокировки, которые отвечают за дверные замки и обеспечивают контроль доступа на основе времени.

2. Коммуникация.

Типичный умный дом использует разнообразные коммуникационные протоколы. Они варьируются от различных вариаций проводной связи до беспроводной связи в различных диапазонах. Как правило, датчики взаимодействуют с помощью домашней автоматизации через такие протоколы, как KNX, Zigbee, Z-Wave и DASH7 или через протоколы сетевой связи, такие как Wi-Fi, Bluetooth, 6LoWPAN, IEEE 802.15.4 или сотовой технологии.

Технологии RFID и NFC также используются для мониторинга и слежения, особенно в области здравоохранения, и обычно применяются в умных дверных замках.

3. Службы управления.

Службы – это программные приложения, размещенные в облаке или внутри домашней системы, которая несет ответственность за реализацию автоматизации, управление устройствами, принятие решений и т. д. Особая категория служб – это контроллеры, которые позволяют управлять подключенными устройствами. Как правило, домашние хозяйства устанавливают такое программное обеспечение на своих смартфонах или планшетах, чтобы локально или удаленно взаимодействовать с устройством.

Далее рассмотрим проблемы безопасности и конфиденциальности. Система умного дома может содержать конфиденциальные данные (например, личные фотографии, видео и цифровые дневники), а также такие устройства, как IP-камеры, которые могут быть удаленно активированы и доступны в любом месте. Кроме того, в ней могут быть микрофоны, которые могут слушать частные разговоры. Например, интеллектуальные акустические системы, такие как Amazon Echo и микрофоны Google Home, которые запрограммированы на прослушивание команд (например, «просыпаться») и голосовой ввод для выполнения таких задач, как уменьшение яркости и воспроизведение музыки. Это требует жестких требований безопасности из-за важности частной информации. Тем не менее, адаптация стандартных средств безопасности для подключений дома сложна, как указано в «IEEE Conference on Communications and Network Security» [4].

Ниже, упомянутые проблемы описываются и сопоставляются с различными архитектурами.

1. Проблемы с устройством:

• Ограниченность ресурсов. Умные домашние устройства часто являются batterydriven (зависят от аккумуляторов) и используют маломощные процессоры с низкими тактовыми частотами и небольшими пропускными способностями. Это делает криптографические алгоритмы, такие как RSA, довольно затратными в вычислительном смысле и их трудно переносить на такие низкие скорости [5]. Это также связано с ограничениями в объемах оперативной и флешпамяти.

• Характер управления. Типичные устройства IoT не имеют клавиатуры, мыши и экрана. Это может вынудить конечных пользователей полагаться на смартфоны или веб-сайты для ввода параметров. Кроме того, это делает такие механизмы, как «уведомление и согласие» более сложными для реализации в умных домах.

• Устойчивые к взлому пакеты. Умные домашние устройства большую часть времени являются физически доступными устройствами и могут быть подвержены физическим атакам. Иногда домовладельцы могут проводить эти атаки, например, атаки подбора параметров к умным счетчикам для уменьшения показателей расходов. Однако техническое вмешательство может также проводиться другими организациями, например, для облегчения взлома и последующей кражи.

2. Проблемы связи:

• Неоднородные протоколы. Разные протоколы связи возможно использовать для соединения устройств с умным домом, но они требуют использования мостов, концентраторов или шлюзов. Дополнительно устройство может использовать проприетарный протокол (например, не IP-адрес) локально и стандартный протокол для подключения к облаку. Эти факторы, связанные с аппаратными ограничениями, должны привести инженеров к выбору более взоломостойких схем шифрования [6].

• Динамические характеристики. Некоторые устройства, такие как носимые трекеры активности, могут подключаться или выходить из домашней сети в любое время и, возможно, из любого места. Это вызывает необходимость разработки устойчивых алгоритмов безопасности, и делает отслеживание и управление активностью непростой задачей. Характеристики мультипротокольной связи вместе с возможностями различных устройств также обеспечивают традиционную безопасность схемы связи, непригодной для домашних устройств [7].

3. Проблемы с обслуживанием:

• Ожидания в отношении срока службы системы. Требуется снижение уязвимостей дистанционного перепрограммирования при обновлении прошивки или программного кода устройства. Однако, это может быть невозможно для всех устройств потому, что операционные системы, протоколы или прошивки могут не поддерживать динамические исправления. Кроме того, некоторые устройства, например, умные счетчики, спроектированы оставаться в сети в течение многих лет, не требуя, чтобы компоненты были заменены или непосредственно поддерживались производителем.

Рассмотренные выше проблемы можно исправить. Технологические подходы к снижению рисков безопасности и конфиденциальности можно разделить на уровневые решения: устройство и связь (сеть) [2]. В работе, в соответствии с описанной архитектурой также добавим улучшение уровня обслуживания.

Идентифицированные методы взяты из работы M. Anwar «Health Policy and Technology» [8] об интегрированной парадигме здравоохранения для умных домашних устройств. Использованы примеры из недавних академических и отраслевых источников.

1. Подходы уровня устройства.

Безопасность на уровне устройств сосредоточена на гарантиях, которые дают производители устройства. Это включает в себя такие методы, как аппаратное шифрование, отказоустойчивость устройства и управление доступом на основе механизмов устройств. Подходы, предлагающие внедрение архитектур безопасности предложены S. L. Keoh в Internet of Things Journal, IEEE, они повышают безопасность транспортного уровня данных [9] и реализацию в аппаратных шифрах IEEE.

Стандартные процедуры обеспечения безопасности на уровне канала 802.15.4 были предложены в «Low power link layer security for IoT» [10]. Кроме того, для ограниченных сред были разработаны оптимизированные версии криптографических алгоритмов, таких как ECDSA. Были также построены различные платформы, которые рассматривают безопасность и конфиденциальность на этапе проектирования. Одна из таких платформ – RERUM [11]. Она охватывает безопасность на всех уровнях стека сетевого протокола с акцентом на элементы управления устройством. Это реализует защиту устройства с использованием безопасной загрузки когнитивной радиотехники и механизмов контроля доступа.

С отраслевой стороны гарантии могут включать использование аппаратного обеспечения и прошивки, сертифицированные по общим критериям и EMVCo IC Security Evaluation. Кроме того, они могут включать использование криптографических алгоритмов, которые одобрены, например, Национальным институтом стандартов и технологий.

На данный момент по-прежнему сохраняется проблема ограниченности ресурсов для большинства устройств. Новые же стандарты являются в основном экспериментальными, ограничивающими их более широкую применимость и преемственность. Кроме того, это (использование новых стандартов) может обернуться крупномасштабными тратами с потенциально высокими дополнительными расходами по сравнению со стоимостью традиционных устройств IoT.

2. Подходы уровня связи.

Решения уровня связи эффективны, когда данные, передаваемые между устройствами, службами и конечными пользователями, защищены. Популярные схемы предусматривают использование виртуальных частных сетей (VPN), межсетевые экраны и системы обнаружения вторжений (IDS) или системы предупреждения вторжения (IPS). Такой подход обычно реализуется в центральном шлюзе/прокси и в облаке.

Применимость брандмауэров, IDS и IPS, в умных домах обсуждалась в «Security in smart home environment» [12]. Вместо использования

брандмауэров и подхода IDS/IPS, в [13] предлагалось использовать анонимную систему на основе TOR для защиты конфиденциальности пользователя и более безопасного использования бытовой техники. В последнее время в продаже начали появляться специализированные интеллектуальные домашние устройства, например, Cujo, Dojo и Keezel, которые подключаются к домашнему маршрутизатору, действующему в качестве сетевого экрана. Cujo и Dojo действуют как мониторинг брандмауэров, анализируют и блокируют угрозы в режиме реального времени. Keezel создает VPN туннель для шифрования устройств и соединений.

Организации безопасности, такие как Европейское сетевое информационное агентство безопасности и Cloud Security Alliance в последние годы разработали обширную документацию, в которой особенно подробно излагаются меры безопасности на уровне сети. Однако на практике существует такая проблема, что некоторые устройства могут изменять адрес в сети и общаться через зашифрованные каналы. Это затрудняет анализ трафика, если поддерживается технологии глубокой проверки пакетов. Более того, устройства могут быть по-прежнему подвержены локальным атакам, например, внедрение вредоносного кода, установленного с помощью взломанной карты памяти.

3. Подходы уровня обслуживания.

Подходы уровня обслуживания ориентированы на программное обеспечение высокого уровня. Типичные подходы включают безопасные процессы разработки, такие как тестирование безопасности, безопасные принципы проектирования и маскировка данных. Последнее может включать использование для сохранения конфиденциальности таких методов, как k-анонимность и криптографические схемы, а также шифрование на основе атрибутов.

С точки зрения промышленности такие организации, как Open Web Application Security, участвуют в предоставлении надежного руководства в области развития, такого, как рамки оценки и руководства по тестированию для разработки устройств IoT. Другие организации, такие как Builditsecure.ly и I Amy Cavalry, предоставляют руководство для создания процессов безопасности. Такими также являются сайты, как Bug Crowd, которые позволяют разработчикам проводить аналитику безопасности и выполнять обзоры кода.

На практике, однако, нет официального руководящего органа или организации, которая обеспечивает гарантии конечным пользователям в отношении репутации конкретного поставщика услуг. Более того, некоторые методы наряду с повышением конфиденциальности или безопасности, могут приносить побочные эффекты. Например, они могут привести к информационным потерям и могут повлиять на функции персонализации, необходимые для определенных домашних устройств.

Следуя наблюдениям из всего вышесказанного, понятно, насколько часто критические вопросы безопасности и конфиденциальности могут остаться незамеченными или плохо изученными исследователями, так как коммерческая сторона этого рынка развивается высокими темпами.

В заключение приведем некоторые темы, связанные с конфиденциальностью и безопасностью умных домов, которые требуют дальнейшего изучения.

1. Управление идентификацией.

Устройства, особенно подключенные к сети Интернет, разрешают проводить операции и могут контролироваться третьими лицами. Это требует тщательной (тщательной?) проверки подлинности и авторизации сторон. Для разработки эффективного решения по управлению идентификацией требуется разработка протоколов управления безопасными ключами. Однако это трудно реализовать для беспроводных сетей и датчиков сети, как сказано C. Lee [4], и еще более осложняется разрозненными, иногда несовместимыми технологиями и отсутствием глобальных схем идентификации, что известно из доклада «A systemic approach for IoT security» [14]. Еще одним сложным аспектом является то, что процедуры аутентификации могут быть сложными для отдельных лиц и это может дополнительно повышать риск конфиденциальности.

2. Методы оценки риска.

Владельцам дома сложно оценить финансовую ценность его личных данных, так как они могут не знать, какие личные данные собираются и были ли эти данные разглашены третьим сторонам. Пользователи не осознают, чем являются эти данные. Кроме того, они могут не понимать и даже не осознавать, насколько легко можно извлечь такие данные и использовать их в незаконных целях. Необходимость использования эмпирических методов оценки риска для использования внутри умных домов были определены в «Towards a Model of Privacy and Security for Smart Homes» как важные для безопасности и как необходимые требования конфиденциальности [15].

3. Подходы к управлению информационными потоками.

Объединенные поведенческие данные могут предоставлять личные данные о поведении и действиях людей. Простые и понятные пользовательские интерфейсы могут помочь отобразить риски конфиденциальности на более интуитивном уровне и в то же время позволяют настраивать функции для последующего использования и распространения таких данных, как сказано в статье «A comprehensive approach to privacy in the cloud-based Internet of Things» [16]. Это сложные требования идентификации, поскольку устройства IoT могут быть спроектированы так, чтобы действовать автономно, без руководства пользователя. Аналогичным образом, необходимо разработать эффективные меры, которые позволяют безопасно удалять сохраненные данные и удовлетворяют нормативным требованиям конфиденциальности.

4. Методы управления безопасностью.

Управление информационной безопасностью, в том числе лучшие подходы к исправлению, обновлению и предоставлению информации домашним хозяйствам на данный момент отсутствуют, говорится в «ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media» [17]. Необходимость интеграции безопасности в дизайне и надежности процессов управления безопасностью обычно не включается в разработку умного дома [15].

Подводя итоги, можно заключить, что умный дом – это место, где ожидается соблюдение конфиденциальности. По сравнению с традиционными цифровыми системами большинство умных домашних устройств имеют ограничения по вычислительной мощности, памяти и энергии. Это делает развитие эффективных мер по обеспечению конфиденциальности и безопасности более сложно реализуемыми в умных домашних системах. Более того, проблемы конфиденциальности и безопасности сложны, и их не всегда легко обнаружить. Тем не менее, соблюдение конфиденциальности и безопасности в умных домах должно рассматриваться как приоритетная задача.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. T. D. P. Mendes et al., “Smart home communication technologies and applications: Wireless protocol assessment for home area network resources,” Energies, vol. 8, no. 7, pp. 7279-7311, 2015
2. V. Sivaraman et al., “Network-level security and privacy control for smart-home IoT devices,” Wireless and Mobile Computing, Networking and Communications, pp. 163-167, 2015
3. C. Debes et al., “Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior,” IEEE Signal Processing Magazine, vol.33, no. 2, pp. 81-94, 2016
4. C. Lee et al., “Securing smart home: Technologies, security challenges, and security requirements,” IEEE Conference on Communications and Network Security, pp. 67-72, 2014
5. K. Islam et al., “Security and privacy considerations for wireless sensor networks in smart home environments,” Computer Supported Cooperative Work in Design, IEEE 16th International Conference on, pp. 626-633, 2012
6. H. Chan and A. Perrig, “Security and privacy in sensor networks,” Computer, vol. 36, no. 10, pp. 103-105, 2003
7. M. M. Hossain et al., “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” Services, pp. 21-28, 2015
8. M. Anwar et al., “Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges,” Health Policy and Technology, vol. 4, pp. 299-311, 2015
9. S. L. Keoh et al., “Securing the internet of things: A standardization perspective, ”Internet of Things Journal, IEEE, vol. 1, no. 3, pp. 265-275,2014
10. D. Altolini et al., “Low power link layer security for IoT: Implementation and performance analysis,” Wireless Communications and Mobile Computing Conference, pp. 919-925, 2013
11. H. C. Pohls et al., “RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects,” Wireless Communications and Networking Conference Workshops, pp. 122-127, 2014
12. G. Mantas et al., “Security in smart home environment,” Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications, pp. 170-191, 2010
13. N. P. Hoang and D. Pishva, “A TOR-based anonymous communication approach to secure smart home appliances,” Advanced Communication Technology, pp. 517-525, 2015

14. A. Riahi et al., “A systemic approach for IoT security,” Distributed Computing in Sensor Systems, pp. 351-355, 2013
15. A. Jacobsson and P. Davidsson, “Towards a Model of Privacy and Security for Smart Homes,” IEEE 2nd World Forum on Internet of Things, vol.2, pp. 727-732, 2015
16. M. Henze et al., “A comprehensive approach to privacy in the cloud-based Internet of Things,” Future Generation Computer Systems, vol. 56, pp.701-718, 2016
17. D. Barnard-Wills et al., “ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media,” ENISA (The European Network and Information Security Agency), 2014