УДК 004.056:004.384
DOI 10.21685/2587-7704-2018-3-2-3

Open Access | RESEARCH ARTICLE

Анализ уязвимостей системы «Умный дом»

А. М. Сливин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. П. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье рассмотрены существующие уязвимости системы «Умный дом». Проанализирована информационная безопасность систем «Умный дом», представленных на рынке. Определены характерные уязвимости информационной безопасности некоторых устройств, входящих в систему «Умный дом». Предложены методы повышения информационной безопасности систем «Умный дом».

Ключевые слова: аутентификация, защита информации, информационная безопасность, несанкционированный доступ, уязвимость, шифрование.

Analysis of vulnerabilities in Smart Home system

A. M. Slivin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. P. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article considers the existing vulnerabilities in the Smart Home system. Information security of marketed Smart Home systems is analyzed. The characteristic vulnerabilities in information security of some devices included in the Smart Home system are determined. The methods to improve information security of Smart Home systems are proposed.

Keywords: authentication, information protection, information security, unauthorized access, vulnerability, encryption.

В настоящее время интеллектуальные системы управления функционированием объектов типа «Умный дом» находят все большее распространение. Такие системы находят применение не только в жилых домах, но и в государственных учреждениях, больницах и других объектах. Но в системах «Умный дом» частично решена проблема информационной безопасности [1].

В числе наиболее распространенных проблем с безопасностью оказались следующие:

1. Слабое шифрование данных внутри системы «Умный дом». В современных информационных технологиях криптографические системы защиты информации подразделяются на симметричные и асимметричные. Большинство устройств, входящих в систему «Умный дом», управляются микроконтроллерами с невысокой вычислительной мощностью. Ввиду того, что асимметричные криптографические алгоритмы требуют больших вычислительных мощностей, чем симметричные, реализация асимметричной криптографии в устройствах системы «Умный дом» потребует более дорогой элементной базы, чем реализация симметричной криптографии (например, симметричного шифрования AES). Это приведет к повышению цен на конечный продукт, что, в свою очередь, негативно повлияет на популярность продукта на рынке.

2. Отсутствие механизма аутентификации санкционированного пользователя. Управление компонентами системы «Умный дом» должно вестись только после аутентификации пользователя в системе и его дальнейшей авторизации. Ввиду того, что управление системой «Умный дом» наиболее часто производится со смартфона или с другого портативного устройства, соединяющегося с систе-

© 2018 *Сливин А. М., Иванов А. П.*
Данная статья доступна по условиям всемирной лицензии Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), которая дает разрешение на неограниченное использование, копирование на любые носители при условии указания авторства, источника и ссылки на лицензию Creative Commons, а также изменений, если таковые имеют место.

мой «Умный дом» посредством беспроводной связи, возникает угроза перехвата идентификационных и (или) аутентификационных данных третьими лицами. Перехват может быть реализован через внедрение вредоносного программного обеспечения в устройства системы «Умный дом», использование существующих уязвимостей программного обеспечения устройств, прослушивание канала связи управляющего устройства (например, смартфона пользователя системы «Умный дом») с устройствами системы «Умный дом» и т.д. Отсутствие механизма аутентификации санкционированного пользователя у большинства устройств, входящих в систему «Умный дом», подтверждается существованием программных средств, с помощью которых можно получить несанкционированный доступ к устройствам системы «Умный дом». Примерами таких программных средств являются Shodan [2] и Censys [3]. Их практическое применение представлено в статье «IoT Privacy and Security Challenges for Smart Home Environments», п. 4.3 «Vulnerability Example» [4].

3. Необходимость наличия защищенных каналов связи. Использование симметричных криптографических систем, дистанционное управление устройствами системами «Умный дом» (например, со смартфона), обновление программного обеспечения устройств системы «Умный дом», преимущественное использование беспроводной связи для коммуникации устройств друг с другом – все это требует наличия защищенных каналов связи в системе «Умный дом». Недобросовестная реализация протоколов защиты информации на одном из устройств может привести к компрометации всех данных, циркулирующих в системе «Умный дом». Так, каналам связи свойственны следующие уязвимости:

– канал Bluetooth является крайне ненадежным и легко может принять файл с вирусом от злоумышленника, не запросив аутентификационных данных;

– по каналу Wi-Fi злоумышленник может авторизоваться во внутренней сети Wi-Fi «Умного дома» и внедрить вредоносное программное обеспечение;

– уязвимости HTTP-канала, по которому устройства из системы «Умный дом» коммуницируют с внешней сетью Интернет, хорошо изучены и могут позволить злоумышленнику получить контроль над «Умным домом», даже не находясь в его локальной вычислительной сети;

– через канал GSM злоумышленник может отправить управляющие команды «Умному дому», подменив свой номер номером санкционированного пользователя;

– если сеть «Умного дома» также находится и в другой локальной вычислительной сети, то вредоносное ПО также может быть внедрено из последней.

4. Потенциальные уязвимости системы «Умный дом» ввиду функционирования в ней устройств от разных производителей. Каждая компания-разработчик разрабатывает устройство по своему собственному технологическому процессу с возможным использованием внутренних (нестандартизированных) протоколов обмена данными. Ввиду этого внедрение устройств от разных производителей в систему «Умный дом» влечет за собой потенциальное наличие уязвимостей информационной безопасности (например, некорректная реализация защищенного соединения между двумя устройствами может привести к перехвату злоумышленником ключевой информации). Такая проблема может быть решена приобретением готовой системы «Умный дом» у одного производителя. Однако, во-первых, компаний, производящих полноценную систему «Умный дом», на данный момент на рынке представлено мало; во-вторых, как показали недавние исследования независимой организации AV-TEST в области информационной безопасности таких систем [5], уровень информационной безопасности систем «Умный дом» у многих производителей находится на низком уровне.

5. Наличие свойственных определенным устройствам уязвимостей информационной безопасности. Устройства системы «Умный дом» обладают различным функционалом и выполняют различные задачи. Соответственно, устройства имеют и различные уязвимости:

– Smart TV. Большинство современных Smart-телевизоров оснащены камерами. При недостаточной информационной безопасности системы «Умный дом» злоумышленники могут использовать данные камеры для слежения за пользователями данной системы и помещением в целом;

– Smart fridges. Холодильники в «Умном доме» проверяют срок годности продукции, анализируют хранящуюся в нем пищу и составляют список продуктов, которые необходимо будет купить хозяину дома. Получив контроль над этими данными, злоумышленник может узнать, в какое время в доме находятся люди, а когда их нет, способствуя тем самым своему последующему проникновению в дом;

– Smart Cars. Согласно последним исследованиям, злоумышленники могут получить контроль над операционными системами «умных» устройств. Таким образом они могут осуществлять управление всеми компонентами данных устройств;

– система автоматизированного управления домом. Система автоматизированного управления домом является главной системой «Умного дома», обеспечивая контроль, в том числе, за дверьми и окнами дома, внешними и внутренними камерами, а также сигнализациями. Получив контроль над данной системой, злоумышленник может абсолютно бесследно произвести физическое проникновение на территорию «Умного дома».

6. Методы повышения информационной безопасности систем «Умный дом». На основе проведенного анализа уязвимостей системы «Умный дом» были предложены следующие методы повышения их информационной безопасности:

– установка пароля высокой сложности на профиль администратора системы;

– обновление ПО всех устройств системы «Умный дом» до последней версии;

– внедрение системы слежения за несанкционированным доступом в систему «Умный дом»;

– настройка сети VPN для системы «Умный дом»;

– установка межсетевого экрана (файрвола) на границе локальной сети системы «Умный дом», а также настройка антивируса под свои потребности;

– использование решений для системы «Умный дом» от одного производителя для избежания потенциальных уязвимостей информационной безопасности.

Также на рынке представлены готовые решения для обеспечения информационной безопасности «Умного дома». Одной из них является проект команды кафедры безопасных информационных технологий университета «Безопасный умный дом» [6]. Данный проект разрабатывается с 2015 г., и за это время была разработана архитектура программно-аппаратного модуля, написан необходимый софт и выбраны безопасные протоколы передачи данных. Итоговый результат позволяет серьезно снизить применимость основных атак на систему «Умный дом».

Библиографический список

1. Борисов, М. В. Актуальные угрозы информационной безопасности интернета вещей / М. В. Борисов, А. П. Иванов // Современные тенденции развития науки и технологий. – 2017. – № 1–1. – С. 23–25.
2. Shodan : поисковик сетевых устройств в сети Интернет. – URL: https://www.shodan.io, свободный.
3. Censys : поисковик сетевых устройств в сети Интернет. – URL: https://censys.io, свободный.
4. IoTPrivacyandSecurity Challenges for Smart Home Environments. – Базель, Швейцария, 2016. – URL: https://www.mdpi.com/2078-2489/7/3/44/htm, свободный.
5. AV-TEST: Test: Smart Home Kits Leave the Door Wide open – for Everyone. – URL: https://www.av-test.org/en/news/test-smart-home-kits-leave-the-door-wide-open-for-everyone, свободный.
6. Безопасный умный дом: сложная технология, полезная каждому. – URL: http://news.ifmo.ru/ru/startups_and_business/startup/news/5832/, свободный.

Сливин, А. М.

Анализ уязвимостей системы «Умный дом» / А. М. Сливин, А. П. Иванов // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-3.