УГРОЗЫ БЕЗОПАСНОСТИ СИСТЕМЫ «УМНЫЙ ДОМ»

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Беларусь

Костюченко В.В.
Алефиренко В.М. – канд. техн. наук, доцент

В настоящее время интеллектуальные системы управления функционированием объектов типа «Умный дом» (англ. Smart Home) находят все большее распространение. Такими системами оборудуются не только жилые дома, но и государственные учреждения, офисы, места массовых мероприятий, АЭС, аэропорты, больницы и другие объекты. Система «Умный дом» это экосистема, имеющая в своей основе программный комплекс тесно связанный с датчиками, контроллером и облачными сервисами. Каждая компания-производитель предлагает свое видение построения систем «Умный дом» для потребителей.

С момента возникновения на рынке систем типа «Умный дом» стало очевидно, что появление вредоносного программного обеспечения лишь вопрос времени. Для понимания возможных каналов распространения вирусов рассмотрим, из каких компонентов строится стандартный современный «Умный дом». Компоненты могут быть от различных производителей, но принцип построения умного дома в большинстве проектов остается неизменным.

На рисунке 1 показана архитектура подключения «Умного дома». «Умный дом» состоит из подключенных устройств, принадлежащих различным приложениям и шлюзам. Шлюзы обеспечивают подключение к поставщикам услуг и другим внешним объектам.

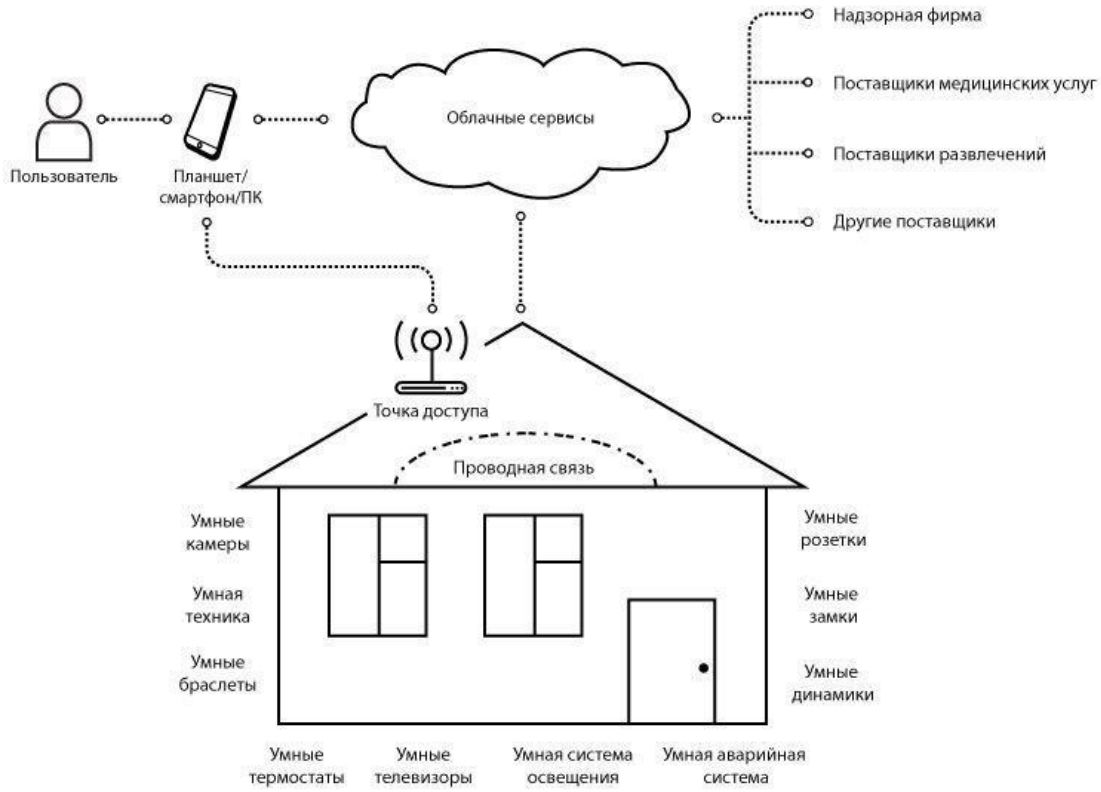

Рисунок 1 - Архитектура подключения «Умного дома»

Компоненты «Умного дома» условно можно разделить на несколько групп: устройства, связь и службы.

1. Устройства

Умные домашние устройства - это аппаратные блоки, обычно включающие датчики, приводы, шлюзы и интеллектуальные объекты.

Типы устройств:

1) Датчики измеряют физическое свойство окружающей среды или физическое лицо. Датчики могут варьироваться от носимых (например, браслетов) к датчикам, непереносимым (например, IP-камерам). Видеокамеры считаются наиболее чувствительными к конфиденциальности датчиками [1] вместе с микрофонами.

2) Приводы выполняют такие действия, как включение / выключение или затемнение света, закрывание окон, срабатывание сигналов тревоги и т. д.

3) Шлюз служит точкой доступа к дому, обычно позволяя владельцу или другому объекту контролировать систему, 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.

4) Умные объекты - это устройства, состоящие из датчиков и / или исполнительных механизмов, которые подключены к Home Area Network (домашняя вычислительная сеть). Например, некоторые из них включают интеллектуальные устройства, такие как интеллектуальные блокировки, за которые отвечают дверные звонки и обеспечивают контроль доступа на основе времени.

2. Связь

Типичный «Умный дом» использует разнообразные коммуникационные протоколы. Они работают по проводной и радиосвязи. 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 сотовые технологии. Технологии RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) и NFC (Near Field Communication — технология беспроводной связи) также используются для мониторинга и отслеживания, особенно в области здравоохранения, и обычно используется умных дверных замках.

3. Службы

Службы - это программные приложения, размещенные в облаке или внутри домашней системы, которые несут ответственность за реализацию автоматизации, управление устройствами, принятие решений и т. д. А особая категория услуг - это контроллеры, которые позволяют управлять подключенными устройствами. Как правило, программное обеспечение устанавливают на смартфоны или планшеты, чтобы локально или удаленно взаимодействовать с устройством.

Важной угрозой безопасности для «Умного дома» являются вирусы, которые могут нарушать работу системы «Умный дом», неправомерно копировать, шифровать или удалять конфиденциальные данные, а также вести слежку за пользователями.

Рассмотрим основные возможные каналы распространения вирусов [2].

1. Сеть Bluetooth. Она является крайне ненадежной и легко может принять файл с вирусом от злоумышленника, не запросив авторизацию [3].

2. Сеть Wi-Fi. Такая сеть может быть легко взломана злоумышленником, который может, обойдя систему авторизации, передать вирус на сервер.

3. HTTP-канал для удаленного доступа. HTTP-обмен с сетью Интернет может быть одним из каналов попадания вируса в систему автоматизированного управления зданием. Множественные уязвимости программных продуктов, построенных на HTTP-протоколе, хорошо известны, но не закрыты [4].

4. GSM канал. Через канал GSM также возможно осуществить несанкционированное управление системой. Например, это можно сделать с помощью передачи SMS-сообщения с поддельным номером отправителя.

5. Сопряженные каналы. Если сервер системы «Умный дом» подключен также и к локальной сети здания, то вирусная программа вполне может попасть из локальной сети.

6. Предустанавливаемое программное обеспечение и логические бомбы. Данный канал внедрения вирусов в серверное обеспечение системы «Умный дом» подразумевает, что при установке такой системы, злоумышленник, например, войдя в доверие к заказчику, устанавливает на сервере вирус самостоятельно. Доказать, что вирус установлен злонамеренно практически невозможно. Обнаружить такой вирус также крайне сложно.

После всего вышесказанного очевидно, что системам «Умный дом» требуется защита, способная контролировать все устройства, службы и связи. Но на данный момент не представлены комплексные системы антивирусной защиты систем «Умный дом».

Рассмотрим, какие задачи должен выполнять такой программный продукт:

– контролировать появление на сервере любых посторонних файлов или программ;

– контролировать несанкционированные подключения устройств к сети;

– контролировать подключения устройств к беспроводным каналам передачи данных;

– контролировать трафик между локальными сетями и непосредственно сервером системы «Умный дом»;

– контролировать взаимодействие сервера с сетью Интернет на предмет проникновения вирусного программного обеспечения;

– контролировать сетевое оборудование на предмет DoS-атак;

– обеспечивать проверку файлов, передаваемых в проводных и беспроводных сетях;

– выполнять эвристический поиск наличия на сервере вирусных программ;

– контролировать целостность системы «Умный дом», которая должна заключаться в проверке текущей конфигурации, управляющих процессов и хранимых данных.

Системы «Умный дом» со временем будут установлены в каждом доме, уже сейчас многие офисные и жилые здания проектируют с учетом установки умных систем. Но, на данный момент, системы такого типа все еще не до конца исследованы и не являются полностью защищенными от множества угроз, что бы пользователи с уверенностью доверяли им личную информацию, жизнь и здоровье.

Список использованных источников:

[1] C. Debes et al., “Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior.” IEEE Signal Processing Magazine, vol. 33, no. 2, 2016, pp. 81-94.

[2] Технологии мобильной связи : услуги и сервисы / А.Г. Бельтов [и др.]. – М. : ИНФРА-М, 2012. – 206 с.
[3] Bluetooth: на пути к миру без проводов // Специальные радиосистемы [Электронный ресурс]. – 2007. – Режим доступа : http://www.radioscanner.ru/info/article95/. – Дата доступа : 21.03.2018.
[4] Касперски, К. Записки исследователя компьютерных вирусов / К. Касперски. – С-Пб. : Питер, 2006. – 216 с.