УДК 681.518.5:004.896

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

УЯЗВИМОСТИ СИСТЕМ «УМНЫЙ ДОМ» И ПРИЧИНЫ ИХ ВОЗНИКНОВЕНИЯ

Аннотация. *Рассмотрены виды систем «Умный дом», виды программного обеспечения и его уязвимости. Показаны основные возможные каналы распространения вирусов. Приведены требования к антивирусным средствам, используемым в программном обеспечении систем «Умный дом».*

Ключевые слова: *система «Умный дом», программное обеспечение, уязвимость, обеспечение безопасности.*

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

SMART HOME SYSTEMS VULNERABILITY AND THE CAUSES OF THEIR OCCURRENCE

Annotation*. Smart Home systems, software and its vulnerability are considered. The main possible virus spreading channels are shown. Antivirus means demands, using in Smart Home systems software are given.*

Keywords: *Smart Home systems, software, vulnerability, security ensuring.*

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.

Существует два основных вида таких систем [1, 2]:

– система с распределенной логикой;

– система с централизованной логикой.

Система с распределенной логикой представляет собой набор функциональных модулей, связанных между собой и работающих на едином стандарте связи. Практически всегда такая система создается одним производителем и не поддерживает подключение модулей от других систем. Главным преимуществом системы с распределенной логикой является сохранение общего функционирования при выходе из строя одного из модулей, а к недостаткам относится малая гибкость системы, сложность масштабирования, высокая стоимость модулей, а также проприетарность

стандартов связи и защиты личных данных пользователя по причине разрозненности и закрытости стандартов производителей.

Система с централизованной логикой представляет собой набор датчиков, приводов и различной домашней техники, связанных в единую сеть и подключенных к контроллеру, с возможным выходом в сеть для подключения к облачным сервисам. Преимуществом данной системы является поддержка сопряжения датчиков и домашней техники разных производителей, так как подключение происходит к единому контроллеру и облачному сервису, а также возможность использования одного датчика для нескольких целей одновременно, что экономит средства потребителя. Система с централизованной логикой легко масштабируется и имеет большой выбор компонентов при их сравнительно малой стоимости. К недостаткам относится закрытость и неисследованность протоколов связи и управления, полная закрытость и неинформативность описания логики использования и хранения личных данных пользователя, а также полный выход из строя системы при поломке контроллера.

Таким образом, каждая система имеет свои положительные и отрицательные качества и может быть использована для автоматизации любого жилого помещения в рамках заданного проекта и требований пользователя. Но каждая система на данный момент имеет одни и те же недостатки – высокое число проблем аутентификации и авторизации, незащищённость при возможности доступа к конфиденциальной информации и личному жилому помещению пользователя. Кроме того, сочетание различных технологий при построении такой системы увеличивает количество возможных уязвимостей, что привлекает внимание злоумышленников.

Большая часть современного расширяющего функциональность оборудования для систем автоматизированного управления объектами, производимого разными компаниями, может быть интегрирована в единые сети. Это становится возможным благодаря гибкости и структурированности автоматизированных сетей. В результате этого здание становится все более функциональным. Однако в такой интеграции существуют и свои недостатки. Это объясняется тем, что сочетание разных технологий при построении одной автоматизированной системы увеличивает количество возможных недостатков решения с точки зрения безопасности функционирования объекта (здания). У каждой технологии, какой бы совершенной она ни была, существуют свои уязвимости. Увеличение числа устройств и технологий, используемых в системе, ведет к увеличению уязвимостей всей системы. Однако пользователь системы всегда хочет больше функциональных возможностей, а значит и устройств, независимо от безопасности их использования. Кроме того, процесс интеграции разных решений не исключает возможности допущения ошибки в проектировании. Это может привести к появлению дополнительных слабых мест в системе [3].

Многие системы автоматизации зданий не имеют полноценной системы безопасности. Большинство решений по защите от кибернетических атак обычно связано с установкой стандартных программ, выполняющих только функции сетевого экрана. В целом системы автоматизированного управления зданием имеют несколько видов программного обеспечения.

К первому виду относится то программное обеспечение, которое обеспечивает функционирование самой сети системы «Умный дом». Такое программное обеспечение отвечает за обработку событий той логики, которая изначально запрограммирована производителем системы. Оно разрабатывается на языках программирования низкого уровня и отвечает за функционирование нижних уровней сетевой модели OSI [4].

Ко второму виду программного обеспечения относится то программное обеспечение, которое отвечает за интерактивное взаимодействие с пользователем посредством командного языка. Оно, как правило, используется для внешнего или удаленного управления устройствами.

Рассмотрим основные принципы, на которых строится подход к разработке программных средств для управления системами «Умный дом».

1. Головной частью любого комплекса программного обеспечения является сервер. Сюда приходят запросы от различных клиентов, с которыми данный сервер может работать. Сервер обрабатывает все команды, анализирует параметры системы жизнеобеспечения и принимает решения о выполнении тех или иных действий. Далее сформированная команда передается на тот или иной драйвер для доступа к сети, в зависимости от того, какая реализация сети выбрана. После чего с помощью драйвера осуществляется непосредственное управление объектами. В обратном направлении данная цепочка также работает. Если, например, от датчика протечки пришел сигнал о том, что уровень воды превысил допустимую отметку, то соответствующая команда приходит на сервер системы «Умный дом».

2. Пользовательский интерфейс представляет собой визуализированную систему управления, где в наглядном виде представлены отдельные компоненты системы. Таким образом, пользователю предоставляется удобное средство для управления различными объектами, находящимися под управлением системы «Умный дом». Такой интерфейс может быть реализован самыми различными способами. Существует несколько подходов к реализации этого компонента программного обеспечения. Каждый из вариантов во многом зависит от того, какой протокол выбран для обмена данными с сервером системы умного дома. Это можем быть Web-браузер, общающийся по HTTP-протоколу или приложение, реализованное на языках программирования высокого уровня под ту или иную операционную систему. Так же это может быть приложение, которое устанавливается на мобильный телефон пользователя и предназначено для обмена командами и сервисными сообщениями посредством TCP/IP соединений или SMS-сообщений. Необходимо отметить, что многие из протоколов, используемых для управления объектами, являются уязвимыми по своей сути, а другие, как правило, будучи использованными для построения подсистем, зачастую при неправильной интеграции приводят к появлению уязвимостей.

Если говорить о первом виде программного обеспечения, то есть о программном обеспечении, отвечающем за функционирование самой сети системы «Умный дом», то это программное обеспечение работает на низком уровне и отвечает за передачу управляющих датаграмм по витой паре или импульсов по силовой линии непосредственно от устройства к устройству или

от сервера к устройствам и обратно. Существует множество стандартов по передаче такой информации: CBUS, EIB/KNX, LonWorks и др. Принципиальное отличие каждого из стандартов в целом заключается в формате данных и адресации устройств в сети.

Рассмотрим основные возможные каналы распространения вирусов [5].

1. Сеть Bluetooth. Она является крайне ненадежной и легко может принять файл с вирусом от злоумышленника, не запросив авторизацию [6].

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 [7].

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.

Следует отметить, что полноценных антивирусных систем, обеспечивающих комплексную защиту от вредоносного программного обеспечения, разработанных специально для систем «Умный дом», не существует [7]. Более того, программный код, свойственный вирусам для таких систем, не опознается большинством сканеров сигнатур [8]. К основным уязвимостям в программном обеспечении систем «Умный дом», которыми пользуются злоумышленники для внедрения вредоносных программ, относятся:

– отсутствие возможности блокировки подключений неавторизованных устройств;

– отсутствие контроля над широковещательной рассылкой датаграмм в сети системы «Умный дом»;

– отсутствие проверки подлинности управляющей программы, передающей пакеты в сеть системы «Умный дом».

На сегодняшний день вирусы для систем «Умный дом» не могут быть опознаны по сигнатурам ни одним из существующих на данный момент антивирусов. Более того, в построении этих систем управления существует такая значительная уязвимость, как полное отсутствие контроля несанкционированных подключений к линиям передачи данных [8, 9]. Фактически, вирус может подключаться к сети, посылать туда управляющие команды, отслеживать все события в сети.

Исходя из изложенного, очевидно, что антивирусное средство для систем «Умный дом» должно выполнять следующие важные функции:

– 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.

К сожалению, следует отметить, что на данный момент в мире не существуют программные средства для комплексной защиты систем «Умный дом».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Отчет компании HP «Internet of Things Security Study: Home Security Systems Report» [Электронный ресурс]. – Электронные данные. – Режим доступа: https://community.softwaregrp.com/dcvta86296/attachments/dcvta86296/sws-22/227/1/InternetOfThings.pdf.
2. Блог компании Лаборатория Касперского [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.kaspersky.ru/blog/study-smart-homes-insecure/4030/.
3. Кусакин, И.И. Программно-аппаратный комплекс автоматизированного контроля целостности инфраструктуры жилых помещений для социального обеспечения / И.И. Кусакин // XV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3. – М.: НИЯУ МИФИ, 2012. – С. 156 – 157.
4. Гололобов, В.Н. «Умный дом» своими руками / В.Н. Гололобов // – М.: НТ Пресс, 2007. – 216 с.
5. Технологии мобильной связи: услуги и сервисы / А.Г. Бельтов, И.Ю. Жуков, Д.М. Михайлов. А.В. Стариковский. – М.: ИНФРА-М, 2012. – 206 с.
6. Bluetooth: на пути к миру без проводов [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.radioscanner.ru/info/article95/.
7. Касперски, К. Записки исследователя компьютерных вирусов / К. Касперски. – С-Пб.: Питер, 2006. – 216 с.

8. Аристов, М.С. Антивирусный программно-аппаратный комплекс для систем автоматизированного здания / М.С. Аристов // XIV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3. – М.: НИЯУ МИФИ, 2011. – С. 151 – 152.
9. Соломатина, Е.В. Обеспечение безопасности систем автоматизированного управления зданием на базе системы X10. / Е.В. Соломатина // Труды VII Межведомственной научно-технической конференции «Проблемы комплексного обеспечения защиты информации и совершенствования образовательных технологий подготовки специалистов в области информационной безопасности». – Том 1. – Краснодар: Краснодарское высшее военное училище (военный институт) имени генерала армии С.М. Штеменко, 2009. – С. 26 – 29.