

Денисов Анатолий Николаевич,

технический директор,

ООО «ВЕКСМАРТ»,

г. Чебоксары, Чувашская Республика, Россия

ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ ЗДАНИЯМИ: ИСПОЛЬЗОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ

В последние годы получили большую известность системы управления объектами или автоматизированные системы комфортного «умного» дома.

Комфортный дом (Умный дом) – это полноценное автоматизированное строение, предназначенное для удобного пользования людей с помощью высокотехнологичных приборов. Это может как обычный жилой дом, так и государственные учреждения, огромные арены и даже аэропорты. В «комфортном» доме одно устройство способно управлять функционалом других устройств по заданным алгоритмам. Основной особенностью «умного» здания является соединение различных устройств в единую сеть, через которую происходит управление целым комплексом. Постоянный контроль сложных объектов – это главная задача, справиться с которой позволяют сегодняшние интеллектуальные системы автоматизации. В больших системах автоматизации жизнеобеспечения следят за климат-контролем, освещением, а также могут координировать движение пассажиров через контроллеры дверей, работу световых указателей и громкоговорителей. В последние годы резко возросло количество функций, за которые отвечают «умные» системы. Большинство современного оборудования, создаваемого для систем автоматизации управления объектами разными компаниями, может быть адаптировано в единые сети. Но в адаптации существуют свои минусы: сочетание различных технологий при построении одной единой системы увеличивает риск появления уязвимости с точки зрения безопасности. В любой технологии, какой бы современной она ни была, имеются свои уязвимости. Увеличение количества аппаратуры и технологий, применяемых в системе, ведет к увеличению её уязвимости.

Мошенники могут знать уязвимые места в современных системах контроля «умного» дома и попытаться атаковать эту систему. Они могут на длительное время заблокировать работу таких больших объектов, как, например, аэропорт, поломать системы жизнеобеспечения, навести панику и, в конце концов, заблокировать систему безопасности во всем здании, что может оказаться очень опасно для жизни.

Программное обеспечение для систем «комфортного дома»

В системах автоматизированного управления объекта существует несколько типов программного обеспечения.

1 тип: программное обеспечение, обеспечивающее функционирование самой локальной сети «умного» дома. Данное программное обеспечение выполняет обработку событий по заданной схеме, которая изначально заложена производителем системы комфортного дома. Оно программируется на языках низкого уровня и выполняет за работу нижних уровней.

2 тип: программное обеспечение, отвечающее за интерактивную работу с пользователем через командный язык. Данный тип обычно применяется для удаленного управления системой.

Основные принципы построения разработки программных средств для удаленного управления системами «умного дома».

Главной частью любого подобного комплекса является сервер. Именно здесь выполняются запросы от различных устройств, с которыми сервер может взаимодействовать. Сервер выполняет все команды, проводит анализ всех систем жизнеобеспечения и решает о выполнении заданных действий.

Следующим шагом команда передается на драйвер устройства для получения доступа к сети. Затем с помощью этого драйвера осуществляется полное управление устройствами. Данная цепочка работает и в обратном направлении. К примеру, если от датчика протечки воды поступил сигнал о том, что уровень воды превысил допустимую норму, то команда поступает на главный сервер «умного» дома.

Интерфейс пользователя представляет собой визуализированный комплекс управления, где наглядно представлены все компоненты автоматизированной системы. Соответственно, пользователь получает удобное средство для управления всей интеллектуальной системой. Такие интерфейсы могут быть реализованы различными способами. На сегодня имеется несколько подходов для взаимодействия этого компонента программного обеспечения.

Каждый подход во многом зависит от выбранного протокола для обмена с главным сервером системы интеллектуального здания. Им может быть и Web-браузер, получающий запросы по HTTP-протоколу, и мобильное приложение, созданное на языках высокого уровня под определенную операционную систему, которое устанавливается на мобильное устройство пользователя и выполняющий обмен командами и сервисными уведомлениями через TCP/IP соединения или же SMS-сообщений.

Основные возможные способы взаимодействия вирусов в системах комфортного дома.

Как уже говорили, серверное программное обеспечение запускается на выделенной вычислительной машине. К этой машине подключают большое количество вспомогательных устройств, передатчиков, контроллеров для передачи данных. Это GSM-модемы, Bluetooth-устройства и Wi-Fi точки доступа. Часто на эту же машину устанавливается программное обеспечение для взаимодействия с компьютерной сетью объекта. То есть получается, что на сервере установлено большое количество единиц программного обеспечения, ответственных за выполнение обработки всех получаемых данных. Также данная вычислительная машина фактически управляет всем «умным» домом.

Основные способы распространения вируса:

- канал Bluetooth. Изначально сети Bluetooth являются очень уязвимы и с легкостью могут получить файл с вирусом от мошенника, даже не запросив авторизацию [4];

- канал Wi-Fi. Сеть Wi-Fi, также как и Bluetooth, может быть с легкостью взломана мошенниками. Он сможет обойти систему авторизации, также передать вирусный файл на сервер;

- канал HTTP для получения удаленного доступа. Сегодня каждая вычислительная машина производит HTTP-обмен с сетью Интернет. Это один из каналов попадания вируса в автоматизированную систему комфортного дома. Большинство уязвимостей программных продуктов, созданных на HTTP-протоколе, довольно хорошо известны;

- канал GSM. Канал GSM также подвержен риску осуществить несанкционированное получение доступа к управлению системой.

На данное время в мире имеются лишь программные способы защиты систем интеллектуального управления объектами. Программные антивирусные решения не могут обеспечить полную защиту систем интеллектуального управления ввиду отсутствия полноценной аппаратной структуры комплекса. Можно сказать, что существующие на сегодняшний день программные антивирусные комплексы не смогут дать гарантию полноценной защиты системы. Поэтому, создание комплекса антивирусной системы для подобных систем автоматизированного управления зданием – это главная задача ближайших лет.

СПИСОК ЛИТЕРАТУРЫ

1. <https://cyberleninka.ru/article/n/issledovanie-uyazvimostey-sistem-umnogo-doma>
2. Гололобов В.Н. «Умный дом» своими руками. – М.: НТПресс, 2007. – 216 с.
3. Бельтов А.Г., Жуков И.Ю., Михайлов Д.М., Стариковский А.В. Технологии мобильной связи: услуги и сервисы. – М.: Инфра-М, 2012. – 206 с.
4. Широков Ф. Bluetooth: на пути к миру без проводов / Открытые системы, 2001. – № 2 [Электронный ресурс] – Режим доступа: <http://www.radioscanner.ru/info/article95/>
5. Касперский К. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2006. – 216 с.