Т. А. Мельникова
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Васькевич**, ст. преподаватель

АНАЛИЗ УЯЗВИМОСТЕЙ В СИСТЕМЕ УМНОГО ДОМА И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ИХ УСТРАНЕНИЮ

С каждым годом система умного дома становится всё популярнее. Основными разработчиками таких систем являются Google, Xiaomi и Яндекс, однако последнее время в создании подобных экосистем не отстают другие фирмы, такие как: Aqara, Tuya Smart, Умный дом Sber, Rubetek и др. Несмотря на то, что уже существуют повсеместно известные лидеры, это не значит, что безопасности их продуктов всецело можно доверять. С одной стороны, такие системы предоставляют удобство и автоматизацию, но с другой подвергают конфиденциальность пользователя опасности.

Основными типами уязвимостей таких систем считаются избыточные разрешения и передача конфиденциальной информации на сервера компаний. Подобные уязвимости введены самими разработчиками для продвижения собственных продуктов пользователям, руководствуясь полученными данными их распорядка дня. Также многие разработчики оставляли для себя полный доступ или контроль над устройствами под предлогом необходимости предоставлять техническую поддержку пользователям.

Благодаря системе умного дома появилась возможность открывать двери, разогревать чайник, включать свет и наблюдать за происходящим в собственном доме с помощью камер. Этими же функциями пользуются и хакеры, ведь не все пароли замков передаются в зашифрованном виде, а в эру голосовых помощников появился распространённый сценарий подделки голоса. Даже существовал такой тип уязвимости, когда незаметное для человеческого глаза мерцание лампочек передавало информацию о паролях пользователя злоумышленнику.

Подведём следующую классификацию по различным аспектам атак системы «умный» дом:

1. Уязвимости физического доступа.

К данному пункту относится всё, начиная от банального вторжения в жилище и манипуляции с устройствами напрямую до проблем реализации протоколов. В устаревших или редко обновляемых устройствах встречаются такие недостатки в коде, которые удалённо исполняют код, перехватывающий управление устройством или выдающий доступ к конфиденциальным данным. Уязвимости в реализации сетевых протоколов (например, Zigbee, Z-Wave, Matter) позволяют злоумышленнику выдавать себя за другое устройство, перехватывать трафик или отправлять вредоносные команды.

2. Уязвимости сети.

Открытые и незащищенные порты на роутере или устройствах умного дома могут быть использованы злоумышленниками для удаленного доступа к устройствам.

Отсутствие или неправильная настройка фаервола позволяет злоумышленникам сканировать и атаковать устройства в сети.

Уязвимости в таких протоколах, как Zigbee, Z-Wave, Bluetooth, используемых устройствами для связи, позволяют перехватывать, подменять или блокировать команды.

3. Уязвимости облачных сервисов.

Отсутствие или слабая аутентификация и авторизация при использовании API облачного сервиса позволяет злоумышленнику получать доступ к данным или управлять устройствами без разрешения. Злоумышленники могут использовать фишинговые атаки для получения учетных данных от пользователей облачных сервисов. Облачный сервис может быть уязвим к распределенным атакам отказа в обслуживании (DDoS), что приведет к недоступности системы умного дома. Утечки данных из облачного сервиса приводят к раскрытию конфиденциальной информации о пользователях и их устройствах.

Облачный сервис может собирать и использовать данные о пользователях и их устройствах без их согласия или в нарушение политики конфиденциальности.

4. Уязвимости приложений.

Приложения запрашивают избыточные разрешения, не необходимые для их функциональности (например, доступ к камере, микрофону, контактам), используют полученные разрешения для сбора и передачи конфиденциальной информации без ведома пользователя. Злоумышленники создают поддельные приложения, имитирующие легитимные приложения умного дома, для кражи учетных данных или внедрения вредоносного ПО.

Уязвимости в безопасности есть практически в любых устройствах для домашней автоматизации. И если мигающий свет и вышедшее из-под контроля отопление не так опасно и не является основной целью для злоумышленников, то взлом умного замка на входной двери или камеры видеонаблюдения звучит опаснее.

В ходе проведенного анализа систем умного дома был разработан ряд рекомендаций для того, чтобы умный дом оставался в первую очередь домом, а не ещё одним потенциально опасным местом:

– ознакомьтесь с руководствами и рекомендациями по безопасности для каждого устройства, чтобы знать о возможных уязвимостях;

– интересуйтесь отзывами на продукт перед его покупкой. Как производитель реагирует на найденные уязвимости? Неравнодушие компании и быстрое реагирование являются хорошим знаком;

– используйте сложные и уникальные пароли для всех устройств и аккаунтов. Избегайте использования стандартных паролей, которые могут быть легко подобраны или угаданы;

– включите двухфакторную аутентификацию (2FA) для всех сервисов и приложений, поддерживающих эту функцию. Это добавит дополнительный уровень защиты;

– обучите членов семьи основам безопасности в интернете и правилам использования умных устройств. Настройте права доступа для пользователей, чтобы только доверенные лица могли управлять умными устройствами;

– убедитесь, что ваши устройства физически защищены от несанкционированного доступа, особенно камеры и замки. Периодически проводите аудит безопасности вашего умного дома, проверяя настройки и устройства на наличие уязвимостей;

– по возможности используйте локальные сети для управления устройствами, чтобы минимизировать зависимость от облачных сервисов. Если вы используете облачные сервисы, убедитесь, что доступ к ним ограничен и защищен;

– если вы не используете камеры и микрофоны, отключите их или закройте физическими заглушками.

Следуя этим рекомендациям, пользователи могут превратить свой умный дом в действительно безопасное и комфортное пространство, где современные технологии служат для улучшения качества жизни, а не становятся источником потенциальных проблем. Главное не забывать, что безопасность умного дома – это непрерывный процесс, требующий постоянного внимания и своевременного обновления знаний и настроек.