Проанализировав схему IoT системы, можно выделить основные направления атаки:

1. Стандартные настройки устройства.

Пользователь многих IoT устройств не меняют стандартные настройки, используемые для аутентификации, такие как логин пароль и т.д. Из-за чего существует угроза компрометации устройства атакой словарём. Таким образом в 2016 году произошла массированная DDoS атака бот-нет сетью Mirai в 2016 году. Решение: замена стандартных настроек устройства, использование трудно подбираемого пароля, использование более сложных систем авторизации (возможно использование OAuth 2.0).

2. Ошибки заводской прошивки.

Некоторые устройства не промеряют достоверность прошивки при обновлении. Например эксплойт CVE‐2011‐4161 стал возможен благодаря тому, что по умолчанию включена опция удаленного обновления прошивки, что позволяет злоумышленнику удаленно установить скомпрометированную прошивку без аутентификации, отправив её на порт 9100. Возможные решения: проверка всех стандартных настроек устройства, блокирование подозрительного трафика.

3. Использование открытых портов.

Многие IoT устройства работают на сетевом уровне модели OSI, что позволяет им подключаться к локальной сети через WiFi или Zegbee. Поэтому устройства становятся подвержены многим веб уязвимостям: активный и пассивный анализ трафика, межсайтовый скриптинг и тд. Так, например, эксплойт CVE‐2018‐13022 позволял выполнять межсайтовый скриптинг на Xiaomi Mi Router 3 версии 2.22.15. При подключении к веб серверу роутера некорректным запросом, отображалась страница 404 Not Founded, в которой отображался сам некорректный URL. Более того, отсутствовал заголовок X‐Content‐Type‐Options: nosniff, что позволяло запускать JavaScript скрипт. Самое страшное, по моему мнению, что с помощью одного скомпрометированного устройства, злоумышленник получает возможность атаковать остальные устройства, подключенные к локальной сети.

Возможные решения: использование файервола внутри локальной сети, максимальное уменьшение количества открытых портов и максимальная их защита.

4. Использование мобильного приложения для IoT.

Многие устройства управляются с помощью мобильного приложения, которое подключается только к облачному сервису, когда IoT устройства имеют постоянное подключения только с сервисом. Что даёт дополнительные векторы атаки для злоумышленников. Например, в 2019 году был создан эксплойт CVE-2019-15745, позволяющий получить доступ к умной розетке. Уязвимость заключается в том, что ключ шифрования AES был записан в .so файле. Дизассемблировав файл, можно получить ключ, с помощью которого можно проходить аутентификация для удаленного сервиса и дистанционно управлять умной вилкой. Данная уязвимость демонстрирует некорректное использование средств криптографического шифрования и последствия использования некриптостойкого шифрования, что приводит появлению уязвимостей подобного рода. Решением данной проблемы может быть использование сложных ключей шифрования, например для RSA ключ не должен быть короче 1000 бит, с учетом затрат шифрования и расшифровку информации, т.к. у устройств вычислительный ресурс ограничен, а также общее повышение квалификации разработчиков в способах и методах шифрования информации.

5. Уязвимости в сканнерах IoT устройств.

Многие (если не все) IoT устройства оснащены определёнными датчиками, которые позволяют реагировать на изменения окружающей среды. Этими детекторами могут быть микрофон, датчик освещённости, датчик глубины, датчик задымлённости и т.п. Эти датчики так же могут быть использованы для выполнения определенного действия устройством. Так, например, USENIX в своей стать пишут о возможности внедрения голосовой команды управления IoT устройства в луч света. С помощью такого луча, направленного в микрофон, можно передать голосовую команду на расстоянии до 110 метров и «попросить» устройство выполнить какое-либо действие. Если устройство не способно различать голоса, то оно будет считать, что команду дал владелец этого устройства и будет иметь соответствующие права, такие как закрыть/открыть дверь, позвонить на определённый номер и все другие действия, доступные владельцу. Возможные способы избегания данной уязвимости: не допускать видимый доступ к микрофонам устройств. Ещё хотел бы добавить, что в некоторых умных колонках, например в Яндекс станции, есть система распознавания голоса, с помощью которой можно построить политику прав доступа для пользователей станции. Например, при распознанном детском голосе, автоматически включается возрастные ограничения. Данная технология так же может предотвратить (или уменьшить) последствия использования этой уязвимости.

После рассмотрения приведённых уязвимостей становится очевидно, что уязвимости могут находиться в самых неожиданных местах, что заставляет более внимательно относиться к выбору IoT устройства и системам, обеспечивающие их безопасность.