Обеспечение безопасности IoT системы

Павел Смоляков, гр. 21214

16 декабря 2023 г.

1 Введение

С возрастающей популярностью интернета вещей все более острым становится вопрос обеспечения безопасности IoT-решений. Данная концепция обмена данных между физическими объектами, оснащенными датчиками и сенсорами, создана для автоматизации многих повседневных процессов и взаимодействия с окружающей средой. Разумеется, даже простейшая IoT-система подразумевает необходимость создания довольно сложной сети с большим количеством одновременно подключаемых устройств и, зачастую, доступом в Интернет.

От «взрослых» сетей производительных компьютеров интернет вещей отличается некоторыми ограничениями - у большинства устройств весьма ограничена производительность, так что в частности проблематично использовать самые криптостойкие алгоритмы шифрования. Отсутствует и должное внимание пользователей к на первый взгляд не такому серьезному оборудованию - тем не менее, как минимум раз в несколько лет [1] множество зараженных устройств оказываются частями огромных ботнет сетей, используемой для массивных DDoS атак на различные организации.

На примере предложенной системы рассмотрим основные службы информационной безопасности, которые предупреждали бы утечку конфидециальных данных и получение доступа к системе.

2 Что защищать

Уместно было бы определить, насколько опасна может быть компрометация IoT-системы. По незащищенному/компрометированному соединению может передаваться приватная информация либо некоторая информация, позволяющая в свою очередь получить доступ к приватной информации. Сюда входит, например, передача паролей и данных банковских карт через обыкновенный HTTP. Более того, специфика голосовых помощников предполагает частую передачу отрывков аудиозаписей, куда могут попасть (и утечь) приватные разговоры.

3 Точка доступа

3.1 Закрытые порты

Желательно произвести реконфигурацию маршрутизатора: отключить проброс портов и UPnP (некоторые особо «умные» устройства могут пробить доступ к себе из Интернета; если роутер сам по себе не спрятан за следующим NAT, то есть у маршрутизатора

белый IP - это потенциально опасно, особенно в совокупности со следующими пунктами). Есть, конечно, и обратная сторона - без проброса портов не будет доступа к сети извне, если необходимость в таком доступе есть - придётся обойтись просто внимательной и правильной настройкой и аутентификацией по ключам, где это возможно.

3.2 Смена стандартного логина и пароля

Многие ботнеты, в том числе, впервые нашумевший в 2016 году Mirai [3] (тогда с его помощью было захвачено около 145,000 устройств на базе процессоров ARC и атакован американский провайдер Dyn), получают доступ к устройствам просто перебирая стандартные логины и пароли. Очевидно, их стоит сменить на нестандартные с достаточной энтропией, еще лучше - менять их периодически.

3.3 Своевременное обновление прошивки

В программном обеспечении для роутеров нередко оказываются уязвимости. При выходе новой версии ПО стоит производить обновление, хотя в новой версии может оказаться и новый 0-day, как недавно получилось у Cisco [2].

4 ZigBee, Wi-Fi

Данные протоколы сами по себе довольно безопасны при правильной конфигурации и не очень уязвимы для снифферов. Для Wi-Fi желательно выбрать WPA2-AES/WPA3 (WPA2-TKIP оставлен для обратной совместимости; считается менее безопасным). В ZigBee используется AES-128 по умолчанию. Все еще возможна атака перехвата рукопожатия и перехват сессионных ключей, однако это очень серьзное усложнение жизни злоумышленнику. Есть и проблема - для малопроизводительных устройств шифрование, к сожалению, оказывается ударом по быстродействию; иногда может пригодиться его вовсе отключить.

5 Доступ в Интернет

Поскольку используются сервисы, требующие доступ в Интернет (Siri, Яндекс.Алиса), желательно включить HTTPS-only режим; в случае подмены сертификата должно появиться предупреждение/ошибка. Опять же, недостаток решения заключается в накладных расходах на рукопожатие и шифрование.

6 Антивирусное обеспечение

Все достаточно продвинутые устройства (смартфоны, планшеты, компьютеры) желательно снабдить антивирусным обеспечением. По возможности настроить фаерволл, НЕ разблокировать загрузчик и НЕ получать рут-права. Не использовать подозрительный софт из неизвестных источников, либо изолировать его в виртуальную машину; впрочем, такой способ подходит в основном для компьютера.

7 Заключение

Предполагается, что выполнения указанных мер и рекомендаций достаточно для предотвращения большинства атак на предложенную IoT-систему.

Список литературы

[1] Pooja Kumari, Ankit Kumar Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, Computers & Security, Volume 127, 2023, 103096, ISSN 0167-4048. - URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404823000068

[2] Cisco zero-day bug allows router hijacking and is being actively exploited, The Register. - URL: https://www.theregister.com/2023/10/16/cisco_ios_xe_zeroday_exploit

[3] The Mirai Botnet – Threats and Mitigations, Center for Internet Security. - URL: https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations