Тема

Уменьшение рисков неавторизованного доступа к приборам умного дома

Автор

Мазяр Алексей Николаевич, 21213

Введение

После просмотра предложенной схемы, мне показалось, что интересно было бы проанализировать угрозу получения нарушителями доступа к критическим приборам умного дома (замки, камеры, двери гаража). Для владельцев этой системы, ущерб при подобном инциденте является значительным, поэтому контрмеры для уменьшения рисков необходимы.
Также желательна возможность подключения гостевых устройств к сети умного дома по простой и дружелюбной инструкции. Это делает систему ещё более открытой для потенциальных атак.

Возможные атаки

Учитывая, что гостевые устройства могут подключаться к сети, они могут попробовать представиться каким-либо более привилегированным устройством, что в частности может использоваться для атаки повторного воспроизведения. Это в свою очередь может быть частью Man-in-the-Middle атаки.

Возможные решения

Гостевая подсеть

Предлагается выделить изолированную сеть для гостевых устройств с отдельными, более низкими привилегиями. Такая сеть поможет предотвратить неавторизованный доступ к устройствам умного дома, находящимся в основной сети, а также предотвратить заражение критических узлов системы при заражении гостевых устройств. Так как общение между этой и основной сетями ограничено, реализация атак повторного воспроизведение и MitM становится сложнее.

Плюсы

1. Простое подключение гостевых устройств к сети
2. Две отдельные сети может быть легче администрировать для выявления подозрительных активностей, ведь трафик разделён
3. Без дополнительных мер атакующий не может послушать даже зашифрованные сообщения в основной сети

Минусы

1. Гости могут захотеть получить больше доступа к устройствам умного дома, что в общем случае усложнит конфигурацию, а при отсутствии мер помимо Гостевой подсети просто уменьшит надёжность системы, ведь гостевым устройствам прийдётся предоставлять доступ к основной сети, хоть и в индивидуальном порядке.
2. Сложная конфигурация и поддержка. Настройка двух связанных сетей сложнее, чем настройка двух раздельных сетей, также как и их администрирование
3. При возможности дистанционного подключения и управления приборами (даже самыми незначительными с точки зрения потерь) может быть эксплуатировано. Например, включая вентилятор, пока владельцы на работе, можно увеличить хотя бы счёт за электричество

Защищённое сопряжение устройств

> Доступ к сети с приборами умного дома не должен осуществляться по паролю, так как это создаёт слишком большой риск для возможных значительных потерь. Альтернативой может стать например NFC или Bluetooth Secure Simple Pairing, позволяющий устанавливать защищённое соединение между мобильными устройствами и IoT. Подобный механизм включает в себя более надёжные методы аутентификации, что повышает защиту системы от атак, когда атакующий выдаёт себя за кого-то более привилегированного. Также он обеспечивает шифрование данных.

Плюсы

1. Упрощённый доступ к сети: предложенные технологии не требуют от пользователей навыков администрирования сети, так что подключение новых мобильных устройств должно быть нетрудным
2. Отсутствие дополнительных затрат на администрирование сети

Минусы

1. Могут возникнуть проблемы совместимости между устройствами с разными Bluetooth версиями
2. Ограничение на расстояние соединения (Bluetooth в среднем работает на расстояние до 10 метров, но например стены могут мешать передаче сигнала, снижая действительное расстояние)
3. В среде с высоким уровнем помех радиочастот (RFI) соединение по Bluetooth может глохнуть

Система контроля и управления доступом

Внутри системы умного дома существует естественное разделение приборов IoT на группы доступа. Например, можно разделить устройства на низкий уровень безопасности (свет, вентиляторы, телевизор), средний уровень (холодильник и терморегулирование), высокий уровень (замки, двери, камеры). В зависимости от сложности системы умного дома можно

подключить Дискреционное (небольшие системы) или Ролевое (относительно большие системы) управление доступом. Как и в случае с гостевой сетью позволяет разграничивать доступ к приборам.

Плюсы

1. Мелкозернистый контроль доступа, остальные сервисы позволяют разделить доступ лишь крупнозернисто
2. Адаптируемость и расширяемость к динамическому списку мобильных устройств пользователей и приборов умного дома
3. Хорошо интегрируема с другими сервисами кибербезопасности

Минусы

1. Слабая устойчивость к ошибочной конфигурации из-за мелкозернистости прав доступа
2. В рамках умного дома строгое разделение приборов на доступные и недоступные может не понравится пользователям. Поэтому скорее всего будут попытки обойти данную политику безопасности

Post scriptum

Хочу отметить, что все 3 решения можно имплементировать вместе друг с другом.