ОСОБЕННОСТИ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ СИСТЕМЫ «УМНЫЙ ДОМ»

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Беларусь

Костюченко В.В.
Алефиренко В.М. – канд. техн. наук, доцент

В мире последнее время начала получать распространение так называемая система «Умный дом» (англ. Smart Home), которая позволяет автоматизировать и упростить управление собственным жилым помещением. Систему «Умный дом» можно рассматривать как экосистему, имеющую в своей основе программный комплекс, который тесно связан с датчиками, контроллером и облачными сервисами.

Самым удобным и простым способом построения «Умного дома» без масштабной реконструкции здания является использование беспроводных технологий. Так как именно этот способ является наиболее распространенной практикой, то кратко рассмотрим самые популярные протоколы беспроводной связи в «Умном доме».

Протоколы беспроводной связи ZigBee и Z-wave на данный момент самые распространенные радиочастотные технологии в системах домашней автоматизации. Z-Wave – это протокол беспроводной связи, который работает в промышленном, научном и медицинском радиодиапазонах. Он передает на частотах 868,42 МГц (Европа) и 908,42 МГц (США), предназначенных для передачи данных с низкой пропускной способностью во встроенных устройствах, таких как датчики безопасности, аварийные сигнальные системы и панели управления домашней автоматикой и т.д. Z-Wave микросхемы имеют 128-битный AES (Advanced Encryption Standard - симметричный алгоритм блочного шифрования), которые используются системами контроля доступа, такими как дверные замки, аутентифицированное шифрование пакетов [1]. Так же доступна версия с открытым исходным кодом для стека протоколов Z-Wave - Open Z-Wave, но пока она еще не поддерживает часть шифрования [2].

В современном цифровом мире на первое место выходит проблема утечки личных данных пользователей. Но при использовании системы «Умный дом» это несет в себе еще и проблему физического проникновения в здание.

Для безопасности использования «Умного дома» важно убедиться, что в системе реализованы следующие условия защиты от возможных угроз [3]:

– подделка устройства: «требуется система, обеспечивающая защиту от несанкционированного доступа, может удалить конфиденциальную информацию, включая ключи безопасности, если обнаружен фальсификатор в сети»;

– транспортировка ключей: «ключ ссылки по умолчанию не должен использоваться, поскольку этот ключ считается общедоступным и, следовательно, обеспечивает тот же уровень безопасности, что и незашифрованный транспорт ключей»;

– установка ключа: «основные ключи, используемые при создании ключа, должны быть распределены по внеполосным каналам». Это может быть достигнуто с помощью чего-то такого же простого, как наклейка с основным ключом, прикрепленным к устройству для входа пользователя во время установки;

– смена ключа: «безопасность связи зависит от секретности сетевого ключа и ключей связи. Сетевой ключ должен периодически меняться. Управление ключами в форме изменения сетевого ключа в рабочий период времени или после ввода определенного количества сообщений. В противном случае может быть обнаружен известный открытый ключ или другие атаки на безопасность AES».

Так же, в каждом современном смартфоне уже есть точный дактилоскопический сенсор, часто встроены сканеры сетчатки глаза и лица. А значит, это можно использовать для дополнения к стандартной аутентификации пользователя, что сильно усложнит взлом в целом системы контроля доступа, но при этом не будет удорожать конструкцию всего «Умного дома», ведь монтаж и установка датчика не потребуется. Так же, производителям стоило бы задуматься об использовании технологии подобной RSA (аббревиатура от фамилий Rivest, Shamir и Adleman, криптографический алгоритм с открытым ключом) ключам доступа, когда вначале требуется ввести приватный пароль, и только потом человек получает доступ к настоящему коду, ожидаемому системой, после ввода которого можно приложить смартфон с NFC (Near Field Communication — технология беспроводной связи) меткой к сканеру. Эти простые меры позволят повысить безопасность доступа к жилищу, не делая более дорогой конструкцию, но сильно осложняя взлом и компрометацию данных пользователей.

В завершении хотелось бы отметить, что системы «Умный дом» год от года становятся безопасней и дружелюбней к пользователям, но производители упускают из виду, что простые изменения и дополнения в конструкции и архитектуре кардинально могут поменять проблему безопасности. У пользователей уже сложились серьезные требования к конфиденциальности и безопасности, когда речь заходит о домашней автоматизации, поскольку она генерирует огромное количество персонализированных данных.

Список использованных источников:

1. "Introduction to the Z-Wave Security Ecosystem." Z-Wave, Aug. 2016, https://z-wave.sigmadesigns.com/wp-content/uploads/2016/08/Z-Wave-Security-White-Paper.pdf. Accessed 21 March 2018.

2. "Z-Wave Devices." Home Assistant, https://home-assistant.io/docs/z-wave/devices. Accessed 21 March 2018.

3. Zillner, Tomas. "ZIGBEE EXPLOITED - The good, the bad and the ugly." Black Hat, https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf. Accessed 21 March 2018.