ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ И ТЕХНОЛОГИЯ eSIM

А.С. Шелков

Интернет вещей (IoT) – одно из самых развивающихся направлений в области информационных технологий и беспроводной связи. Одной из важных проблем в развитии данного направления является информационная безопасность (ИБ) инфраструктуры IoT. Инфраструктура IoT представляет собой совокупность устройств: датчиков, измерительных устройств, видеокамер, управляемых переключателей и т.д. Указанные компоненты, взаимодействуя между собой, или с внешней средой по определенным протоколам, образуют IoT. С момента создания концепции IoT отсутствовали жесткие ограничения и стандарты информационной безопасности устройств IoT, что делает небезопасным применение IoT для реальных задач. К основным слабым сторонам использования IoT относятся следующие пункты: питание датчиков, отсутствие единой стандартизации архитектуры и протоколов, отсутствие системы управления правами доступа, трудности обновления ПО, использование небезопасного ПО и др. Существенная часть этих недостатков может быть устранена применением технологии embedded SIM (eSIM) для устройств IoT. eSIM – технология, позволяющая виртуализировать модуль идентификации абонента (SIM): виртуальная SIM загружается через OTA-интерфейс на встроенный в мобильное устройство чип (eUICC). Идентификационные данные для виртуальной SIM предоставляются провайдером связи на узел SM-DP (Subscription Manager Data Preparation), который формирует профиль SIM-карты, впоследствии загружаемый и устанавливаемый в eUICC мобильного устройства. Применение этой технологии позволит реализовать следующие меры безопасности:

1) устройство становится частью сети сотового оператора, чем решается вопрос с аутентификацией;

2) провайдер услуг IoT может внедрить в профиль eSIM сканирующее ПО, которое может быть в дальнейшем использовано как часть IDS;

3) устройства с поддержкой eSIM должны проходить сертификацию GSMA;

4) появляется возможность обновления ПО устройства при помощи технологий OTA;

5) провайдер IoT может предоставлять специальных платформу для централизованного контроля и управления устройствами IoT для конкретных объектов.

Использование eSIM не решает всех вопросов ИБ, но позволит нивелировать самые критические уязвимости.

ПОДХОДЫ К БЕЗОПАСНОМУ КОНФИГУРИРОВАНИЮ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

А.С. Шилов, О.В. Бойправ

Операционные системы семейства Windows имеют ряд схожих характерных черт, в частности, защитные технологии, что облегчает обеспечение их безопасности и отчасти сводит его к правильной конфигурации параметров безопасности системы администратором. Данные параметры могут быть классифицированы в зависимости от механизмов операционной системы, с которыми они связаны: параметры контроля учетных записей, параметры устройств, параметры сетевого доступа, параметры завершения работы, параметры аудита, параметры входа в систему и т.д.

К критически важным параметрам безопасности относятся, в первую очередь те, которые связаны с учетными записями. В связи с неограниченным числом попыток неверного входа для данной записи, следует отключать параметр «состояние учетной записи «Администратор»» на рабочих машинах рядовых пользователей сети, что не позволит использовать данную запись при обычном входе, а также отключить автоматический вход администратора в консоль восстановления. Также необходимо ограничивать возможности пользователей по добавлению новых учетных записей настройкой параметра «блокировать учетные записи Майкрософт» и использование встроенной учетной записи «Гость», отключив параметр «состояние учетной записи «Гость»». Также следует контролировать установку