В.Воротников, руководитель отдела перспективных исследований и проектов компании "С-Терра СиЭсПи"

Мобильных устройств стало значительно больше, чем раньше. К мобильным телефонам, цифровым фотоаппаратам и плеерам добавилась и электроника, которую мы носим с собой: умные часы, фитнес-трекеры, видеорегистраторы, навигаторы и т.д. Есть ряд причин, осложняющих обеспечение их безопасности. Причины эти тесно связаны с последними тенденциями рынка мобильных устройств и ожиданиями пользователей. Чего хочет пользователь от мобильного устройства? Широкой функциональности, легкой связи с внешним миром, предельной простоты использования, компактности. Упрощение интерфейса и интеграция с различными облачными и социальными сервисами – одни из главных трендов развития индустрии мобильных устройств. Но для безопасности все эти тенденции – катастрофа.

Функциональность. Чем шире функциональность устройства, тем большее количество полезной информации может получить злоумышленник: каждый датчик (GPS, микрофон, камера, монитор сердечного ритма и т.д.) увеличивает количество полезной информации, которую устройство может собирать. С первого взгляда, акселерометр или датчик освещенности не может дать злоумышленнику ничего полезного. Но это не так. С помощью информации с любого из этих датчиков можно получить набираемые на устройстве данные: акселерометр выдает характерные показания при нажатии на разные точки экрана. Таким образом можно, например, определить, какой пин-код или пароль набирал пользователь. Аналогичное поведение показывает и датчик освещенности, т.к. при нажатии на разные точки экрана происходит смещение датчика яркости относительно источника света с изменением угла падения лучей.

Связь с внешним миром. Чем больше у устройства способов связи с внешним миром, тем больше появляется каналов утечек. И если о существовании Wi-Fi или Bluetooth среднестатистическому пользователю известно, то про поддержку своим телефоном технологии NFC (Near Field Communication) пользователь может даже не подозревать, хотя несколько уязвимостей в реализации этого протокола уже было обнаружено. Похожая ситуация с протоколом IPv6 (Internet Protocol version 6), который включен на многих устройствах по умолчанию, о чем пользователь даже не подозревает.

Простота использования. Часто простота использования противопоставляется безопасности. Удобно ли, чтобы цифровой фотоаппарат из рюкзака автоматически подключался к бесплатной сети Wi-Fi в кафе и сбрасывал все свежие фотографии на облачное хранилище, которое доступно пользователю отовсюду? Конечно – да! Безопасно ли это? Определенно – нет. Простота использования – это часто ловушка, за которой скрывается потеря контроля над тем, что происходит в устройстве.

Компактность. Уменьшение размеров не так явно связано со снижением безопасности, но корреляция есть. Так, например, часто в компактных устройствах ограничен объем памяти, и устанавливаемая на них операционная система (обычно основанная на Unix/Linux) может быть сильно уменьшена и не иметь возможности обновления при выходе критических обновлений безопасности. Некоторые компактные устройства настолько малы, что управляются и настраиваются только с внешнего устройства или пульта. Протоколы связи между управляющим и управляемым устройством часто бывают проприетарные и слабозащищенные.

Таким образом, складывается следующая картина. Люди носят с собой все больше и больше "умных" устройств. Объемы данных от этих устройств экспоненциально растут, чего не скажешь о контроле за этими потоками. Во всю мощь стучится в дверь казавшееся забавным пару лет назад понятие "Интернет вещей". Что со всем этим делать? Можно закрыть глаза или спрятаться в кусты, надеясь, что проблема пропадет сама собой. Можно отрицать проблему или бороться со "всякими модными" проявлениями в стиле "держать и не пущать"! Так иногда делают, но это не работает. Глупо идти против прогресса. Наша задача как квалифицированных, ответственных специалистов по безопасности – обеспечить прозрачную и эффективную безопасность в сетях, сервисах и приложениях. Сделать так, чтобы безопасность перестала быть антонимом простоты использования. Пользователю скучно придумывать сложный пароль – давайте использовать другие способы аутентификации. К вашей корпоративной сети подключаются удаленные сотрудники – стоит подумать о сохранности и конфиденциальности данных (например, с помощью построения частных защищенных сетей VPN), а также о централизованной инспекции трафика на корпоративном антивирусе, межсетевом экране и IPS (Intrusion Prevention System). ■