УДК 004.056.53

АНАЛИЗ АТАК ПО СТОРОННИМ КАНАЛАМ НА ФИТНЕС-ТРЕКЕРЫ ДЛЯ ДОМАШНИХ ЖИВОТНЫХ

В.А. Варюхин, Р.А. Мостовой , Э.Д. Андреев (Санкт-Петербургский Государственный Университет Информационных технологий, Механики и Оптики, Санкт-Петербург)
Научный руководитель – А.Б. Левина (Санкт-Петербургский Государственный Университет Информационных технологий, Механики и Оптики, Санкт-Петербург)

В настоящее время становятся популярным использование фитнес-трекеров в виде ошейников для животных, т.к они помогают контролировать местоположение, активность и даже эмоциональное состояние питомцев. Счета на услуги ветеринаров растут с каждым годом, и, как следствие, растут страховые взносы владельцам. Зарубежные страховые компании уже на протяжении 5 лет используют трекеры для расчетов стоимости страховки для домашних питомцев. Данный ошейник может помочь поддерживать свою собаку в хорошей форме, и помогает страховым компаниям снижать свои расходы.

В комплектацию данных средств мониторинга активности чаще всего включены датчики, акселерометры, микрофоны, GPS, WiFi, Bluetooth и другие модули. В связи с тем, что используется большое количество технологий, становится актуальным вопрос защищенности хранимой и передаваемой информации данного устройства. В работе рассматриваются атаки по сторонним каналам на компоненты трекера.

Атаки по сторонним/побочным каналам – вид криптографических атак, использующих информацию, полученную по физическим каналам связи (ЭМИ, акустические и акустические каналы).

Объектом исследования являются фитнес-трекеры для домашних животных от компаний Jagger&Lewis и FitBark.

Данная работа сфокусирована на вопросах получения секретной информации (закрытый ключ, ip адреса и порты удаленного сервера подключения и т.д.) хранящейся в устройстве, а также на попытке перехвата сведений компрометирующих данные собаки, а значит и ее владельца.

Система Jagger&Lewis представляет типичную архитектуру клиент-серверного взаимодействия. Используется 2 типа клиента: клиент-собаки (трекер) и клиент-владелец (аккаунт в мобильном приложении). Сервер является агрегатором данных присланных с ошейника. После применения специальных алгоритмов обработки владельцу отсылается актуальная информация о текущем состоянии питомца.

При первичной инициализации приложения происходит взаимная привязка трекера и аккаунта посредством Bluetooth. После требуется указать параметры WiFi для того чтобы устройство могло автономно отправлять накопленные данные. В свою очередь мобильное приложение требует большое количество разрешений: доступ к местоположению, контактам, файловой системе.

Система FitBark 2 имеет схожую клиент-серверную архитектуру. Отличительным признаком данного трекера является то, что данные могут приходить не только в специальное приложение, а также интегрироваться в такие сервисы как Fitbit, Apple Healthkit или Google Fit посредством специального API. Инициализация и дальнейшее использование устройства повторяют действия, что и трекер от Jagger&Lewis.

Угрозы безопасности, обнаруженные после исследования данных устройств, делятся на 2 вида: угроза подмены данных, которые отправляются от трекера удаленному серверу, и угроза доступа к смартфону по используемым каналам связи.

Осуществление компрометации данных для дальнейшей отправки на сервер является типичной

атакой Man In The Middle. Угроза является осуществимой, если удается получить доступ к WiFi сети, к которой подключено атакуемое устройство.
Получение доступа к мобильному телефону может быть осуществлено только в том случае если удается «снять» информацию о Bluetooth-характеристиках трекера, для её дальнейшего внедрения в свое устройство. «Лже-трекер» в свою очередь сможет запрашивать необходимые привилегии у смартфона для извлечения требуемой злоумышленнику информации.
Следует отметить, что данные атаки выгодны не только стороннему лицу, т.к. могут предоставить доступ к смартфону, но и самим владельцам данных систем, т.к. при подмене данных можно вводить в заблуждение страховые компании, а значит минимизировать свои расходы.
Полученные результаты, после проведения вышеописанных атак, показали, что устройства являются надежными для использования в домашних условиях, только при условии хорошо защищенной Wifi сети.

Авторы _____/Варюхин В.А.
_____/Мостовой Р.А.
_____/Андреев Э.Д.

Научный руководитель _____/Левина А.Б.

Декан факультета БИТ _____/Заколдаев Д.А.