ПУТИ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ АБОНЕНТА МОБИЛЬНОЙ СВЯЗИ ОТ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ

Найденова Д. Р.
Научный руководитель – д.т.н., проф. Антипов И.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, кафедра ИРТЗИ
(057) 702 14 30) e-mail: diana.naidonova@nure.ua, тел.: (095) 416 55 37

Theses is about increase of information security of the mobile user and his privacy improvement. Paths to get information about the mobile user location are shown. Outlined who are interested in this information. Organizational and technical measures to complicate the location of the mobile user are proposed.

По мере развития информационно-телекоммуникационных и сопутствующих технологий, пользователям мобильных устройств становятся доступными всё более разнообразные услуги и возможности. С одной стороны многое существенно улучшается, упрощается и удешевляется. Но, с другой стороны, эти же технологии позволяют получать, накапливать и хранить много разнообразной информации о самом пользователе. Доклад посвящён организационным и техническим мерам, которые заботящийся о своей безопасности пользователь может предпринять, чтобы ограничить сбор и накопление информации, касающейся своей частной жизни, в частности, о своем местонахождении, и, вместе с тем не лишаться тех возможностей, которые современные технологии предоставляют.

Можно выделить несколько структур, которые могут быть заинтересованы в получении информации о местоположении пользователей. Во-первых, это операторы мобильной связи, ведь сам принцип её мобильности предполагает знание местонахождения абонента. Кроме того, данные о нахождении и перемещении абонентов (даже в «обезличенном» виде) могут использоваться для развития сети. Во-вторых, производители товаров и услуг, заинтересованные в целенаправленной рекламе. В-третьих, спецслужбы, действующие в интересах общественной безопасности.

И, наконец, злоумышленники, к которым могут быть отнесены и излишне подозрительные «друзья» или родственники, и чрезмерно навязчивые рекламодатели, недобросовестные конкуренты и т. д. Также не лишена оснований теория о намерении неких структур («мирового правительства»?) установить контроль если не над каждым конкретным пользователем, то, по крайней мере, над определёнными сообществами и лидерами общественного мнения. Настораживает то, что из современных мобильных устройств нельзя извлечь аккумулятор, невозможно физически отключит видеокамеру и микрофон. Кроме того, назначение ряда функций их операционных систем не очевидно. А компания Google даже не скрывает, что собирает сведения о местонахождении всех устройств с операционной сис-

темой Android (Разумеется под предлогом, что программу запустили исключительно для того, чтобы улучшить качество связи, и готовы отказаться от подобной практики [1]).

В докладе выделяются следующие источники информации о местоположении пользователя мобильной связи. Во-первых, это сами операторы связи, постоянно располагающие данными о ближайших к абоненту базовых станциях. Во-вторых, спутниковые навигационные приёмники, имеющиеся в большинстве современных смартфонов. Данные от этих приёмников могут (даже без ведома пользователя) накапливаться и передаваться на сторонние ресурсы. В-третьих, Wi-Fi сети, находящиеся в зоне радиовидимости от мобильного устройства. Они могут накапливать и передавать на сторонние ресурсы информацию обо всех устройствах, оказавшихся в зоне их действия. То же может делать и само мобильное устройство. В докладе указаны точностные характеристики приведенных методов, степень сложности и оперативности получения данных для различных категорий заинтересованных в них.

Далее в докладе рассмотрены меры, которые следует предпринять, чтобы затруднить сбор информации о местонахождении. В качестве простой организационной меры предлагается отказаться от повсеместного использования смартфона. Функции мобильных устройств должны быть строго разделены. Постоянно включённый мобильный телефон без дополнительных функций используется исключительно для разговоров и получения текстовых сообщений. Это в три раза уменьшает количество путей получения информации о местоположении абонента. Смартфон же постоянно находится в «авиарежиме», предусматривающем отключение всех имеющихся в нём передатчиков и даже встроенных GPS- и FM-приёмников. В этом режиме он может использоваться как электронная книга, фотоаппарат, диктофон и элемент определяющий статус владельца. Он выводится из «авиарежима» только при неотложной необходимости доступа к сети или определения своего местоположения. При этом снижается энергопотребление и уменьшается зависимость от смартфона, которая ведёт к психическим расстройствам и снижению когнитивных функций мозга [2]. Предложен также ряд других мер организационных мер.

В качестве технической меры в докладе рассмотрена структура и принцип действия устройства, работающего подобно GSM-шлюзу, но использующего в качестве составной части любой мобильный телефон.

Ссылки

1. https://www.1tv.ru/news/2017-11-23/336716-google_sledit_za_polzovatelyami_gadzhetov_rabotayuschih_na_android

2. This is what your smartphone is doing to your brain – and it isn't good // [Электронный ресурс.] Режим доступа: http://www.businessinsider.com/what-your-smartphone-is-doing-to-your-brain-and-it-isnt-good-2018-3