А. Г. Бельтов, И. Ю. Жуков, А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский

ВОПРОСЫ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

Мобильный телефон является неотъемлемой частью жизни любого современного человека. Пользователи, находясь практически в любом месте земного шара, могут использовать различные возможности своих телефонов: посылать друг другу SMS-сообщения, осуществлять телефонные вызовы, просматривать и редактировать документы любых форматов, получать доступ в Интернет. Многие хранимые и передаваемые данные являются конфиденциальными.

К сожалению, стремительное развитие мобильных технологий не всегда сопровождается разработкой соответствующих средств защиты. Наличие серьезной конкуренции заставляет производителей сотовых телефонов и смартфонов торопиться с выпуском все новых и новых устройств и стандартов, позволяющих пользователям обмениваться информацией всевозможных форматов, выходить в сеть Интернет, оплачивать счета в любое время и в любом месте, определять свое местоположение с помощью встроенных модулей GPS и осуществлять многие другие возможности. При этом вопросы безопасности остаются на втором плане и защита носит реактивный характер: соответствующие меры предпринимаются только после проведения атак на мобильные устройства.

Тем не менее с распространением мобильных устройств по всему миру с их помощью злоумышленники могут получить доступ к более важной информации, завладеть которой позволяют уязвимости применяемых для мобильной связи протоколов и структур. Несмотря на то что эти технологии не являются полностью доверенными и не используются для передачи секретной информации, даже некоторые персональные данные высокопоставленных лиц могут содержать косвенные указания на сведения государственной важности. Злоумышленники могут завладеть списком контактов жертвы, историей текстовых сообщений и поисковых запросов, информацией о местоположении владельца телефона, журналом вызовов и даже расшифрованными записями самих разговоров.

Вопрос безопасности мобильных устройств важен и для коммерческих структур, не обязанных следовать государственным стандартам безопасности и повсеместно использующих современные технологии для деловых переговоров, хранения и пересылки важных документов. Особенно это актуально для крупных корпораций, сведения о сделках которых могут представлять политический интерес.

Рассмотрим основные технологии, применяемые в мобильных устройствах, и средства, используемые ими для обеспечения одного из самых важных аспектов безопасности — конфиденциальности. Наиболее распространенными и широко используемыми из них в настоящее время являются: стандарт сотовой связи GSM, предоставляющий, в частности, такие популярные сервисы, как SMS/MMS, GPRS/EDGE, протоколы Bluetooth, NFC, Wi-Fi.

Поскольку все перечисленные технологии передачи данных являются беспроводными, злоумышленник имеет возможность перехватить трафик, для этого ему достаточно расположить оборудование мониторинга сетей (так называемые сетевые анализаторы) не дальше определенного расстояния от субъекта атаки.

Сети, основанные на стандарте GSM, имеют три ключевые уязвимости, позволяющие атаковать их абонентов [1, 2, 3]:

- устройства никак не верифицируют соту, к которой подключаются;
- сигнальный (управляющий) протокол SS7, который используется в стандарте GSM, не имеет никаких средств аутентификации или шифрования;
- криптостойкость поточных шифров семейства A5 является чрезвычайно низкой.

Все эти недостатки в совокупности позволяют злоумышленнику перехватывать разговоры, SMS- и MMS-сообщения, пакетные данные, передаваемые с помощью технологий GPRS и EDGE [3].

Стандарт беспроводных сетей Wi-Fi известен уже более 10 лет. Встроенные механизмы аутентификации и шифрования не защищают пользователя от взлома с помощью обычного персонального компьютера, для проникновения в «защищенную» сеть злоумышленнику требуется только ПК с Wi-Fi адаптером [4].

Протокол Bluetooth обладает целым рядом серьезных уязвимостей, используя которые злоумышленник может осуществлять различные виды атак: получение доступа к телефону, прослушивание разговоров абонента, внедрение в систему жертвы программ-закладок, вывод аппарата из строя и др. [5]. Также, благодаря стремительному распространению Bluetooth и все большей популярности устройств, поддерживающих его, особую актуальность приобретает опасность заражения телефона мобильными вирусами, многие из которых еще не распознаются недостаточно совершенными антивирусами для мобильных платформ.

NFC является наиболее динамично развивающейся технологией ближнего беспроводного взаимодействия. Она используется в таких критических приложениях, как оплата товаров и услуг с помощью банковского счета, ограничение доступа в помещения. Однако стандарт NFC сам по себе не включает каких-либо средств защиты, что позволяет практически любому злоумышленнику с помощью подмены устройств завладеть конфиденциальной информацией, установить на телефон жертвы вредоносное приложение или похитить средства со счета пользователя без его ведома [6].

С широким распространением смартфонов на рынке мобильных устройств все больше функций передается сторонним приложениям, часто поставляемым независимыми разработчиками. Ошибки и недочеты в коде подобной программы могут привести к появлению уязвимостей, угрожающих не только корректной работе приложений, но и в ряде случаев функционированию аппаратной части мобильного устройства.

Рассмотренные выше технологии не обладают достаточными средствами защиты от атак, направленных на получение конфиденциальной информации. У каждой из них есть целый ряд недостатков, позволяющих злоумышленнику, даже не имеющему высокой квалификации, завладеть персональными данными владельца мобильного устройства.

Технические решения, представленные на рынке в настоящее время, не позволяют гарантированно обезопасить себя от подобных нападений.

Решением проблемы может стать разработка дополнительных средств защиты информации, а также отказ от использования некоторых особо уязвимых технологий.

В качестве путей обеспечения должного уровня защищенности может быть использовано дополнительное, более стойкое, чем встроенное сегодня в мобильные телефоны, шифрование данных, а также разработка и внедрение безопасности операционной системы, обеспечивающей

повышенную безопасность данных, и адаптация ее под все распространенные в настоящее время мобильные платформы.

Последнее особенно важно для российского рынка мобильных устройств, так как использование зарубежного программного обеспечения не может считаться гарантированно безопасным из-за возможного наличия в нем так называемых «закладок» — вредоносного кода, встроенного в систему производителем и действующего без ведома пользователя.

Важно отметить, что для обеспечения полноценной защиты мобильного телефона необходимо использовать все перечисленные методы в качестве единого комплекса мер в сочетании с постоянным аудитом работы системы и своевременным реагированием на вновь возникающие угрозы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Heine G.* GPRS Signaling and Protocol Analysis. Vol. 1: RAN and Mobile Station. Artech House Publishers, Bern, 2002. — 242 p.
2. *Драйберг Л., Хьюитт Дж.* Система сигнализации № 7 (SS7/OKC7). Протоколы, структура и применение. Вильямс, London, 2006. — 752 с.
3. *Михайлов Д. М., Жуков И. Ю., Ивашко А. М.* Защита мобильных телефонов от атак. М.: Фойлис, 2011. — 192 с.
4. *Prabhaker M.* Hacking Techniques in Wireless Networks. Dayton, Ohio: Department of Computer Science and Engineering — Wright State University, 2005.
5. *Михайлов Д. М., Жуков И. Ю.* Исследование уязвимостей Bluetooth-передатчика мобильных телефонов // Научная сессия НИЯУ МИФИ-2010. XIII Международная телекоммуникационная конференция студентов и молодых ученых «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3 частях. Ч. 2. М.: НИЯУ МИФИ, 2010. — С. 204
6. *Haselsteiner E. , Breitfuss K.* Security in near field communication (NFC) // Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec. July 2006. P. 45—47.