Научная статья
Original article
УДК 004.056

ПРОСЛУШИВАНИЕ И ИЗЪЯТИЕ ИНФОРМАЦИИ СО СМАРТФОНОВ. МЕРЫ ЗАЩИТЫ

LISTENING AND TAKING INFORMATION FROM SMARTPHONES. PROTECTION MEASURES

Прокопайло Александр Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону, mrakfest@gmail.com

Prokopaylo Alexander Alexandrovich, Master's student, Don State Technical University, Rostov-on-Don, mrakfest@gmail.com

Аннотация. Настоящая работа посвящена обзору на различные методы изъятия информации с мобильных устройств. Подробное описание каждого аспекта по сбору информации с телефона и рекомендации по обеспечению безопасности своего мобильного устройства

Abstract. This paper is devoted to an overview of various methods of information retrieval from mobile devices. A detailed description of each aspect of collecting information from the phone and recommendations for ensuring the security of your mobile device

Ключевые слова: прослушивание, мобильные устройства, смартфоны, информация, данные с телефона, защита смартфона.

Keywords: listening, mobile devices, smartphones, information, data from the

phone, smartphone protection.

Сегодня у каждого из нас есть личный смартфон. С помощью него мы звоним друг другу, общаемся в соцсетях, делимся различными файлами и фотографиями. А задумывались ли Вы о том, что ваши разговоры может слушать другой человек? Или же иметь доступ ко всем файлам на вашем устройстве? В настоящее время остается актуальным вопрос о прослушивании и считывании информации с мобильных устройств. Операторы сотовой связи обязаны в течение трех лет хранить всю информацию об абонентах (звонки, сообщения и переданные изображения). Приведем пример некоторых данных, которые можно собрать:

1) Геолокация
2) Физическое прослушивание
3) Данные журнала
4) Данные мессенджеров
5) Данные об установленных программах, скачанных файлах
6) Данные о контактах, истории браузера и т. д.

В связи с этим возникает вопрос: «Как защитить свой смартфон от взлома, слежки или прослушки?». Рассмотрим некоторые из них.

На сегодняшний день обладатели смартфонов обычно оставляют невероятно много следов в соцсетях, загружают фото в инстаграм и т.д. В поле зрения так же попадает не только ваш аппарат, но и телефоны, часто оказавшиеся около него. Нет смысла менять SIM-карты или же сами смартфоны, ибо если вы уже вставили вашу сим-карту в другой телефон, то в системе он будет ассоциирован с вами. И точно так же в случае если вы в свой телефон вставите в другую симку, то система так же эту сим-карту станет ассоциировать с вами. Вынимание батареи – надежный способ избежать отслеживания. Кроме того в продаже есть чехлы для мобильных смартфонов и одежда с карманами, блокирующая сотовый сигнал. Перед использованием, нужно проверить – действительно ли аппарат, находящийся в чехле,

оказывается вне зоны действия сети.

Прослушивание

Существует оборудование и для дистанционного подслушивания разговоров. В теории мобильный телефон можно использовать как скрытый и управляемый на дистанции диктофон. И уж тем более ваш разговор может быть записан, если вы сами звоните по телефону. Зная номер жертвы, злоумышленники могут прослушать мобильное устройство путем подключения к сигнальной сети Signaling System 7 (SS7). Сделать это можно следующим образом:

1) Сначала внедряемся в сеть сигнализации SS7, где через каналы отправляем сообщение SRI4SM, указывая при этом в качестве параметра телефонный номер жертвы.

2) В ответ на наше сообщение домашняя сеть жертвы присылает некоторую техническую информацию: IMSI абонента и адрес его коммутатора MSC.

3) Затем, с помощью сообщения ISD внедряем в базу данных обновлённый профиль жертвы, изменяя при этом адрес биллинговой системы на адрес своей системы.

4) Далее жертва совершает исходящий вызов, тем самым его коммутатор обращается вместо реальной биллинговой системы к нашей системе, которая, в свою очередь, даёт коммутатору директиву перенаправить вызов на третью сторону, которая так же находится под нашим контролем.

5) На этой третьей стороне собирается конференц-вызов из трёх абонентов, два из которых реальные, а третий внедрён нами несанкционированно. Далее можно спокойно слушать и записывать разговор.

При разработке SS7 в ней не было заложено механизмов защиты от таких атак. Эта система должна была быть защищена от внедрений извне, но на практике злоумышленник может найти практически любой способ присоединиться к данной сети.

К SS7 можно подключиться в любой стране мира — и нам будут доступны коммутаторы всех операторов в России, США, Европе и других странах. Такой метод позволяет прослушать любого абонента в мире, даже на другом конце земного шара. Так же звонить следует не напрямую через оператора, а через приложения, поддерживающие шифрование. К таковым относятся: Скайп, ВотсАп, Вайбер или звонки в Фейсбук. Они будут наиболее надежным способом сохранить анонимность, чем обычный телефонный звонок.

Изъятие информации из сообщений

SMS является самым опасным из всех форм общения. Личная информация в самых обычных мессенджерах также может быть украдена. Самым безопасным средством общения на сегодняшних день остается приложение «Телеграмм». В Телеграм существуют безопасные «секретные чаты». Чтобы прочитать ваше сообщение, злоумышленнику придется завладеть вашим телефоном. Вам же в свою очередь необходимо настроить автоматическое удаление истории сообщений после определенного периода времени, а затем, даже украв мобильный телефон, злоумышленник не сможет прочитать Ваши sms. Почти любой взлом мобильного устройства можно избежать при условии, что в нем имеется двухфакторная идентификация (ДА). Важно отметить, что двухфакторная аутентификация не обязательно означает подтверждение с помощью SMS. Кроме того, такое подтверждение не является безопасным. Например, ее можно настроить с помощью Токена. ДА действительно работает на практике.

Информация из телефона

Получить доступ, к смартфону можно найдя уязвимость в операционной системе и заразив его вирусом, но эта задача крайне сложная. Спецслужбы также не имеют прямого и непосредственного доступа к «софту», хотя и предпринимают попытки получить. Так что, хранящуюся в телефоне информацию проще всего приобрести, физически овладев вашим

смартфоном. На смартфонах работают сервисы, хорошо зарекомендовавшие себя на «больших пк»: Tor или защищенная почта Riseup. Телефон должен иметь последнюю версию ОС и установленных приложений, все дополнения должны быть установлены только из доверенных источников. Мессенджеры с открытым исходным кодом, использующие end-to-end кодирование и, по возможности, двухфакторную аутентификацию, достаточно безопасны при правильном использовании. Если к человеку имеют серьезный интерес спецслужбы, нельзя быть полностью уверенным в том, что специально под ваш телефон не написана вредоносная программа, которая не выдает себя и отправляет различную информацию с вашего устройства. Но в Российской федерации это редкость. Спецслужбам гораздо проще прослушать вашу квартиру, чем Скайп или Вайбер.

Рекомендации по обеспечению безопасности

Лучший способ защититься от утечки информации через телефон – не использовать его для передачи конфиденциальных данных. В этом случае стоит соблюдать некоторые рекомендации:

1) Не стоит оставлять смартфон без присмотра;
2) Нужно иметь с собой еще один телефон чтобы передавать конфиденциальные данные;
3) Всегда иметь пароль или графический ключ на телефоне;
4) Не подключаться к тем ПК которым не доверяете;
5) Поставить пароль на соединение по блютуз;
6) Проверять смартфон антивирусом;
7) Ни в коем случае не переходить по сомнительным ссылкам;
8) Проверять списки загрузок и удалять все сомнительные файлы;
9) Запретить всем приложениям самостоятельно скачивать и принимать файлы;

В заключении хотелось бы сказать, что эти рекомендации

действительно помогут защитить ваш смартфон от прослушки или изъятия информации. Такие меры безопасности помогут избежать только бытовые прослушивания, например ревнивой второй половинки или же слишком контролирующих родителей. Для более серьезных случаев потребуется применение несколько других, более серьезных методов.

Литература:

1. Как понять, что ваш телефон прослушивают. [Электронный ресурс] – Режим доступа: https://rtvi.com/stories/kak-ponyat-chto-vash-telefon-proslushivayut/
2. Прослушка сотовых телефонов спецслужбами. [Электронный ресурс] - Режим доступа: http://myagent007.ru/phones-and-apps/wiretapping-cell-phones-security-services.html
3. Защита от прослушки телефона. [Электронный ресурс] - Режим доступа: http://tehno-bit.ru/zashhita-ot-proslushki-telefona/
4. Как защитить смартфон от прослушивания и слежки? Советы хакеров и экспертов по безопасности [Электронный ресурс] - Режим доступа: https://www.macdigger.ru/news/post/kak-zashhitit-smartfon-ot-proslushivaniya-i-slezhki-sovety-xakerov-i-ekspertov-po-bezopasnosti5. Deep Web. [Электронный ресурс] - Режим доступа: https://siddh.ru/mistika/deep-web
5. Незащищенная связь: 9 способов прослушать ваш телефон. [Электронный ресурс] - Режим доступа: https://lifehacker.ru/9-sposobov-proslushat-telefon/

Literature

1. How to understand that your phone is being tapped. [Electronic resource] - Access mode: https://rtvi.com/stories/kak-ponyat-chto-vash-telefon-proslushivayut/
2. Wiretapping of cell phones by special services. [Electronic resource] - Access mode: http://myagent007.ru/phones-and-apps/wiretapping-cell-phones-security-services.html

3. Protection against wiretapping of the phone. [Electronic resource] - Access mode: http://tehno-bit.ru/zashhita-ot-proslushki-telefona/
4. How to protect your smartphone from eavesdropping and surveillance? Tips from hackers and security experts [Electronic resource] - Access mode: https://www.macdigger.ru/news/post/kak-zashhitit-smartfon-ot-proslushivaniya-i-slezhki-sovety-xakerov-i-ekspertov-po-bezopasnosti5. Deep Web. [Electronic resource] - Access mode: https://siddh.ru/mistika/deep-web
5. Unsecured communication: 9 ways to listen to your phone. [Electronic resource] - Access mode: https://lifehacker.ru/9-sposobov-proslushat-telefon/

© Прокопайло А.А, 2021 Научно-образовательный журнал для студентов и преподавателей «StudNet» №11/2021.

Для цитирования: Прокопайло А.А, ПРОСЛУШИВАНИЕ И ИЗЪЯТИЕ ИНФОРМАЦИИ СО СМАРТФОНОВ. МЕРЫ ЗАЩИТЫ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №11/2021.