Будни большого города или что знают о вас мобильные приложения?

Безмалый В.Ф.

Microsoft Security Trusted Advisor

— Где служишь?
— Я работаю в СБ.
— Расскажи что-нибудь интересное…
— О тебе или о себе?

Боб никогда не думал, что станет полицейским детективом. Он окончил престижный технический университет и рассчитывал на престижную работу в банке или другой крупной корпорации. Однако последние летние каникулы резко изменили его судьбу. Что произошло?

Смена работы и судьбы

Боб давно пытался ухаживать за красавицей Лиззи, но после школы их судьбы разошлись. Он уехал в один университет, она — в другой, где каждый занимался своим любимым делом. Боб — компьютерами, а Лиззи — филологией. Прошло 4 года.

— Боб! Привет! Говорят, ты стал крутым компьютерщиком?

— Да нет, просто пытаюсь стать инженером, а что?

— Да проблема у меня… Представляешь, с моей карты пропали деньги. Банк обещает разобраться, но говорит, что я сама виновата, ведь даже SMS-банкинг меня не спас! Я же каждую свою транзакцию в интернете подтверждала с помощью SMS-кода!

— Погоди, а всё остальное нормально?

— Да нет! У меня чёрная полоса. И деньги с телефона пропали.

— А что сказал твой провайдер?

— Говорит, что я сама отправила SMS на платный номер. И не одну. Хорошо, что я ввела лимит на оплату мобильного.

— Ты что, привязала к мобильному счёту основную карту?! Лиззи, мне кажется, что придётся повозиться с твоим телефоном.

— Я только «за». Сможешь сегодня?

— Смогу. Приноси смартфон. Только подумай, это может быть не один час.

— Ничего.

Вечером Лиззи принесла смартфон, однако работа над ним затянулась на всю ночь. Ведь как бы быстро мы с вами не стремились найти и победить зловред, на практике всё оказывается куда медленнее и сложнее.

Утром уставший и небритый Боб, тихо ругаясь, отдавал смартфон.

— Итак, Лиззи, ты понимаешь, что ты устанавливаешь? У тебя здесь масса приложений для выбора причёски, макияжа, игры какие-то.

— И что такого? Я же девушка.

— А то, что минимум четыре из них просят доступ к SMS.

— И что?

— Проблема в том, что они могут не только читать SMS со смартфона, но и отправлять SMS, MMS. А раз так, то какое-то из приложений прочло твою SMS из банка и подтвердило платёж от твоего имени. Кстати, похожее случилось и с твоим мобильным счётом. Просто отправлялись SMS на платные номера, пока у тебя не закончились деньги! Думать желательно до, а не после. Милая, будь аккуратнее и старайся не давать такие разрешения, хорошо? На самом деле опасных разрешений много, гораздо больше, чем я сказал.

Так Боб сделал свой первый шаг в выборе профессии.

Разрешение SMS

- **Что это:** Разрешение на отправку и прием SMS, MMS и WAP push-сообщений, а также на просмотр сообщений в памяти смартфона.
- **Чем опасно:** Приложение с этими правами сможет читать/писать SMS, включая сообщения из банков с одноразовыми кодами для входа в интернет-банк и подтверждения транзакций.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Разрешения приложений -> SMS*

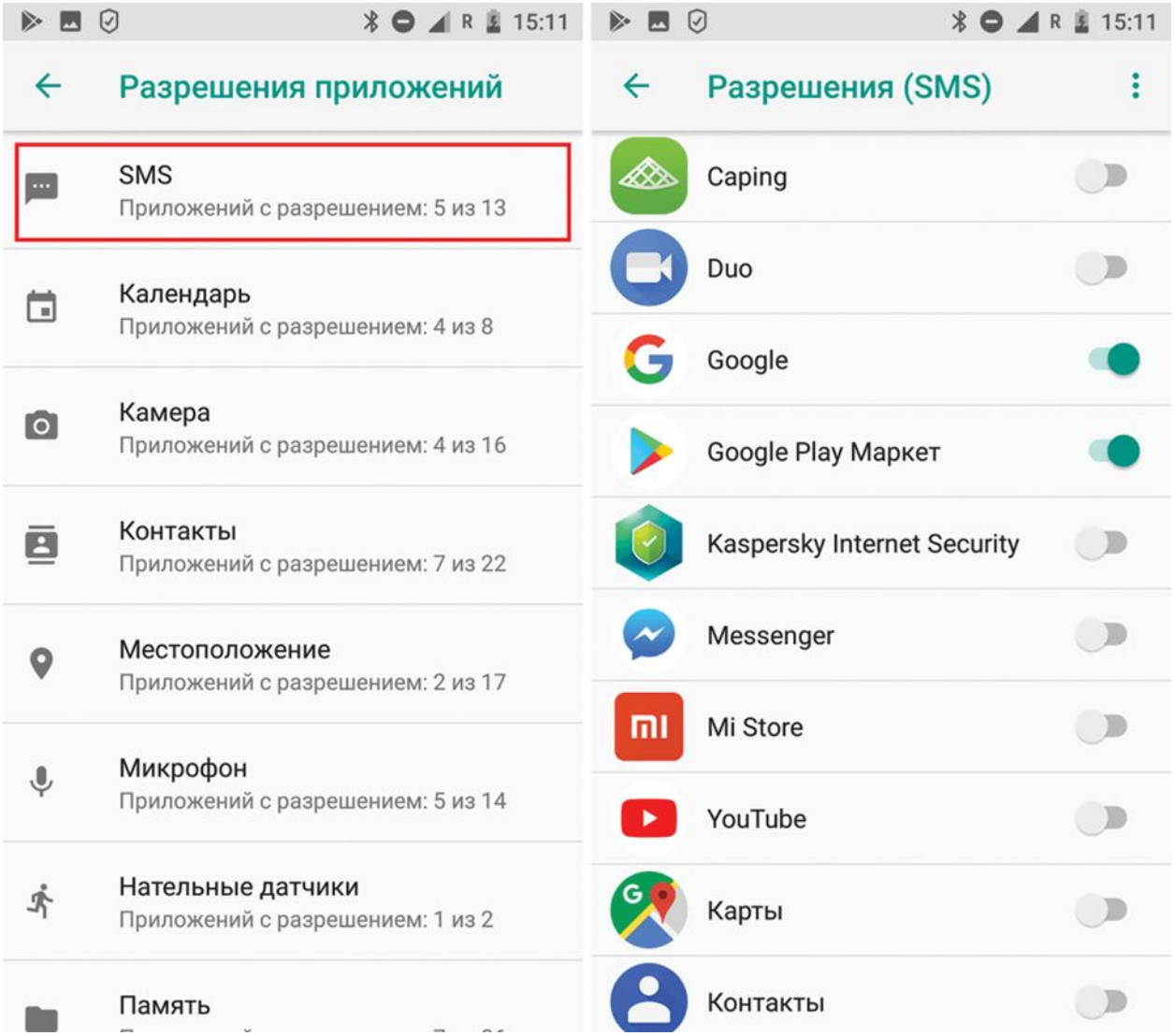

Рисунок 1. Разрешение SMS

Однако ключевой стала совсем другая история.
Произошло это буквально через неделю.

Фальшивый звонок

В тот год в их городок пришла большая беда. Тропические штормы и ураганы в городке бывали регулярно. Но такого ещё не было никогда. Казалось, что летающими крышами никого не удивить, но в этот раз была разрушена практически половина городка.
Поздно вечером в доме матери Боба раздался звонок.
— Мэм, вас беспокоят из городского полицейского участка. Ваш сын, Боб, находится в городском госпитале, и ему срочно нужна операция. Вы могли бы приехать? От вас потребуется найти его страховое свидетельство, а так как лечение не покрывается страховкой, то внести денежный платёж на сумму…
— Да, конечно! Говорите куда.

После разговора мать Боба решила к нему дозвониться.
— Боб? Как здоровье? Ты в госпитале?
— Мама, я через 5 минут буду дома. Какой госпиталь? Тебя просто обманули!
— Погоди, но звонил шериф, Питер Уайт! Мы знакомы с детства, и я знаю его голос.
— Мама, успокойся! Я сейчас при тебе перезвоню шерифу и всё выясню.
— Шериф, вы звонили моей матери 10 минут назад?
— Я? Боб, мне сейчас некогда. Нет, не звонил.
— Интересно, а кто же тогда звонил ей от вашего имени и вашим голосом? Да и номер определился как ваш.
— Самому интересно. Завтра будем разбираться!
На следующее утро мобильный оператор дал неутешительную информацию. Звонили действительно с карты шерифа, а говорили его голосом с помощью специальной программы подделки голоса. Как?
На смартфоне шерифа была обнаружена программа с доступом к разрешениям класса «Телефон». После этого Боб окончательно понял, что количество подобных преступлений будет только расти. А ведь к этому нужно добавить то, что пользователи, да и сами сотрудники правоохранительных органов, имеют весьма слабые представления о подобных преступлениях. А значит, ему просто необходимо поступать на должность кибердетектива. Ведь если не он, то кто?

Разрешение Телефон (Phone)

- **Что это:** Разрешение на чтение и изменение истории звонков; считывание вашего телефонного номера, данных сотовой сети и статуса исходящих звонков; добавление голосовой почты; доступ к IP-телефонии; просмотр номера, на который вы в данный момент звоните, с возможностью завершить звонок или переадресовать его на другой номер; ну и, конечно же, исходящие звонки на любые номера.
- **Чем опасно:** По сути, обладая этим разрешением, приложение может делать всё, что угодно, если это касается голосовой связи.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Разрешения приложений -> Телефон*

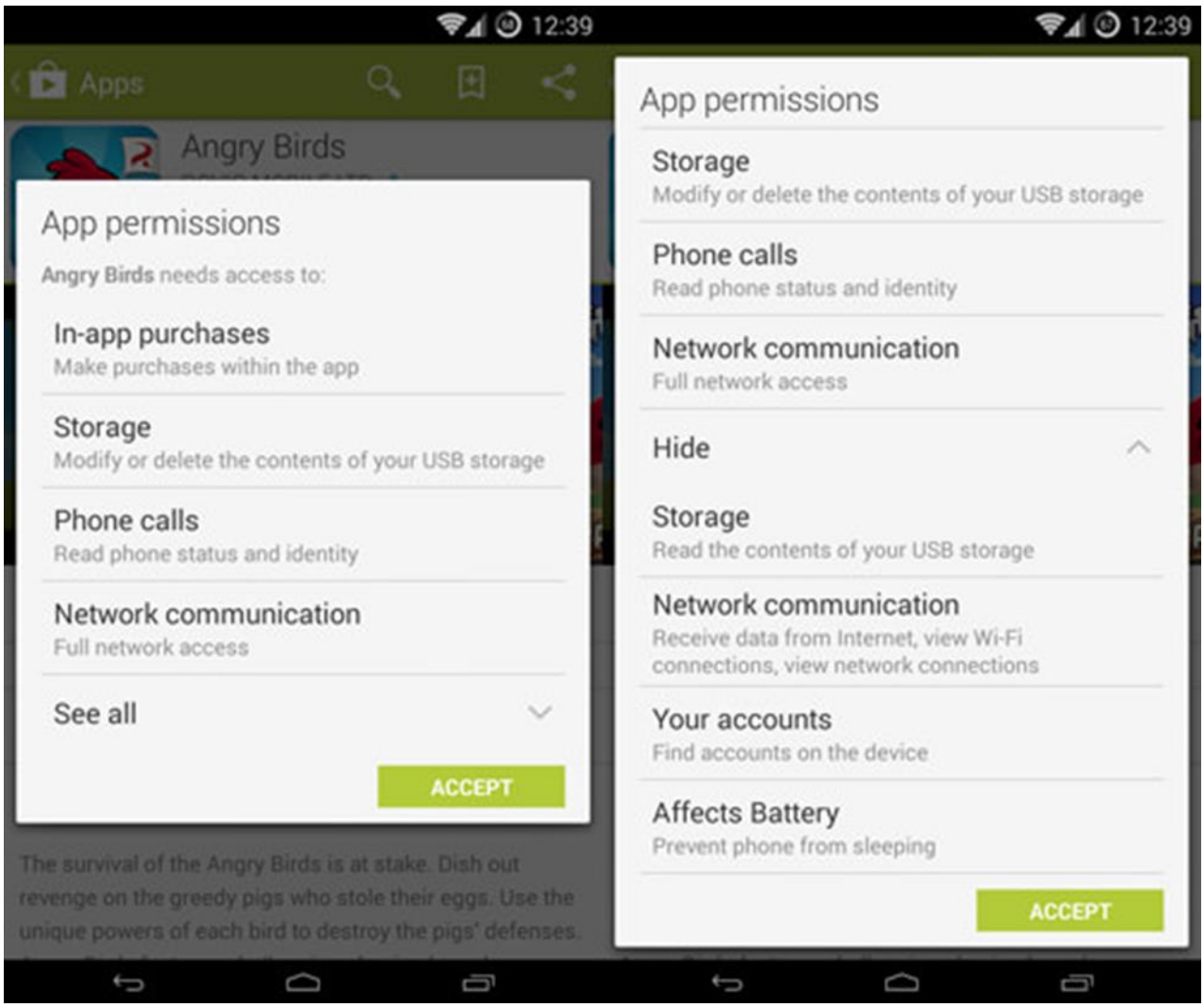

Рисунок 2. Разрешение Телефон (Phone)

Прошло полгода.

Незаконная съёмка

— Боб, у нас странное дело.

— В чём проблема?

— К нам пришла госпожа М. Она пожаловалась, что кто-то разместил в Интернете её снимки, мягко говоря, в почти обнажённом виде.

— Вы разобрались, где сняты эти фотографии?

— Да. Они сняты в доме госпожи М. Но у неё нет скрытых фото- и видеокамер и не видно, чтобы они устанавливались. Более того, судя по всему, фотографии были сняты на её же смартфон.

— Вы уверены?

— Да. Они удалены со смартфона, но мы сумели их восстановить.

— Что дала проверка смартфона?

— На смартфоне была установлена новая игрушка.

— Бесплатная?

— Нет, в том-то и дело. Дешёвая, но не бесплатная. Она требовала доступ к «Камере». Официально, чтобы фотографировать пользователя во время игры. А потом должен был проводиться конкурс на самую забавную фотографию. Призовой фонд около 10 000.

— И пользователи решили устанавливать?

— Ну да.

— Интересно, а когда они поймут, что, однажды получив это разрешение, приложение сможет в любой момент сделать фото или записать видео, не предупреждая их об этом? Такой компромат злоумышленники могут использовать с самыми разными целями.

Камера (Camera)

- **Что это:** Разрешение на доступ к камере, чтобы приложение могло делать фотографии и записывать видео.
- **Чем опасно:** Однажды получив это разрешение, приложение сможет в любой момент сделать фото или записать видео, не предупреждая вас об этом.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Разрешения приложений -> Камера*

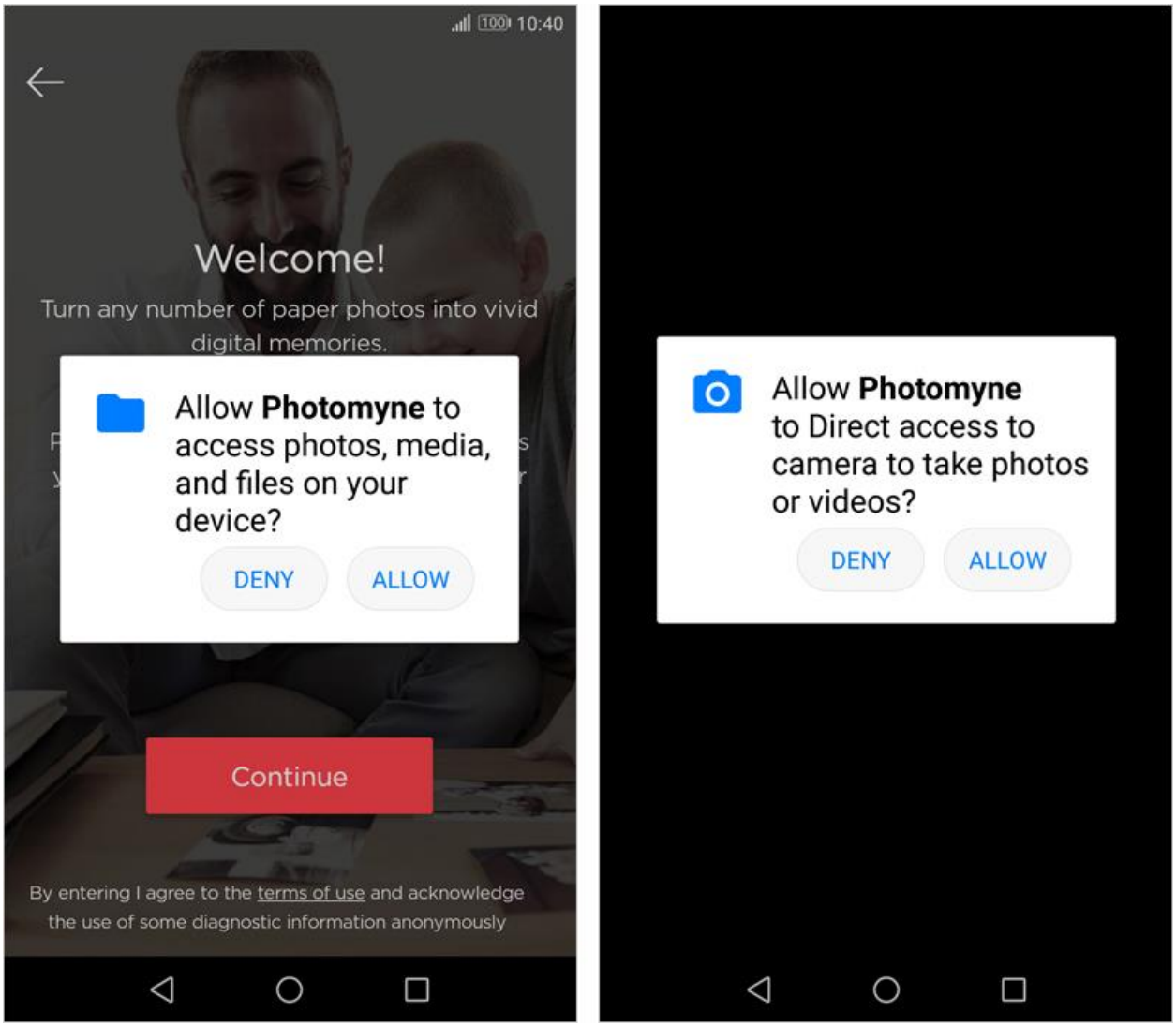

Рисунок 3. Разрешение Камера

Слежка

Утро начиналось, как обычно. Боб успел сварить кофе и даже выпить его на кухне, и тут зазвонил телефон.

— Боб? Ты ещё дома?

— Да. Я успеваю на службу, ещё почти 45 минут, а мне тут пешком минут 15, не более!

— На сборы тебе 3 минуты. Сейчас к тебе приедет патрульная машина. Вопросов не задавай, всё равно ребята ничего не знают. Их задача тебя отвезти. Все расскажут потом на месте.

— Понял, выхожу. А можно хоть намекнуть, шеф?

— Да сам не знаю. Приказ сверху.

— Понял.

Ещё никогда Боба не везли с такой скоростью по городу. Машина летела, как на пожар. Вдруг они выехали за город и свернули куда-то в лес.
— Мы куда?
— Куда приказано!
— Кем приказано?
— Кем надо! Все ответы на вопросы узнаешь сам. Моё дело – дорога. И вообще, уже приехали.
Машина въехала в коттеджный посёлок. Боб заметил, что охрана в посёлке вооружена автоматическим оружием.
— Всё! Приехали. Заходите в дом.
— Добрый день, Боб! Присаживайтесь! Кофе будете? Насколько я знаю, позавтракать вы не успели? Предлагаю совместить приятное с полезным.
— Где я?
— У друзей. Большего вам пока знать ни к чему. Нам нужна ваша помощь. С вашим руководством всё согласовано. Не волнуйтесь! Итак, у нас есть мистер, назовём его А. Нам нужно проследить его маршруты. Но сделать это нужно без его ведома. Увы, установить слежку мы не можем.
— Что вы знаете о нём?
— Любит скачки, американский футбол, покер. Использует смартфон от компании G. Активно играет в спортивный тотализатор с него.
— Вы сможете мне добыть его смартфон на полчаса? Или просто узнать, в каком приложении он играет?
— Приложение я вам скажу. Это Sport от компании X. А зачем нам это?
— Дело в том, что это приложение каждые 5 минут отсылает данные о местоположении клиента на сервер. А сама компания X принадлежит бывшему сотруднику службы безопасности. Вам не составит труда убедить его делиться этими данными, верно? Вот и всё. А вы сможете не только узнать маршруты его передвижения, но и сопоставить эту информацию с маршрутами общественного транспорта.

Местоположение (Location)

- **Что это:** Доступ к вашему местоположению как примерному (на основе данных о базовых станциях мобильной сети и точках доступа Wi-Fi), так и более точному (на основе данных GPS и ГЛОНАСС).
- **Чем опасно:** Позволяет приложению шпионить за всеми вашими перемещениями в пространстве.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Разрешения приложений -> Местоположение*

Рисунок 4. Местоположение

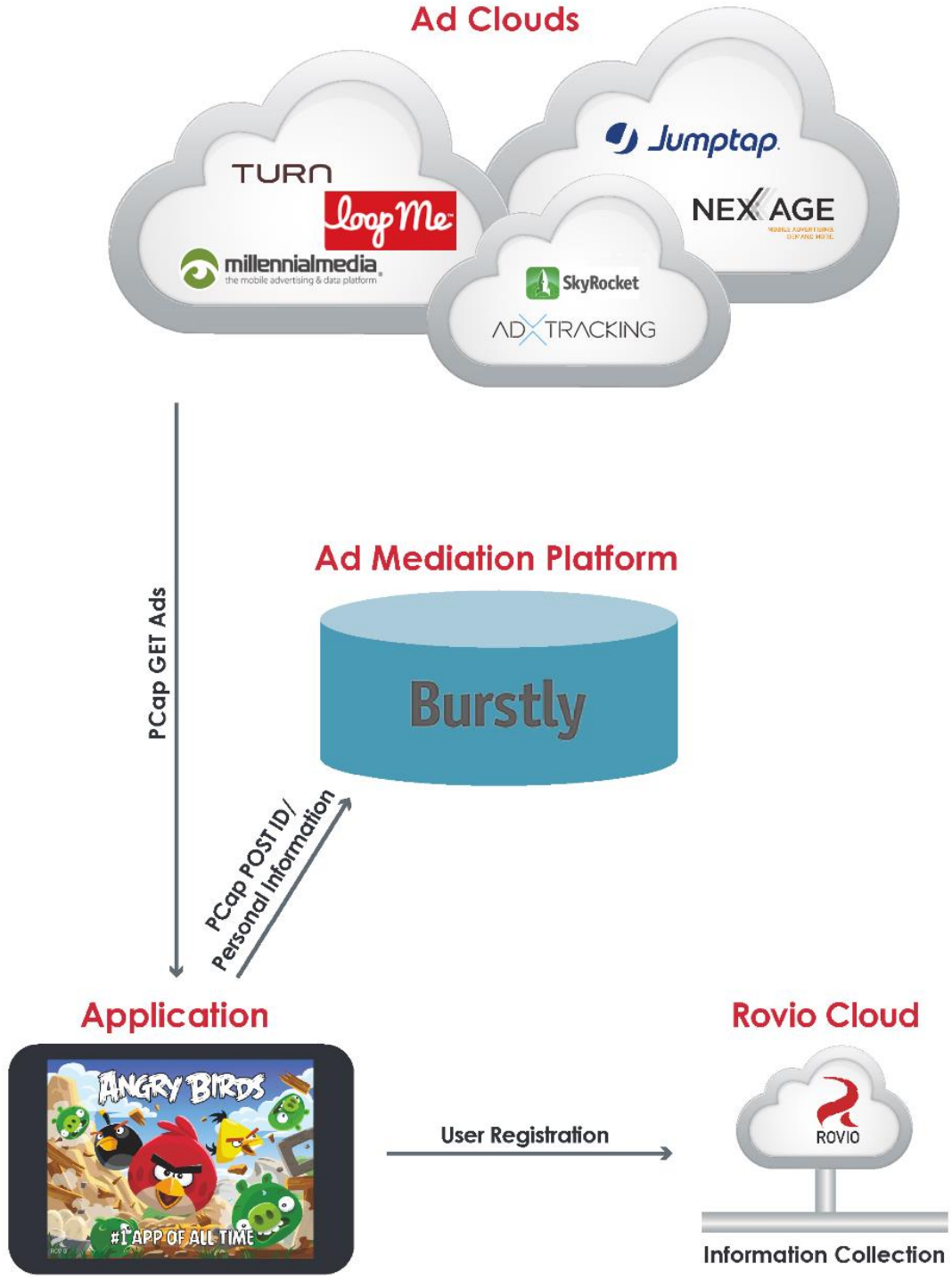

Рисунок 5. Местоположения. Сторонние приложения

Вечер у моря

Славный вечер! Наконец-то можно отдохнуть от службы после сумасшедшего дня и тихонько прилечь на диване перед телевизором с банкой пива. Тем более сегодня играет его любимая университетская команда. Пиво, пицца, телевизор…

В такую жару приехавший из столицы инспектор заставил их сдавать физподготовку. Идиот!!! Неудивительно, что теперь с дивана даже за пивом вставать лень…

Но, увы, счастье было так близко…

Зазвонил телефон.

— Кого чёрт принес? Я отдыхаю!

— Боб, это твой капитан. Извини, есть идея. Приезжай ко мне на побережье. У нас тут чудесное барбекю. Я понимаю, что ты решил расслабиться с банкой пива, а может, и не одной. Но ты мне нужен! Прямо сейчас. Пиво и не только — с меня! Я тебя жду.
Боб со стоном сполз с дивана, умылся и поехал к шефу. Интересно, что же там случилось.
— Шеф, привет! Только не говорите, что вы рады меня видеть после того, как целый день гоняли по жаре, как бешеного кролика.
— И не буду. У меня проблема. Внук взял поиграть мой смартфон. Результат? Мой телефон виснет с идиотской надписью после 10 минут работы.
— Что он пишет?
— Заплатите 10 долларов, и игра будет продолжена…
— Понятно. Зовите вашего оболтуса. Нужно узнать, что он загружал.
— Джонни! Что ты устанавливал на смартфон?
— Игрушку, у нас все в неё играют.
— А что она спрашивала во время установки?
— Вы думаете, я читал? Я быстро отвечал «Да», ведь хотелось поиграть.
— Ну что ж… Сейчас сделаю. Но все ваши сегодняшние добавления в список контактов будут утеряны, как и звонки, и СМС.
— Не страшно. Но что это было?
— Это? Обычный блокировщик экрана. Скорее всего, ваш внук ответил «Да» на предложение «Поверх других окон».
— А что ты будешь делать?
— Сброшу всё, верну заводские установки. Ваш телефон сам делает резервную копию, как только вы подключитесь к Wi-Fi. А сейчас мы его восстановим. И всё. Но не давайте больше телефон ребенку!

Поверх других приложений (Display over other apps)

- **Что это:** Это разрешение позволяет приложению выводить изображение поверх других приложений.
- **Чем опасно:** Вредоносные приложения могут скрывать от пользователя какие-то важные предупреждения, а также подсовывать ему фальшивые формы ввода номера кредитной карты или пароля поверх окон легитимных приложений.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Расширенные настройки -> Специальный доступ -> Доступ к функции «Поверх других приложений »*

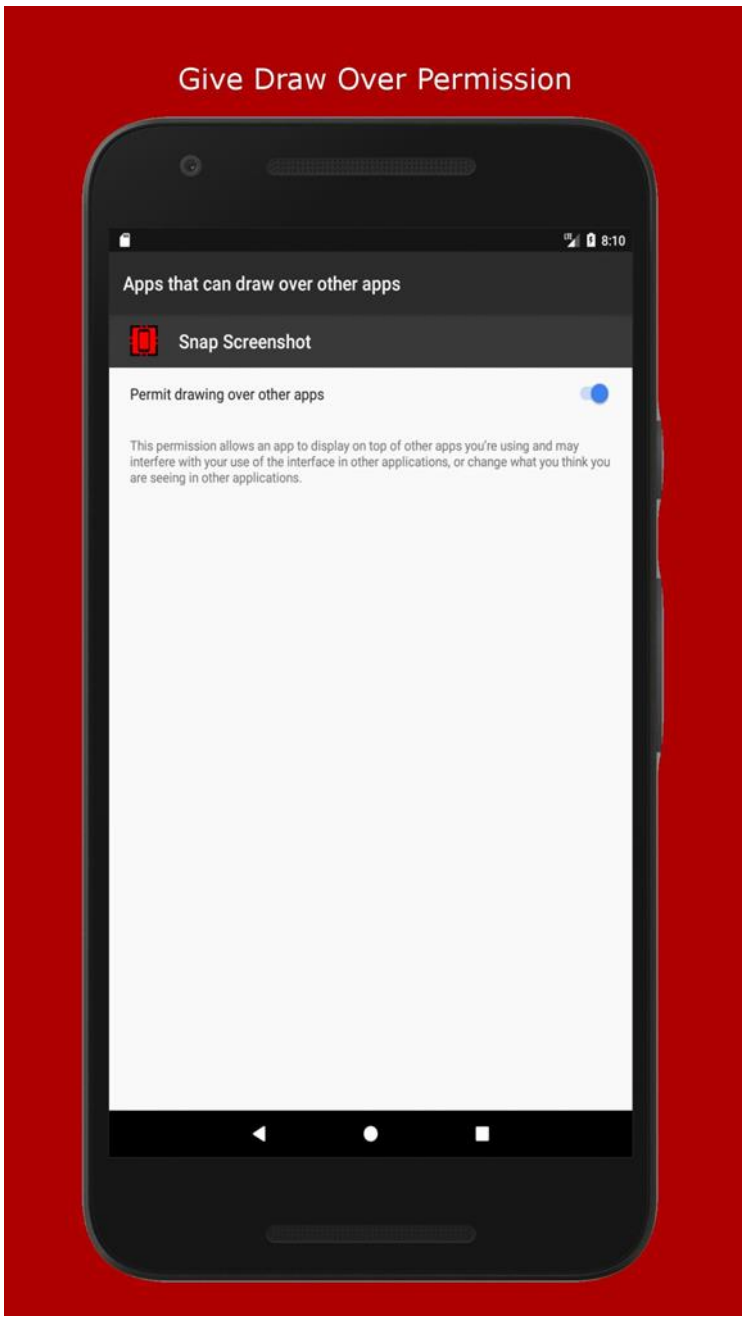

Рисунок 6. Поверх других приложений

Ограбление

«Неужели уже прошло три года, как я начал работать в полиции? — подумал Боб. — Сколько времени прошло, сколько раскрыто дел. Но сколько ещё предстоит… Вот и сегодня шеф задал задачу. У мистера Д. с карты украли деньги. Двухфакторная аутентификация включена. Банк клянётся, что SMS-подтверждение пришло… Что произошло? Кажется, придётся лететь к друзьям за помощью».

— Боб, так что с банком? Выяснил?

— Выяснил, да только проблема стала ещё непонятнее. Шеф, я проверил логи банковского сервера. Всё верно. Пароль введён правильно, SMS-подтверждение банком отправлено и получено. А на телефоне клиента нет ничего. И провайдер клянётся, что SMS не могло быть доставлено, так как доставку отклонил сам клиент. Кто же тогда?

— Ну… Боюсь, я тебе не помогу. Увы. Ты у нас самый умный. Думай.

— Шеф, я посоветуюсь с полицией штата. Я такого ещё не видел.

— Звони, кто тебе мешает…

Прошло полчаса.

— Привет, Мигель!

— Привет, Боб! Что случилось? Ты всегда звонишь только в случае больших неприятностей.

— Увы, так и есть. Не понимаю. У клиента увели деньги с карты. Причём банк отправил SMS и получил подтверждение. Но клиент клянётся, что ничего не получал. Более того, провайдер заявляет, что SMS отклонена смартфоном клиента.

— А ты проверил смартфон клиента?

— Да. Там все по работе и какое-то приложение для покупки билетов.

— Проверь функцию «Не беспокоить», она есть в новейших функциях Android. Ты же помнишь? Она фактически позволяет полностью отключить звук всех входящих сообщений. А если у твоего билетного приложения есть это право?

— Ты прав, этого я ещё не видел. У меня нет такого в смартфоне.

— Не болтай! Проверь!

— О! Ты был прав. Действительно, у него стоит «Не беспокоить» в период с 12 дня до 15. Вернее стоял. По состоянию на позавчера. Сейчас он выключен. А доступ к этому режиму есть только у приложения «Покупка билетов».

— Ну, вот и разгадка. Вредоносное приложение в нужный момент включило режим «Не беспокоить», чтобы владелец телефона пропустил какие-то важные звонки или сообщения. Например, звонок от службы безопасности банка в момент совершения подозрительной транзакции. Или SMS-оповещение.

Доступ к функции «Не беспокоить» (Do Not Disturb access)

- **Что это:** В новейших версиях Android есть функция «Не беспокоить» с массой настроек. Она позволяет полностью отключить звук голосовых звонков и сообщений, скрывать всплывающие уведомления.
- **Чем опасно:** Вредоносное приложение может в нужный момент включить режим «Не беспокоить», чтобы владелец телефона пропустил какие-то важные звонки или сообщения.
- **Где настроить:** *Настройки -> Приложения и уведомления -> Расширенные настройки -> Специальный доступ -> Доступ к функции «Не беспокоить»*

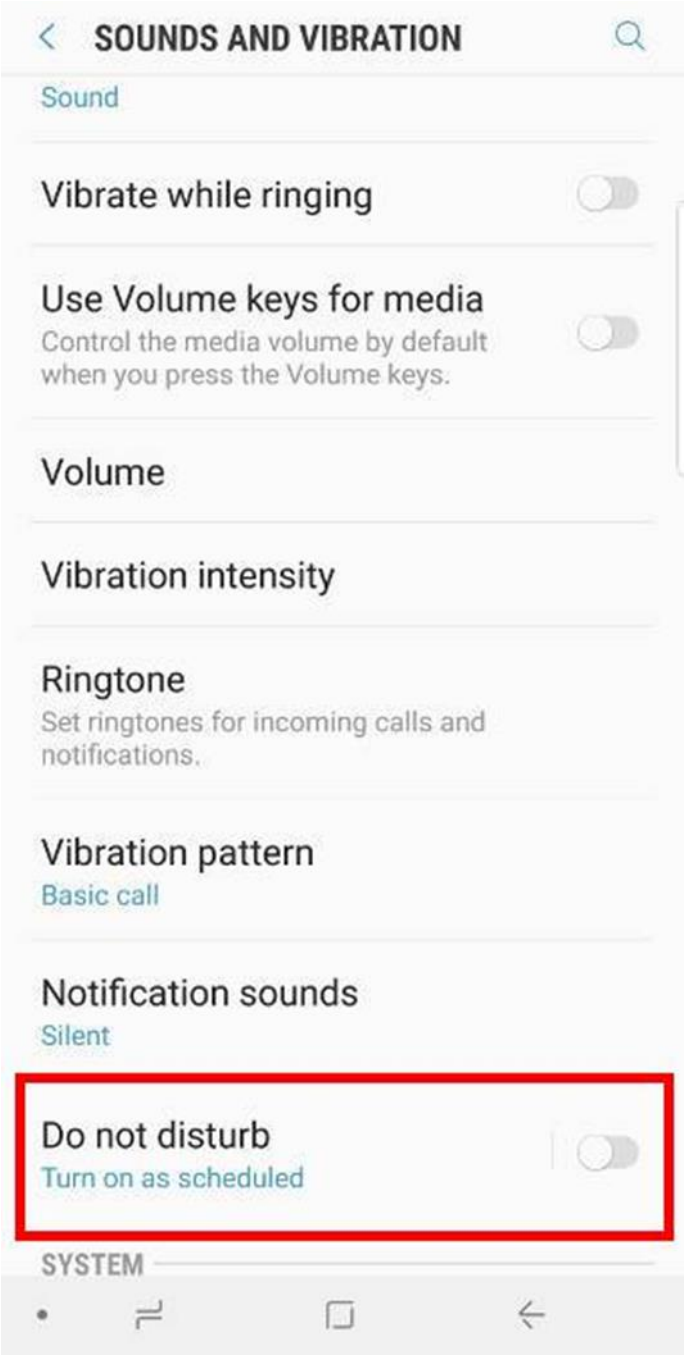

Рисунок 7. Не беспокоить