



Мобильная безопасность

Олег Серов (Access Now)



Мобильное устройство - обработка данных пользователя

- Уровень ОС (Android / iOS / Windows Mobile / ...)
- Системные службы и встроенное ПО (магазин приложений, службы геолокации, службы установки обновлений)
- Сторонние приложения (объем данных зависит от предоставленных разрешений)
- Сервисы мобильного оператора



Какие данные могут собираться

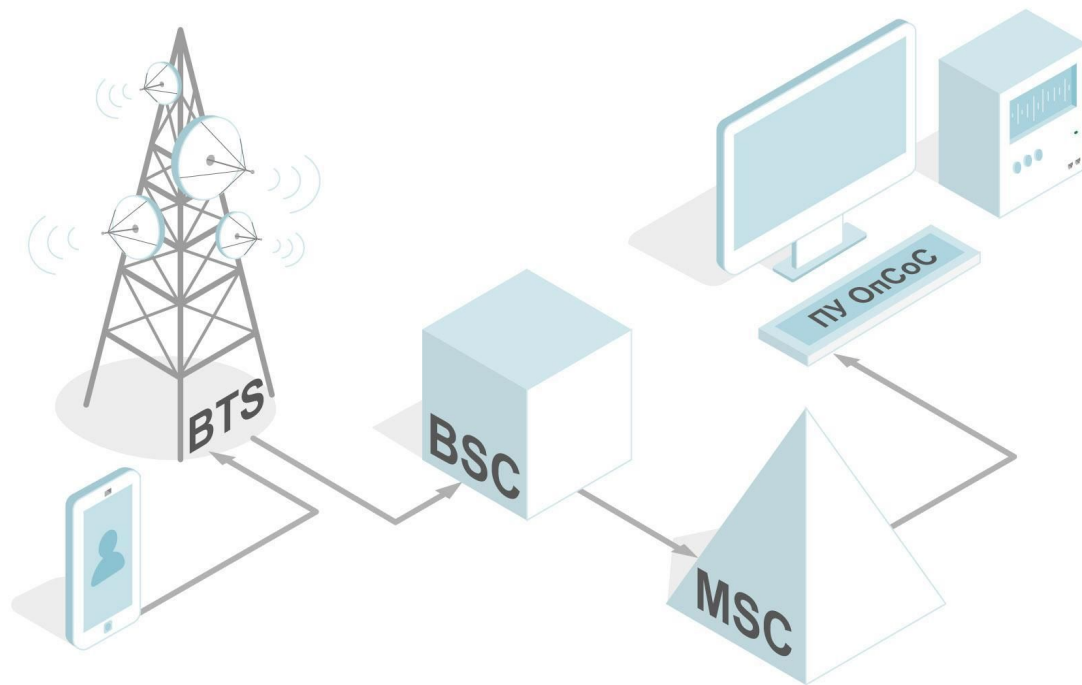
- Персональная информация
- Контакты, круг общения
- Местоположения и маршруты
- Увлечения, предпочтения
- Финансовое благосостояние
- Данные камеры, микрофона



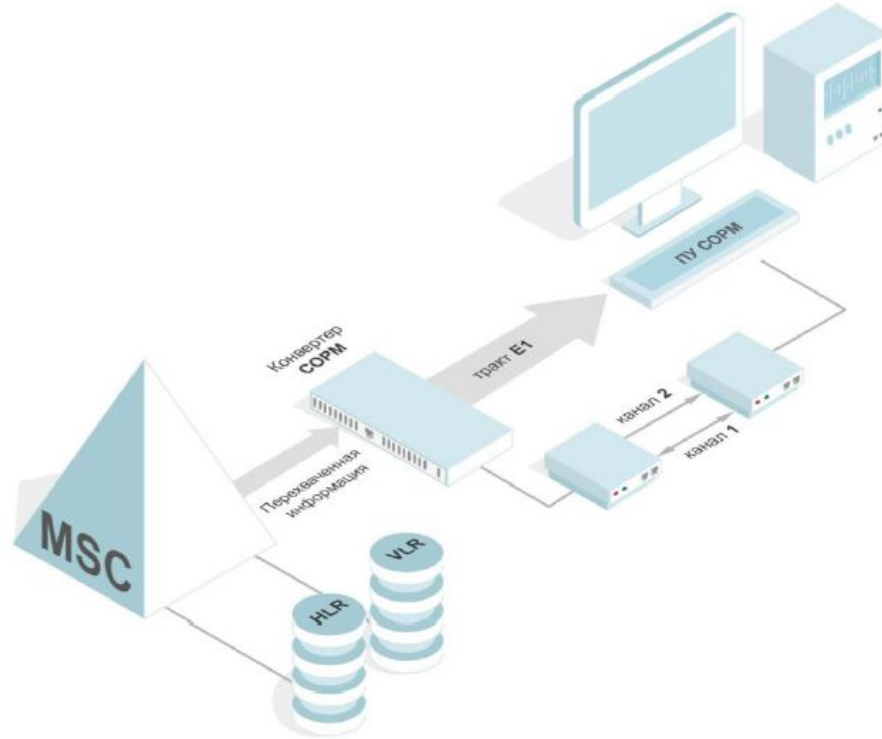
Цели сбора данных

- Статистика по использованию приложений (“фидбек”)
- Таргетирование рекламы по предпочтениям
- SMM-активности
- Предоставление информации по запросу правоохранительных органов

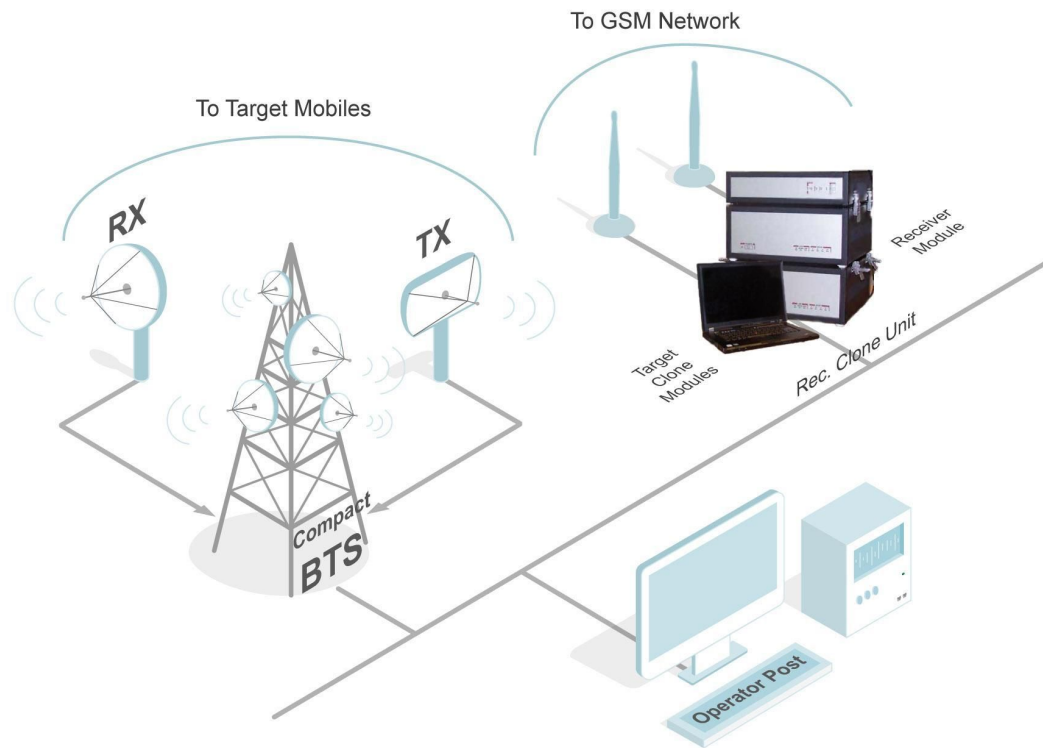
Сбор данных - оператор сотовой связи



Сбор данных - COPM



Перехват трафика в радиоканале





Сценарии атаки на мобильное устройство

- Физический доступ
- Вредоносное приложение на устройстве
- Атакующий в канале связи
- Удаленная атака
- Определение местоположения владельца устройства



Кража / потеря телефона

- Установка блокировки устройства
- Полнодисковое шифрование
- Удаленное управление устройством
- Сброс устройства при попытке подбора пароля



Защита от вредоносных приложений

- Средства ОС (изоляция, права доступа, защита памяти)
- Антивирусное ПО / межсетевой экран
- Мониторинг ресурсов



Защита от злоумышленника в канале связи

- Избегать использования незащищенных соединений
- Использовать VPN
- Отключать средства связи, которые не используются (Bluetooth)
- Использовать средства коммуникации с оконечным шифрованием