СОРМ — Lurkmore

> **Осторожно! Ложь, пиздёж и провокация!**
>
> Существует мнение, что эта статья лжет! Некоторые участники уверены, что факты, изложенные в ней, вовсе и не факты, а нелепые домыслы. См. страницу обсуждения для подробностей.*А на самом-то деле* **Информация неактуальна**

Система оперативно-розыскных мероприятий (аббр. *СОРМ*) — концепция, разработанная нашим замечательным правительством для борьбы с преступностью. Аналог американской CALEA, соответствующей европейской, и хреновой горы международных/блоковых систем, разработанных их замечательными правительствами для борьбы с «циркуляцией в Интернете материалов, запрещённых с точки зрения этики, морали, религии или борьбы с терроризмом».

Заключается в том, что оператор телефонной связи за свой счёт должен протянуть канал к органам, используя который, те могли бы в любой момент анонимно получить список звонков, совершённых и принятых тем или иным абонентом, или попросту подслушивать телефонные разговоры, тайно онанируя на сплетни двух молоденьких блондинок. Да, и хранить снятую инфу от нескольких месяцев до нескольких лет — в разных странах по-разному. Разумеется, всё оборудование на стороне наблюдающих приобретено за деньги оператора (читай абонента) и опять за тридцатикратную цену у правильного поставщика.

Пришествия СОРМ

- СОРМ — Появилась в 1996 году. Просто возможность для прослушки телефонии (в том числе недавно появившихся опсосов). Использовать её силовикам было чрезвычайно неудобно. Нужны были ордера или судебные решения, нужен был физический доступ к оборудованию, нужны были навыки и IT-знания. И вообще — не было практически никакой автоматизации, всё надо делать ручками. Не барское это дело.
- СОРМ-2 — Появилась в 2000 г и внедрялась в общей сложности до второй половины нулевых. Система записи и ретрансляции трафика интернет-провайдеров, созданная россиянскими силовиками для облегчения идентификации пользователей Интернета. Главное новшество второго пришествия — анальный зонд для провайдеров интернетов. Принцип работы следующий: анально принужденные унизительно закупают и унизительно устанавливают, за свой счёт, разумеется, указанные им свыше «чёрные ящики» и также не менее унизительно организуют отдельный канал связи до ближайшего управления ФСБ. Весь трафик отныне должен проходить через их чёрные ящики, когда нужно — в режиме реального времени снимается дамп трафика интересующего гебню абонента. Провайдер не обладает возможностью контролировать и обнаруживать эти обращения. Вопреки расхожему мнению, система записывать трафик абсолютно всех абонентов не могла, ибо мощи у тогдашней техники пока что не хватало. Только взятых на карандаш юзеров, имевших неосторожность спалиться в сети или в случае деанона IRL. В дальнейшем обрастала различными свойственными и не очень функциями — распознавание по сигнатуре голоса, семантические анализаторы, различные варианты для блокировок (DPI/URL), улучшения для работы по бурно развивавшимся тогда соцсетям и блогам.
- СОРМ-3 — официально введена в строй в июле 2014. Главное новшество третьего явления СОРМ — особая система для обеспечения долгосрочного хранения и последующего оперативного доступа ко всему объему прошедшей через систему информации. Официально данные хранятся «до 12 часов», но мы-то все знаем повадки наших органов. Плюс к этому, в наше время цена на носители информации упала до неприличного уровня, а ёмкость носителей — ещё более неприлично выросла. Со всеми вытекающими. Система также более продвинуто собирает метаданные: структурированную информацию о вас в виде номера телефона, звонках, интернет-сессиях т.д. Как в пиндосских фильмах, когда о тебе по твоему ФИО известно сразу всё — даже номера кредиток. Также появилась фича в виде непосредственного анального подключения прямиком к интересующему ресурсу, если владелец ресурса отказался от функции добровольного вертухая (сохранять подробный лог учетной записи в течение полугода).

Теоретическая допустимость и пути обхода

Технически обеспечить поиск слов-маркеров типа «бомба», «взорвать», «теракт» в диалогах — возможно: сейчас это может любая мобила, хотя и кривовато, конечно (называется эта функция «голосовой ввод»)

ещё с 2001-го (тогда был «голосовой набор»), чего уж говорить о компьютерах (и тем более о серверах, где всё это дело может обрабатываться). Небольшая статья, которая проходила как «история дня» на anekdot.ru ещё в 1998-м — четверо студентов решили проверить, правда ли то, что «Большой Брат следит за тобой»: в течение месяца перебрасывались сообщениями вида «калашей нужно 16 ящиков, высылайте на обычную явку», «легенда о студентах в силе, плутоний в понедельник привезёт Ахмед» и т. д., причём шифровали их 128-битным ключом, чтобы уж наверняка, но при том не слишком;

неизвестно чем шифровали, но взломать 128 бит AES "в лоб" невозможно. 64бит всем миром 5 лет ломали (за 10 лет качественно ничего не изменилось)
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Known_attacks

хохма перестала быть таковой на 1 апреля, когда студенты вдруг начали один за другим «исчезать» (причём, как автор отмечает, лучшего дня для нейтрализации не придумаешь: начнёшь что-нибудь заявлять — не поверят, так как сочтут за шутку).

Кровавая фсбня привезла их в лес, где заставила вырыть себе могилы. Расстреливать их не стали («вы пошутили — ну и мы пошутили, с 1-м апреля»), но осадок, как говорится, остался: действительно за всеми следят, и в этом конкретном случае — довольно эффективно (взламывать систематически 128 бит для всех шифрованных писем всей 100-миллионной аудитории mail.ru требует неслабых мощностей).

В Штатах в 2013-м году запись переговоров с лежащего на столе телефона, выполненная без ведома владельца телефона, была признана в суде доказательством, имеющим юридическую силу (был создан первый прецедент), до этого случая данные, полученные «прослушкой», не считались доказательствами либо не использовались как таковые, однако ниггеры и маргиналы стали использовать сленг при обозначении запретного (наркотиков в основном) в разговорах (не только телефонных) задолго до этого: вспомните «Лицо со шрамом» (с Аль Пачино который) — «I got the money… And I got the yayo» — здесь главный герой вместо очевидного для прослушивающих маркера «наркотик» использует неочевидное расплывчатое «yayo», которое и словом-то не является (произносится как зевок — на суде можно сказать — мол, зевнул, бывает).

Сейчас даже в фильмах широко используются заменители маркеров типа «stuff» (российский аналог — «товар», «порошок»), «snow» (рус. «снежок»), «shit» (рус. «говно», «дурь») и другие, при этом возможные вариации для слова «наркотик» практичные пиндосские наркодилеры всё время меняют, чтобы создать спецслужбам лишний геморрой при выявлении маркеров. Для одной только марихуаны — самого распространённого наркотика — придумали десятки слов-заменителей, способных свести с ума любой прослушивающий компьютер с его мудрёными программами (mary, maryjane, maria, weed, hemp, tea, ganja, и т. д., российские торчки не отстают — «ракета», «базука», «чай» и др.). Таким образом, для защиты от излишне любопытных органов до сих пор работает старая школа, придуманная ещё во времена Шерлока Холмса и Штирлица — «Слоны идут на север».

Реализация

Ввиду того, что самым сложным и высокотехнологичным оборудованием, используемым в «органах», являются счёты и аппараты «Феликс», а также учитывая полный раздолбизм и пострунизм (одновременно, ага) телефонных операторов, система в большинстве случаев реализуется только на бумаге, с необходимым числом подписей и откатов. Происходит это потому, что более 3/4 замкадных сетей связи были построены во времена советского союза. Поэтому оборудование на них даже не цифровое. Более того, цифровые АТС (в основном) были сделаны для того, чтобы люди звонили и дозванивались. Примерно у половины этих цифровых АТС не хватает мощности даже для того, чтобы фиксировать информацию обо всех звонках, которые прошли через неё. Фантазировать на тему того, что с АТС есть мега-провод, по которому можно слушать весь телефонный трафик АТС, можно, но физически это реализовать нельзя (невыгодно, проще взорвать АТС). Самих АТСочек по центральному округу более 10 тыс. Даже имей к каждой по проводу, у спецслужб ухов не хватит слушать. Взять, например, АТС на 10 тыс. абонентов, каждый из которых за сутки позвонил и поговорил по часу. Если слушать одну АТС, на прослушку материала за одни сутки надо 416 человек, которые будут по 24 часа в сутки слушать или 1250 человека, которые за 8-часовую норму всё прослушают.

Но… Если кто-то вдруг решит записать эти данные, достаточно воспользоваться одним из алгоритмов сжатия речи, MELP, например. В этом случае 1 секунда займет 280 байт, и один день АТС уместится в 10 Гбайт, если каждый позвонит по часу. Дней 30 в месяц — значит, на месяц надо 300 Гб. Один жёсткий диск за 100$ (2008 г.). Запись месяца разговоров каждого из анонимусов — один цент.

Считается, что даже в мохнатом 98-м году у ФСБ гарантированно была аппаратура, которая позволяла в полностью автоматическом режиме по ключевым фразам отслеживать до 1 млн телефонных соединений одновременно. А это было 15 лет назад. Но это всего лишь слух и городская легенда, так как:

1. во-первых, необходимо достаточно точно вычленять определённые слова при условии, что абоненты могут говорить невнятно или с акцентом.

2. во-вторых, для того, чтобы проанализировать все совершающиеся разговоры, необходима огромная вычислительная мощность, которую и сейчас-то не многие способны предоставить, и уж тем более ни одна АТС не способна физически передать весь свой трафик по параллельному каналу в «органы» для анализов
3. в-третьих, никто в здравом уме в XXI веке никогда не соберёт список слов, которые, если встречаются в разговоре, достоверно указывают на общение террористов. Такие слова, как «бомба», «теракт», «сиськи», «писькы» и другие — чаще встретятся в обычном разговоре двух кухарок, обсуждающих последние новости и перемывающих косточки соседям. А прослушивать сплетни про нижнее бельё у наших «органов» не хватит ни терпения, ни человеков.
4. в-четвёртых, какой смысл записывать только часть разговора, которая следует после произнесения слова из списка?

А тем временем в октябре 2013 всплыла информация о грядущем апгрейде СОРМ-3: Проект приказа о правилах Минкомсвязи. Если коротко:

- возможность выбирать и хранить:
  - стр.4 4.4.а IPv4/IPv6 адрес (и удалённый и локальный)
  - стр.5 4.4.г используемые клиентом почтовые адреса, если используется нешифрованный канал
  - стр.5 4.4.д в том числе из веб интерфейсов ряда сервисов (стр.79), при том же условии
  - стр.5 4.4.з логины адресатов VoIP? (из заголовка SIP-пакетов. Логины и номер вызываемого пира не шифруются)
  - стр.5 4.10 и вообще *весь* трафик за последние 12 часов
- стр.55 3.1 ну и, конечно, возможность передавать товарищу майору как записанные IP пакеты целиком, так и запись данных с прикладного уровня.
- стр.79 список «зашкваренных» сервисов: радует что из IM пока только аська. Но это пока.

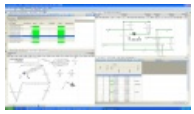
Применение

Аббревиатура «СОРМ» используется для вызова состояния благоговейного ступора у страдающих ФГМ, а также для запугивания молодых дрочеров, дабы они не качали порнухи из интернета на кровные родительские денежки. Алкснису она тоже по нраву, еще как!

Также не стоит забывать, что б**о**льшая часть этой статьи написана анонимусами.

Галерея







Из слитой базы воронежского Билайна

Ссылки

- Реакция сообщества на попытки слежки
- Приказ и Соглашение о внедрении технических средств СОРМ
- Приказ для СОРМления опсосов.
- Городская легенда, говорите? Вот ее реализация И еще одна
- Почитать для упоротых. Первая в списке книга ищется по гуглю + скачать бесплатно
- Стоимость системы Тотального Прослушивания Всего и Всех
- Адекватная статья — как оно есть на самом деле

- А это в Сахалинском УФСБ поставили FlylinkDC
- Наиболее полное описание СОРМ 1, 2, 3
- Та самая история про студентов

См. также

- Идентификация пользователей в интернете
- Городские легенды
- Закладки
- ФСБ
- Tor

Эта страна

228 282 статья 9 мая Adidas Encyclopedia Dramatica/Russia M4 Роман Абрамович Адыгея Астрахань Байкал Баня Бессмысленный и беспощадный Биробиджан Бирюлёво Бичпакет Бутик Ватник Владивосток Воркута Воткаят Вписка Генерал Мороз Георгиевская ленточка Главная проблема музыки в России ГЛОНАСС Горбушка Горжусь Россией! Горячие финские парни Госдума Грудинин Двойники Путина Десятые Диггеры Дороги России Древнерусские мемы Духовность Европейцы ли русские? Евроремонт ЕГЭ Единая Россия Екатеринбург Жлоб За Абрамовича Завод Заводы стоят Закопанные дома Замкадье Зеленоград Золотая медаль Зюганов ИТМО Кавказские Минеральные Воды Калининград Киров Ковёр Коктейль Лужкова Колыма Комбинат «Маяк» Компьютерный клуб Коробка из-под ксерокса Красная ртуть Краснодар Красноярск Кронштадт Крым Куда ты денешься с подводной лодки? Курильские острова Левиафан Люби Россию, пидор! Магадан МГИМО Медведев Милиция Мордовия Москва Москвичи зажрались Мухосранск Мытищи Нанотехнологии Национальная идея Наше всё Нижний Новгород НМУ Новосибирск Норильск Ночные Волки Нургалиев разрешил Общежитие Общепит Омск Операция «Неформал» Оскорбление чувств верующих Особенности национальной охоты Откат Охрана Пельмени Перепись населения Пермь Петербург Пипл хавает

Менты

228 282 статья A.C.A.B. Chris-chan Dexter Kunteynir Noize MC Robocop Ёбаный насос АК-47 Академовские маньяки Александр Пичушкин Алексей Дымовский Алкоголик Алкснис Берия Бомж Брачный аферизм Леонид Василевский Василий Федорович Владимир Бельский Владислав Галкин Гастарбайтер Генерал Ветров ГИБДД Гоблин Гопник Госнаркокартель Граждане СССР Демократизатор Детектив Джек-потрошитель Джордж Флойд Диггеры Дима Зубов Днепропетровские маньяки Евсюков Ежов Зацепинг Зая, я убила мента Зодиак Изнасилование Илья Фарафонов Интересная личность Кардинг Кевин Митник Кокаинум Коломбо Колыма Компьютерные пираты Константин Крестов Кровавая гэбня Ломай меня полностью Маньяк Марш несогласных Мафия Милиция Милиция/Юниты Мир криминала Моссад Наркоман Наталья Поклонская Неверные менты Нотариально заверенный скриншот Нургалиев разрешил Операция «Неформал» Охрана Парам-пам-пам Пативэн Пацан к успеху шёл Пашка Пира Пистолет Макарова Прокуратура Противогаз Психонавт Путин Радиопираты Рамзан Кадыров Распечатать лицензию на Линукс Растаманы Ричард Рамирес Руфинг Рыжий Тарзан Сектор Газа Скинхед СОРМ СР Борис Стомахин Терморектальный криптоанализатор Топор НКВД Тюрьма УАЗ Улицы разбитых фонарей Участковый с маленьким окладом Участники форума mvd-ua.com насилуют мальчиков! ФБР Флорентийский монстр ФСБ Футбольный хулиган

Just Another Fucking Acronym

14/88 1C 265 A.C.A.B. ADSL AFAIK AFK AISB AJAX Aka All your base are belong to us AMV ASAP ASL ASMR ASUS EEE BAT BBS BDSM BOFH BRB BSOD BTW CMS Command & Conquer Copyright Counter-Strike CYA DC DDoS Delicious flat chest Direct Connect DIY DJ Doki Doki Literature Club! DOS DRM EFG Etc Five Nights at Freddy's Frequently asked questions FTL FTN FTW FUBAR GIF GIMP GNAA GPON Grammar nazi Grand Theft Auto GTFO Happy Tree Friends HBO How It Should Have Ended I see what you did there I2P IANAL IDDQD IIRC IMHO In before Internet Explorer IRC IRL ITT JB (ЛОР) JFGI Kerbal Space Program KFC KISS Let's get ready to rumble! LFS Livejournal.com LMAO LMD LOL Low Orbit Ion Cannon M4 MacOS Microsoft MILF MMORPG MSX MTV N.B. NASCAR NEDM NES NoNaMe Not Your Personal Army NRB NSFW O RLY? OK OMG OS/2 P. S. P2P Panty and Stocking with Garterbelt

w:COPM