«СОУД и СОРМ»: всё началось с телефонных проводов

На протяжении более 150 лет физики, радиотехники, конструкторы и дизайнеры неустанно трудились над совершенствованием телефонной связи. Первый прототип телефона был создан в 1860г.

Первый телефон Александра Белла

Серьёзные технические устройства — серьёзные цели: истинные, подлинные, первостепенные. Так было всегда и так будет — стационарный телефон, мобильная связь, Интернет — неважно.

Советская Система Объединённого Учёта Данных о стратегическом противнике «СОУД» была спроектирована накануне Международных олимпийских игр в Москве (1980г.) с целью оперативного сбора данных для контрразведывательных мероприятий. На тот момент КГБ владел информацией о том, что западные спецслужбы в процессе соревнований намереваются провести враждебные акции. Руководство СССР предоставляло «СОУД» в пользование спецслужбам из дружественных государств «Варшавского договора». Но естественно, лишь частично, скрывая истинный потенциал разведывательной системы и от них.

Конечно, «СОУД» не появился из ниоткуда и имеет под собой прочный фундамент, если так можно выразиться — исторически сложившуюся традицию «прослушки» отечественных пенатов. Начало было положено ещё в 1913г., когда телефонные переговоры народных избранников IV Госдумы Санкт-Петербурга прослушивались специальным оборудованием. Чуть позже радиотехники стали «снабжать» подслушивающим модулем каждую АТС.

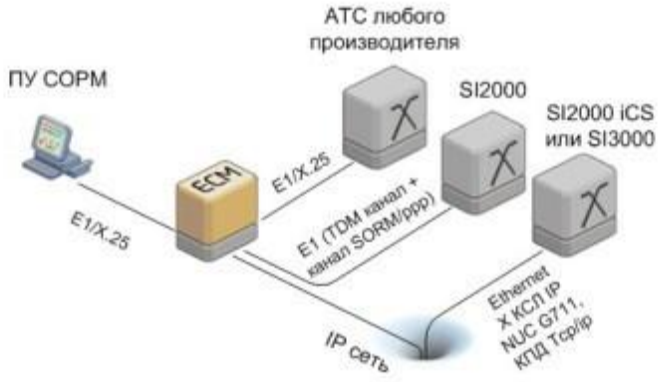
Когда-то аппараты с автоматическим определителем номера (АОН) гордо носили статус ноу-хау и стоили, кстати, весьма недешёво. А сегодня потребителей связной коммуникации удивляет другое — отсутствие этой функции в них. Но интересен в этой истории иной факт — кем и для чего была разработана система распознавания входящих звонков.

Думаете телефон, оснащённый АОН, был создан для повышения комфорта связи? Определитель номера являлся одной из засекреченных функций АТС. Это потом «левши», так сказать умельцы из народа, раскусили её техническую суть и начали активно внедрять в конструкции стационарных моделей. Хотя не исключено и то, что «закрытая» система АОН, в начале 90-х, когда Советский

Союз начал разваливаться, благополучно была продана в частные руки. Законно или нет — опять-таки, остаётся догадываться.

Современнная АТС с АОН

Но АОН была лишь пробной репетицией тотального контроля. В 1994г. государственные спецслужбы начинают внедрять систему внутреннего мониторинга СОРМ (система оперативно-розыскных мероприятий). Её функции активируются с ПУ (пульта управления), установленного в ФСБ, МВД или ФСК ЕЭС. Она имеет больший приоритет, чем станции АТС. И обладает практически безграничными возможностями отслеживания абонентов.



Система СОРМ

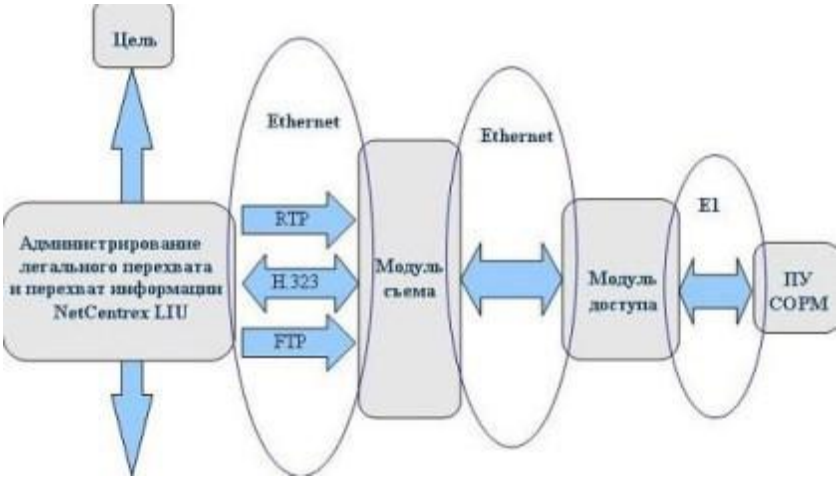
- В арсенал СОРМ входят: контроль входящих/исходящих вызовов любого значения (от местных до междугородных);
- контроль вызовов абонентов, пользующихся дополнительными видами обслуживания, — переадресацией, сокращёнными номерами и др;
- разъединение и блокировка входящих/исходящих звонков абонента с ПУ;
- конспиративное подключение с ПУ к абонентским линиям связи, в том числе и с установленным соединением;
- запись телефонных разговоров на любых линиях.

СОРМ «открывает» работникам госбезопасности полный обзор данных:

- порядковый номер абонента, находящегося под контролем;
- статус/уровень контроля;
- номер линии при полном прослушивании;
- отметка о полуавтоматическом режиме входящей связи;
- номер вызываемого абонента (каждая цифра в порядке набора);
- определение номера вызываемого абонента до его ответа в пределах внутристанционной связи;
- определение номера вызываемого абонента после ответа при установлении входящей связи с других станций;
- установление номера входящего пучка связного канала (когда невозможно определить номер вызываемого абонента);
- время начала/окончания и длительность прослушиваемого разговора.

Во второй половине 90-х были созданы модифицированные версии СОРМ:

- СОРМ-1(1996 г.) — для прослушивания переговоров по телефону;
- СОРМ-2 (2000 г.) — для протоколирования телефонных соединений и действий пользователя в интернете.



Система СОРМ для Интернета

СОРМ М-200

Документ министерства информационных технологий и связи, описывающий свод правил и полномочий СОРМ, называется «Приказ №6» (от 16 января 2008 г.)

Американцы, спустя 5 лет после выхода СОРМ, создали его «урезанный» вариант. Он получил двоякое название: «Carnivore» (плотоядное животное) и Digital Collection System (по версии ФБР). Его применяют для отслеживания электронной почты подозреваемых граждан.

Эволюция разведывательных технологий: американская система «Эшелон»

За порогом миллениума, безусловно, стационарный телефон утратил свою былую актуальность. На гребне волны НТР засияли светочем науки новые достижения — сотовая связь, GPS. И снова, казалось бы, мирные пользовательские блага окрасились в тона милитаризма и информационной войны: разведывательные службы никогда не были равнодушны к космическим средствам слежки, а в XXI веке и подавно.

Американские блюстители порядка и политического спокойствия видимо уловили «ветер инновационных перемен» раньше остальных и создали глобальную шпионскую сеть Echelon («Эшелон»). Выдающееся изобретение и в то же время страшное: система «Эшелон» сканирует множество диапазонов частот, включая протоколы мобильной и релейной связи. Перехватывает информацию и фильтрует её посредством специального программного обеспечения по заданным ключевым словам. Другими словами говоря, это некое планетарное ухо со встроенным собственным поисковиком — впечатляющий тандем системы космических спутников и мощнейших вычислительных ресурсов.

Первые лица США без иронии и лукавства заявляют, что миссия Echelon исключительна — беспощадная борьба с коварным злом: с террористами и наркодельцами международного значения. Возможно, это правда — но не вся. Только ли это может разведывательная сеть? Такого класса, уровня, с такими возможностями. Навряд ли. Echelon может разузнать (мягко говоря!) обстановку в любом регионе Земли — и в джунглях, и в горах, и в океане. А, как известно, кто владеет информацией, тот владеет миром. Буквально так! Если известно чем «дышит» и «живёт» то или иное государство, если понятно (слышно!) какие прения ведутся среди её вождей и руководителей, почему бы не изменить ход избирательной компании в ней (например на должность президента)? Вполне!

Система Эшелон

Космическая разведка особенно незаметна и особенно опасна. Там, в невесомости, не всё так спокойно и мирно, как может показаться в пределах невооружённого глаза или в телескоп астронома-любителя. На планетарной орбите происходит негласный передел «вакуумного пространства» — Америка, Россия, Китай, Евросоюз.

США лидирует и не скрывая своих «аппетитов» стремится стать единоличным хозяином околопланетного космоса. Ибо тут на расстоянии от 100 до 300 км до Земли можно разместить шпионские спутники, ракеты, лазерное оружие и ещё не бог весть какие технологии. Угрожающие,

доказывающие стратегическое преимущество, осуществляющие глобальную слежку за людьми, объектами, странами, материками. Или что ещё хуже — управляющие психическим и физиологическим состоянием людей.

Потусторонние «прелести» мобильной болтовни

Размах мобильной связи достиг апогея в 2007г. Хотя и нынче статистика её, так сказать, потребления, рдеет нездоровыми пиками и зашкаливаниями. При всех удобствах факты и цифры определённо заставляют тревожиться: всё в том же, 2007 году, молодые люди в возрастной категории 5-24 лет потратили на мобильные переговоры более 150 млрд. долл; в среднем, подросток тратит времени на телефонные переговоры по сотовому в 8 раз больше, чем на прослушивание полюбившихся музыкальных хитов.

А ведь средине 90-х эти характеристики были практически равны нулю. К чему это всё? К масштабности! Мобильная связь как вирус окутала планету. Но как же? Она приносит пользу, она состоит на службе у людей. Безусловно, да. Но есть в ней и другая сторона… тёмная, вне интересов «простых смертных».

Прослушка мобильных телефонов

Вернёмся к системе «Эшелон». Мобильная связь для его хозяев — кладезь информации. Есть доказательства того, что она в обязательном порядке отслеживает переговоры по мобильным телефонам на территории США, Европы, Азии и Африки. Суперкомпьютеры «Эшелона» упорно трудятся не только в интересах безопасности Америки и партнёров НАТО, но и в целях повышения конкурентоспособности компаний этих стран.

Подробней о возможностях системы «Echelon»

Первый прототип системы «Эшелон» был создан в эпоху «холодной войны», в 1945г. Тогдашний президент Америки Гарри Трумэн отлично понимал, как важно знать, видеть и слышать, что делает их главный политический и экономический оппонент — Советский Союз. В контексте стратегической задачи, он дал указание спецслужбам создать систему перехвата радиосигналов, «проникающих» с территории СССР. Спустя 3 года после создания системы, в 1948г., США подписывает с Великобританией договор под названием «UKUSA» о единых правах пользования системой. Поскольку проект был совместным, в нём принимали участие учёные из нескольких странах. Другие страны, доля чьих усилий в создании системы «Эшелон» была меньшей, получили статус ограниченного пользования.

База Эшелона

После падения «железного занавеса» разведывательная система не прекратила работу, а лишь была перефокусирована на другие задачи — не менее глобальные в плане информационной безопасности: отслеживание банковских переводов; сбор политических компроматов; выявление крупных теневых сделок (заключения контрактов, «отмывания» финансовых средств); пополнение/обновление баз данных служб безопасности (объекты, люди, промышленные комплексы) и т.д.

Глобальная система радиоэлектронной разведки «Эшелон» процеживает крупицы искомых данных в бурном инфопотоке, как кит отлавливает в океане планктон. Её спутники-ищейки для осуществления радиоперехвата используют замаскированные, так называемые «отводы» от коммутационных связных линий. Для достижения цели получения данных — прослушивания — задействуются все средства (радиоразведывательные базы, коммерческие спутники, радиосети в т.ч. и стратегического значения). Стоит ли говорить о скрытности такой процедуры?

Телефонные переговоры, телеграфные сообщения, пакеты данных, отправленные по факсу, веб-траффик (электронная почта) и прочие телекоммуникационные каналы находятся в поле зрения/слышания системы «Эшелон». А точнее её владельцев. Но и это ещё не всё! Смерч «глобального информационного любопытства» только набирает силу. Американским производителям, выпускающим телекоммуникационное оборудование, в вежливой форме свыше дают указание: так, мол, и так, в программное обеспечение вашей системы/станции/гаджета нужно добавить наш код; всего несколько килобайт, для обеспечения госбезопасности. Многие независимые технические эксперты склонны думать, что именно, благодаря таким «указаниям» и «модификациям», спецслужбы США добывают до 85% разведданных.

«Эшелон» — шпионский конвейер, информационный пылесос с высшим балом IQ. И это ни дифирамбы, ни хвала. Совсем нет. Скорее выражение чувства ужаса: децентрализованная сеть супермощных компьютеров системы способна принимать и анализировать в течение 24 часов более 1 млрд. «добытых» сообщений. Много это или мало? Предостаточно, чтобы быть в курсе всех событий планеты Земля. Причём не абстрактно, а в подробностях — секретных, пикантных — каких угодно.

Информационные трофеи «Эшелона» бережно раскладываются по полочкам громаднейшей базы данных. По своим функциям и возможностям она ничем не уступает интернету, только разве что имеет меньшие размеры. Её обслуживает огромный штат программистов (и наверняка весьма талантливых). Эти же «товарищи» по директивам разведки предоставляют из БД все необходимые данные по интересующему объекту — номера телефонов, адреса, фамилии и пр. Если вы вызвали подозрение у агентов госбезопасности, они посредством «Эшелона» запросто могут вас поставить «на карандаш». Как минимум, существует три причины присвоения этого статуса:

Номер «в разработке» — получен агентурой при задержании подозреваемого, изъятии документов, от «информаторов».Номер, привлёкший внимание «Эшелона», по определённым ключевым словам, внушающим опасение/угрозу государству, компании или какому-либо человеку. Номер, представляющий потенциальный стратегический интерес (например, локализован в зоне базы террористов).

Не остаётся без внимания и веб-пространство. Центры обработки данных (ЦОД), транзитные каналы Европы и США активно «прорабатываются» шпионской машиной со времён начала глобализации Интернета, начала 90-х. И главное — официально, исключительно на законном основании: согласно положению протокола IUR и документа «Международные требования по перехвату». Результаты и методы сканирования трафика публикуются в документе Enfopol. Его новая версия выходит примерно раз в полтора года.

Конфиденциальность «MasterCard», «Visa», «Diners Club» и других популярных платёжных систем, по аналогии со средствами телекоммуникации, тоже носит весьма символичный характер. Пусть и на уровне государственных структур, но всё же. Транзакции и переводы проверяются на предмет необоснованных перемещений в пределах государства, платежи — касательно «странных покупок». В особом фокусе спецслужб — обналичивание крупных сумм. Вот и получается, что пластиковые карточки, не только удобное средство для осуществления финансовых операций, но и ещё инструмент для отслеживания коммерческой активности того или иного субъекта, юридического лица. Уникальный номер «пластика», его электронный след не так-то просто скрыть. Именно платёжные карточки «рассказывают» федеральным агентам, какие «спонсорские» взносы и от кого получают криминальные структуры.

«Человек посередине» — шпионская стратегия нового поколения

Не ровен тот час, когда характеристики компании Google будут измеряться одноимённым математическим числом «гугол» — 10 в 100 степени. Доходы, пользователи, гигабайтные просторы на серверах — да всё, что можно. Титан IT-технологий уже сейчас может себе позволить практически всё. Да хоть и дружбу с американским АНБ (агентством национальной безопасности). Кстати, это факт: АНБ и Google таки питают к друг другу определённые симпатии. Часть их «отношений», конечно, открыта: защита киберпространства, вселенное и всенощное бдение конфиденциальности — в общем, чуть ли ни антихакерская коалиция. Но в том-то и дело, что только часть. Ведь свои методы ведения «обороны» они не афишируют в СМИ. Хотя и так всё понятно: когда кто-то лезет с ломом, ему навстречу, как правило, подставляют другой лом. Шпионские уловки, разведка, слежка наверняка в арсенале этой компании есть. И, конечно, в больших количествах! А по-другому было бы не солидно. Ещё один аргумент, подкрепляющий эту теорию, — засекреченные документы о партнёрских отношениях АНБ и Google: результаты покажем, а что за кулисами не скажем.

Весной 2012 года на страницах издания IT World промелькнуло острословное эссе, в котором деятельность таких гигантов веб-индустрии, как Facebook и Google, для наглядности сравнивалась с хакерской атакой «человек посередине» (MITM). Контекст «одни и те же методы» автор поста взял из реальности.

Атака MITM (человек посередине)

Судите сами: что хакер, что провайдеры сервисов делают незримый перехват данных пользователя. Ну и кто они с точки зрения инфозащиты? Шпионы! Правда, справедливости ради, стоит отметить, что перехваченные пользовательские данные «мегамонстры IT», в отличие от киберпреступников, используют в других целях. Но, без сомнения, корыстных — целевой маркетинг, статистика потребления, интересы и прочие «денежные премудрости». Хотя это для своих нужд, но есть ещё и большой брат из правительства — АНБ. Почему бы не поделиться с ним? Так ведь и делятся. И не только Google: и ИТ -компании не отстают в «дружбе» с госслужбами.

Вынужденное любопытство или виртуозный шпионаж

Помните Плюшкина из поэмы Гоголя «Мёртвые души»? Так вот, Google поразительно похож на этого «коллекционера». Только собирает он не предметы и утварь, а данные. Все данные пользователя, какие-то только есть, какие-то только можно выудить: IP, ID, конфигурация ПК, диагональ дисплея, версия браузера, Flash — всё этой «любопытной варваре» нужно «черкнуть» в свою БД. Авось пригодится.

Благодаря независимому расследованию Ноя Шахтмена, автору блога «Danger Room», посвящённому деятельности разведки и армии США, на поверхность «всплыли» новые факты о раннем сотрудничестве Google со спецслужбами. Так, со слов Шахтемна, особого внимания заслуживает компания с многозначительным названием «Записанное будущее» (Recorded Future). Эти ребята во всеуслышание прямо и чётко заявляют, что владеют принципиально новой технологией слежки и сбора разведданных. И параллельно приводят цифры и опции своего потенциала: сканирование в реальном времени до 100 тыс. веб-сайтов, блогов, Twitter-аккаунтов; выявление взаимосвязей между пользователями, определение событий, паттернов. А далее, после перечня «услуг», Recorded Future как бы подытоживает: «на основе полученных данных мы можем предсказать будущее».

Согласитесь, громко сказано. Почти как в поэме «Мёртвые души». Но не стоит успокаивать себя мыслью, что это рекламный «фарс». Установление скрытых связей, данных, логика, анализ — всё указывает на реальное существование подобной технологии. О серьёзности подхода и намерений Recorded Future говорить не приходится. Их инвесторы, всё те же «два друга» — ЦРУ и Google. Шахтмену даже удалось выяснить их покровителей — это «Google Ventures» (подразделение инвесторов) и некая компания In-Q-Tel (коммерческое детище ЦРУ). А сколько ещё таких засекреченных цепочек?

Летом 2010 года авторитетный «Washington Post» поведал своим читателям о масштабах разведсообщества США за период прошедшего десятилетия. Информация была изложена в формате журналистских расследований. В потоке раскрытых материалов фигурировало имя «Google». В своих сообщениях репортёры, ссылаясь на авторитетные источники, указывали на то, что Google разрабатывает картографическое и поисковое ПО для армии и разведки США, и что некоторые работники компании имеют повышенный приоритет допуска к гостайнам с меткой «Top Secret».

Каноны демократической прослушки

Илья Сачков, директор «Group-IB», в интервью изданию «Ведомости» сообщил, что российские спецслужбы вот уже на протяжении нескольких лет прослушивают и определяют местонахождение пользователей в программе Skype. Он однозначно резюмировал: «Поэтому наши работники не обсуждают дела компании в Skype».

Проявлять повышенную осторожность к популярному коммуникатору рекомендует и Евгений Чичваркин, основатель «Евросети». Кроме того, он отмечает, что в 2009 году уровень конфиденциальности Skype был куда выше (Евгений использовал эту программу при обыске «Евросети»). Большую доступность и демократичность в плане конфиденциальности самая востребованная «говорилка» Интернета получила чуть позже…

Максим Эмм, эксперт и исполнительный директор «Peak System» рассказывает: «В мае 2011 года Skype купила Microsoft и снабдила программу технологией отслеживания. По запросу спецслужб или решению суда любого государства коммуникационный канал подозреваемого пользователя переключается в режим прослушки. Причём его ключи шифрования генерируются не в личном ПК/телефоне, а на сервере Microsoft». Более того, Н.Прянишников, глава российского филиала «Microsoft», сообщает: «В случае необходимости, компания может предоставить исходный код коммуникатора Skype службе ФСБ в целях быстрой дешифровки передаваемых данных». Хотя спецслужбам из Китая возможно такая услуга и не пригодится. И не то чтобы они нелюбопытные и небдительные…

Джеффри Нокел, программист из университета Нью-Мексико, исследовав китайский дистрибутив Skype, установил, что он оснащён, ни много ни мало, кейлоггером — шпионским ПО, регистрирующим нажатые пользователем клавиши. Проворный «помощник» госбезопасности КНР кропотливо анализирует «писанину» юзеров и, обнаружив в переписке подозрительные словечки, сливает зафиксированные логи (текст сообщений) в соответствующие инстанции. Разобрав алгоритм кейлоггера на шпунтики и винтики, Нокелу также удалось обнаружить и перечень запрещённых слов. В их числе: «BBC News», «Репортёры без границ», площадь «Тяньаньмэнь», на которой в 1989 году была жестоко подавлена акция протеста.

Хакеры в противовес разведке

Сообщество «свободных художников» киберпространства, как выяснилось, вполне может утереть нос и разведке, и контрразведке, и прочим «механизмам» госбезопасности. Ещё и как: известнейший немецкий хакер StarBug (Ян Крисслер) со своим коллегой Тобиасом Фибигом 27 декабря 2014 года на конференции Chaos Computer Club в Гамбурге наглядно продемонстрировали несостоятельность биометрической идентификации (механизма авторизации пользователя по отпечаткам пальцев и радужной оболочке глаза). Им удалось клонировать отпечатки Урсулы фон дер Лайен, министра обороны Германии, причём из обычных фотографий. Различные углы проекции пальцев министра на снимках Ян и Тобиас обработали при помощи коммерческой технологии VeriFinger и, в итоге, получили «потенциальные ключи» для доступа к военным тайнам и засекреченным объектам страны.

По окончанию своего доклада Крисслер в шуточной форме подытожил свои достижения: «в скором времени видным политикам придётся на публичных собраниях выступать в перчатках. Кстати, мы хотели добыть отпечатки Ангелы Меркель, но у нас ничего не вышло. И всё из-за её привычки держать пальцы рук скрещенными».

Постскриптум настоящего будущему — «прозрачный» мир

Компьютеры, спутники, коммуникационные сети, глобальная паутина… что будет дальше? Можно ли будет одному человеку сказать другому что-то украдкой, по секрету, вдалеке от чужих ушей? Нет, не виртуально в интернете — ведь сегодня, в XXI веке, эпоху вездесущей виртуальной слежки, этого сделать уже нельзя. А так, просто, тет-а-тет — в кафе за чашкой чая, на опушке леса, в дебрях дачной глуши. И какая разница с кем и о чём: можно или нет? Во втором десятилетии миллениума на этот вопрос, к сожалению, уже однозначно ответить нельзя.

Поразительно! Но если переместиться на 100, да что там, на 50-30 лет назад во времени и рассказать какому-нибудь обывателю прошлого эту проблему, как бы он отреагировал? Рассмеялся, покрутил бы пальцем у виска и посоветовал сходить к доктору — провериться на синдром «мании преследования». Наверняка, его ответ выглядел бы именно в таком стиле. Нонсенс и закономерность в одном лице.

А какой будет информационная безопасность в будущем, в аллегорическом «завтра» и «послезавтра»? Имплантация электронного чипа в первые минуты рождения, доступ к социальным благам по ID на руке, матрица? Суровые догадки и гипотезы на ум приходят неспроста, не без основания. И совсем не хочется вспоминать «клеймо зверя» из откровений Иоанна Богослова. Так, руины «информационной войны», жертвы «информационного оружия» — люди, существа разумные, состоящие из тела и души…

SINHROFASOTRON