Укрепим Интернет против тотального прослушивания!

На прошлой встрече IETF88 в Ванкувере широко обсуждалась проблема всеобщего прослушивания, масштаб которой открылся благодаря разоблачениям Эдварда Сноудена. Я писал об этом в статье «Что мы знаем о защите информации в Интернете?» (http://www.ripn.net/articles/Anti-surveillance/).

С тех пор общественность и журналисты немного охладели к этой теме, политики выступили с нужными заявлениями, но проблема по своей сути и масштабу по-существу не изменилась. IETF же определил проблему в технических терминах и начал дискуссию об уязвимых местах протоколов и способах их устранения. За день до начала заседания IETF89 в Лондоне, IAB (www.iab.org) и W3C (www.w3c.org) совместно организовали рабочее совещание STRINT (https://www.w3.org/2014/strint/) в ходе которого попытались всесторонне рассмотреть угрозы, пути противодействия и имеющийся и желаемый инструментарий.

Анатомия тотального прослушивания

Анализ угроз

Прежде чем говорить о решениях проблемы, необходимо эту проблему определить. От того насколько верно определены параметры проблемы зависит и качество и полнота предлагаемых решений. В области безопасности для этого принято использовать т.н. модель угроз, которая помимо уязвимостей системы учитывает присутствие и мотивацию атакующего. Поскольку даже при наличии уязвимости, отсутствие у атакующего желания ее использовать, предполагает отсутствие атаки как таковой. Документ «Атака тотального прослушивания: модель угроз и определение проблемы» («Pervasive Attack: A Threat Model and Problem Statement», http://datatracker.ietf.org/doc/draft-barnes-pervasive-problem/?include_text=1) описывает следующие категории атак:

- Широкомасштабный сбор Интернет-трафика
- Атаки типа MITM (Man-in-the-middle, человек посередине, http://ru.wikipedia.org/wiki/Человек_посередине)
- Использование имплантатов - модифицированного программного обеспечения или вредоносных программ.

Рассмотрим эти категории подробнее.

Широкомасштабный сбор Интернет-трафика

Как следует из документов, раскрытых Эдвардом Сноуденом, одним из способов получения больших объемов трафика оказался традиционный способ прослушивания опорных телекоммуникационных каналов. Газета The Guiardian в качестве примера приводит программу агентства GCHQ (http://www.gchq.gov.uk) под кодовым названием Tempora. В рамках этой программы проводится прослушивание 1500 основных каналов, обеспечивающих Интернет-связность Великобритании (http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work), обеспечивающее доступ к данным объемом 21.6 петабайт в день.

Другим вариантом является предоставление данных по требованию правоохранительных органов. Например, программа PRISM обеспечила агентству NSA (http://www.nsa.gov/) доступ к данным Google, Facebook, Microsoft, Skype, Apple, Yahoo. Точная информация о степени кооперации этих компаний отсутствует, но очевидно, что речь шла не о целевых запросах, а о сплошном сборе данных с последующим анализом.

Интересно отметить, что хотя оба варианта сбора доступны лишь крупным игрокам - государственным агентствам, - факт существования точек концентрации, практически на всех уровнях - канальном, передачи и маршрутизации трафика, а также приложений и услуг, является серьезной уязвимостью сегодняшнего Интернета. Формированию этих точек концентрации способствовали экономические

факторы, такие как эффект масштаба и сетевой эффект, несмотря на то, что базовые архитектурные принципы Интернета способствуют формированию распределенной и пиринговой модели.

Атаки типа MITM (человек посередине)

Прослушивание может также быть реализовано с использованием более активных атак, например, т.н. атак "человек посередине". В этих случаях атакуемый становится невидимым посредником в обмене информацией между отправителем и получателем. При этом данные могут быть как просто скопированы, так и модифицированы. Вариантов реализации такого рода атак несколько. Например известно, что программа NSA под кодовым именем QUANTUM использует несколько способов перехвата трафика HTTP, таких как изменение ответов DNS или использование HTTP перенаправления (код 302).

Другие варианты перехвата трафика могут использовать уязвимости глобальной системы маршрутизации и протокола BGP, перенаправляя потоки данных через сеть атакующего. Примером такого перенаправления является т.н. утечка маршрутов (route leaks), когда маршрут, полученный сетью-клиентом от одного провайдера транзита переанонсируется другому транзитному оператору. Атаки такого типа отнюдь не теоретические, нарушение политики клиент-провайдер было неоднократно замечено в Интернете. (См., например, статью «Why Google Went Offline Today and a Bit about How the Internet Works», http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about).

Другим способом является захват префикса (prefix hijack) с возвратом трафика в прежнее русло - атака Пилосова-Капеллы (от этой атаке я писал в статье «Безопасность системы маршрутизации Интернета», http://www.ripn.net/articles/secure_routing/) . Атаки такого рода также случаются регулярно, см. статью Renesys «The New Threat: Targeted Internet Traffic Misdirection» (http://www.renesys.com/2013/11/mitm-internet-hijacking/).

Использование имплантатов - модифицированного программного обеспечения или вредоносных программ.

Известно также, что NSA использовало различные методы для ослабления систем шифрования и анонимности, используемых в Интернете - например, шифрования трафика с помощью технологий TLS (http://ru.wikipedia.org/wiki/TLS) или системы аномизации Tor (https://www.torproject.org/).

В пассивных и активных (MITM) атаках перехвата NSA активно применяло системы дешифровки с помощью цифровых ключей, собранных в рамках программы BULLRUN. Похоже, что в рамках этой и ряда других программ производилось систематическое внедрение "задних дверей" в криптографические технологии, коммерческие устройства и системы защиты. Некоторые примеры этой деятельности приведены в статье, опубликованной в Нью-Йорк Таймс «Secret Documents Reveal N.S.A. Campaign Against Encryption» (http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0).

Архитектурная концентрация

Что отличает широкомасштабное прослушивание от известных атак, таких как «человек посередине» или использование вредоносного программного обеспечения, так это масштаб. Так же как «большие данные» открывают новые качественные возможности доступа к информации, так и широкомасштабное прослушивание предоставляет качественно новые возможности корреляции на первый взгляд независимых данных, получая широкую и в то же время детальную информацию о пользователях Интернета.

Сегодня значительный объем Интернет-трафика криптографически не защищен. Это, вкупе с описанными возможностями секретных государственных агентств, существенно облегчает задачу.

Но это лишь часть картины. Другим мощным фактором является архитектурная концентрация на всех уровнях, начиная от топологии и заканчивая приложениями и контентом.

На инфраструктурном уровне мы наблюдаем значительную концентрацию объема передаваемого трафика через трансатлантические каналы, инфраструктуры крупных дата-центров и точек обмена трафиком. Доступ к этим объектам означает доступ к колоссальному объему информации.

На Интернет-уровне мы наблюдаем концентрацию в виде так называемых провайдеров верхнего уровня – т.н. Tier-1. Эти провайдеры обеспечивают глобальный транзит трафика, и существенная часть потоков либо маршрутизируется между этими провайдерами, либо между сетями-клиентами этих провайдеров. Другим аспектом концентрации на этом уровне является уязвимость BGP, позволяющая «утечку маршрутов», через которую атакующий может получить доступ к потокам между теми же провайдерами Tier-1.

Наконец, **на уровне приложений и услуг** происходит колоссальное сосредоточение данных и метаданных в руках нескольких организаций. Количество пользователей Google, Facebook, Twitter, Skype идет на сотни миллионов, а обмен данными с этими концентраторами составляет значительный процент всего трафика Интернета. Например Google составляет четверть всего трафика североамериканских Интернет сервис-провайдеров, во много благодаря YouTube, конечно. Открытый DNS-резолвер Google Public DNS обслуживает 7% всех запросов! Хотя данные DNS не конфиденциальны, характер запросов может многое рассказать о пользователе.

Неудивительно, что эти точки растущей концентрации Интернета весьма привлекательны для секретных служб, и следовательно являются уязвимыми местами, может быть даже большими, чем открытый трафик сам по себе.

Анализ трафика, данные и метаданные

Когда речь идет о тотальном прослушивании, метаданные играют даже более важную роль, чем собственно данные. Какими сайтами интересуется пользователь, с кем он общается, где находится – при обширном и долговременном наблюдении этой информации вполне достаточно, чтобы сформировать точный портрет пользователя.

Новый проект лаборатории Media Lab Массачусетского технологического института immersion (https://immersion.media.mit.edu/) позволяет получить предоставление, как много могут рассказать метаданные. Проект строит социальную сеть пользователя лишь анализируя «метаданные» его электронной почты – поля «From», «To», «Cc» и временные штампы. На рис.1 представлена сеть одного из моих почтовых аккаунтов.

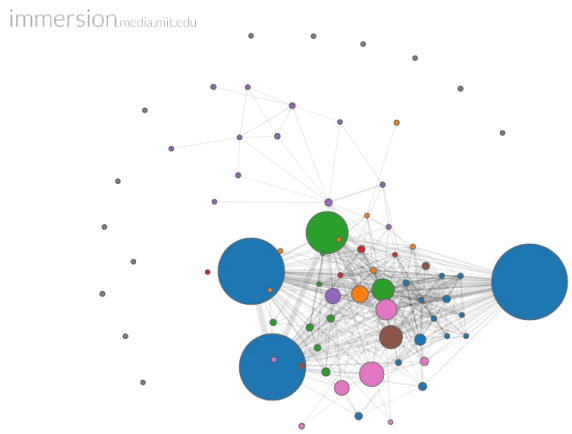

Рис 1. Социальная сеть пользователя электронной почты, построенная проектом immersion в результате анализа метаданных. Размер круга обозначает интенсивность обмена, а цвета – принадлежность людей к той или иной группе.

Сбор метаданных возможен теми же методами, что и для пассивного и активного прослушивания. Но иногда для получения метаданных атакующему даже необязательно перехватывать сами потоки.

Например, метод IdleScan (http://nmap.org/book/idlescan.html) позволяет определить наличие потоков данных между компьютерами в сети. Метод использует идентификационный номер фрагмента IP-пакета, т.н. IP ID. Многие операционные системы просто увеличивают этот индекс при отправлении каждого пакета.

В статье «Spying in the Dark: TCP and Tor Traffic Analysis» (http://freehaven.net/anonbib/papers/pets2012/paper_57.pdf) показано, что единственным требованием успешного наблюдения является то, что прослушиваемый пользователь также обменивается данными с сайтом атакующего. Отслеживая изменение индекса IP-ID в ответ на пробные пакеты, атакующий может достаточно достоверно установить факт обмена данными между определенными компьютерами. Этот метод может также достаточно успешно использоваться даже если пользователи используют анонимные сети Tor.

Даже временные характеристики передачи, например продолжительность сессии или размеры пакетов, могут быть скоррелированы, давая информацию о пользователях сети.

Проблема заключается в том, что метаданные гораздо труднее скрыть от посторонних глаз, чем сами данные. Основу метаданных составляют данные протоколов более низкого уровня, например, IP или транспортного – TCP. Другой проблемой является то, что многие метаданные широко используются в управлении сетями, например для мониторинга производительности, планирования и классификации трафика. Функционирование многих устройств сетевой защиты базируется на метаданных.

Но и для новых протоколов уменьшение "необходимых" сети метаданных может привести к блокированию трафика. Примером может служить высокая степень блокирования фрагментированного трафика. Дело в том, что фрагментированные IP пакеты не содержат достаточной информации о потоке данных и многие сетевые экраны такие пакеты попросту отбрасывают.

Арсенал

Оппортунистическое шифрование

Наиболее очевидной защитой против пассивных атак прослушивания является шифрование передаваемых данных. Действительно, если соединение между браузером и вэб-сервером, приложением электронной почты и почтовым сервером, между самими почтовыми серверами, между «облачными» серверами и т.д. защищено технологией TLS, атакующему по крайней мере необходимо затратить гораздо больше усилий для получения доступа к контенту.

Преимущества и необходимость шифрования канала очевидны, когда речь идет о приложениях электронной торговли или обмен конфиденциальной информацией. Но действительно, стоит ли шифровать канал доступа пользователя скажем к статьям Википедии или новостным сайтам? Имеет ли смысл шифрование обмена данных DNS, которые по определению являются общедоступными?

В контексте тотального прослушивания считается, что затраты скорее всего превысят преимущества, что тем самым приведет к изменению стратегии атакующего. Вместо тотального прослушивания – сфокусированное прослушивание определенных потоков данных.

Чтобы лучше понять проблемы, связанные с шифрованием потоков на транспортном уровне, вкратце рассмотрим технологию TLS.

TLS, или Transport Layer Security (Безопасность транспортного уровня), представляет собой криптографический протокол, обеспечивающий как безопасность, так и целостность данных для потоков транспортного уровня на основе протокола TCP. TLS позволяет осуществлять обмен данными в Интернете, например между браузером и веб-сервером, не допуская подслушивания и фальсификации данных, тем самым обеспечивая аутентичность и конфиденциальность в публичных сетях. TLS является новейшей версией протокола SSL, хотя имя SSL по прежнему используется при разговоре о защищенных соединениях.

Протокол основан на ассиметричной криптографии для первоначального рукопожатия, аутентикации отправителя данных и создания разделяемого симметричного ключа (т.н. ключа сессии), который затем используется для шифрования данных.

Процесс обмена ключами и создание защищенного канала TLS схематически представлен на рис.2.

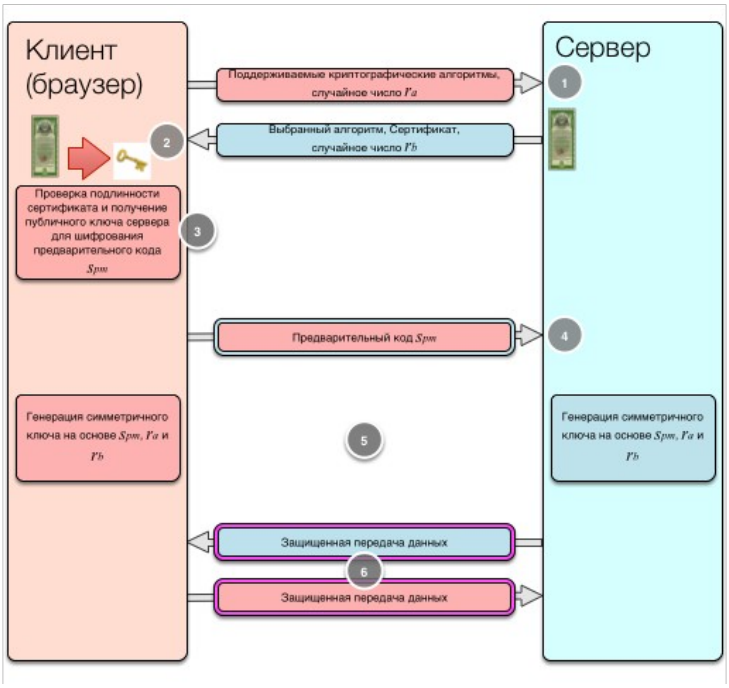

Рис. 2. Фаза «рукопожатия» и создания защищённого канала в протоколе TLS при использовании системы кодирования RSA.

Для проверки подлинности отправителя, например веб-сервера, обычно используется инфраструктура публичных ключей (Public Key Infrastructure, PKI). Так, с помощью PKI вэб-браузер сможет проверить подлинность серверного сертификата, соответствие имени субъекта сертификата имени сервера и, в идеальном случае, не был ли сертификат отозван (revoked).

Оппортунистическое шифрование обычно означает, что при установлении соединения с сервером клиент изначально пытается использовать шифрование и выбирает открытый канал только, если попытка использования шифрования не удалась.

Наиболее известным примером оппортунистического шифрования является расширение STARTTLS (http://ru.wikipedia.org/wiki/STARTTLS), которое позволяет создать зашифрованное соединение прямо поверх открытого канала.

Другим аспектом оппортунистического шифрования является возможность создания защищенного канала без удостоверения подлинности принимающей стороны. Примером такой ситуации является использование самоподписанного серверного сертификата, подлинность которого не может быть установлена. В этом случае многие браузеры реагируют предупреждением и позволяют пользователю вручную разрешить создание канала как исключение. Однако оппортунистическое шифрование предполагает, что создание защищенного канала происходит невидимо для пользователя, и с точки зрения пользователя канал не становится защищенным, даже при успешном создании такого соединения. Это понятно, ведь оппортунистическое шифрование обеспечивает дополнительную защиту против пассивного атакующего и бессильно против атак типа MITM.

Perfect forward secrecy

Даже если передача данных происходит по защищенному каналу, атакующий может продолжать собирать данные, рассчитывая в определенный момент каким-либо образом скомпрометировать серверный ключ. Например, сервер подлежит списанию, злоумышленник получает доступ к жесткому диску и соответственно к секретному ключу. Заполучив ключ, атакующий может теперь расшифровать все собранные им данные. Процесс генерации и обмена ключами, рассмотренный ранее (рис. 2) является уязвимым для такого типа атаки.

Основной проблемой создания защищенного канала с помощью алгоритма RSA (скажем с использованием криптопакета RSA_WITH_AES_128_CBC_SHA) является то, что один и тот же ключ используется как для проверки подлинности сервера – аутентикации, что является моментальной операцией, так и для шифрования данных, защита которых долгосрочна.

Избежать такой ситуации позволяет криптографическая система при которой компрометация долговременного серверного ключа в будущем не позволит расшифровать прошлый обмен данными. Такая особенность системы получила название «идеальной прямой секретности» (perfect forward secrecy, или PFS).

В протоколе TLS PFS реализуется путем использования RSA только для аутентикации сервера, а для генерирования и обмена ключами – протокол Диффи-Хеллмана (Diffie-Hellman, http://ru.wikipedia.org/wiki/Протокол_Диффи_—_Хеллмана), позволяющий создать разделяемый секрет (симметричный ключ) между сторонами, обменивающимися данными по открытому каналу. В этом случае ключ для шифрования данных действует только на протяжении сессии, а затем уничтожается. Такие ключи получили название эфемерных, а алгоритм – DHE (Diffie-Hellman Ephemeral). Поскольку эти ключи независимы от долгосрочного серверного ключа, компрометация последнего не позволяет расшифровать прошлые обмены данными. Злоумышленнику в этом случае придется взламывать ключи для каждой сессии, что делает задачу доступа к данным почти невыполнимой.

Работа TLS в режиме DHE показана на рис. 3.

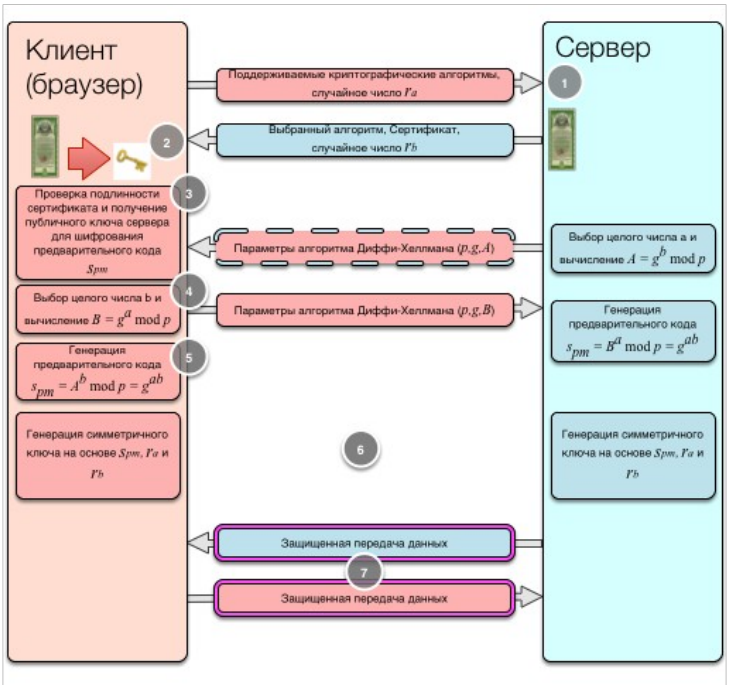

Рис.3. Обмен ключами в TLS по протоколу Диффи-Хеллмана с реализацией PFS.

Использование DHE требует большей компьютерной мощности и ведет к потере производительности, поэтому некоторые администраторы веб-серверов не поддерживают этот алгоритм. Алгоритм Диффи-Хеллмана с использованием криптографии эллиптической кривой имеет лучшие характеристики и используется более широко. Сегодня большинство браузеров и многие ведущие провайдеры контента и социальные сети поддерживают эти алгоритмы и, соответственно, PFS.

Проблемы Web PKI

Под термином Web PKI обычно понимают систему аутентикации и шифрования веб-транзакций, основанную на технологии X.509 PKI, используемую сегодня производителями браузеров и операторами веб-сайтов. Суть системы проста – веб-сайт получает сертификат X.509 от удостоверяющего центра, именем субъекта сертификата является доменное имя сайта, а ключом сертификата является публичный ключ сайта. Сертификат используется протоколом TLS, и с его помощью клиент-браузер может шифровать и дешифровывать данные, которыми он обменивается в этим сайтом.

Система эта, позволившая обеспечить возможность электронной коммерции и по сегодняшний день служащая ее основой, имеет ряд существенных проблем.

Основной проблемой является то, что типичный браузер содержит список из около ста удостоверяющих центров, которым он, а следовательно и пользователь, доверяет. Центры эти различаются по качеству и тщательности проверок при обработке запроса на сертификат. В некоторых случаях проверки настолько минимальны, что получение сертификата для доменного имени является лишь вопросом уплаты взноса.

«Аккредитацию» и создание этого списка каждый производитель клиентского ПО – браузеров осуществляет самостоятельно на основании рекомендаций организации CAB (CA/Browser) Forum (https://cabforum.org). Например, с подробными требованиями, предъявляемыми к УЦ со стороны компании Mozilla, разработчика браузера Firefox, можно познакомиться на их сайте: http://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/.

Другой особенностью является то, что компрометация «аккредитованного» удостоверяющего центра позволяет злоумышленнику создать необходимые сертификаты. Случай взлома УЦ DigiNotar в 2011 году – яркий тому пример (см., например, http://www.xakep.ru/post/59572/default.asp?utm_source=dlvr.it&utm_medium=twitter). Наконец, секретные агентства государств, в юрисдикции которых находится УЦ, имеют дополнительный рычаг воздействия на этот УЦ.

О некоторых из этих проблем я писал в статье «Путевые заметки: IETF-84» (http://www.ripn.net/articles/IETF84/). Там же я привел возможное решение многих проблем Web PKI - DANE (DNS-based Authentication of Named Entities). DANE позволяет владельцу доменного имени опубликовать сертификат TLS или указатель на доверенную систему PKI, в которой такой сертификат находится. Преимуществом этого подхода является то, что для проверки подлинности DANE использует систему, хотя и напоминающую PKI, но базирующуюся на DNS и полностью конгруэнтной с DNS - это DNSSEC. Таким образом обеспечивается такая же криптографическая защита, как и в традиционных PKI, но цепочка доверия полностью соответствует доменной иерархии. Другими словами, DANE позволяет получить достоверный сертификат от самого владельца имени без посредников.

Существующие протоколы

Новый взгляд на существующие атаки поставил также вопрос – соответствует ли уровень защищенности существующих протоколов сегодняшним требованиям? Насколько хорошо они защищены от атак тотального прослушивания?

Для работы в этом направлении в IETF был начат процесс анализа существующих спецификаций. Желающие внести свой вклад могут зарегистрировать его на вики: https://trac.tools.ietf.org/group/ppm-legacy-review/.

Вопросы внедрения

Ценность идей и решений напрямую связана с потенциалом их внедряемости. Особенно в области информационной безопасности, где затраты могут быть существенны, а преимущества скрыты, особенно для пользователя. Усиление защиты зачастую ведет к дополнительной сложности разработки и использования протокола и приложений, построенных на его основе. Это может, в свою очередь, затруднить внедрение протокола, сведя на нет большую часть усилий.

В этом смысле понятен фокус на оппортунистическое шифрование, при котором минимизируются и затраты провайдеров контента (веб-сайтов) – возможность использования собственных самоподписанных сертификатов, и от пользователя не требуется дополнительных усилий. По-существу речь здесь идет о решимости производителей ПО веб-серверов и браузеров нести свой вклад в повышение общей безопасности.

Другим моментом является повышение осведомленности общественности об атаках тотального прослушивания. И хотя для большинства обычных пользователей после сенсационного всплеска жизнь вернулась в свою прежнюю колею, многие организации более внимательно смотрят на аспекты защиты собственных данных, особенно при использовании облачных сервисов.

Кое-кто считает, что ничего принципиально нового в раскрывшихся деталях прослушивания нет. Дескать, для секретных служб это всегда было одним из основных видов деятельности. Однако масштаб – прослушиванию подвергались все доступные пользователи, и технологические возможности – объемы данных и возможность их корреляции, поставили эти атаки на качественно новый уровень.

Будем надеяться, что ответом на это станет качественно новый уровень защиты данных в Интернете.

Андрей Робачевский

Мнения, представленные в статье, не обязательно отражают официальную позицию ISOC