№2
декабрь 2015

MSK IX

Интернет изнутри

Безопасность

Содержание:

Иформационный сборник «Интернет изнутри»

По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №2, дата выхода: декабрь 2015 г.

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Дизайн:
Чернега Наталья

Безопасный Интернет

главный редактор,
Андрей Робачевский

Дорогой читатель!

В качестве ведущей темы этого номера мы выбрали Безопасность. Это очень важная и одновременно очень трудная тема.

Важная, потому что по мере того, как мы больше и больше зависим от Интернета – начиная от доступа к информации, хранения данных, совершения онлайн-транзакций, участия в социальных сетях или использования мириадов различных приложений, - вопросы защищенности данных и инфраструктуры встают все более остро.

Трудная эта тема по нескольким причинам.

Во-первых, хорошая безопасность неосязаема. О проколах в защите мы узнаем из новостей, будь то утечка личных или финансовых данных или атака отказа в обслуживании, или из личного опыта, когда оказывается, что наш компьютер инфицирован или что платеж ушел в никуда. Хорошую безопасность мы не замечаем и поэтому, как ни парадоксально, не очень ценим.

Во-вторых, в такой гиперсвязной системе как Интернет собственная безопасность не может быть достигнута в одиночку. Слишком уж много внешних зависимостей. Если мы посмотрим на безопасность инфраструктуры, будь то система передачи данных, маршрутизации или трансляции имен DNS, то увидим, что защищенность собственной системы или ресурса в значительной степени находится в руках других участников.

Наконец, в-третьих, эти другие участники зачастую не заинтересованы во внедрении мер по повышению «внешней» безопасности и уменьшению рисков от собственных услуг или инфраструктуры. Так называемый business case слабоват ввиду отсутствия экономических факторов и недостаточных мер по повышению ответственности участников.

Две статьи сегодняшнего номера иллюстрируют эти трудности обеспечения безопасности в Интернете. Статья «Еще больше «утечек» маршрутов» анализирует различные пути укрепления безопасности и устойчивости глобальной системы маршрутизации, а статья «Анатомия рефлекторных атак» рассказывает об источниках и составных частях атак отказа в обслуживании, основанных на отражении с усилением. Хотя темы различны, обе статьи сходятся во мнении, что хотя технологии и «строительные блоки» существуют, для решения этих проблем нужны новые, нестандартные подходы.

Что же касается технологий и «строительных блоков», то о них расскажут статьи «TLS: двадцать лет спустя» и «Краткий путеводитель по IETF-94».

Есть в этом номере и печальная страница – 1 декабря 2015 года на 72 году жизни скончался один из основателей европейского Интернета, сообщества RIPE и Региональной интернет-регистратуры RIPE NCC **Роб Блокзайл**. Его памяти мы посвятили небольшую статью.

Итак, перед вами второй выпуск. Надеемся, что он оправдает ваши ожидания. Расскажите нам, что вам понравилось, а что – нет, о чем бы вы хотели прочитать в следующих номерах. Ждем ваших отзывов и предложений по адресу info@internetinside.ru.

Словарь терминов

Безопасность информации (данных) (англ. information (data) security) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) (англ. IT security) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы — состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Источник: Информационная безопасность, стандартизированные определения

Еще больше «утечек» маршрутов

Джефф Хьюстон (Geoff Huston)

Большую часть времени почти везде большая часть Интернета функционирует просто прекрасно. И действительно, кажется, что Интернет работает достаточно хорошо - вплоть до того момента, когда начинаются серьезные неприятности. После этого он превращается в повод для заголовков в отраслевой прессе.

Большую часть времени почти везде большая часть Интернета функционирует просто прекрасно. И действительно, кажется, что Интернет работает достаточно хорошо - вплоть до того момента, когда начинаются серьезные неприятности. После этого он превращается в повод для заголовков в отраслевой прессе.

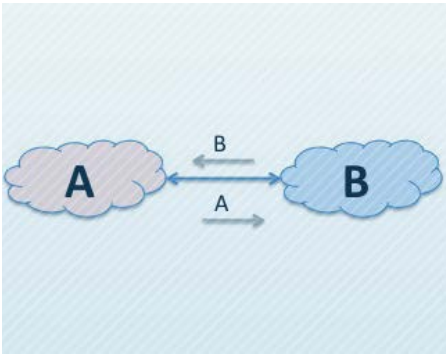
В этот раз проблемы начались 12 июня в Малайзии у крупного интернет-провайдера страны - компании Telekom Malaysia. Рассматривая сейчас, что случилось и почему это произошло, возможно, полезно будет начать с краткого резюме, описав то, каким образом Интернет «знает», где все находится. Итак, краткое отступление на тему системы маршрутизации.

Связность и маршрутизация в Интернете – краткий курс

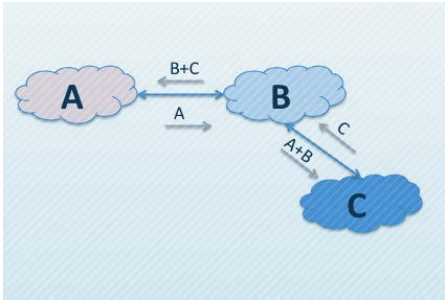
При установлении соединения двух сетей способ, с помощью которого они узнают друг о друге, заключается в обмене маршрутной информацией. В этом случае сеть можно себе представить как набор достижимых IP-адресов (маршрутов), а соединение двух сетей реализует простую форму следующего утверждения: *«Я скажу тебе мои маршруты, а ты расскажешь мне о своих»*.

Давайте рассмотрим две сети и назовем их A и B. И давайте предположим, что сети A и B соединены между собой таким способом. Теперь если источник в сети A желает отправить пакет в некий пункт назначения в сети B, то поскольку A и B напрямую соединены между собой, сеть A знает все о наборе IP-адресов, которые достижимы в сети B.

Поэтому система маршрутизации сети A направит пакет в сеть B.

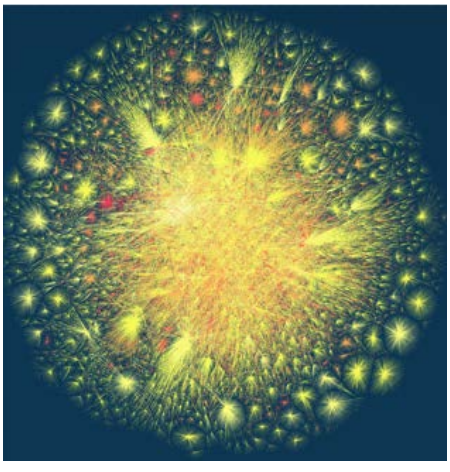


Теперь давайте добавим в эту модель третий элемент. Что если у нас имеется третья сеть, C, которая соединена с сетью B? Если сеть B была подготовлена, чтобы действовать в качестве «транзитного» провайдера услуг, тогда B может объявить маршруты сети C в A в дополнение к своим собственным маршрутам и объявить маршруты сети A в C. Теперь все точки этих трех сетей могут достигнуть друг друга. Если источник в сети A отправляет пакет в пункт назначения в сети C, то система маршрутизации сети A направит пакет в сеть B, поскольку сеть A узнала о маршрутах в C через сеть B. Система маршрутизации сети B признает адрес назначения как расположенный в сети C и передаст пакет в C.



Обычно мы называем сети A, B и C Автономными системами, а протоколом маршрутизации, используемым для обмена маршрутами в Интернете, является BGP (Border Gateway Protocol, Протокол пограничной маршрутизации). Если вы повторите вышеприведенный сценарий межсетевого соединения еще 50 тысяч раз для учета взаимных соединений 50 тысяч сетей и примените протокол BGP для обмена информацией о маршруте по 560 тысячам маршрутов, то у вас получится что-то, по масштабам напоминающее современный Интернет.

Существует множество способов для соединения между собой 50 тысяч Автономных систем с использованием базового парного соединения. Можно использовать линейные соединения, кольца, веерную структуру или любую форму топологии соединений. Один из примеров визуализации межсетевого соединения в Интернете показан ниже:



Что формирует конкретную конфигурацию Интернета? Лучший ответ, который я могу предложить, заключается в том, что форму Интернета определила комбинация

денег и географии. География – это тенденция сетей соединяться с другими сетями, которые расположены на физически близком расстоянии. Существует мощная индустрия, посвященная эксплуатации так называемых точек обмена по всему миру.

Точка обмена представляет собой выделенную систему, к которой локальные сети могут подсоединиться и использовать коммутационное оборудование точки обмена для установления соединения со всеми другими сетями, представленными в этой точке. Заинтересованность в географической близости объясняется производительностью и, конечно, деньгами. Если две сети соединены каналом, который проходит по всему миру, то время, необходимое пакету для прохода по этому расширенному пути, будет гораздо больше того интервала, который потребуется пакету для путешествия по соединению, охватывающему область города или региона. Поэтому более близкое соединение позволяет предоставить более качественные услуги пользователям. И хотя это и не является универсальной истиной, чаще всего более протяженные маршруты, особенно пересекающие один или несколько океанов, имеют более высокую стоимость из расчета на пакет, чем менее длинные «дороги». В общем, получается, что более короткие пути дешевле.

Деньги являются главной движущей силой для установления межсетевых соединений, поскольку в конечном счете именно деньги двигают вперед эту индустрию. Для того, чтобы это проиллюстрировать, давайте вернемся к нашему простому примеру сетей A, B и C. Когда сеть C соединяется с B, что будет мотивировать сеть B на анонсирование маршрутов в C для сети A? Не забудьте о том, что в этом случае трафик, текущий между A и C, будет потреблять сетевые ресурсы B, однако сеть B не имеет прямых отношений с любым из конечных пользователей, которые генерируют этот поток трафика. Поэтому сеть B не может выставить счета ни заказчику сети A, ни заказчику сети C для получения компенсации за предоставление этой услуги. Одно из жизнеспособных решений заключается в том, что сеть C платит сети B за эту транзитную услугу. В действительности сеть B является провайдером сети C или, если посмотреть с другой стороны, C является клиентом B. Теоретически возможно так организовать мир соединенных между собой сетей, чтобы превратить его в соединительную сетку, используя для этого только взаимоотношения типа клиент-провайдер, однако сделать это порой довольно сложно. Для того, чтобы это проиллюстрировать, давайте добавим в наш пример еще одну сеть – сеть D, которая является клиентом A. Теперь, когда D обменивается трафиком с C, эта сеть будет платить A, а C будет платить сети B - согласно тому, что можно ожидать от отношений типа клиент-провайдер. Но что можно сказать об отношениях между сетями A и B? В ряде случаев, когда A и B имеют сходный размер и масштаб, нелегко естественным образом определить, кто является провайдером, а кто клиентом. Индустрия ISP (провайдеров интернет-услуг) изобрела дополнительную форму отношений для разрешения именно такой ситуации, которая представляет собой отношение «с равным по положению», в рамках которого две сети соединяются между собой, но соглашаются не выставлять друг другу счета (это представляет собой старое соглашение SKA, или Sender Keeps All – соглашение о бесплатном пиринге).

В результате у нас имеются три возможные роли сети в сфере межсетевого соединения: клиент, провайдер и равный партнер, или пир. При этом многие сети играют все три роли одновременно. Имея в виду, что сеть генерирует доход со своих клиентов, тратит деньги на провайдеров и занимает нейтральное положение в отношении доходов для своих пиров, очевидно, что провайдеры стремятся максимизировать привилегии в отношении своих клиентов по сравнению с пирами и провайдерами и предпочитают партнеров провайдерам. Таким способом провайдер может максимизировать свой доход и свести к минимуму расходы.

Способ, которым это реализовано в маршрутизаторах сети, заключается в использовании в BGP локальных настроек предпочтений. Все внешние соединения просто относят к одной из этих категорий, после чего можно использовать локальную настройку предпочтений, чтобы предпочесть объявленные клиентом маршруты по сравнению с объявленными партнером

Рис.1. Размер таблицы маршрутизации: неделя, начинающаяся с 9 июня 2015 г. (www.potaroo.net)

и провайдером, а объявленные партнером маршруты - по сравнению с объявленными провайдером. Поэтому если сеть видит один и тот же маршрут, анонсированный со стороны клиента, а также со стороны партнера или провайдера, то локальная настройка предпочтений гарантирует, что сеть выберет маршрут через клиента, а не через партнера.

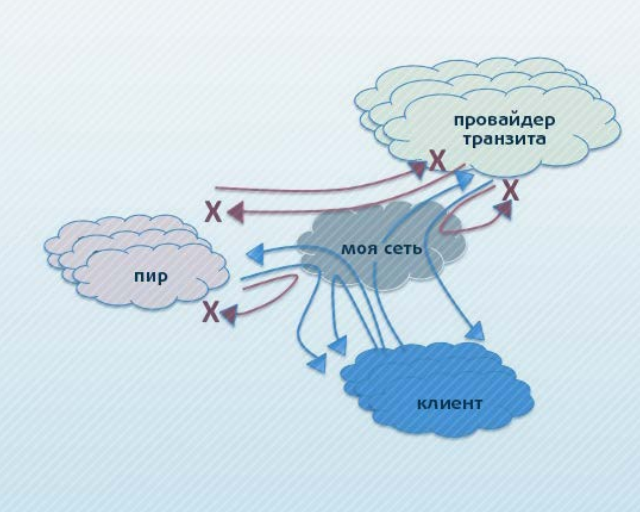
Эти локальные настройки предпочтений имеют высокий приоритет в алгоритмах принятия решений BGP: локальные предпочтения переопределяют алгоритм сравнения BGP по умолчанию, который сравнивает длину маршрутов между Автономными системами. Поэтому даже если сеть использует механизм добавления AS в AS-PATH для того, чтобы повлиять на выбор маршрута, настройки локальных предпочтений берут вверх.

Кроме того, полезно понимать предпочтения сети относительно ре-анонсирования, поскольку они также являются частью процесса попыток сети оптимизировать свое положение за счет максимизации доходов и минимизации расходов, а также прекратить «бесплатную езду», при которой ресурсы сети используются нефинансируемым трафиком.

Для выполнения этой задачи большинство сетей использовало следующие базовые правила распределения анонсов:

- маршруты, о которых стало известно от клиента, анонсируются клиентам, пирам и провайдерам;
- маршруты, о которых стало известно от пира, анонсируются клиентам, но не другим партнерам или провайдерам;
- маршруты, о которых стало известно от провайдера, анонсируются клиентам, но не другим провайдерам или пирам.

Эти правила схематично показаны на рисунке ниже. Крестиками отмечены недопустимые анонсы.



Что произошло?

Теперь давайте возвратимся в 12 июня и посмотрим на то, что случилось. Совершенно определенно что-то произошло, как это можно увидеть на приведенных ниже двух графиках. Первый представляет собой почасовой график общего количества префиксов, объявленных в таблице маршрутизации Интернета (рис.1).

Это выглядит так, будто в систему маршрутизации были добавлены дополнительные 2500 маршрутов, а затем через пару часов примерно 5500 маршрутов были отозваны, после чего 2500 маршрутов были восстановлены, оставив в таблице маршрутизации примерно на 500 маршрутов меньше по сравнению с исходным состоянием.

Похожая картина становится очевидной при взгляде на обновления в BGP за тот же самый период, в рамках которого изменение в размере таблицы BGP совпало с соответствующим взрывом в операциях обновления BGP. Смотреть рисунок 2.

Этот взрыв активности имел своим источником AS4788 – сеть, которую эксплуатирует компания Telekom Malaysia.

Telekom Malaysia – это относительно крупный провайдер в Малайзии. Клиентская база этой компании составляет примерно 15 миллионов пользователей из своей собственной сети, кроме того, она предоставляет транзитные услуги 64 другим сетям, большая часть из которых базируется в Юго-Восточной Азии. Эта сеть также, по-видимому, соединена с 13 восходящими (более крупными) провайдерами. Восходящие провайдеры и количество префиксов, видимых через каждого провайдера с пункта наблюдения, расположенного в Австралии в AS131072, имеют следующий вид: Смотреть таблицу 1 (*По-видимому это некий вид ошибки маршрутизации)

Рис.2. Активность обновления маршрутизации: неделя, начинающаяся с 9 июня 2015 г.

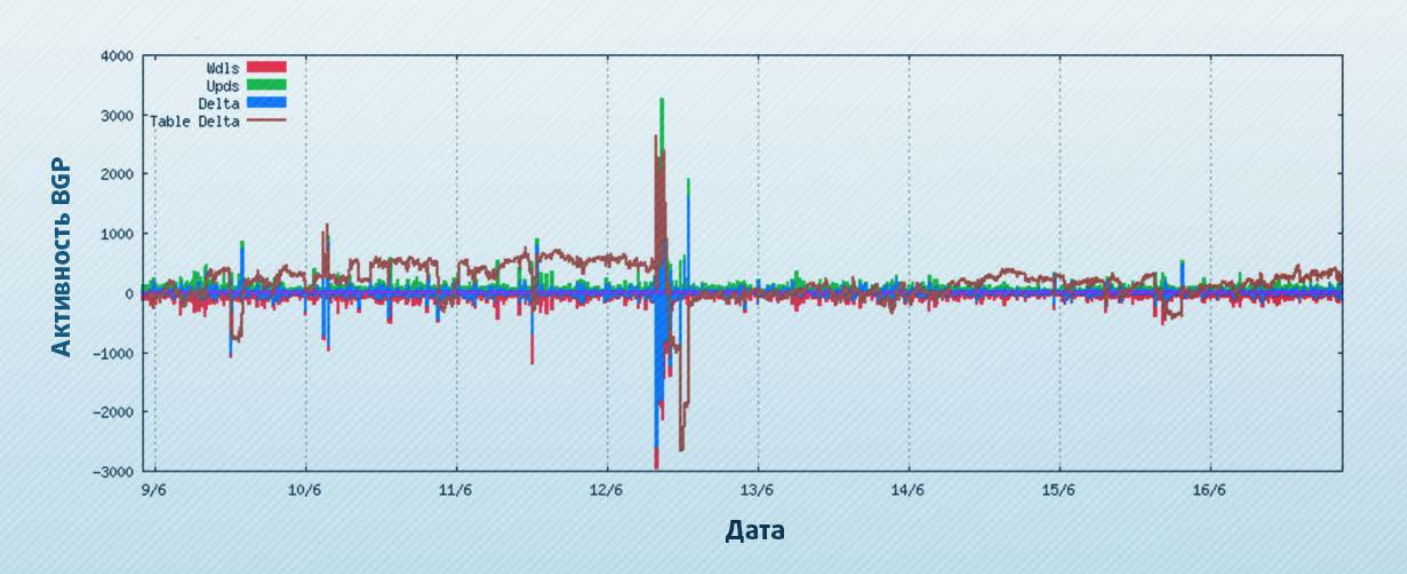


Таблица 1. Провайдеры транзита и количество префиксов

AS3320	DTAG Deutsche Telekom AG, DE (7 префиксов)
AS3356	LEVEL3 - Level 3 Communications, Inc., US (1 префикс)
AS4637	ASN-TELSTRA-GLOBAL Telstra Global, HK (1,131 префиксов)
AS9304	HUTCHISON-AS-AP Hutchison Global Communications, HK (1 префикс)
AS24115	ASN-EQIX-MLPE Equinix, HK (1,296 префиксов)
AS6453	TATA COMMUNICATIONS (AMERICA) INC, US (2 префикса)
AS2516	KDDI KDDI CORPORATION, JP (2,074 префиксов)
AS18206	VPIS-AP VADS Managed Business Internet Service Provider, MY (1 префикс *)
AS1273	CW Cable and Wireless Worldwide plc, GB (183 префиксов)
AS3257	TINET-BACKBONE Tinet SpA, DE (179 префиксов)
AS1299	TELIANET TeliaSonera AB, SE (3 префикса)
AS6939	HURRICANE - Hurricane Electric, Inc., US (2,222 префиксов)
AS17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited, PK (15 префиксов)

Подобно многим другим ISP с большим набором восходящих провайдеров, Telekom Malaysia использует метод анонсирования более детальных маршрутов для управления нагрузкой трафика через различные межсетевые соединения. В данном случае компания Telekom Malaysia взяла 56 блоков адресов IPv4, которые она получила от своей локального Регионального Интернет-регистратуры и анонсировала примерно 2.200 отдельных префиксов, в основном используя префиксы /24 («more specifics» – более детальные префиксы, которые имеют приоритет в маршрутизации BGP), извлеченные из изначальных блоков адресов. Анонсирование 1.144 более детальных префиксов делает Telekom Malaysia одним из крупнейших генераторов таких префиксов в современном Интернете, но отнюдь не самым крупным. Этот подход, который заключается в регулировании трафика, передаваемого по различным физическим соединениям, при помощи выборочного анонса более детальных префиксов, может быть общей практикой, однако он по-прежнему остается сложным. И конечно, сложные подходы часто превращаются в эксплуатационно хрупкие способы и методы реализации, которые имеют склонность к поломкам.

И это именно то, что случилось 12 июня с Telekom Malaysia.

То, что увидел остальной мир, было всплеском анонсов маршрутов, источником которого стала сеть AS4788, включая примерно 2500 новых префиксов, которых раньше не было. Через пару часов случился крупномасштабный отзыв примерно 5500 префиксов, после чего состоялась стабилизация с повторным объявлением около 2500 префиксов, согласно показанному на рис. 3.

Если мы посмотрим на сеть AS4788 и взглянем на обновления, поступающие из этой Автономной системы, то их можно разбить на префиксы, порожденные самой сетью AS4788, и префиксы, для которых AS4788 является транзитным провайдером. График анонсов для AS4788 за 12 июня показывает быстрый рост активности в 08:43, который продолжается 9 минут.

Большая часть этой активности по обновлению маршрутов имела место в виде анонсов маршрутов, в которых сеть AS4788 была транзитной AS, а не новых маршрутов от самой AS4788.

Так что же произошло? Существуют два главных вида утечки маршрутов: один, при котором сеть импортирует узнанные через eBGP маршруты в одной части своей сети и преобразовывает внутренние маршруты в экспортируемые eBGP маршруты в другой части сети. Маршруты, которые по ошибке обрабатываются таким образом, видятся другим сетям, как будто они берут начало в этой сети. Другой вид утечки заключается в том, что полученные через eBGP маршруты из одной сети-пира по ошибке экспортируются другому пиру. В этом случае внешнее представление заключается в том, что утекшие маршруты указывают на эту сеть как на транзитную.

В случае данной конкретной утечки мы видим утечку транзитных маршрутов, при которой сеть AS4788 ошибочно аннонсировала маршруты, узнанные от одного пира, другому пиру.

Какие маршруты были при этом затронуты? Список, включающий все 22.577 маршрута, слушком длинный, чтобы приводить его здесь, однако давайте взглянем на набор соседних Автономных систем, чьи маршруты, по-видимому, повторно аннонсировались сетью AS4877 в течение этого периода. В таблице 2 приведены верхние 20 строк списка, увиденные с наблюдательного пункта BGP, расположенного в сети AS4777 в Японии.

Этот список сильно отличается от списка провайдеров транзита, который приведен в таблице 1. Вероятная причина заключается в том, что сеть AS4788 присутствует в целом ряде точек обмена (трафиком) и принимает большое число маршрутов из этих точек обмена. В ходе этого инцидента с маршрутами сеть AS4788 переаннонсировала эти полученные маршруты обратно провайдерам транзитам. Для маршрутов, транзитный путь которых через AS4877 являлся более коротким, этот альтернативный путь был выбран этими транзитными сетями и распространен дальше их собственным пирам.

Теперь мы, вероятно, достаточно близки к тому, чтобы понять, что произошло 12 июня внутри сети AS4788. В рамках приведенного выше «букваря» маршрутизации говорилось, что, как показывает опыт, существуют три руководящих принципа маршрутизации:

- маршруты, о которых стало известно от клиента, анонсируются клиентам, пирам и провайдерам;
- маршруты, о которых стало известно от пира, анонсируются клиентам, но не другим партнерам или провайдерам;
- маршруты, о которых стало известно от провайдера, анонсируются клиентам,

Таблица 2. Утечка транзитных маршрутов

Префиксы	ASN	Описание
5,545	6695	DECIX-AS DE-CIX Management GmbH, DE
3,699	9394	CTTNET China TieTong Telecommunications Corporation, CN
3,381	1273	CW Cable and Wireless Worldwide plc, GB
1,594	4788	TMNET-AS-AP TM Net, Internet Service Provider, MY (объявленные префиксы)
818	8359	MTS MTS OJSC, RU
781	38285	M2TELECOMMUNICATIONS-AU M2 Telecommunications Group Ltd, AU
643	2119	TELENOR-NEXTEL Telenor Norge AS, NO
561	3209	VODANET Vodafone GmbH, DE
422	8708	RCS-RDS RCS & RDS SA, RO
365	17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited, PK
260	16150	PORT80-GLOBALTRANSIT Availo Networks AB, SE
242	12552	IPO-EU IP-Only Networks AB, SE
241	23520	COLUMBUS-NETWORKS - Columbus Networks USA, Inc., US
220	3741	IS, ZA
186	4635	HKIX-RS1 Hong Kong Internet Exchange--Route Server 1, HK
162	41095	IPTP IPTP LTD, NL
153	5588	GTSCE T-Mobile Czech Republic a.s., CZ
147	2647	SITA Societe Internationale de Telecommunications Aeronautiques, FR
144	8426	CLARANET-AS ClaraNET LTD, GB
143	2686	ATGS-MMD-AS - AT&T Global Network Services, LLC, US

но не другим провайдерам или партнерам.

Судя по всему, сеть AS4877 переанонсировала маршруты, которые она получила от пиров (возможно от DECIX), своим провайдерам транзита, осуществив своего рода «захват» маршрутов. По-видимому, это произошло из-за ошибки конфигурации политики маршрутизации в маршрутизаторе eBGP внутри сети AS4877.

Предотвращение

Этот вид утечки маршрутов не является редкостью. Однако когда это происходит, последствия могут быть крайне разрушительными. Можно ли предотвратить такую утечку?

RPKI?

Сегодня мы слышим много рассуждений об инфраструктуре открытых ключей для ресурсов нумерации (Resource Public Key Infrastructure, RPKI) и объектов авторизации маршрутов (Route Origination Authorisations, ROA). Если бы соседи сети AS4877 по eBGP внедрили управление фильтрацией на основе ROA, то предотвратили бы эту утечку маршрутов?

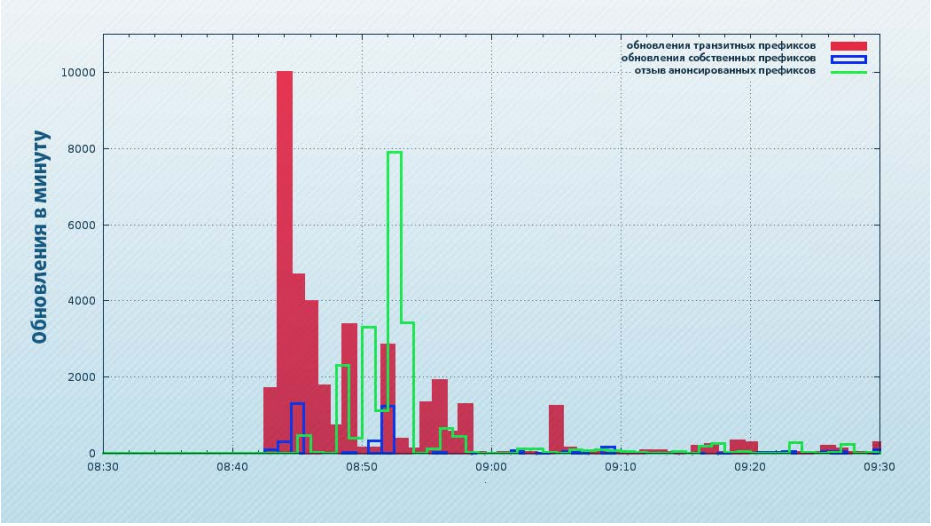
Объекты ROA удостоверяют источник маршрута и не дают неавторизованным Автономным системам инициировать маршрут для префикса. В нашем случае из 22 577 утекших маршрутов только 1594 имели своим началом сеть AS4877. Это означает, что в лучшем случае механизм фильтрации маршрутов на основе ROA – если бы он был внедрен всеми пирами AS4877 и всеми держателями префиксов – был бы эффективен при отфильтровывании только 7% утекших маршрутов. Проблема же заключается в том, что утекала информация о транзите, поэтому фильтры, базирующиеся на определении происхождения (маршрутов), оказались бы, в основном, не эффективны.

Если это так, то что произойдет, когда мы реализуем защиту пути следования AS-PATH? Что если все соседи сети AS4877 внедрили бы полный пакет BGPSEC и применили валидацию пути для всех маршрутов, полученных от AS4877. Наверняка это позволит обнаружить проблему и отклонить утекшие маршруты. Да?

Нет.

Если вы получаете маршрут с AS-PATH: A B C и источник в AS C был проверен, то единственным способом, с помощью которого вы можете определить, что этот маршрут является ненамеренной утечкой по сравнению с обычной работой BGP, это не просмотр того, как работает протокол сам по себе, а изучение намерений в политике маршрутизации сетей A, B и C и определение того, является ли, согласно наблюдениям, поведение пути следования AC намеренным в рамках политик маршрутизации этих сетей. Однако защищенный протокол BGP не содержит информации о политиках маршрутизации. Защищенный протокол BGP может позволить вам проверить, что держатель префикса уполномочил C на инициацию маршрута, а это он и делает. Защита пути в рамках защищенного BGP может также позволить вам проверить, что сеть C передала объявление в сеть B, которая, в свою очередь, передала его в A. Поэтому с точки зрения безопасного BGP в этом маршруте нет ничего недопусти-

Рис.3. Активность обновления маршрутизации: AS4788 0830 – 09:30, 12 июня



мого. BGPSEC не может информировать вас о том, является ли это намеренным объявлением маршрута или неавторизованной утечкой маршрута.

Поэтому сервис RPKI здесь не поможет. Нет ничего «неправильного» в работе протокола маршрутизации BGP как такового, и не было и умышленных попыток фальсифицировать информацию о маршрутизации. Проблема заключается в том, что информация о маршрутизации, которая в остальном является правильной, была переанонсирована соседям, которые не ожидали услышать об этих маршрутах. Клиент сети переанонсировал транзитные маршруты, и без наличия дополнительных знаний о концепциях политики маршрутизации, таких, как «транзит», «клиент» и «пир», система маршрутизации не может автоматически обнаружить такие пробелы в целостности предполагаемой политики маршрутизации.

Реестры маршрутов?

Использование Реестров интернет-маршрутизации (Internet Routing Registries) и связанного с ними Языка спецификаций политики маршрутизации (Routing Policy Specification Language, RPSL) (RFC 2622, RFC4012) является альтернативным подходом к ручному управлению фильтрами маршрутов. RPSL – это относительно богатый язык, он, как говорит его название, позволяет пользователю описывать политики импорта и экспорта сети в терминах взаимоотношений с соседними Автономными системами и ее политики транзита (переанонсирования).

Использование таких описаний в контексте реестра маршрутизации позволяет оператору сети перечислить все префиксы, инициированные локальной Автономной системой, и политики транзита, которые связаны с этими маршрутами. Кроме того, это позволяет оператору сети описать свои политики анонсирования, задав соседние AS и политики маршрутизации для маршрутов, полученных от соседних AS.

Если бы каждая Автономная система поддерживала точный, актуализированный и полный набор префиксов и записей политики маршрутизации в Реестре интернет-маршрутизации, то, по-видимому, для AS было бы теоретически возможным сгенерировать набор фильтров префиксов и AS-PATH для всех своих соседей путем поиска в рамках всего содержимого реестра. И действительно, существуют инструменты, которые пытаются сделать именно это для существующих реестров маршрутов.

Тогда почему мы все не делаем именно это? Почему мы не используем эти инструменты для реестра маршрутов как часть стандартной процедуры эксплуатации?

История использования реестров маршрутов вызывает очень смешанные чувства.

Эти реестры существуют в той или иной форме вот уже на протяжении почти двадцати лет. Некоторые регионы мира очень усердно принуждали каждого сетевого оператора своего региона вести точную информацию в локальных реестрах маршрутизации. Однако в других случаях история реестра маршрутов не была столь обнадеживающей.

RPSL – это сложный язык, с его помощью может быть довольно трудно точно описать хитросплетения некоторых политик маршрутизации. Часто происходит, что реестр заполнен записями «на всякий случай», а также историческими записями, поэтому чрезвычайно трудно отсортировать то, что относится к текущим концепциям маршрутизации от других посторонних данных. Выполнение этой задачи с помощью автоматического инструмента для сканирования реестров до сих пор оказывалось невозможным. Справедливо также и то, что сетевые операторы часто используют уровень детализации, связанный с каждым сеансом eBGP между соседними AS, тогда как RPSL использует более грубый уровень детализации – отдельные AS. Поэтому труднее описать отдельные политики маршрутизации, которые применяются к различным сеансам BGP между одними и теми же двумя AS. Кроме того, существует вопрос относительно того, насколько комфортна для сетевых операторов публикация такой детальной информации о своих политиках маршрутизации.

Используемые сегодня реестры маршрутов имеют разнообразные модели аутентичности и целостности. Во многих случаях возможно, чтобы пользователь реестра вводил информацию о маршрутизации для сторонних префиксов, не имея полномочий со стороны фактического владельца префикса. Отделение достоверной информации от недостоверной не поддерживается моделью данных реестра, которая обычно не включает в себя информацию о валидации или полномочиях. Кроме того, существует множество реестров маршрутов, и часто они содержат противоречащую информацию. Какой из реестров должен иметь приоритет, если кто-то попытается разрешить эти содержащиеся в данных противоречия? И почему?

Эта проблема достаточно сложна уже сама по себе, однако ее еще больше усугубляет тот факт, что во многих областях Интернета операторы отказались от применения реестров маршрутов и полагаются на собственные кастомизированные инструменты. Поэтому меняется не только качество информации, содержащейся в реестрах маршрутов, но и полнота этой информации.

«Безовражная» маршрутизация?

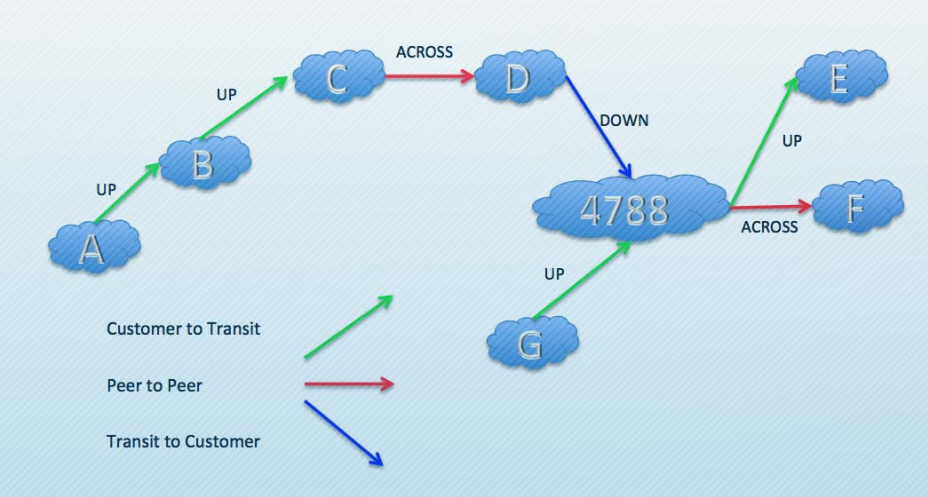
Возможно мы пытаемся быть слишком умными и используем излишне сложные инструменты для решения того, что в действительности является простой проблемой. Проблема, которая произошла в сети

AS4778, заключалась в переанонсировании маршрутов, о которых стало известно от пиров и транзитных систем, другим транзитным системам.

Принцип политики маршрутизации, целью которого является предотвращение этого вида утечки маршрутов – это концепция, получившая название «valley-free routing» — маршрутизация «без долин» или «безовражная» маршрутизация.

Если маршрут проходит из сети клиента в сеть транзитного провайдера, то этот сегмент называют «восходящим» сегментом. Если маршрут проходит пиринговое соединение, то это «пересекающий» сегмент. И если маршрут проходит из сети транзитного провайдера в сеть клиента, то это «нисходящий» сегмент. Последовательность этих маршрутных пар может начинаться с последовательности восходящих сегментов, затем самое большее один пересекающий сегмент и после этого последовательность нисходящих сегментов. Путь «безовражного» маршрута не включает нисходящий сегмент, сразу за которым следует восходящий.

Рис.4. Пример топологии между AC для маршрутизации без долин



В показанном здесь примере (рис. 4) маршрут, начинающийся в AS A, может быть распространен по пути A B C D до сети AS4788, и при этом он удовлетворяет «безовражному» ограничению. Однако после получения сетью AS4778 маршрут не может быть продолжен в E или F, поскольку это нарушит «безовражное» ограничение (эти пути формируют своего рода овраг – прим. ред). Маршрут, начатый в G, может быть продолжен в D, E и F согласно тому же принципу. Если он продолжен в D, то согласно данному принципу он может быть далее продолжен из D в C, B и A. С другой стороны, маршруты, начинающиеся из E и F, могут быть продолжены сетью AS4788 только в G, но не в D.

Такое ограничение можно относительно легко встроить в протокол BGP как атрибут транзитного сообщества, называемый UP. Если маршрут начинается с атрибутом UP, то его можно анонсировать во все соседние узлы eBGP. Однако обращение с атрибутом при продолжении маршрута зависит от отношения между сетью и соседней сетью. Если сосед является транзитным провайдером, то атрибут UP остается неизменным. Если сосед является пиром или нисходящим клиентом, то атрибут UP снимается при переходе маршрута к соседу. Если маршрут начинается без атрибута UP, то его можно передать только нисходящим соседям-клиентам.

Хотя такой механизм является простым и, несомненно, эффективным во многих сценариях, возможно, он слишком простой. В теории, каждая AS имеет единую политику маршрутизации, и все отношения Автономных систем можно однозначно классифицировать как провайдер-клиент или пиринг, однако в реальном мире присутствуют более тонкие нюансы, и отношения между AS нельзя втиснуть в эту очень простую модель.

И это весьма печально в некоторых отношениях, поскольку такой более простой мир сделал бы обнаружение и предотвращение утечек маршрутизации гораздо более легкой задачей!

Куда теперь?

Некоторые многолетние проблемы являются такими давними из-за того, что мы не сумели применить подходящий аналитический подход к их решению. Решение где-то рядом, но нужно приложить некоторые усилия по его поиску!

Мы можем в очередной раз попробовать принудить индустрию к использованию реестров маршрутов для внешней маршрутизации, однако чем будет отличаться этот призыв к использованию реестров маршрутов от всех других подобных призывов в прошлом? И если отличий не будет, то почему такой призыв встретит более радостный отклик по сравнению с тем, что случилось в прошлом?

Возможно, мы могли бы использовать цифровые подписи и RPKI, чтобы объединить аутентичность информации с реестрами маршрутов. Однако проблема, с которой мы столкнемся в этом случае, будет заключаться в том, что и так уже сложная система станет еще более сложной и трудной в использовании.

Возможно, данная конкретная проблема относится к другому типу многолетних проблем. Некоторые проблемы становятся давними просто потому, что они являются исключительно трудными проблемами!

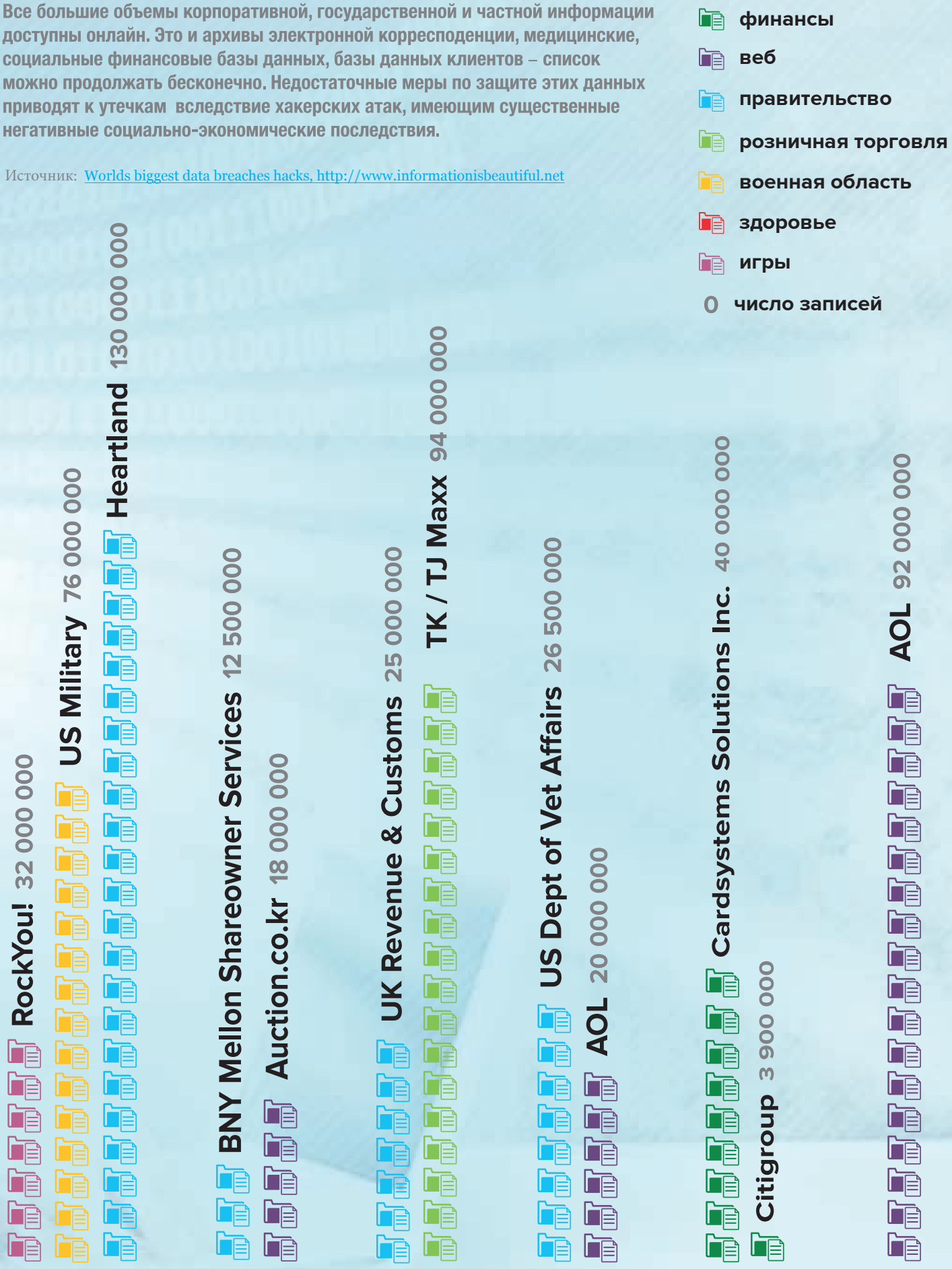
Это заставляет меня задаться вопросом, существуют ли альтернативные перспективы в той области, в которой мы работаем. Например, не стали бы мы рассматривать эту проблему по-другому, если бы думали о маршрутизации не как об инструменте топологии и достижимости, а как о распределенном алгоритме для решения системы уравнений. Уравнения здесь выражают политики маршрутизации, а целью алгоритма является нахождение решений, которые решают отдельные уравнения, а также нахождение общесетевого решения максимальной связности. Будет ли такая перспектива обеспечивать получение отличающихся выводов относительно способа, в рамках которого взаимодействуют политики и протоколы маршрутизации? И может ли такая перспектива обеспечить получение предложений относительно того, каким образом мы можем защитить систему маршрутизации не только от умышленных злоупотреблений и неправомерных действий, но от несчастных случаев в форме утечек маршрутов?

Источник: “More Leaky Routes” . Geoff Huston. The ISP Column

Крупнейшие случаи утечки данных за последнюю декаду

Все большие объемы корпоративной, государственной и частной информации доступны онлайн. Это и архивы электронной корресподенции, медицинские, социальные финансовые базы данных, базы данных клиентов – список можно продолжать бесконечно. Недостаточные меры по защите этих данных приводят к утечкам вследствие хакерских атак, имеющим существенные негативные социально-экономические последствия.

Источник: Worlds biggest data breaches hacks, http://www.informationisbeautiful.net



TLS: двадцать лет спустя

Александр Венедюхин

Группа технологий TLS - самый распространённый инструмент защиты информации в современном Интернете. При помощи TLS защищают не только веб-трафик, но и электронную почту, а также целый ряд других сервисов, в том числе, трафик мобильных приложений. Технологии защиты информации — интересный, бурно развивающийся сектор интернет-технологий, относящийся к фундаменту глобальной Сети. Например, без TLS невозможна работа банковских онлайн-сервисов, однако в современной ситуации защищённый протокол необходим для всякого веб-сайта. Успешное внедрение TLS требует понимания архитектуры протокола.

В 90-х годах прошлого века, вместе с приходом веба, Интернет стал активно превращаться в транспорт для коммерческой активности. Неотделимым элементом этой активности являлась необходимость совершения различных финансовых и околофинансовых транзакций. Подобные транзакции не могут проводиться без средств защиты информации, а традиционный веб был полностью открыт - не только открыт для прослушивания, но и вообще никак не защищён. Так появился первый прототип технологии, которую сейчас называют TLS/SSL (Transport Layer Security / Secure Sockets Layer). Сейчас оба варианта обозначения - TLS и SSL - могут использоваться в качестве синонимов, но каноническим является имя TLS. Аббревиатура TLS появилась в качестве замены обозначения SSL после того, как протокол окончательно стал интернет-стандартом.

То, что первоначальным предназначением TLS являлось всего лишь получение более или менее безопасного канала коммерческих онлайн-транзакций, а не передача секретной информации, никак не помешало этой технологии превратиться в краеугольный камень современного здания пользовательской «приватности» и «безопасности» в сети. Самым распространённым, с точки зрения пользователя, применением TLS сейчас является защищённый веб-протокол HTTPS. На него сейчас принято полагаться даже в случае обмена критически важной информацией, причём не только информацией рядового пользователя: HTTPS (и, соответственно, TLS) нынче приходится встречать и в промышленных системах управления (SCADA), где от надёжности протоколов зависит работоспособность технологического оборудования.

Новая, весьма популярная тема - Интернет вещей: предполагается, что в обозримом будущем едва ли не каждый предмет человеческого быта превратится в «интеллектуальное устройство», которое будет взаимодействовать с различными глобальными информационными системами, в том числе, с другими интеллектуальными предметами быта. Выстроить такую систему без инструментов защиты информации вряд ли возможно, так что распространённость TLS только увеличится - недалёк тот замечательный день, когда TLS придёт не только в ваш смартфон и телевизор, как сейчас, но и в зубную щётку, и в кроссовки. Следующая версия базового протокола веба — HTTP/2, — которая близка к финальной стадии разработки, также будет включать TLS по умолчанию. Более того, в HTTP/2 средства установления защищённого соединения непосредственно встроены в протокол, что составляет одно из ключевых отличий от HTTP. Заметьте, TLS используется и в электронной почте. Иными словами — без TLS нынче нельзя и шагу ступить. Если, конечно, ходить безопасно.

Впервые SSL реализовали в качестве проприетарной технологии в браузере Netscape Navigator, одном из первых веб-браузеров. Первая версия протокола никогда не была официально опубликована. Она так и осталась внутренней разработкой Netscape, развивавшейся в 1994-95 годах. Спецификация SSLv2 - следующая, вторая версия - из-за обнаруженных дефектов и организационных накладок (кроме прочего, связанных с патентами и интеллектуальной собственностью) так и не вышла из состояния черновика (draft). Более того, хоть в SSLv2 и скорректировали отдельные дефекты и уязвимости v1, протокол всё равно оказался изначально ненадёжным, по причине наличия целого ряда архитектурных недочётов. Необходимо подчеркнуть, что это вполне нормальная - для открытых интернет-протоколов - эволюция: рекомендации постепенно улучшались, так сложилось исторически. Процесс улучшения, идущий с переменным успехом, не прекращается до сих пор. Иногда можно услышать мнение, что если бы SSL разрабатывали только инженеры специальных служб США, то сразу был бы получен качественный протокол. Но, во-первых, АНБ и так приложило руку к становлению TLS, а во-вторых, веб всё же был слишком новым направлением, чтобы кто-то мог гарантировано выдать безошибочный рецепт защищённого протокола. Ведь некоторые специалисты в 90-х годах всерьёз полагали, что в Интернете можно без изменения использовать механизмы защиты, подобные четырёхзначным PIN-кодам банкоматов. Кроме того, становление первых версий SSL пришлось на период так называемых криптовойн (их второй эпохи), когда правительство США активно регулировало развитие общедоступных технологий защиты информации, вводя разнообразные «экспортные ограничения» и прочие препоны.

Эти «экспортные ограничения» из 90-х годов прошлого века аукнулись TLS не далее чем в 2015 году, двадцать лет спустя:

использование заведомо небезопасных алгоритмов в паре с древним архитектурным дефектом протокола - обеспечили наличие долгоиграющей уязвимости, ставшей в 2015 году широко известной как Logjam.

SSLv2 давно (более 15 лет назад) и без оговорок признан небезопасным, поэтому сейчас не должен использоваться: если в 2015 году ваш сервер или клиент всё ещё поддерживает SSLv2, можно смело сказать, что у вас нет безопасного канала.

Протокол SSLv3 — первая версия SSL, получившая полноценную спецификацию RFC, правда, в статусе исторического документа и значительно позже появления самого протокола: RFC 6101. Именно на время SSLv3 пришлось становление TLS как полноценной интернет-технологии. SSLv3 в 2015 году «официально» перешёл в статус не рекомендуемых: в июне этого года выпущен документ RFC 7568, требующий исключить SSLv3 из разряда поддерживаемых клиентами и серверами протоколов. Теперь остались только версии TLS.

Для всех трёх версий TLS есть полноценные RFC (RFC 2246, RFC 4346, RFC 5246), кроме того, многие аспекты применения TLS описаны в других, дополнительных RFC. В общей сложности, только ядро важнейших для TLS RFC насчитывает сейчас более дюжины документов (в этой популярной статье мы не будем их все перечислять). К сожалению, местами эти документы не очень прозрачны и однозначны в своих рекомендациях, а кроме того, они насыщены взаимными уточнениями и исправлениями. TLS - весьма непростая технология. Это считается её главным недостатком, так как сложность в системах защиты информации всегда ведёт к ошибкам и уязвимостям.

Существенное влияние на текущее состояние дел оказывает практика реализации TLS. Прежде всего — в браузерах, именно они, вместе с крупнейшими по веб-трафику сервисами, служат тем локомотивом, который вытягивает из туннеля всё новые и новые вагоны-дополнения. Нередко стандартным становится отступление от рекомендаций RFC. Показательным примером является порядок SSL-сертификатов в ответах TLS-серверов: RFC предписывает строгий порядок следования — от серверного сертификата к сертификатам удостоверяющего центра. Однако на практике не все серверы этот порядок соблюдают. Обычно - из-за незнания тонкостей протокола администратором, или просто по ошибке. Требования RFC, это, конечно, хорошо, но распространённые браузеры успешно игнорируют неверный порядок сертификатов, пытаясь проверить на возможность валидации все их перестановки. Казалось бы, такая мягкая практика — весьма полезна. И это действительно так. Однако многие, так сказать, TLS-пуристы, настаивают, что в криптографии важна именно строгость, до последнего бита — иначе можно собрать кучу проблем.

Слои, шифры и контекст

Как работает TLS? Прежде всего, нужно договориться о контексте этой работы (понятие контекста, кстати, является важнейшим и для самого протокола, так что мы не зря его упомянули). Протокол TLS предназначен для создания между двумя узлами сети защищённого от прослушивания и подмены канала связи, пригодного для передачи произвольных данных в обоих направлениях (шифрование и аутентификация сообщений). TLS также должен позволять провести проверку того, что обмен данными происходит между именно теми узлами, между которыми и планировался (аутентификация узлов). Для работы TLS требует существующего между узлами «потокового» соединения (однако есть «диалект» под названием DTLS, который предназначен для работы в режиме негарантированной доставки пакетов, без потокового соединения, например, по UDP; но DTLS мы не рассматриваем).

Таблица 1. Таблица уровней работы TLS: от пользователя (наверху) — к физическому каналу (внизу)

Пользователь, смотрящий в окно браузера или запустивший почтовый клиент.
...
Приложения: HTTP(S), IMAP, POP3, SMTP и др.
TLS-сообщения: здесь, грубо говоря, происходит установление TLS-соединения.
TLS-записи: здесь передаются защищённые TLS блоки данных.
TCP: это транспорт для блоков данных TLS, обеспечивающий доставку и формрование канала между узлами.
IP: базовый транспортный протокол Интернета.
...
Физическая среда распространения сигнала: например, оптоволокно.

TLS предполагает, что между узлами установлено относительно надёжное соединение, поэтому, например, протокол TLS не охватывает повторную отправку потерянных пакетов данных. Обычно TLS работает поверх TCP. Последний позволяет надёжно обмениваться данными, но содержимое пакетов (за исключением специальных случаев) может быть легко прочитано, если у третьей стороны есть доступ к каналу связи. Кроме пассивного прослушивания, TCP позволяет легко заменить сами пакеты, а также частично подменить передаваемые в них данные. Именно для защиты от этих угроз и используется TLS.

В TLS есть своя иерархия уровней протокола (таблица 1), там используются два «слоя»: нижний — это уровень *TLS-записей*, где передаются данные. Записи проще всего представлять как блоки данных, имеющие установленный формат. Шифрование, коды аутентификации — явления этого, нижнего слоя. Уровнем выше — другой слой: здесь расположились управляющие логические конструкции, состоящие из последовательностей *TLS-сообщений*, отвечающих за установление защищённого канала и за контроль его успешной работы. Ниже мы практически не касаемся уровня TLS-записей, а больше говорим о том, что происходит на уровне сообщений. Сообщения, конечно, также имеют установленный формат.В целом, при использовании TLS предполагается, что атакующий может как угодно вме-

шиваться в канал связи, в том числе активно подменять пакеты. Задачи TLS состоят в обеспечении трёх ключевых моментов:

- конфиденциальность, то есть защита от утечек передаваемой информации;
- обнаружение подмены, то есть сохранение целостности передаваемой информации;
- аутентификация узлов, то есть обеспечение проверки подлинности узлов, обменивающихся информацией.

TLS пытается решить перечисленные задачи, но с некоторыми «граничными условиями». И у нас нет никаких оснований полагать, будто TLS решает данные задачи полностью. Это важнейший момент практического применения TLS. Нередко приходится слышать, что TLS полностью обеспечивает и конфиденциальность, и целостность, и аутентификацию. Но такая оценка является большой ошибкой. Да, протокол и его реализации пытаются решить описанные задачи, однако TLS в целом не обладает доказанной стойкостью, как не обладают ей и многие важнейшие составляющие части протокола. Косвенным результатом этого является тот поток уязвимостей, который устремился на страницы технической прессы, как только за протокол взялось большое количество опытных исследователей. Верна такая рекомендация: не следует доверять TLS и связанным технологиям свою жизнь или жизнь других людей.

Строго говоря, TLS позволяет обмениваться информацией в открытом виде. Такое решение встречается крайне редко, но оно возможно. Может показаться, что смысла в таком канале нет. Это не так: исключение шифрования не отменяет использования аутентификации узлов и кодов аутентификации сообщений. То есть открытый вариант TLS-соединения будет защищать от подмены данных и позволит узлам проверить подлинность друг друга.

Вернёмся к контексту. В TLS для успешного обмена данными узлы должны находиться в одном контексте, это означает, что они успешно согласовали целый ряд криптографических параметров, среди которых исходные данные для выработки сеансового ключа шифрования, используемый шифр, код аутентификации сообщений и другие. Часть этих параметров объединяется спецификациями в типовой, фиксированный набор: Cipher Suite, или, на русском, — шифронабор. Шифронабор — важнейшая составляющая практики использования TLS. Шифронабор определяет криптосистемы, которые применяются при обмене информацией в данном сеансе. В шифронабор входят: криптосистема электронной подписи, симметричный шифр, алгоритм дайджеста сообщений (хеш-функция).

Шифр — это некоторый набор обратимых преобразований данных, каждое из которых определяется параметром, обычно называемым ключом шифрования. Также важен порядок применения этих преобразований, который принято называть режимом шифрования. Криптосистемой называют конструкцию более высокого, относительно шифра, уровня. Простейшая криптосистема может включать лишь один шифр, то есть, грубо говоря, состоять из одного алгоритма шифрования и (обратного к нему) алгоритма расшифрования.

В современной криптографии известны два типа криптосистем: симметричные и асимметричные (к последним относятся и криптосистемы с открытым ключом, например, RSA). В симметричных системах знание шифрующего ключа позволяет легко получить расшифровывающий ключ, то есть расшифровать секретное сообщение. В используемых сейчас массовых симметричных криптосистемах шифрующий и расшифровывающий ключи просто совпадают. Другими словами, симметричные системы подразумевают, что обе стороны, обменивающиеся информацией по закрытому каналу, знают некий общий секрет — например, секретный симметричный криптографический ключ, который позволяет как шифровать, так и расшифровывать сообщения. Этот секрет, вместе с тем, не должен быть известен прослушивающей канал стороне: иначе эта сторона сможет легко расшифровать сообщения.

Примерами симметричных криптосистем являются как наивные исторические шифры — например, шифры простой замены букв текста на естественном языке, где в качестве ключа может выступать та или иная перестановка алфавита, - так и современные шифры, вроде AES и 3DES. Базовая идея современных симметричных криптосистем, используемых на практике, состоит в «перемешивании» символов открытого текста: традиционно такими символами являются биты. Ключом в массовых современных симметричных криптосистемах является целое число достаточно большой разрядности — 128 бит и более. Основной объём зашифрованного трафика в Интернете шифруется именно симметричными криптосистемами. Главной проблемой использования симметричных криптосистем является распределение ключей: очевидно, ключ не может быть передан по открытому каналу, а для организации защищённого канала — нужен ключ.

Асимметричные криптосистемы не позволяют простым способом получить из шифрующего ключа расшифровывающий. То есть сторона, знающая шифрующий ключ, может только зашифровать некоторое сообщение, но не может прочитать другие зашифрованные сообщения. Применительно к асимметричным криптосистемам принято говорить о паре ключей: открытом и секретном. Отсюда другое название асимметричных систем — системы с открытым ключом. Открытый ключ является шифрующим. Секретный — позволяет расшифровать сообщение. Асимметричные криптосистемы — новое изобретение, они появились в 70-х годах прошлого века. Поэтому наивных и исторических примеров здесь нет, а примером современной распространённой криптосистемы является RSA. Фундаментальной идеей современных асимметричных криптосистем является однонаправленная функция, имеющая «секретный ход», который позволяет эту функцию обратить, если известен дополнительный параметр. Однонаправленная (односторонняя) функция позволяет легко вычислить «зашифрованный» блок, но не позволяет простым способом выполнить обратную операцию — найти аргумент по известному зашифрованному блоку. «Секретный ход» однонаправленной функции позволяет найти аргумент, то есть расшифровать блок, но требует использования дополнительного параметра — таким параметром и является секретный ключ. Так, в случае с криптосистемой RSA, однонаправленной функцией является возведение в фиксированную степень (называемую шифрующей экспонентой) в некотором алгебраическом кольце, а секретным параметром, позволяющим обратить операцию, является знание обратного к шифрующей экспоненте показателя степени — расшифровывающей экспоненты. Таким образом, в криптосистеме RSA открытый ключ состоит из модуля (числа, задающего кольцо, в котором производятся операции) и шифрующей экспоненты; секретный ключ - из секретной экспоненты (модуль используется тот же).

Также различают блочные и потоковые шифры. Блочный шифр, как нетрудно догадаться по названию, работает с блоками входных данных фиксированной длины; он требует разбиения открытого текста на подходящие блоки. Потоковый шифр — работает с непре-

рывным потоком входных данных, без разбиения на блоки. Существуют режимы шифрования блочных шифров, по сути, превращающие их в потоковые.

Необходимо различать шифры, предназначенные для сокрытия информации, и системы электронной подписи, предназначенные для аутентификации, установления подлинности информации и/или её источника. Криптосистема RSA, как и всякая криптосистема с асимметричным шифром, может быть использована и в качестве шифра, и в качестве системы электронной подписи. Однако другие системы электронной подписи не могут служить шифрами. К таким системам относится ECDSA — современная система, работающая на эллиптических кривых.

В сеансе TLS обычно используется минимум две криптосистемы: одна из них - это система электронной подписи, вторая — симметричная криптосистема. Первая необходима для того, чтобы узлы смогли выработать общий секретный ключ. Передаваемые же данные шифруются симметричной системой. Дело в том, что симметричные шифры работают несравнимо быстрее асимметричных (то есть RSA), поэтому применять ту или иную систему с открытым ключом для шифрования потока данных - неэффективно.

Взглянем на шифронаборы, используемые в TLS, чуть подробнее. Криптосистема электронной подписи служит для аутентификации сервера и выработки общего для узлов секретного ключа симметричной системы: подробнее об этом рассказано ниже. Симметричная криптосистема (обычно это блочный шифр, используемый в том или ином режиме) обеспечивает шифрование потока данных. Код аутентификации сообщений (MAC) служит для проверки целостности, он позволяет определить, что данные не изменялись в процессе передачи.

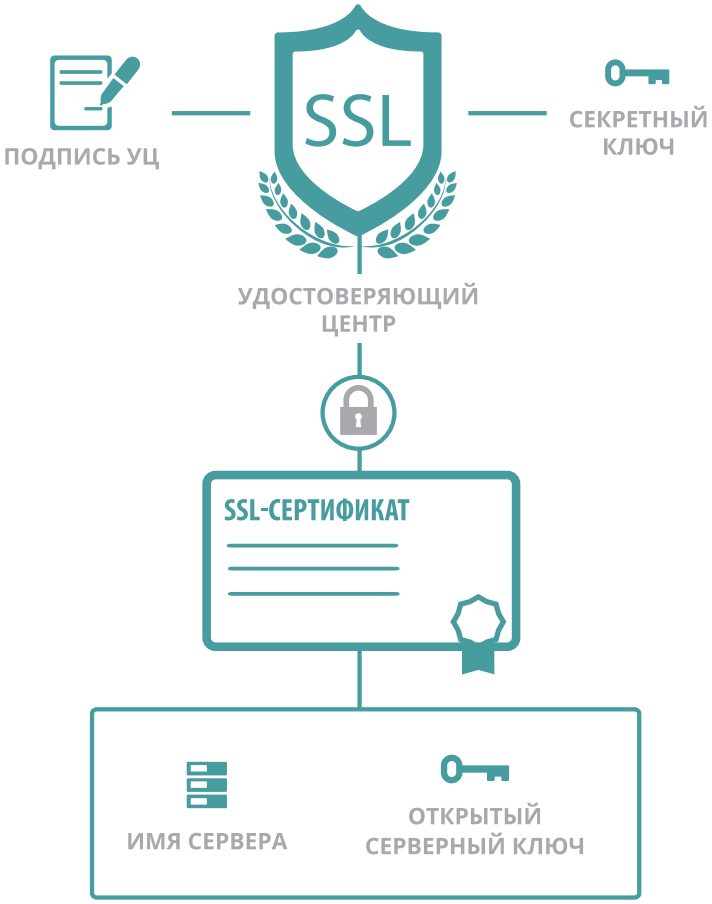
Типовые шифронаборы находятся в реестре, который ведёт IANA, а обозначаются специальной строкой символов. Например, TLS_RSA_WITH_AES_128_CBC_SHA означает, что будет использована криптосистема RSA для передачи сеансового ключа, AES со 128-битным ключом в режиме CBC в качестве симметричного шифра, SHA-1 в качестве хеш-функции HMAC. Современной рекомендацией является использование шифров в режиме аутентифицированного шифрования (AEAD), из доступных вариантов - это AES в режиме GCM. Особенностью этого режима шифрования является то, что механизм аутентификации встроен в алгоритм применения блочного шифра, поэтому дополнительный код аутентификации сообщению не требуется.

Выбор шифронабора является ключевым действием для обеспечения надёжности защиты канала TLS. Ненадёжная криптосистема делает канал слабо защищённым, даже если все другие параметры выбраны верно. Очевидно, что слабый шифр (например, DES с

Другой важнейший протокол, используемый в TLS, это протокол Диффи-Хеллмана. Он не является шифром или алгоритмом электронной подписи (строго говоря, на основе протокола можно построить асимметричную криптосистему; также существует математически родственная этому протоколу система электронной подписи, но их нельзя перепутать). Этот протокол позволяет участникам обмена информацией договориться об общем секретном ключе через открытый канал связи. Задача Диффи-Хеллмана, лежащая в основе протокола, связана с алгебраической задачей дискретного логарифмирования в конечной группе — на вычислительной сложности этой задачи построена защита протокола от перехвата секретного ключа. Сейчас используются два варианта протокола — «классический» и «эллиптический». Математические операции протокола в обоих случаях эквивалентны, отличие кроется в используемых группах: «эллиптический» вариант работает на группе точек эллиптической кривой, а «классический» - на группе, в простейшем случае относящейся к более привычной из курса высшей алгебры структуре: это мультипликативная группа кольца вычетов, заданного некоторым простым числом (модулем). Мы, впрочем, оставим алгебраические подробности в стороне. В общих чертах протокол Диффи-Хеллмана может быть изложен без привлечения излишне технических подробностей.

Для того чтобы получить общий секретный ключ, стороны сначала выбирают общие параметры Диффи-Хеллмана — это модуль, задающий группу (простое число), а также некоторое число, называемое генератором, соответственно, P и G. Оба параметра открыты и могут стать известны третьей стороне. В случае с TLS действующие параметры передаются сервером в открытом виде при установлении соединения. На следующем шаге каждая из сторон выбирает собственное секретное число a (и, соответственно, b) и вычисляет значение A = G^amod P (соответственно, B = G^bmod P). Все операции проводятся по модулю P. Далее стороны обмениваются по открытому каналу значениями A, B и каждая вычисляет A^bmod P и B^amod P. Полученные значения равны, так как, из свойства степеней, A^b = (G^a)^b = B^a = (G^b)^a = G^ab. Таким образом, стороны получили общий секретный ключ G^ab. В случае TLS сервер передаёт в сторону клиента параметры Диффи-Хеллмана и свой открытый ключ (A), который удостоверяет электронной подписью (либо RSA, либо ECDSA). Удостоверение необходимо для того, чтобы активно перехватывающая канал третья сторона не могла подменить ключ на свой.

Прослушивающая канал сторона знает значения P, G, A и B. Но для того, чтобы определить значение секретного ключа, необходимо вычислить a или b, решив относительно x уравнение вида A = G^xmod P. Стоящая за решением этого уравнения задача и называется задачей дискретного логарифмирования в конечной группе. Она вычислительно сложна, если, конечно, P является достаточно большим. Сейчас для классической версии протокола рекомендуется разрядность модуля не менее 2048 бит, а для версии на эллиптических кривых — не менее 224 бит. Как упоминалось выше, отличие версии протокола на эллиптических кривых состоит лишь в арифметической структуре группы точек выбранной эллиптической кривой: на кривой групповая операция определяется совсем иначе, чем при построении кольца вычетов.



SSL-сертификат представляет собой не что иное, как небольшой электронный документ (файл) установленного формата, снабжённый электронной подписью. Вопреки расхожему мнению, сертификаты непосредственно не связаны с шифрованием, но информация из сертификата используется в процессе генерации общего секретного ключа. Предназначение SSL-сертификата — привязка некоторого открытого криптографического ключа к некоторому сетевому имени, не более того. Такая привязка, в свою очередь, обеспечивается с помощью механизма электронной подписи, удостоверяющей сертификат: удостоверение подписей реализовано при помощи иерархии удостоверяющих центров (УЦ). К этой иерархии есть много претензий, так как компрометация УЦ позволяет нивелировать многие аспекты TLS.

40-битным ключом) практически не защищает передаваемые данные от прослушивания. Но в TLS с выбором криптосистем связаны и более тонкие уязвимости. Так, уже упоминавшаяся уязвимость Logjam основана на том факте, что протокол Диффи-Хеллмана (сам по себе считающийся стойким) может использовать слабые параметры, а именно - короткий (либо некоторый типовой) модуль, задающий группу, в которой производятся операции протокола. В случае с Logjam оказывается, что третья сторона может восстановить этот ключ из-за того, что выбранные параметры криптосистемы несовершенны, а именно — используется короткий типовой модуль, заранее известный атакующему.

В шифронабор входит несколько криптографических примитивов. Из-за архитектурных особенностей TLS дефект в любом из этих примитивов приводит к тому, что сеанс связи оказывается уязвим в целом. Это ещё одна слабая сторона TLS: несмотря на достаточную сложность технологии, в ней нет некоторого логического резервирования, защищающего от ошибок, как в ряде других систем безопасности.

Установление соединения

Всякая сессия TLS начинается с установления соединения. Этот процесс представляет собой обмен специальными сообщениями между узлами. Сообщения следуют в строгой последовательности, а само установление соединения регулируется собственным протоколом (часть TLS).

Установление соединения (см. Рис1) требует обмена несколькими сообщениями:

- клиент отправляет сообщение Client Hello. Это сообщение, например, содержит список шифронаборов, которые поддерживает клиент. Кроме того, в составе Client Hello передаётся случайная байтовая строка, которая будет использована при выработке общего сеансового ключа, а также целый ряд так называемых расширений, содержащих большое число дополнительных параметров, важных для устанавливаемой TLS-сессии;

- при успешной обработке Client Hello сервер отвечает определённым набором (кортежем) сообщений, первым из которых всегда будет Server Hello. Server Hello прежде всего задаёт выбранный сервером шифронабор. Следом за Server Hello могут быть переданы сообщения, содержащие сертификаты (серверные), параметры для создания сеансового ключа и другие данные. Замыкает кортеж серверных сообщений сообщение Server Hello Done;

- если клиент принял решение продолжать установление соединения, то он отвечает своим кортежем сообщений. Этот кортеж, в частности, включает сообщение Client Key Exchange, которое служит источником сеансового ключа шифрования;

- важную часть протокола установления соединения составляют специальные сигналы Change Cipher Spec (за которыми следуют сообщения Finished) — Change Cipher Spec обозначают, что установление параметров шифрования завершено, криптографический контент согласован, а клиент (и сервер) переходят на защищённый обмен сообщениями.

- после обмена собщениями Finished начинается TLS-сессия, в рамках которой данные приложений передаются в составе

защищённых сообщений Application Data.

На этапе установления соединения узлы проводят аутентификацию и генерируют общий секретный ключ, требуемый для симметричной криптосистемы. Именно на этом этапе в игру вступает самый известный среди пользователей аспект TLS - SSL-сертификаты. Надо отметить, что SSL-сертификаты вовсе не являются необходимым элементом TLS-соединения. Протокол определяет SSL-сертификаты как опциональный фактор, который, впрочем, требуется для аутентификации сторон. Без сертификатов возможно установить только анонимное соединение (за редкими, весьма экзотическими исключениями). Анонимное соединение уязвимо для атаки типа «человек посередине».

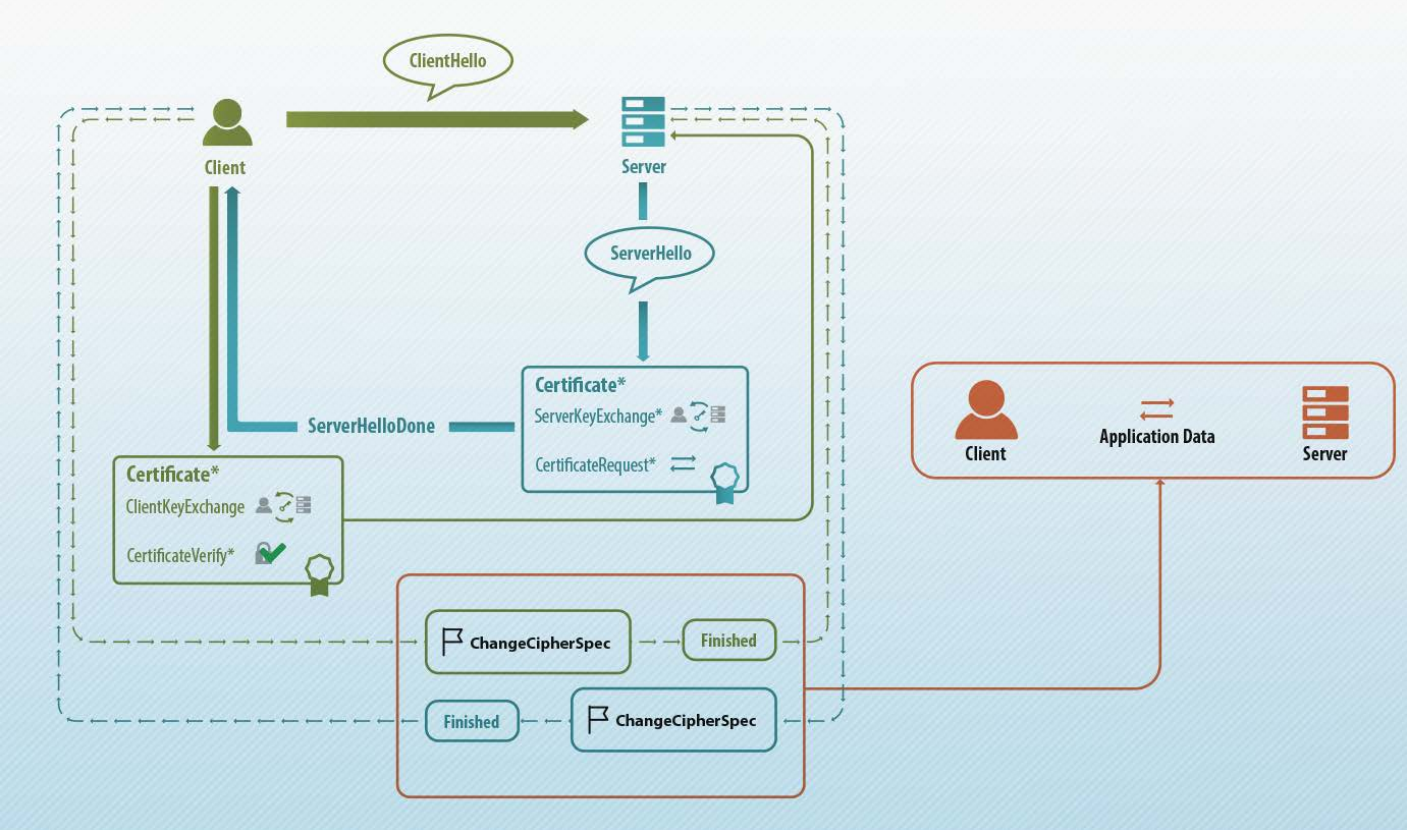
Протокол позволяет использовать два типа сертификатов: клиентские и серверные. На практике клиентские сертификаты встречаются крайне редко, а серверные необходимы для корректной работы веб-браузера по HTTPS, поэтому распространены повсеместно. Как несложно догадаться, серверный сертификат служит для аутентификации сервера клиентом.

SSL-сертификат представляет собой не что иное, как небольшой электронный документ (файл) установленного формата, снабжённый электронной подписью. Вопреки расхожему мнению, сертификаты непосредственно не связаны с шифрованием, но информация из сертификата используется в процессе генерации общего секретного ключа. Предназначение SSL-сертификата — привязка некоторого открытого криптографического ключа к некоторому сетевому имени, не более того. Такая привязка, в свою очередь, обеспечивается с помощью механизма электронной подписи, удостоверяющей сертификат: удостоверение подписей реализовано при помощи иерархии удостоверяющих центров (УЦ). К этой иерархии есть много претензий, так как компрометация УЦ позволяет нивелировать многие аспекты TLS. Однако рассмотрение данной иерархии вывело бы нас далеко за пределы протокола TLS, поэтому оставим его за рамками данной статьи.

Сертификат может иметь разные типы электронной подписи. В современном вебе подавляющее большинство сертификатов - сертификаты с подписью RSA. Примерно с 2013 года стала заметна доля ECDSA-сертификатов (они используют криптографию на эллиптических кривых, которая, по ряду практических свойств, превосходит криптосистему RSA). Других типов сертификатов практически не встречается. Серверный сертификат позволяет клиенту проверить, что он соединяется именно с тем узлом, с которым планировал. Для этого клиент проверяет подпись сертификата, сверяя источник этой подписи со списком доверенных ключей, принадлежащих удостоверяющим центрам. То, что в распоряжении сервера имеется соответствующий секретный ключ, гарантируется механизмом создания общего сеансового ключа сессии, корректное завершение которого невозможно без наличия на сервере секретного ключа сертификата.

Получение сторонами общего сеансового секретного ключа, который будет использоваться в симметричном шифре, - другой ключевой аспект процедуры установления соединения. Для того, чтобы прослушивать TLS-соединение, третьей стороне достаточно получить сеансовый ключ. Знание же секретного серверного ключа из сертификата само по себе не даёт возможности чтения сеанса. Однако существуют исторические реализации TLS, в которых серверный ключ позволяет расшифровать сеансовый. Это касается схемы, использующей RSA: в этом случае во время установления соединения клиент (обычно это браузер) генерирует 48-байтовое случайное число, которое служит основой для выработки сеансового ключа, шифрует это число открытым RSA-ключом сервера, полученным в сертификате, и передаёт результат на сервер; если сервер знает соответствующий секретный ключ, то он сможет расшифровать данные клиента. Но то же самое сможет проделать и третья сторона, прослушивающая канал и знающая секретный серверный ключ RSA, а

Рис.1. Схема обмена Handshake-сообщениями



так как остальные данные, необходимые для получения сеансового ключа, открыты, эта третья сторона сможет вычислить и его. Неустранимая для данного механизма генерации ключа архитектурная уязвимость позволяет раскрывать ранее записанный трафик TLS-сессий, даже если серверный ключ стал известен много позже записи трафика.

Проблема секретности здесь вовсе не является надуманной. Так например, в 2008 году была обнаружена ошибка в процедуре генерации псевдослучайных чисел в ветке Debian популярнейшего набора криптобиблиотек OpenSSL. Ошибка радикально сокращала число возможных вариантов начального состояния генератора и приводила к тому, что количество различных ключей, генерируемых библиотекой, измерялось всего лишь десятками тысяч - такое множество элементарно перебирается за минуты. Так как OpenSSL применяют и для генерации серверных ключей RSA, все ключи, созданные уязвимой версией, оказались известны, что, потенциально, позволило раскрывать ранее записанный TLS-трафик. Отметим, что использование ECDSA вместо RSA не позволяет вырабатывать сеансовый ключ описанным выше способом, так как криптосистема ECDSA не позволяет зашифровать данные, а лишь сгенерировать значение электронной подписи.

Современные реализации TLS должны использовать при установлении соединения протокол Диффи-Хеллмана (рекомендуется вариант на эллиптической кривой). Сервер лишь удостоверяет электронной подписью (от ключа, соответствующего сертификату) свой открытый ключ Диффи-Хеллмана. Как упоминалось выше, шаг с подписью необходим для того, чтобы предотвратить возможную атаку «человек посередине», которой подвержен протокол Диффи-Хеллмана. Сеансовый ключ записанной сессии, таким образом, оказывается недоступен атакующему, который позже получил секретный серверный ключ. То есть можно говорить, что данная криптографическая схема обладает так называемой прогрессивной секретностью (Forward Secrecy): компрометация серверного ключа не приводит к раскрытию ранее записанных сообщений. Интересно, что если атакующая сторона обладает серверным ключом сертификата и может проводить активный перехват трафика, то она сможет перехватить новую сессию, подменив открытый ключ Диффи-Хеллмана на свой.

Но не следует полагать, что использование протокола Диффи-Хеллмана полностью защищает от последующей расшифровки трафика. Сеансовый ключ некоторое время сохраняется и на сервере, и на клиенте, а утечка ключа возможна с обоих узлов. Более того, на серверной стороне сеансовый ключ может передаваться в открытом виде и записываться системами инспекции трафика. Например, распространена практика экспорта сеансового ключа во внешние (относительно веб-сервера) системы противодействия атакам и обнаружения вторжений. Также в TLS существует оптимизация, позволяющая возобновлять ранее сохранённую сессию по сокращённой схеме (Abbreviated Handshake). Хранение сессии на стороне сервера подразумевает сохранение и сеансового ключа - время, в течение которого этот ключ сохраняется, может измеряться сутками.

Большинство современных сценариев использования TLS подразумевают только аутентификацию сервера клиентом. Однако протокол позволяет проводить и «обратную» аутентификацию - клиента сервером. Для этого служат клиентские SSL-сертификаты, которые клиенты передают в ответ на запрос сервера. Так как использование клиентского сертификата не связано с выработкой сеансового ключа, для подтверждения обладания соответствующим секретным ключом клиент подписывает блок данных, переданный сервером. Клиентские сертификаты иногда используются для авторизации в веб-интерфейсах, например, в платёжных системах или в системах управления контентом сайта.

После того, как клиент и сервер успешно договорились о криптосистемах и выработали общий сеансовый ключ, TLS-соединение можно перевести в защищённый режим, включив шифрование. Переключение происходит при помощи обмена специальными сигналами. С этого момента новые сообщения передаются в зашифрованном виде. Для транспортировки полезной нагрузки служат сообщения специального типа (Application Data). Каждое сообщение не только шифруется, но и, как описано выше, снабжается кодом аутентификации. Таким образом и клиент, и сервер могут проверить, что сообщение не было подвержено изменению. Кроме того, код аутентификации защищает от повтора атакующей стороной переданных ранее сообщений.

TLS также содержит и корректную процедуру закрытия соединения. Конечно, на практике канал просто может быть разорван, из-за ошибки или действий третьей стороны. Такая ситуация не вызывает фатальных проблем у узлов. По крайней мере, если протокол правильно реализован. Однако криптографический протокол должен содержать и часть, позволяющую закрыть соединение штатным образом: в TLS для этого предусмотрен обмен специальными сигналами, которые передаются в защищённом виде.

Протокол TLS относится к одному из самых изученных протоколов современного Интернета. Тщательно изучаются и его реализации. Казалось бы, многолетний и всесторонний аудит должен был бы давно искоренить большинство ошибок. Тем не менее, ошибки и уязвимости и в реализациях TLS, и в самом протоколе, продолжают находить регулярно. Нет оснований полагать, что в ближайшее время не будет найдено новых критических уязвимостей.

Современное состояние

TLS используется в сети повсеместно. Это касается и веба. В 2015 году уже можно сказать, что если вы веб-мастер, но ваш сайт не поддерживает HTTPS в качестве основного протокола, то вы сильно отстаёте. Сайты массово переходят на защищённый протокол. Может показаться, что HTTPS требуется только там, где сайт работает с конфиденциальными данными. Но не нужно забывать о второй, не менее важной, чем шифрование, функции TLS - протокол обеспечивает целостность данных. То есть использование HTTPS позволяет веб-мастеру быть уверенным, что страницы его сайта не будут изменены на пути к пользователю, что в их составе не возникнет «вдруг» дополнительный контент - какой-нибудь замысловатый javascript-код. Это отнюдь не выдуманная угроза: на инъекциях в веб-страницы дополнительного кода, показывающего рекламу, уже попадались весьма крупные провайдеры интернет-доступа. Некоторые — попадались не один раз. Поэтому, если веб-мастер заботится о сохранении контента на пути до пользователя, то он обязательно внедряет HTTPS, на любом сайте. Не так давно и Google стал ранжировать выше сайты, доступные по HTTPS.

Протокол TLS относится к одному из самых изученных протоко-

лов современного Интернета. Тщательно изучаются и его реализации. Казалось бы, многолетний и всесторонний аудит должен был бы давно искоренить большинство ошибок. Тем не менее, ошибки и уязвимости и в реализациях TLS, и в самом протоколе, продолжают находить регулярно. Нет оснований полагать, что в ближайшее время не будет найдено новых критических уязвимостей. Некоторые ранее найденные дефекты исправляются достаточно медленно. Рекордсменом, по всей вероятности, является уязвимость веб-сервера IIS - CVE-2010-3332: об уязвимости стало известно в 2003 году, но корпорация Microsoft исправила дефект в реализации SSL своего веб-сервера лишь семь лет спустя, в 2010.

Фундаментальным недостатком TLS является большая сложность использования этого протокола. Да, в TLS можно выделить технологическое ядро, которое окажется относительно простым и, как говорится, обозримым для квалифицированного разработчика, а не только для специалиста в области защиты информации, специально занимающегося TLS. Это ядро включает в себя протокол установления соединения и небольшой набор современных типовых шифров. Проблема в том, что в чистом виде подобное ядро не используется, да и использовать его просто не выйдет: реализации окутаны многочисленными дополнениями и уточнениями, многие из них возникли как оптимизации, придуманные разработчиками того или иного массового сервиса. Например, инженеры и учёные Google предложили целый ряд модификаций для TLS, в том числе, модификаций, затрагивающих самые основы протокола (к таким относится TLS False Start и другие, частично перекочевавшие в черновики TLS 1.3). То есть изменения в TLS диктует практика использования протокола, но это не приводит к его упрощению, из-за того, что протокол из версии в версию тянет за собой огромное историческое наследие.

Сейчас в стадии разработки в IETF находится версия TLS 1.3. С самого начала работы над ней было предложено удалить многие и многие невостребованные особенности и дополнения, чтобы упростить протокол и, опять же, сделать его обозримым. Например, обсуждается запрет на сжатие данных: все предыдущие версии предусматривают возможность сжатия данных перед шифрованием, с использованием некоторого алгоритма (это наверняка будет DEFLATE, являющийся небезопасным); сжатие используется крайне редко и несёт с собой дополнительные уязвимости. Однако едва ли не каждая попытка удаления подобного «исторического наследия» приводит к возражениям: современный Интернет настолько разнообразен, что в нём не только не трудно найти TLS-серверы, поддерживающие SSLv2, но и всякая экзотическая технология неожиданно оказывается востребованной тем или иным малоизвестным сервисом. А пренебречь интересами даже небольшой группы пользователей - крайне нелегко.

Тем не менее, рабочей группе есть чем похвалиться: список выкидываемого «старья» не так уж и короток. Спецификация TLS 1.3 пока находится в статусе черновика, но многие полезные изменения уже зафиксированы. Так, исчезнет поддержка алгоритма электронной подписи DSA - в Интернете такие сертификаты сейчас не встречаются, сам алгоритм считается историческим и неперспективным. Более того, упоминавшаяся выше схема обмена сессионным ключом с использованием шифрования RSA также удалена из протокола установления соединения, как не обладающая прогрессивной секретностью.

Достаточно серьёзно урезано число потенциальных каналов утечки метаинформации, характерных для TLS. Например, поле, обозначающее тип записи (Content Type) и ранее передававшееся в открытом виде, будет зашифровано: информация о типе записей является одним из каналов утечки метаинформации, так как позволяет стороне, ведущей пассивное наблюдение за каналом, видеть некоторые события - например, поступление сообщения об ошибке протокола. Метаинформация вообще является богатым источником сведений о ходе защищённого обмена данными и даже позволяет строить идентификационные профили и узнавать конкретные сервисы, которые посещает пользователь.

Исключается поддержка хеш-функции SHA-1 в составе криптосистемы электронной подписи: данная хеш-функция считается устаревшей и недостаточно стойкой (к нахождению коллизий). Также, наконец-то, из протокола удаляется поддержка хеш-функции MD5, а для полноты картины — и SHA-224.

Изъята целая пачка разнообразных алгоритмов «пересмотра» параметров соединения, которые ранее могли быть применены как на этапе установления соединения, так и в ходе сеанса. Считается, что наличие подобных «обходных тропинок» ведёт не к оптимизации использования вычислительных ресурсов, а к возникновению новых источников уязвимостей. Тем более, что многие из этих протоколов реально не использовались.

Большая чистка идёт. TLS 1.3 будет существенно отличаться от предыдущих версий TLS. Есть шанс, что технология обретёт положенную ей строгость и стойкость. К сожалению, можно с ничуть не меньшей уверенностью сказать, что новой версии также будут сопутствовать новые уязвимости. Остаётся надеяться, что среди них архитектурные дефекты протокола окажутся в меньшинстве.

С подробным техническим описанием TLS, интересным для специалистов, можно ознакомиться в отдельной статье автора.

Краткий путеводитель по IETF-94

К каждой встрече IETF, которые проводятся три раза в год в различных точках земного шара, Internet Society подготавливает «Краткий путеводитель по IETF». Этот путеводитель рассказывает о текущей деятельности различных рабочих групп IETF, направленной на разработку стандартов Интернета. Особое внимание уделяется таким направлениям, как разработка и внедрение стандартов по IPv6, стандартов безопасности системы маршрутизации, DNS, а также обеспечению конфиденциальности и повышению доверия в Интернете в целом. Под этой рубрикой в этом номере мы публикуем три статьи «Краткого путеводителя». Полную версию «путеводителя» вы можете прочитать на сайте: http://www.internetsociety.org/rough-guide-ietf94

Доверие, идентичность и конфиденциальность

Карен О'Донохью (Karen O'Donoghue)

В этой статье мы сосредоточим внимание на деятельности в рамках совещания IETF-94 в Иокогаме, связанной с повышением доверия в Интернете, включая такие вопросы, как защита личностной идентификации и конфиденциальность.

Момент, с которого я хочу начать свой обзор, пусть и не входит в сферу IETF полностью, но, тем не менее, является важным совместным проектом. Группа W3C Privacy Interest Group (PING) снова провела очную встречу параллельно с совещанием IETF. Целью этой встречи являлось обращение к широкому сообществу IETF, обмен информацией между участниками различных инициатив по конфиденциальности и дальнейшая проработка методов PING, включая черновик опросника по конфиденциальности и безопасности для авторов спецификаций.

Что же касается рабочих групп IETF, в настоящее время сразу несколько групп занимается связанными вопросами. Некоторые из них, чьи встречи состоялись на IETF-94, перечислены ниже.

Рабочая группа по средам автоматизированного управления сертификатами Automated Certificate Management Environment (acme) стремится снизить барьер развертывания сертификатов для Web PKI. В настоящее время проверка доменных имен в сертификатах осуществляется с помощью разовых, несистематических механизмов. В частности, рабочая группа acme занимается автоматизацией процесса выдачи, проверки, отзыва и возобновления сертификатов. В этот раз встреча рабочей группы была посвящена исключительно текущей редакции документа (https://datatracker.ietf.org/doc/draft-ietf-acme-acme/) и проблемам, занесенным в трекер (https://github.com/ietf-wg-acme/acme/issues).

В ответ на все усиливающиеся опасения касательно массовой слежки IETF стремится улучшить положение с наблюдаемыми данными во многих своих протоколах. Рабочая группа DNS PRIVate Exchange (DPRIVE) была создана для разработки механизмов, которые будут обеспечивать конфиденциальность между клиентами DNS и итеративными резолверами. В повестке дня встречи группы в рамках IETF-94 — DNS поверх DTLS, DNS поверх TLS и шифрование DNS без сохранения состояния. Поскольку практически вся интернет-коммуникация так или иначе использует трансляцию имен, дополнительный уровень конфиденциальности для механизмов DNS отнюдь не повредит укреплению доверия в Интернете.

Рабочая группа Web Authorization Protocol (oauth) уже довольно долго трудится над набором документов, которые позволят поль-

зователю предоставить третьей стороне доступ к защищенным ресурсам, не предоставляя долгосрочные учетные данные пользователя. Группа подготовила длинный список RFC. Встреча в рамках IETF-94 была посвящена запросам авторизации, проверке обладания, обмену токенами и использованию OAuth для нативных приложений. OAuth постепенно становится ключевым компонентом систем сетевой идентичности, и эта встреча явилась очередным этапом развития OAuth.

Рабочая группа Open Specification for Pretty Good Privacy (OpenPGP) изначально завершила свою работу в 2008 году, подготовив решение для шифрования объектов, подписания объектов и сертификации идентификации (RFC 4880). В последнее время стало ясно, что пришло время подготовить обновление RFC 4880, и рабочая группа OpenPGP была восстановлена для этой цели. Эта версия будет содержать потенциальное включение эллиптических кривых, рекомендованных CRFG (Crypto Forum Research Group), симметричный механизм шифрования, который обеспечивает современную защиту целостности сообщений, обновление выбора обязательного к реализации алгоритма, исключение слабых алгоритмов и обновленный механизм «отпечатков пальцев» открытого ключа.

Инфраструктура сертификатов web PKI продолжает оставаться источником эксплуатационных проблем Интернета, связанных с доверием. Основным направлением деятельности рабочей группы Public Notary Transparency (trans) является создание стандартизованной версии экспериментального RFC 6962 о прозрачности сертификатов. Прозрачность сертификатов предназначена для ведения журнала сертификатов, выданных удостоверяющим центром. Это дает возможность отслеживать проблемы сертификационной инфраструктуры в глобальном масштабе. Основным фокусом дискуссии на этой неделе явилось обновление RFC 6962, анализ угроз и протокол «сплетен» (англ. gossip protocol).

Чуть отклонясь от темы, хочу упомянуть рабочую группу Network Time Protocol (ntp). По мере развития Интернета некоторые ключевые аспекты инфраструктуры, которые мы часто принимаем как должное, тоже должны время от времени пересматриваться в свете нынешней операционной среды. Время - ключевой компонент установления и поддерживания доверительных отношений, и ему часто не уделяют достаточно внимания. Рабочая группа ntp сейчас решает две задачи для того, чтобы повысить достоверность инфраструктуры времени. NTS (Network Time Security) определит обновленный фреймворк и механизмы для аутентификации серверов времени. А новая спецификация BCP (Best Current Practice) создается для решения распространенных эксплуатационных проблем, которые все чаще используются в качестве лазеек.

Чтобы еще раз подчеркнуть всю важность работы IETF в направлениях доверия, идентичности и конфиденциальности, я хочу упомянуть свое участие в состоявшемся в конце октября совещании Технического пленарного и наблюдательного совета Консорциума World Wide Web Consortium (W3C) (TPAC) в Саппоро. Одним из ярких моментов мероприятия стала пленарная панельная дискуссия с участием Тима Бернерса-Ли, Винта Серфа и Джуна Мураи. Там был особо затронут вопрос создания лучшего уровня доверия для Всемирной паутины. Винт Серф ответил, что сообщества IETF и W3C совместно работают над разрешением вопроса «Чего не хватает в пространстве протоколов для того, чтобы получить сильную аутентификацию, высокий уровень целостности и другие механизмы создания доверия?»

Источник: Trust, Identity, and Privacy

Безопасность и устойчивость системы маршутизации

Андрей Робачевский

Несколько рабочих групп IETF проводят значительную работу по обеспечению более безопасной и устойчивой инфраструктуры Интернета, как в краткосрочном, так и в долгосрочном планах.

Обеспечение безопасности имеет отношение не только к маршрутизации, хотя она находится в центре внимания, но и ко всем уровням и компонентам архитектуры Интернета. Некоторые из этих рабочих групп провели свои заседания в Йокогаме в рамках IETF-94 1-6 ноября.

Рабочая группа по Безопасной междоменной маршрутизации (Secure Inter-Domain Routing WG, SIDR) сосредотачивает свои усилия на обеспечении системы глобальной маршрутизации.

Архитектурно предлагаемое решение базируется на Инфраструктуре открытых ключей (PKI) для номерных ресурсов (Resource PKI, RPKI), которая обеспечивает основу аутентификации BGP и является важным компонентом увеличения защищенности этого протокола в лице BGPSEC, также разработанного группой SIDR. RPKI является ключевой технологией для повышения доверия к инфраструктуре глобальной маршрутизации.

Два главных улучшения в междоменной маршрутизации, проверка подлинности источника маршрута (Origin Validation, OV) и проверка подлинности пути маршрута (BGPSEC), успешно приняты; несмотря на это, работы ведутся активно и особое внимание сейчас приковано к деталям. Поскольку OV был первым компонентом, разработанным IETF, доработки предлагаются, исходя из практического опыта внедрения и использования. Примерами являются протокол RPKI Repository Delta, способствующий улучшению общей расширяемости и производительности работы системы или внеполосный протокол, призванный упростить изначальную конфигурацию протоколов RPKI между двумя сторонами.

Но на повестке дня также и более значительные изменения, как предложение об изменении процесса проверки сертификата.

Авторы документа «RPKI Validation Reconsidered», которому присвоен информационный статус, заменили его на другой, более краткий документ с предполагаемым статусом стандарта, который обновляет процесс проверки RPKI-сертификата, описанного в RFC6487 в разделе 7.2. Все более зрелым становится и другой компонент - BGPSEC. Спецификация протокола BGPSEC находится в 13-й доработке и практически готова перейти в фазу Last Call рабо-

чей группы. Но работа до сих пор не завершена, потому что продолжают обнаруживаться новые возможные уязвимости — и необходимы некоторые уточнения.

В то же время, уже существуют практические реализации этой спецификации, разработанные параллельно с процессом стандартизации. Например, существует реальный код, который добавляет расширения BGPSEC к открытому ПО демона маршрутизации BIRD.

Но существует серьезная угроза, которую SIDR-технологии не могут устранить: так называемая утечка маршрута. Проще говоря, этот термин подразумевает формально правильный анонс маршрута, который, тем не менее, нарушает предполагаемую сферу распространения.

Например, мультисетевой клиент совершает «утечку» маршрута при переанонсировании его от одного провайдера к другому. Из-за того, что это является нарушением политики маршрутизации, а не протокола, ни OV, ни BGPSEC не могут обнаружить или снизить вероятность таких атак. В документе «Методы обнаружения и устранения последствий BGP-утечек» авторы предлагают усовершенствовать BGP для повышения вероятности обнаружения утечек и устранения их последствий для BGPSEC.

В проекте предлагается новое поле защиты от утечек (Route Leak Protection, RLP), которую операторы должны установить при анонсе маршрутов своим клиентам и пирам.

Получив анонс BGP, где установлено RLP со значением «01» («не распространять вверх или горизонтально») для одного или более сегментов пути, оператор может установить, что такой анонс представляет «утечку» и должен быть соответствующим образом обработан (например, путем предпочтения «чистого» маршрута от провайдера или пира).

Этот проект обсуждается в Рабочей группе Междоменной маршрутизации (IDR). Другая рабочая группа, GROW (Global Routing Operations), которая акцентирует внимание на функциональных проблемах, связанных с системой глобальной маршрутизации, также активно работает над вопросами безопасности и устойчивости глобальной маршрутизации.

Говоря о DDoS-атаках: недавно была создана ещё одна рабочая группа - DDoS Open Threat Signaling (DOTS). DDoS-атаки не связаны непосредственно с системой маршрутизации Интернет-коммуникации, но они могут оказывать серьёзное влияние на обеспечение общей устойчивости системы. Цель этой группы - разработка стандартного протокола, направленного на автоматизацию координации борьбы с подобными атаками.

DDoS-атаки, направленные на членов точек обмена интернет-трафиком (IXP), могут послужить причиной перегрузки портов пиров. Чтобы ограничить отрицательный эффект атаки на нормальный трафик, точки обмена интернет-трафиком адаптировали так называемый блэкхолинг. Участник может запустить эту процедуру через роут-сервер. Понятие блэкхолинга в точках обмена интернет-трафиком сходно с этим же термином в iBGP [RFC3882] и фильтрующим расширением RTBH [RFC5635]. Документ «Атрибут BLACKHOLE для блэкхолинга в точках обмена интернет-трафиком» предлагает определить значение BGP community, чтобы позволить оператору указывать роут-серверу IXP, от каких маршрутов следует отказаться. Эта инициатива, вероятно, будет принята в качестве документа рабочей группы.

Говоря о DDoS-атаках: недавно была создана ещё одна рабочая группа - DDoS Open Threat Signaling (DOTS). DDoS-атаки не связаны непосредственно с системой маршрутизации интернет-коммуникации, но они могут оказывать серьёзное влияние на обеспечение общей устойчивости системы. Цель этой группы - разработка стандартного протокола, направленного на автоматизацию координации борьбы с подобными атаками. Этот протокол должен поддерживать запросы об услугах по устранению DDoS-атак и обновление статуса через межорганизационные административные границы.

Источник: Routing Security & Resilience

Укрепление роли Интернета

Карен О'Донохью (Karen O'Donoghue)

Непрерывная работа интернет-сообщества по укреплению Интернета была продолжена на конференции IETF-94 в Иокогаме. Казалось бы, только вчера мы собирались в Праге на IETF-93 – а уже есть новые достижения и новые направления деятельности. В этой заметке мы обсудим программу конфиденциальности и безопасности IAB, включая недавно прошедший семинар MaRNEW, деятельность исследовательской группы Crypto Forum Research Group и рабочей группы TLS, включая грядущий семинар TRON.

Internet Architecture Board (IAB) — в рамках своей программы конфиденциальности и безопасности Privacy and Security Program - прилагает массу усилий по укреплению Интернета путем анализа угроз, мер их устранения и моделей систем доверия. За время, прошедшее с окончания IETF-93, был опубликован документ RFC 7624 "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement". Программа IAB сейчас работает над следующим документом, в котором рассматриваются соответствующие меры устранения, озаглавленным "Confidentiality in the Face of Pervasive Surveillance». Кроме того, принят проект документа, идентифицирующий проблемы и пути решения для ряда ключевых вопросов, связанных с инфраструктурой Web PKI, "Problems with the Public Key Infrastructure (PKI) for the World Wide Web". Оба этих документа обсуждались на встрече в Иокогаме. Кроме того, с момента оконча-

ния IETF 93 участники IAB провели совместный семинар с GSMA на тему управления радиосетями в мире шифрования (Managing Radio Networks in an Encrypted World, или сокращенно MaRNEW). Доклады, программа семинара и презентации доступны по адресу https://www.iab.org/activities/workshops/marnew/. Краткий отчет об этом семинаре опубликован в недавнем выпуске IETF Journal, а полный отчет о семинаре ожидается к концу года.

Далее, исследовательская группа Internet Research Task Force (IRTF) Crypto Forum Research Group (cfrg) продолжает заниматься использованием криптографии для протоколов IETF. Ее усилия во многом сосредоточены на выборе новых эллиптических кривых для использования в протоколах IETF, и примерный консенсус по этому вопросу закреплен в документе "Elliptic Curves for Security". После IETF-93 этот документ был закончен и направлен редактору RFC Series на публикацию. В числе тем обсуждения на IETF-94 - эллиптические кривые, PAKE, пост-квантум защищенные подписи и обмен ключами. Всем заинтересованным в будущем направлении развития криптографических кривых и алгоритмов рекомендуется следить за этими дискуссиями. В рамках IETF-94 прошли встречи множества рабочих групп, которые занимаются укреплением Интернета. В этом выпуске я уделю основное внимание TLS.

Рабочая группа безопасности транспортного уровня TLS (Transport Layer Security) активно работает над обновлением протокола TLS. Это очень активная рабочая группа, в ее планах - опубликовать обновление TLS в 2016 году. Встреча рабочей группы была посвящена разрешению насущных вопросов текущей спецификации, задокументированных в трекере: https://github.com/tlswg/tls13-spec/issues.

Заметим также, что рабочая группа TLS планирует доработать спецификацию TLS 1.3 и взять краткую паузу, чтобы дать исследователям проблем безопасности время на анализ спецификации. В рамках этого запланировано провести семинар TLS1.3 Ready or Not (TRON), совместный с Network and Distributed System Security Symposium (NDSS). Семинар состоится в феврале 2016 года. Идет прием докладов, мы приглашаем к участию всех заинтересованных в повышении прочности новой спецификации TLS.

Подводя итоги, скажу, что ведется большая работа в направлении того, чтобы сделать шифрование более распространенным и упростить его использование в целях укрепления Интернета.

Источник: Strengthening the Internet

Эволюция IANA: подготовка новой фазы

Андрей Робачевский

Мы продолжаем серию статей, рассказывающих об истории и эволюции IANA, включая текущую стадию передачи надзорной роли правительства США в руки международного сообщества. Сегодня мы остановимся на структуре IANA, рассмотрим вопросы разделения ролей определения политики, надзора и исполнения. Наконец, расскажем о сути проектов передачи, операционными сообществами, — параметров протоколов, номерных ресурсов и имен. А также — о спорных вопросах и процессе формирования согласованного предложения.

Создание ICANN обозначило важную веху в системе координации централизованных функций Интернета – администрирование корневой зоны, глобального пула адресного пространства IP и уникальных параметров протоколов Интернета.

В духе стратегии приватизации Интернета была создана формально независимая от правительства США частная корпорация. В духе общей тенденции глобализации Интернета в процесс принятия решений относительно администрирования этих критических ресурсов были вовлечены глобальные сообщества. Часть этих сообществ, например, сообщество разработчиков протоколов IETF, адресное сообщество вокруг РИРов, сформировалась в ходе эволюции Интернета и функционировала в соответствии с нормами и политиками, проверенными практикой. С именами дело обстояло гораздо сложнее.

Монопольная позиция NSI в отношении администрирования корневой зоны и основных доменов верхнего уровня была причиной отсутствия организованного сообщества, объединенного общими интересами, совместно принятыми правилами и политиками. Для заполнения этого пробела сообщество имен в рамках структуры ICANN было организовано следующим образом:

- Представители администрации национальных доменов были объединены в организацию поддержки национальных доменов – ccNSO.
- Для общих доменных имен также была создана организация поддержки – GNSO, однако ее структура оказалась куда более сложной и отражала широкий круг заинтересованных сторон: коммерческих организаций (бизнес, интеллектуальная собственность, интернет сервис-провайдеры), некоммерческих организаций, а также регистратур и регистраторов.
- Наконец, интересы интернет-пользователей и правительств государств были учтены путем создания консультационных комитетов – ALAC (At-Large Advisory Committee) и GAC (Government Advisory Committee).

Описанная выше структура представляет органы, принимающие решения и определяющие политику, на основании который IANA создает и обслуживает соответствующие реестры. При этом IANA, оставаясь подразделением ICANN, выполняет административные функции и не принимает активного участия в разработке политик.

Определение политик, обслуживание регистратур и надзор

Для того, чтобы лучше увидеть роль NTIA и других участников «экосистемы» IANA (Рис. 1), стоит поподробнее остановиться на трех основных аспектах глобальной регистратуры – политики, исполнения и надзора.

Задачей всех вышеописанных структур принятия решений в отношении IANA является **выработка соответствующих политик**, начиная от создания специальных реестров и заканчивая правилами внесения изменений.

Так, сообщество IETF в процессе разработки протокола определяет необходимость создания реестра и правила его сопровождения. Эта “политика” документируется в разделе “IANA considerations” соответствующего стандарта. Документ RFC 5226 «Guidelines for Writing an IANA Considerations Section in RFCs» содержит практические рекомендации по разработке таких правил и их документации в этом разделе. Хочу отметить, что ICANN в плане разработки или утверждения таких правил не имеет никакой роли.

В отношении номерных ресурсов – IP адресов и номеров автономных систем - дело касается утверждения глобальных политик - правил управления глобальным пулом номерных ресурсов, который администрирует IANA. Сами политики разрабатываются РИР-сообществами, но затем утверждаются ASO (Address Supporting Organization, Организация поддержки адресов) ICANN. Заключительным шагом является ратификация глобальной политики советом директоров ICANN. Эти политики действительны только в отношении реестров так называемых глобальных номерных ресурсов, делегированных РИРам для последующего распределения. Часть адресного пространства (и соответствующие реестры) обслуживается в соответствии с политикой IETF и является либо зарезервированной, либо предназначенной для специального использования (см., на-

пример, http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml).

Разработка политики в отношении доменов верхнего уровня, общих и национальных, происходит в рамках соответвтующих организаций поддержки и координируется соответствующими советами – советом ccNSO и советом gNSO. Политики утверждаются советом директоров ICANN. Замечу, что большинство политик и рекомендаций, разработанных этими сообществами, непосредственно к IANA отношения не имеют. Эти политики регулируют деятельность регистраторов имен второго уровня в общих доменах верхнего уровня. Основные же правила, относящиеся к администрированию корневой зоны, либо внешние (как, например, допустимые имена национальных доменов, определяемые стандартом ISO 3166-1), либо проходят как инструкции и рекомендации, разработанные самой ICANN (например, процесс ре-делегирования).

Сама же IANA выполняет сугубо **административную функцию**, а именно обслуживает запросы на изменение соответствующих реестров:

- Для доменных имен – собственно корневую зону, файл хинтов*, и базу данных доменов верхнего уровня, т.н. whois, содержащую помимо прочего контактную информацию администратора домена. В зону ответственности IANA также входит регистрация имен в домене .int, а также информация и реестры, относящиеся к DNSSEC – ключи точек доверия, материалы церемоний подписания и т.п. (https://www.iana.org/domains).
- Для номерных ресурсов – реестры глобальных адресов и реестры номеров автономных систем (https://www.iana.org/numbers).
- Для параметров протоколов – различные реестры для протоколов, разработанных IETF (https://www.iana.org/protocols).

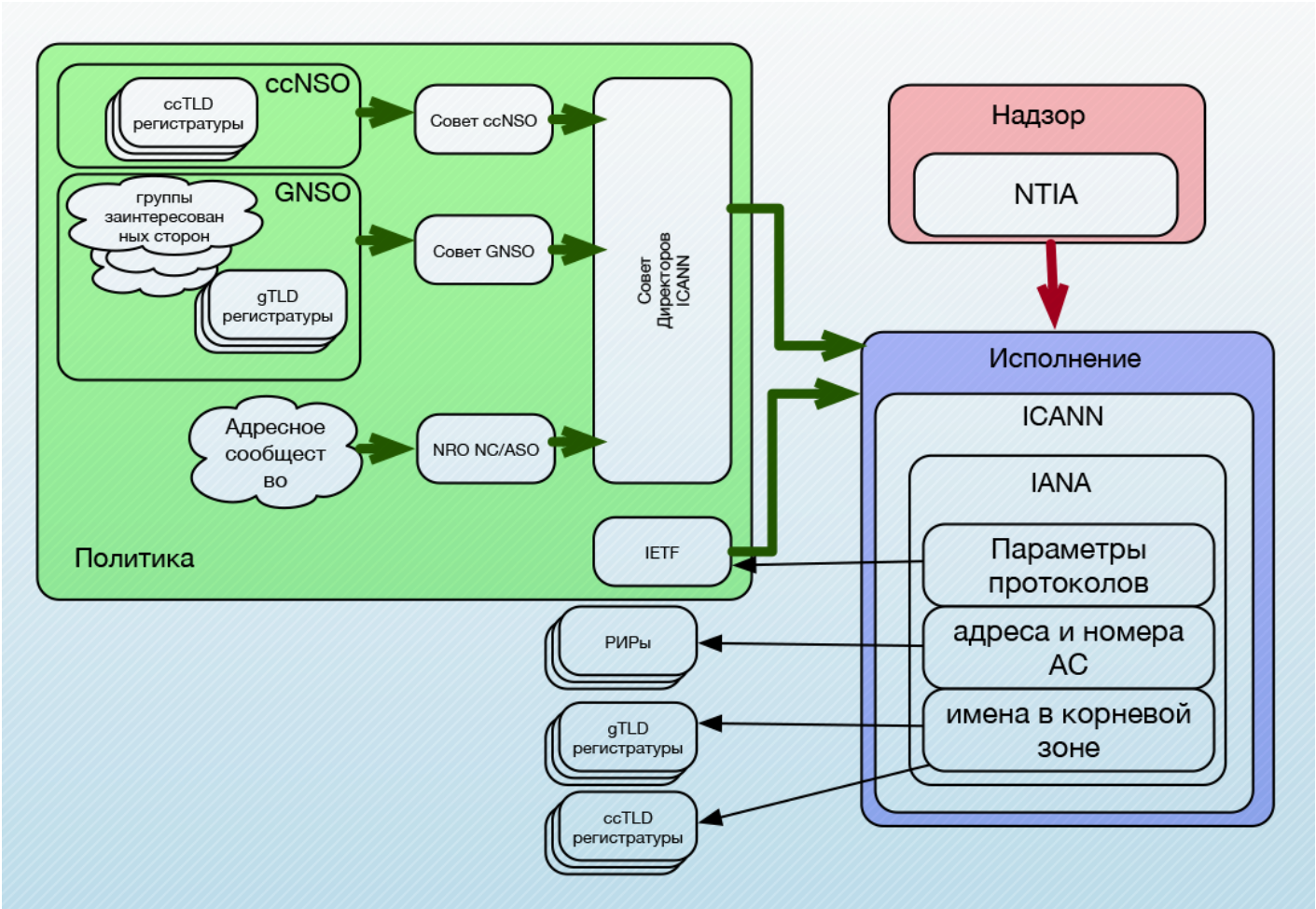
Наконец, функцию **надзора** выполняет правительство США в лице NTIA, поскольку именно это агентство министерства торговли является держателем договора на предоставление услуг IANA. Этот договор, как я говорил в предыдущей статье, был заключен в начале 2000 года и фактически легитимировал поглощение ICANN IANA, но также восстановил контроль правительства США над этими ключевыми функциями.

В рамках стандартной практики правительства США происходит периодическое перезаключение этого договора, формально открывающее возможность для других, кроме ICANN, претендентов завоевать этот контракт и стать IANA. Хотя бы на три года** .

Для доменных имен NTIA выполняет еще и дополнительную надзорную функцию – а именно утверждает любые изменения в корневой зоне и базе данных whois. Целью этой функции является проверка, что при обслуживании запроса на изменение ICANN следовала существующим правилам и процессу. Без этого утверждения Verisign, которая собственно технически обслуживает и публикует корневую зону, изменений в нее не внесет.

О передаче именно этой надзорной функции и шла речь, когда NTIA опубликовала заявление о намерении передать

Рис.1. Взаимодействие функций разработки политик, исполнения и надзора в «экосистеме» IANA



ключевые функции глобальной системы имен DNS в руки мирового сообщества.

Адреса и протоколы

- В своем заявлении NTIA обозначила процесс разработки плана передачи и основные требования к нему. ICANN поручалось созвать заинтересованные стороны глобального интернет-сообщества для разработки плана. Результат должен быть поддержан широкими массами и удовлетворять четырем основным принципам:
- поддерживать и укреплять модель мультистейколдеризма;
- обеспечивать безопасность, стабильность и прочность системы DNS;
- удовлетворять потребности и ожидания глобальных потребителей и партнеров услуг IANA;
- поддерживать открытость Интернета.

Отдельной строкой было выделено условие, что роль NTIA не может быть передана государственной или межгосударственной организации.

В результате нескольких месяцев интенсивных дискуссий был согласован план создания плана передачи, согласно которому «операционные сообщества» — протоколов, номерных ресурсов и имен – должны разработать части плана, соответствующие их области деятельности, а созданная Координирующая группа (IANA Stewardship Transition Coordination Group, ICG) должна будет скомпилировать общий согласованный план, при этом не добавляя отсебятины.

Общий план предполагал, что все три части будут готовы к 15 января 2015 года, что позволит ICG консолидировать их в единое предложение, собрать комментраии, предоставить NTIA на рассмотрение, получить утверждение и перейти к исполнению. И все это - до окончания действия контракта 30 сентября 2015 года. Как вскоре стало понятно, план оказался нереалистичным.

План сообщества IETF разработать было достаточно просто – он по существу документировал статус кво. Присутствие NTIA в IETF ощущалось только при перезаключении контракта, который с точки зрения самого IETF был совершенно излишним. Дело в том, что уже в 2000 году между IETF и ICANN был заключен меморандум, определяющий роли ICANN как провайдера услуг IANA и IETF как потребителя этих услуг, документирующий требования к предоставляемым услугам, - другими словами, договор на предоставление услуг IANA. Каждая из сторон вправе расторгнуть данный договор с 6-месячным уведомлением.

Договор решает проблему подотчетности – если провайдер не выполняет оговоренных задач и не обеспечивает качества услуг, договор может быть расторгнут и найден новый провайдер.

Разработка плана проводилась в духе IETF согласно процессу разработки стандартов. Для этого была организована рабочая группа IANAPLAN - и к концу 2014 года консенсус был достигнут и план был готов. Структура этих взаимоотношений представлена на рис.2.

Сообщество номерных ресурсов взяло подход IETF за основу, однако выработало специальный процесс для разработки плана. Процесс разработки глобальных политик являлся слишком длительным (консенсус должен быть достигнут во всех региональных сообществах), чтобы иметь практическое применение. Вместо этого РИРы предложили создание небольшой группы из 15 представителей региональных сообществ (по три от каждого) для разработки и обсуждения плана, который получил название Консолидированного предложения РИР по координирующей роли (Consolidated RIR IANA Stewardship Proposal, CRISP).

Для номерных услуг IANA роль NTIA также сводилась к держателю контракта с ICANN. Эту роль предлагалось передать пяти РИРам, которые, в свою очередь, заключили бы договор, или Соглашение об уровне услуг (Service Level Agreement, SLA) непосредственно с ICANN. Предлагалось также создать ревизионный комитет из представителей сообщества для контроля качества предоставляемых услуг. Эту роль предлагается совместить с существующей группой Совета ASO. Комитет имеет чисто консультативную роль, решения в плане пересмотра контракта или параметров предоставляемых услуг остается за РИРами.

Оставался один с виду незначительный момент, в отношении которого по не вполне понятным причинам IETF не решился занять сильную позицию. Я имею в виду торговые знаки и интеллектуальную собственность. Или, более конкретно, - знак и имя IANA, доменное имя iana.org и содержимое регистратур. Группе CRISP было очевидно, что если ICANN будет продолжать быть держателем этих ресурсов, это может существенно затруднить возможность перезаключения контракта и перехода к другому оператору – ключевой элемент решения вопроса надзора.

План CRISP предлагал передать эти ресурсы в руки независимой организации, а IETF Trust рассматривался в качестве возможного кандидата.

Таже одним из условий договора являлась возможность его расторжения без конкретных причин, но с достаточным уведомлением.

И этот план был готов в срок, и еще до 15 января был передан в группу ICG для рассмотрения. Схематично он представлен на рис.2.

Имена

С именами дело обстояло гораздо сложнее. Как видно из рисунка 1, вся деятельность сообщества имен тесно интегрирована в структуру самой ICANN. Другими словами, организации, представляющие интересы этого сообщества – ccNSO, gNSO, – сами являются частью ICANN. Поэтому простой подход договорных отношений, который был принят сообществами протоколов и номеров, здесь не работал.

Для разработки плана была создана группа CWG – Сквозная рабочая группа сообщества имен (также получившая название CWG-Stewardship, CWG-Координирующая роль). Рабочая группа была сформирована из представителей поддерживающих организаций и комитетов, имеющих отношение к именам: ccNSO, SSAC, GNSO, ALAC, GAC. В дополнение к этим 19 членам группы в дискуссиях приняли активное участие 137 “наблюдателей” (в принципе, эта категория была открыта для всех заинтересованных лиц), которые впоследствии были переименованы в “участников”. При этом утверждение консенсуса и принятие решений является прерогативой членов группы.

После продолжительных обсуждений, встреч и телеконференций сообщество имен предложило решить проблему подотчетности ICANN самой себе путем создания нового отдельного юридического лица «IANA после передачи» (Post Transition IANA, PTI) в форме некоммерческой корпорации (точнее - корпорации по обеспечению общественных интересов, зарегистрированной в штате Калифорния). В соответствии с планом, эта корпорация является филиалом

или дочерней компанией ICANN, а ICANN - ее полным и единственным собственником.

В рамках предложения предполагалось, что ICANN заключит с PTI контракт на выполнение деятельности в качестве Оператора функций IANA (IANA Functions Operaotr, IFO) в части функций, связанных с именами. Весь персонал теперешнего отдела IANA и соответствующие ресурсы, процессы, данные и «ноу-хау» будут переданы PTI.

Обслуживание корневой зоны

Не секрет, что хотя в задачу IANA и входит внесение изменений в корневую зону DNS, техническое обслуживание и публикация зоны в глобальной DNS выполняется компанией Verisign. Об истории этого соглашения, включая неудавшуюся попытку Джона Постела (Jon Postel) изменить его, я рассказывал в предыдущей статье «Эволюция IANA: от записной книжки Джона Постела до ICANN».

Также неясно будущее существующего соглашения между NTIA и Verisign. История этого договора берет начало в 1993 году. Изначально это был договор между NSI и NSF, позже перешедший в руки NTIA, по которому NSI, а затем Verisign выполняли функции технического обслуживания корневой зоны (внесение изменений и предоставление зоны корневым серверам), а также функцию регистратуры доменов .com, .net и .org. Этот договор сегодня содержит 32 поправки, от-

Рис.2. Консолидированное предложение ICG

В структуре были предусмотрены два органа надзора – IFR (Группа проверки функций IANA) и CSC (Постоянный комитет потребителей). В задачу первого органа входит периодический (раз в несколько лет) анализ качества работы PTI на соответствие договору между ICANN и PTI, а также описанию работ IANA (IANA SOW) в части функций, связанных с именами. В задачу CSC входит оперативный контроль для обеспечения постоянного удовлетворительного качества исполнения функций IANA для прямых потребителей услуг, связанных с именами. Это, в первую очередь, операторы регистратур доменов верхнего уровня, но также и другие организации, например, операторы корневых серверов. Эти органы показаны на рис. 2.

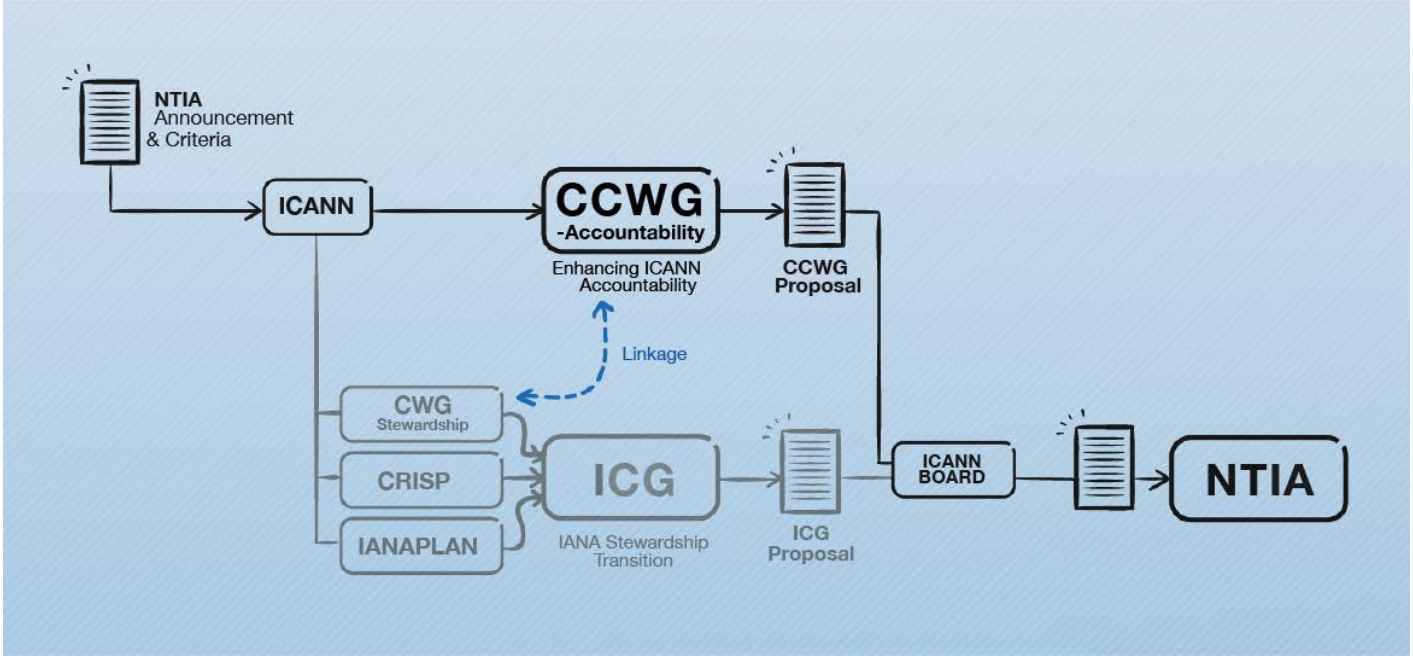
Удивительно, но этот ключевой элемент не попал в поле зрения группы CWG, предложение которой не содержит никаких требований касательно отношений между Оператором функций IANA и организацией, отвечающей за техническое обслуживание и публикацию – Verisign. В то же время этот элемент был подготовлен в ходе частных переговоров между ICANN и Verisign по просьбе NTIA. Сообщество потребовало, чтобы этот контракт прошел публичное обсуждение, но пока форма и содержание его неизвестно. В любом случае, это соглашение осталось за рамками предложения по передаче координирующей функции.

ражающие постепенно менявшуюся роль Verisign от монополиста до аккредитованного регистратора и регистратуры доменов .com и .net.

Подотчетность

Хотя заключение договора с отдельной организацией-провайдером услуг IANA вроде бы передавало контроль за этой функцией сообществу, неувязка все же оставалась. В конце концов, ICANN заключала договор со свей же дочерней организацией, что хотя безусловно обеспечивало лучшее разделение функций определения политик от администрирования реестров и корневой зоны в соответствии с этими политиками, и прозрачность этих отношений, но по-преж-

Рис.3. Процесс подготовки предложения для утверждения NTIA (источник: презентация CCWG на конференции ICANN54)



нему оставляло значительную часть этого контроля в руках ICANN и ее Правления. Например, ICANN могла не утвердить или недопустимо урезать бюджет PTI, также ICANN могла вставлять палки в колеса, зайди речь о передаче функций IANA от PTI к какой-либо сторонней организации.

Поэтому неотделимым от вопроса передачи координирующей роли встал вопрос общей подотчетности ICANN. Простого решения здесь также не предвиделось.

Для решения этой проблемы была создана еще одна группа - Сквозная рабочая группа сообщества по повышению подотчетности ICANN (Cross-Community WG Group – Accountability, CCWG). В ее состав вошли 28 членов, номинированных поддерживающими организациями и комитетами ICANN, а также 169 участников.

Предложение CCWG, которое все еще находится в стадии разработки, призвано увеличить контроль сообщества в лице поддерживающих организаций и комитетов за действиями Правления. Например, досрочно отозвать члена Правления, делегированного организацией. Или расформировать Правление целиком. Сообщество также должно получить дополнительные полномочия в отношении обсуждения и возможного отклонения бюджета, стратегического плана и внесений изменений в устав. Также будет разработан процесс апелляций для разрешения конфликтов. Основным механизмом принятия решений предполагается использовать консенсус.

Что дальше?

Предложение CWG было передано в ICG 25 июня 2015 года. К концу июля был скомпилирован черновик общего предложения, который был открыт для общественного обсуждения. Период обсуждения длился до 8 сентября, а 29 октября группа выступила со следующим заявлением:

«Координирующая группа ICG закончила работу над предложением по передаче координирующей роли, за исключением одного незавершенного пункта. Часть предложения, относящегося к именам, зависит от релизации механизмов подотчетности ICANN, которые в настоящее время находятся в стадии разработки в рамках Сквозной рабочей группы сообщества по повышению подотчетности ICANN (CCWG). Перед отправкой заключительного предложения в NTIA через Правление ICANN ICG должна получить от CWG подтверждение того, что ее требования подотчетности выполнены».

Схема взаимоотношений в консолидированном предложении показана на рис. 2.

Общий процесс подготовки предложения представлен на рис. 3.

Сможет ли группа CCWG прийти к удовлетворительному соглашению в ближайшее время? Выскажет ли Правление ICANN особое мнение при передаче окончательного предложения NTIA? Как пойдет процесс обсуждения внутри правительства США и какую роль будет играть Конгресс? Сможет ли NTIA дать зеленый свет процессу передачи до того, как предвыборная лихорадка США отодвинет эти вопросы на второй план?

Возможно, ответы на эти вопросы мы сможем обсудить в следующей статье этой серии.

*Файл хинтов (hints) содержит адреса всех корневых серверов и необходим для изначального запуска процесса трансляции имен резолвером.

**Три года – такова стандартная продолжительность контракта с возможностью двухразового продления, растягивающей его до максимального срока в семь лет.

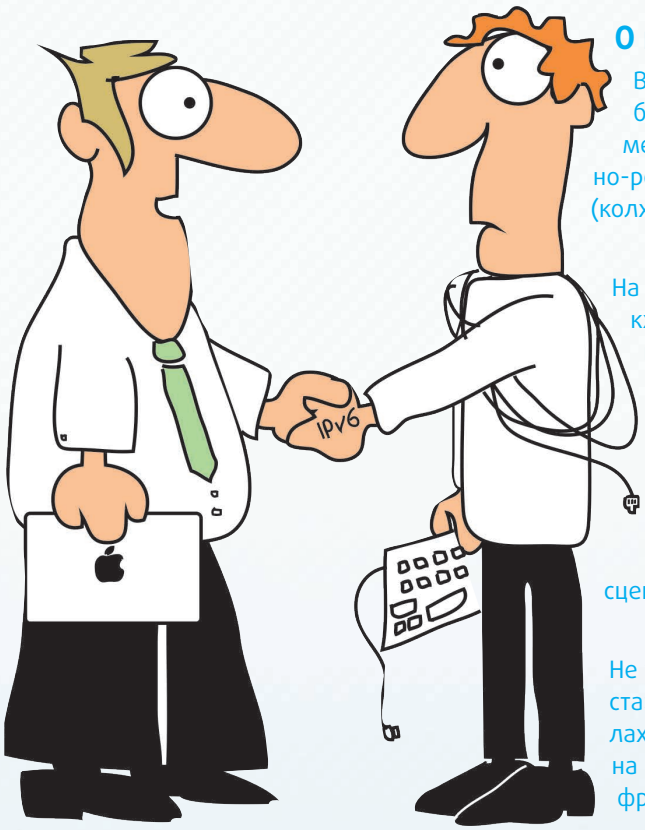
Мультистейкхолдерские кунштюки

Уважаемый читатель.

Бывают кунштюки цирковые, бывают интеллектуальные, а у нас — мультистейкхолдерные.

Мультистейкхолдеры, надо сказать, люди разные — из различных стран, разного воспитания и образования. Тем больше удовольствия доставляет наблюдать за их поступками и словами в зале заседаний и за его пределами — порой ощущаешь себя этаким Джеральдом Даррелом от управления интернетом.

С удовольствием делюсь с читателями некоторыми историями про своих колоритных коллег.



О пользе знания

В советские времена ни один предвыборный список нерушимого блока коммунистов и беспартийных не обходился без учителя местной школы (советская интеллигенция), наладчика карусельно-револьверного станка (рабочий класс) и доярки-передовика (колхозное крестьянство).

На заседаниях ICANN же, согласно определению мультистейкхолдерного управления Интернетом, в президиуме всегда представители основных стейкхолдеров: государства, бизнеса, академического, технического сообществ и сообщества пользователей.

Как-то раз — дело, помнится, было в Сингапуре - президент ICANN Фади Шехаде объявляет о начале пленарного заседания по вопросам мультистейкхолдеризма и приглашает на сцену соответствующих представителей.

Не успели они усесться в популярном формате «давосского насеста» (кто не видел, это когда все на сцене сидят рядком в креслах), как в партере встал и возвысил голос Себастиан Б. — мужчина грузноватый и в очках, но, как истинный француз, — известный фрондер и забияка, да к тому же и член Правления ICANN.

— Минуточку! - громогласно возвестил он. — Эта панель нелегитимна и не может считаться мультистейкхолдерной!

В этот момент опешил даже такой опытный оратор, как Фади.

— Почему же, Себастиан? — мягко вопросил он, явно, чтобы собраться с мыслями.

— Здесь нет представителей сообщества интернет-пользователей! — столь же громогласно отозвался Себастиан.

В зале послышался шепоток — не иначе интернет-пользователи вполголоса нахваливали бескомпромиссного Себастиана или — что тоже вполне вероятно — делали ставки на его шансы остаться в Правлении.

Вот тут-то Фади и явил себя в полном блеске. Он сделал шаг к авансцене, очки его заблистали, он раскинул руки, как бы стремясь обнять каждого из сидящих в зале, и голосом библейского пророка молвил:

— Себастиан! Ну зачем же нам представитель этого сообщества на сцене, когда мы все здесь в зале — интернет-пользователи!

Аллилуйя. Туше́. Заседание продолжается.

— Так в чем же мораль? — спросит въедливый читатель. Да просто знай, люби и творчески применяй бессмертную формулу мультистейкхолдеризма. А Себастиан Б., кстати, в Правление, переизбран не был.

Анатомия рефлекторных атак

Андрей Робачевский

Рефлекторные атаки с усилением являются постоянно растущей угрозой для нормального функционирования Интернета, нанося существенный экономический и социальный ущерб. Гигантская асимметрия между незначительными силами и затратами атакующего и сокрушительной мощностью атак, еще более усиленная невозможностью обнаружения и наказания преступников, делают этот класс атак сущим проклятьем Сети. Благодаря чему такие атаки возможны, каковы пути решения проблемы DDoS-атак в Интернете — об этом мы поговорим в этой статье. Этот феномен иллюстрирует особенный аспект безопасности Интернета, которая зависит не только от того, насколько хорошо удается управлять рисками, представляющими угрозу для организации и ее ресурсов, но также, что очень важно, от рисков, «исходящих» от самих участников.

В марте 2013 года, компания Spamhaus, обслуживающая так называемые черные списки сетей, являющихся источником спама и прочего безобразия, стала объектом гигантской распределенной атаки отказа в обслуживании (Distributed Denial of Service attack, DDoS attack). Услуги компании попали под обстрел сотнями миллионов пакетов в секунду и трафиком, по некоторым оценкам достигшим пика в 300 Гбит/с, сметающим на своем пути сетевое оборудование.

Эта атака не исключение. В первом квартале 2015 года, по данным компании Arbor Networks, имела место атака в 334 Гбит/с. В том же квартале они зафиксировали 25 атак с объемом трафика больше, чем 100 Гбит/с. Большая часть этих атак является рефлекторными DDoS-атаками с усилением.

Этот тип атак также не нов – «технология» рефлекторной атаки с усилением впервые получила широкую известность в 1997 году. Но что действительно вызывает озабоченность, так это насколько относительно легко такие атаки организовать. Действительно, атаки этого типа довольно незатейливы и в то же время весьма разрушительны, благо «строительного материала» в Интернете предостаточно. Основными «строительными блоками» является наличие ботов с возможностью подмены IP-адреса источника (установка его на IP-адрес жертвы) и «рефлекторы» - например, открытые DNS-резолверы. Хорошо выбранный запрос DNS может предоставить 100-кратное усиление, что означает, что нужно сгенерировать 100 запросов общим потоком в 3 Гбит/с для создания сокрушительного суммарного потока в 300 Гбит/с. Этого можно достичь с помощью относительно небольшого набора клиентов.

Есть, конечно, DDoS-атаки, которые не используют эти два компонента; они бомбардируют жертву напрямую от многих глобально распределенных источников. Но такие атаки можно оттрассировать и они на два порядка сложнее и дороже.

Давайте попробуем разобраться, как работает рефлекторная атака, каковы условия ее эффективного проведения, способы противодействия и возможности искоренения этого зла.

Рефлекторные атаки с усилением

Суть рефлекторной атаки достаточно проста и базируется на трех основных ингредиентах:

- **Использование возможности «спуфинга»** — подмены IP-адреса отправителя на адрес «жертвы» с протоколами вроде UDP или ICMP, обеспечивающего передачу дейтаграмм без создания соединения. Такие широко распространенные услуги Интернета, как SNMP и DNS используют именно этот протокол передачи. Ключевым фактором здесь является отсутствие необходимости «рукопожатия», как, например, в случае с TCP, для начала передачи данных.
- **Рефлекторы и усилители**. Поскольку режимом работы многих услуг, основанных на протоколе UDP, является «запрос-ответ», подмена адреса отправителя на адрес «жертвы» приведет к тому, что ответ на запрос будет доставлен именно туда. Представьте, что такого типа запросы посланы из различных точек Интернета. Все ответы на эти запросы будут направлены на один адрес, обеспечивая значительную концентрацию трафика в направлении «жертвы». «Хороший» рефлектор также является усилителем, что означает, что размер ответа во много раз превышает размер запроса. Это позволяет создать асимметрию, когда относительно незначительный трафик запросов превращается в мощный ответный поток.
- **Ботнеты**. Для эффективных атак такого рода необходима хорошо распределенная сеть источников. Инфицированные компьютеры, объединенные в ботнеты, являются для этого прекрасной стартовой площадкой.

Смешав эти ингредиенты, мы получим рефлекторную атаку с усилением.

Работает она следующим образом.

- Выбирается один или несколько усилителей-рефлекторов. В качестве таковых могут служить DNS-серверы и «открытые» резолверы (о них мы поговорим чуть позже), готовые предоставить ответ на запрос со значительным коэффициентом усиления. Типичным является усиление трафика в 30-60 раз, но в некоторых случаях коэффициент усиления может достигать нескольких тысяч – см. таблицу 1 «Типичные усилители».

- Компьютеры ботнета получают инструкцию начать атаку на жертву. По команде они посылают заданные запросы выбранным усилителям-рефлекторам, подменяя адрес отправителя на IP-адрес жертвы.

- Серверы-рефлекторы отвечают на невинные с виду запросы, реально поступающие от различных клиентов, в то же время обрушивая усиленный трафик на жертву. Поскольку обычно используется большое количество рефлекторов, расположенных в различных точках Интернета, объем трафика увеличивается по мере приближения к жертве.

- Объем сгенерированного трафика превышает пропускную способность каналов или максимальную производительность атакуемого сервера, тем самым вызывая отказ в обслуживании, или невозможность предоставления услуг. Услуга, подвергшаяся атаке, на какое-то время перестает быть доступной в Интернете. Этот процесс схематически представлен на рис.1.

Классическим примером рефлекторной атаки является так называемая атака “smurf” (получившая это название по имени модуля атакующей программы smurf.c, появившейся в Интернете в 1997 году, более подробно). По сценарию этой атаки атакующий посылает запрос ICMP на широковещательный (broadcast) адрес локальной сети, в то же время подменяя адрес источника на адрес жертвы. По правилам все устройства локальной сети должны отреагировать на этот запрос, тем самым генерируя трафик в направлении жертвы. В зависимости от числа устройств локальной сети трафик может достигать значительного объема.

В качестве рефлекторов-усилителей также могут служить устройства поддерживающие открытый доступ к услуге SNMP (Simple Network Management Protocol), используемой для мониторинга и управления сетью. Например, сценарий проведения SNMP-атаки включает использования ботнета для генерирования сотен тысяч запросов “GetBulkRequest” к сотням таких устройств. В этих атаках часто используются оконечные пользовательские устройства/домашние маршрутизаторы, на которых по умолчанию включена поддержка SNMP на «публичном» (обращенном к глобальному Интернету) интерфейсе. Размер типичного запроса “GetBulkRequest” составляет 60-102 байт (RFC3416), в то время как ответ на него гораздо больше — 423-1560 байт, что может обеспечить усиление в более чем 25 раз.

Поскольку атакующий генерирует незначительный трафик с географически распределенного ботнета, этот трафик трудно идентифицировать и заметить что-либо подозрительное. В подавляющем большинстве владельцы компьютеров ботнета сами не подозревают, что они являются источником атаки. А использование спуфинга адреса отправителя делает задачу определения источника практически невозможной.

Таблица 2. Типичные Усилители.
Источник: C. Rossow, «Amplification Hell: Revisiting Network Protocols for DDoS Abuse»

Протокол	Протокол/ Порт	Наблюдаемый коэффициент усиления	Число доступных рефлекторов-усилителей
DNS	UDP/53	100	7-15M
SNMPv2	UDP/161	12	5M
NTP	UDP/123	4600	1.5M
CHARGEN	UDP/19	360	90K
SSDP	UDP/1900	80	3.7M

Спуфинг – неизлечимое зло?

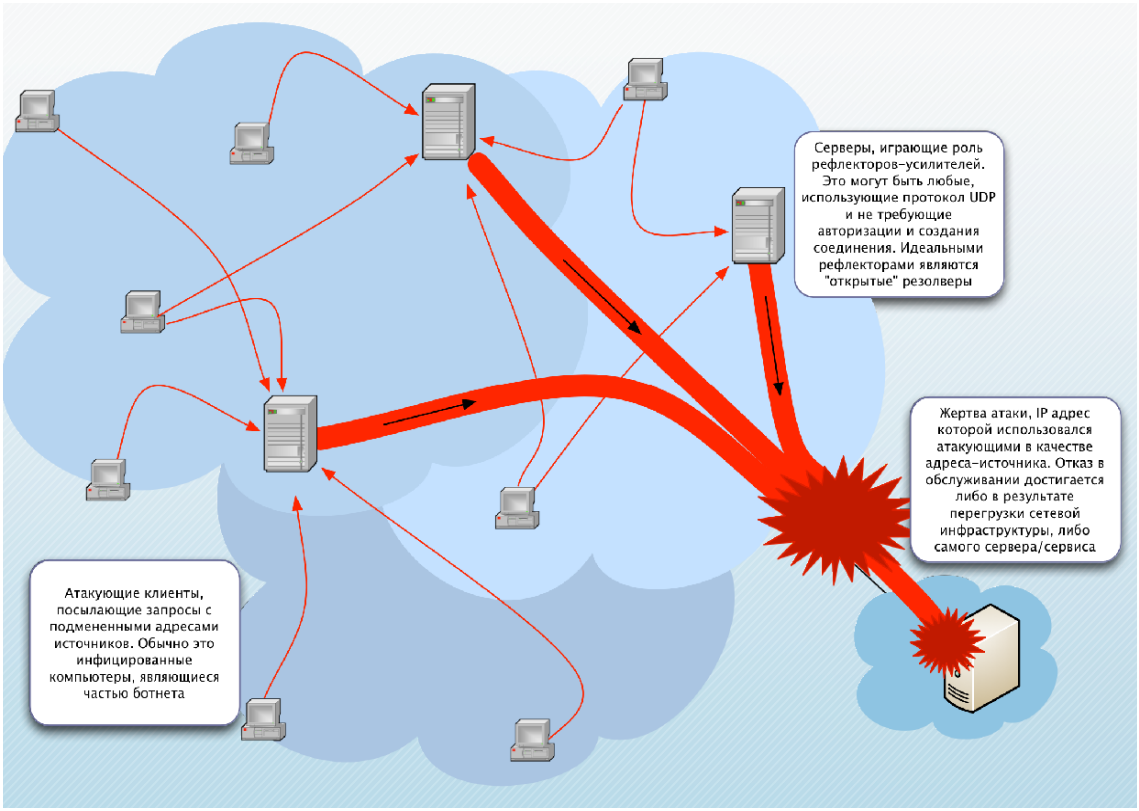
В Интернете маршрутизация, за редкими исключениями, происходит на основе адреса получателя. Каждый маршрутизатор на пути следования пакета смотрит на IP-адрес получателя и определяет лучший путь к нему, передавая его следующему маршрутизатору, и так далее, пока пакет не достигнет конечного пункта назначения. При этом на адрес отправителя мало кто обращает внимание.

Это означает, что какой бы адрес получателя мы ни задали, пакеты все равно найдут своего получателя. Использование «чужого» адреса, или спуфинг, считается неправомерным, но с точки зрения системы маршрутизации, вполне допустимым.

Разумеется, спуфинг не имеет никакого смысла для простого пользователя услуг Интернета, поскольку обычно предполагается двусторонний обмен данными — и получение ответов обратно. Но для проведения рефлекторных атак, как мы уже говорили, эта возможность незаменима. Более того, спуфинг позволяет атакующему практически не оставить следов. Отслеживание источника трафика с подмененными адресами чрезвычайно сложно и требует кооперации со стороны многих сервис-провайдеров, сбора и обмена данными и т.п. И даже если источник будет найден, он приведет к инфицированному компьютеру и его не ведающему о своем участии в атаке владельцу.

Возможность использования спуфинга для проведения атак известна давно – уже упоминавшиеся smurf-атаки использовали эту возможность для атаки жертвы с помощью протокола ICMP. Спуфинг может быть использован в любой рефлекторной атаке, а в качестве рефлектора может выступать практически любое устройство, подключенное к Интернету и принимающее входящие запросы. Все серверы, обеспечивающие услуги на базе TCP, например, веб-серверы, являются рефлекторами, поскольку на запрос на создание

Рис.1. Схема рефлекторной атаки с усилением



соединения TCP SYN сервер ответит пакетом SYN-ACK. Однако такие атаки не обладают усиливающим эффектом, что значительно снижает их привлекательность.

BCP38

В начале века были предложены способы противодействия спуфингу. Эти рекомендации известны под именем BCP38. Суть их проста - интернет сервис-провайдер должен отфильтровывать пакеты своих клиентов, адрес отправителя которых находится вне диапазона зарегистрированных адресов этого клиента. Разумеется, наиболее эффективным и безошибочным будет применить эту фильтрацию именно на границе между провайдером и его клиентом.

Основным методом является фильтрация трафика клиентов на основе списков доступа ACL (Access List), пропускающая любые пакеты с адресом источника в диапазоне сетей клиента и блокирующая любой другой трафик.

В случае типичного интернет сервис-провайдера такая фильтрация происходит на маршрутизаторах доступа, служащих для подключения сетей клиентов.

В случае сетей широкополосного доступа идеальным местом искоренения спуфинга являются широкополосные концентраторы доступа (Broadband Access Concentrators, BAC), которые агрегируют пользовательские каналы. Примерами BAC являются DSLAM (Digital Subscriber Line Access Multiplexer) для DSL-сетей или CMTS (cable modem termination system) для кабельных широкополосных сетей. Преимуществом использования BAC в качестве места фильтрования трафика с подложными адресами является то, что здесь можно отдельно идентифицировать каждое соединение, далее они мультиплексируются и задача становится сложнее.

Задача фильтрации в широкополосных сетях осложняется, если назначение IP-адресов пользователей происходит динамически, с помощью DHCP. В этом случае BAC должен контролировать все DHCP-запросы/ответы, извлекая из них информацию о назначенных адресах.

Надо заметить, что спуфинг в широкополосных сетях доступа может представлять серьезную проблему для самого оператора (в отличие от более распространенной ситуации, когда спуфинг скорее является угрозой для других сетей). Например, с помощью спуфинга злоумышленник может перехватить трафик другого пользователя, нарушить систему учета, получить неавторизованный доступ к услугам или запустить атаку отказа в обслуживании на других пользователей сегмента. Не случайно проверка адреса источника SAV (Source Address Verification) является обязательной частью спецификации DOCSIS 3.0 (Data-Over-Cable Service Interface Specifications), определяющая передачу данных в кабельных сетях.

uRPF

Для автоматизации фильтрации пакетов с подложными адресами в сетях операторов, предоставляющие услуги доступа в Интернет другим сетям, в 2004 в документе BCP84 было предложено использование механизма uRPF (Unicast Reverse Path Forwarding).

Идея uRPF заключается в использовании информации в таблице передачи FIB (Forwarding Information Base) — дистиллированной версии таблицы маршрутизации – для определения, может ли пакет с определенным адресом отправителя быть принят на конкретном сетевом интерфейсе.

Логика uRPF проста: если пакет получен с сетевого интерфейса, который, согласно FIB, используется для передачи данных, адресованных отправителю этого пакета, то пакет считается прошедшим проверку. В противном случае пакет отбрасывается.

Чтобы проиллюстрировать эту идею, рассмотрим сетевого оператора, обеспечивающему доступ нескольким сетям-клиентам (Рис. 2).

Предположим, что сеть-клиент анонсирует свои префиксы сетевому оператору. В этом случае записи таблицы FIB оператора для данных префиксов будут указывать на сетевой интерфейс, через который получен анонс и через который должна производиться передача данных, адресованных этой сети. Если через этот сетевой интерфейс будет получен пакет с адресом отправителя, не соответствующим ни одному из анонсируемых префиксов для данного интерфейса (203.0.113.1), – он будет отброшен.

Ситуация осложняется, когда сеть-кли-

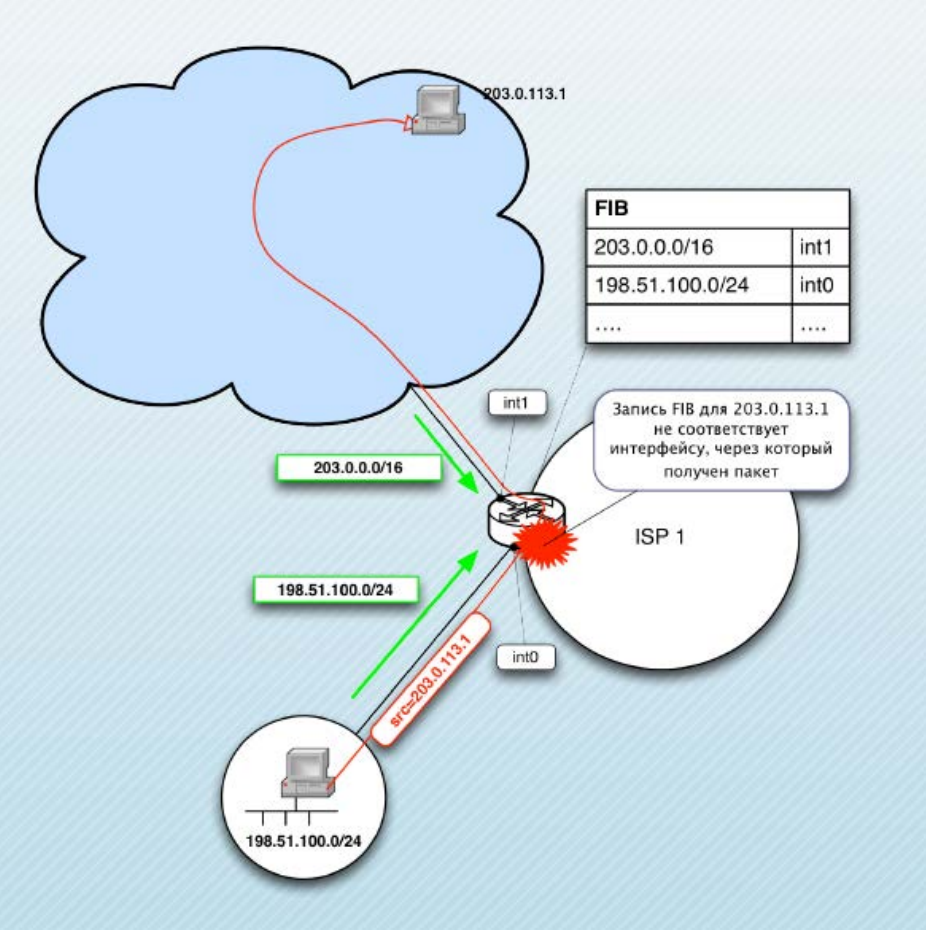
ент использует несколько провайдеров, поскольку uRPF предполагает, что прием и передача данных для конкретного адреса производится через один и тот же интерфейс. В данной же ситуации анонсы префикса клиента могут быть приняты с нескольких интерфейсов (Рис. 3) – например, непосредственно от клиента и от пиров, также являющихся его провайдерами. Поскольку FIB содержит лишь «лучший маршрут», а именно только один интерфейс, через который следует передавать данные сети-клиенту, возникает асимметрия: легитимные пакеты могут быть получены с интерфейса, отсутствующего в FIB, и, соответственно, отброшены.

Для решения этой проблемы, существенно ограничивающей область применения данного метода, в uRPF были внесены изменения, получившие название feasible uRPF. В рамках усовершенствованного метода проверка адреса источника производится относительно не только «лучшего маршрута», но и всех других возможных маршрутов, полученных от пиров. За счет этого feasible uRPF работает в подавляющем большинстве случаев многопровайдерного подключения.

Существуют, правда, ситуации, когда маршрут не анонсируется провайдером, но передача данных от этой сети все равно возможна. Во многих случая это симптом какой-либо аномалии, независимо от uRPF, и фильтрация трафика позволяет выявить их. Однако в ряде случаев, например, когда сеть-клиент осуществляет балансирование трафика между несколькими провайдерами, анонсируя им только часть сетей и не заботясь о пути, по которому передается обратный трафик, такая асимметрия вполне допустима, и использование uRPF приведет к отбрасыванию легитимного трафика клиента.

Еще одной особенностью является применение uRPF в случае, когда используется не полная таблица маршрутизации, а так называемый default маршрут. В этом случае для трафика, полученного с интерфейса, на который указывает маршрут default, любой адрес источника, даже при отсутствии соответствующей записи FIB, пройдет проверку, поскольку «default» означает «все возможные маршруты», что, собственно, эквивалентно отсутствию фильтрации вообще. Решением в данной ситуации является использование feasible uRPF на клиентскихи пиринговых интерфейсах и не использование uRPF на интерфейсе, с которого получен default маршрут.

Рис.2. Работа uRPF в простейшем случае подключения



Идеальные рефлекторы

Начиная с конца 1990-х DNS активно используется в качестве рефлектора и усилителя. Действительно, DNS является для этого идеальной услугой:

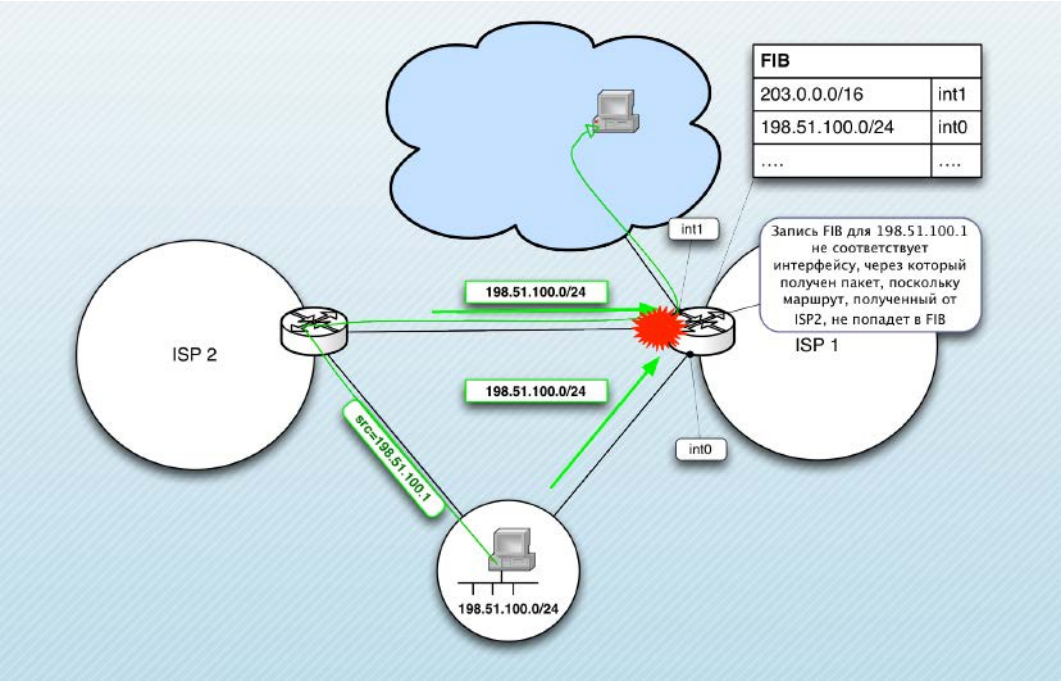
- DNS использует UDP, не требующий создания соединения и, таким образом, позволяющий спуфинг;
- DNS является жизненно необходимой услугой, поэтому фильтрация входящего DNS-трафика практически не применяется;
- DNS является хорошим усилителем трафика, поскольку всегда можно найти запрос, размер ответа на который намного превышает размер самого запроса.

Это последнее свойство было известно с самого начала, однако ограничение максимального размера ответа в 512 байт позволяло достичь лишь 8-9-кратного усиления. Ситуация существенно изменилась с внедрением расширений EDNS0, позволяющих использовать дейтаграммы размером более 512 байт, и DNSSEC, включающих дополнительные данные. Если раньше для создания максимально возможного ответа использовались синтетические записи (например, специально созданная запись TXT для определенного домена), то теперь стало возможно генерировать ответы большого размера для запросов, не вызывающих подозрения и использующих вполне безобидные домены.

Еще одной особенностью DNS является факт, что его распределенная сеть состоит из сотен миллионов серверов, обеспечивающих обработку запросов. Здесь уместно заметить, что все серверы можно разделить на две основные категории – так называемые авторитетные серверы, отвечающие за определенные домены и связанные с ними записи, и кэш-резолверы, обслуживающие весь рекурсивный процесс разрешения имен для клиента и предоставляющие последнему окончательный ответ.

Операционная практика предписывает авторитетным серверам отвечать только на запросы по доменам, которые они обслуживают, а резолверам – обрабатывать только запросы собственных клиентов – например, пользователей корпоративной сети. В реальности, к сожалению, зачастую авторитетные серверы также выполняют функцию резолверов, а резолверы готовы обслужить

Рис.3. Работа uRPF и возможные проблемы в условиях подключения клиента к нескольким провайдерам



запрос любого клиента. Такие серверы получили название «открытых» резолверов.

Открытые резолверы представляют серьезную проблему, поскольку являются идеальными рефлекторами-усилителями: они готовы обслужить запросы от любого клиента, их число колоссально, они повсеместны. По подсчетам проекта "Open Resolver" сегодня существует более 15 миллионов таких серверов!

Решение этой проблемы, или «закрытие» резолвера, обычно состоит в задании списков доступа, в который включаются сети локальных клиентов, для которых данный резолвер обеспечивает трансляцию имен. Рекомендации по обеспечению правильного функционирования резолвера опубликованы в RFC5358. Однако следует иметь в виду, что даже в этом случае, при отсутствии мер по антиспуфингу, о которых мы только что говорили, остается возможность использования резолвера для атаки локальных клиентов.

Response Rate Limiting (RRL) – ограничение частоты ответов

С появлением возможности генерирования ответов большого размера со значительным усилением авторитетные серверы также могут эффективно использоваться в атаках в качестве усилителей-рефлекторов. Для уменьшения этого риска Пол Викси (Paul Vixie) и Вернон Схряйвер (Vernon Schryver) предложили механизм ограничения частоты ответов, сначала внедренный в ПО BIND 9 (ISC), а впоследствии в Knot DNS (CZ-NIC) и NSD (NLnet Labs).

Идея механизма проста: сервер отвечает только на ограниченное число запросов от одного и того же клиента, которым соответствует один и тот же ответ, в соответствии с заданным администратором параметром – числом ответов в секунду. Идентичными являются ответы для одного и того же существующего доменного имени (qname) и типа записи (qtype). Ответы на несуществующие поддомены (NXDOMAIN) или пустые запросы (NODATA) также считаются идентичными и, соответственно, учитываются при подсчете.

В отношении клиентов идентичными считаются клиенты, принадлежащие одной и той же сети (адресному блоку), размер которой задается администратором.

Этот механизм в первую очередь предназначен для авторитетных DNS-серверов. В случае рекурсивных резолверов применять его следует с большой осторожностью, чтобы не нарушить работу локальных клиентов. Дело в том, что ввиду недостаточного кэширования DNS-ответов многими приложениями повторимость одинаковых запросов к резолверам от локальных клиентов достаточно велика, что может включить механизм ограничения. Например, при получении почтового сообщения почтовый сервер SMTP сделает запрос на записи NS, PTR, A и AAAA для входящего SMTP-соединения. Далее при получении команды MailFrom для этого же сообщения сервер сделает дополнительные запросы для записей NS, A, AAAA, MX, TXT и SPF.

Некоторые веб-браузеры также запрашивают одни и те же имена при обработке встроенных в веб-страницу изображений. Как мы уже говорили, наиболее правильным решением в этом случае является «закрытие» резолвера таким образом, что он отвечает только на запросы, поступающие от локальных клиентов.

Как я уже упоминал, DNS является не единственным эффективным усилителем. На рис. 4 показан растущий тренд использования других приложений. Например, по данным системы ATLAS компании Arbor Networks, в первом квартале 2015 года серверы точного времени, использующие протокол NTP, применялись в качестве рефлекторов-усилителей почти в 14% всех зафиксированных атак. Проект "NTP Scanning Project" содержит статистику потенциально открытых серверов времени, а также рекомендации по их проверке и правильной конфигурации. Другим популярным протоколом стал SSDP, использующийся для обнаружения устройств UPnP (Plug&Play). Многие оконечные устройства домашних сетей поддерживают этот протокол и являются открытыми для приема запросов извне сети, делая их замечательными рефлекторами, подобно открытым DNS-резолверам. Не исключено, что в будущем мы увидим новых фаворитов.

Как защититься?

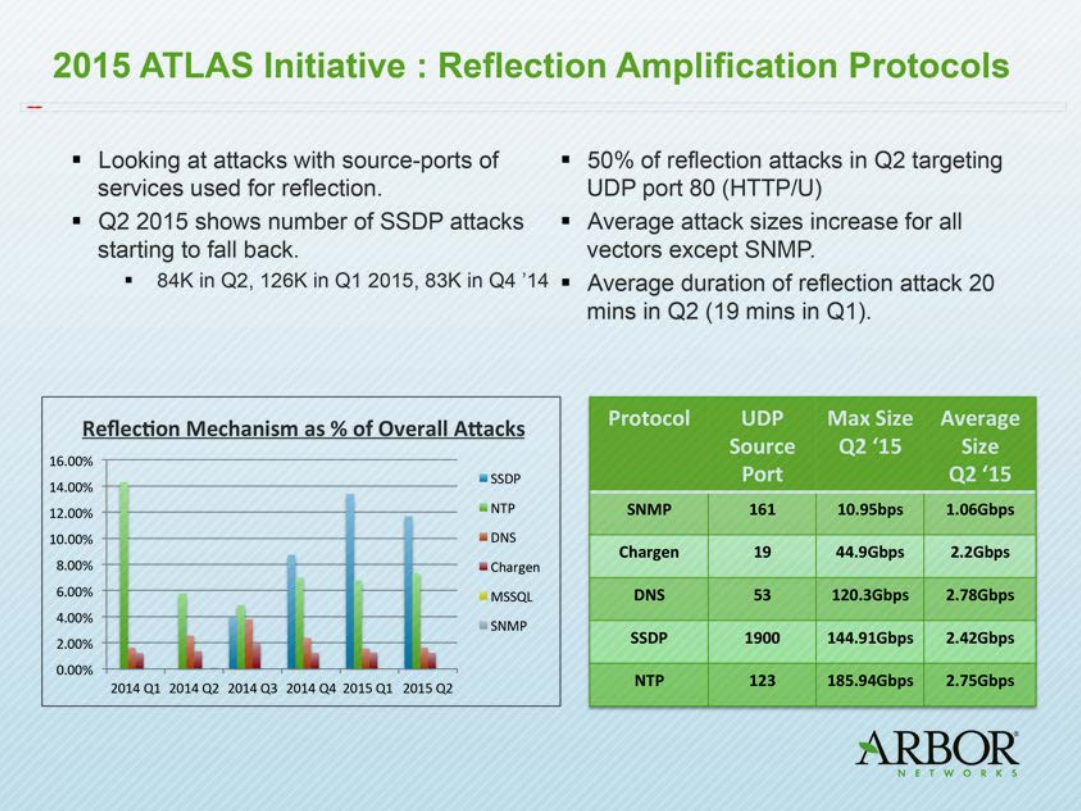
Надеяться на то, что атаки DDoS при всей простоте их проведения и плодородности среды их обитания сойдут на нет, нереалистично. И хотя полностью защититься от атаки DDoS во многих случаях либо не представляется возможным, либо это является очень дорогостоящим удовольствием, каковы же возможности уменьшения ущерба от атаки?

Наращивание производительности

Чем больше пропускная способность вашей сети и мощность серверов, тем потре-

буется более мощная атака и больше времени, чтобы привести к отказу в обслуживании ваших услуг. Однако силы здесь, к сожалению, неравны. Сгенерировать трафик в 1 Гбит/с несравнимо проще и дешевле, чем его обработать. Тем не менее, географически распределенная инфраструктура предоставления услуги и хорошая связность, в том числе с использованием многочисленных провайдеров транзита, может существенно усилить противостояние атакам.

Рис.4. Использование различных «усилителей» в рефлекторных атаках. Источник: Данные ATLAS компании Arbor Networks, http://www.slideshare.net/Arbor_Networks/atlas-q2-2015final



Использование технологии anycast

Для ряда услуг, особенно использующих транспортный протокол UDP и не требующих создания соединения, все более широкое распространение получает технология anycast. Суть ее заключается в анонсировании оператором одной и той же сети (префикса IP и автономной системы) в различных частях Интернета. Благодаря архитектуре системы маршрутизации, для любого клиента существует единственный и самый «короткий» путь к любой другой сети Интернета. Таким образом, anycast позволяет клиенту установить связь с наиболее близкой в топологическом смысле сети anycast без дополнительных изменений в ПО и протоколах.

Хотя эта технология наиболее широко используется для предоставления услуг DNS, при определенных условиях она может также быть использована даже для веб-услуг.

В отношении DDoS anycast позволяет уменьшить концентрацию трафика и локализовать атаку, создавая местные «точки притяжения».

Блокирование трафика на границе

Для больших географически распределенных сетей, например, для сетевых операторов, предоставляющих интернет-доступ корпоративным клиентам, атаки DDoS могут концентрироваться внутри самой сети, блокируя часть внутренней инфраструктуры и вызывая побочный ущерб, затрагивающий не только атакуемого, но и других клиентов. В этом случае блокирование атакуемого трафика необходимо осуществить как можно раньше, на границе сети.

Распространенным способом автоматизации этого процесса и значительного уменьшения времени реакции на подобные инциденты является метод RTBH (Remotely Triggered Black Hole, дословно «черная дыра, управляемая на расстоянии»). С его помощью внутреннее анонсирование атакуемой сети по протоколу iBGP специальным образом приведет к отбрасыванию трафика, адресованного этой сети, на граничных маршрутизаторах. Таким образом удается устранить побочный ущерб, хотя сама атака достигает желаемого результата – отказа в обслуживании. Подробно метод RTBH описан в RFC5635 .

Координация с пирами и провайдерами транзита

В противодействии начавшейся атаке большую помощь могут оказать пиры и провайдеры транзита. Как правило, в их сетях объем трафика атаки еще не достигает разрушительного размера — и они могут предпринять какие-либо действия, в то время как поток на границе вашей сети уже может превышать доступную мощность. И если вы в такой ситуации бессильны, ваши пиры могут, например, блокировать определенный тип трафика в своей сети, тем самым уменьшив ваши страдания.

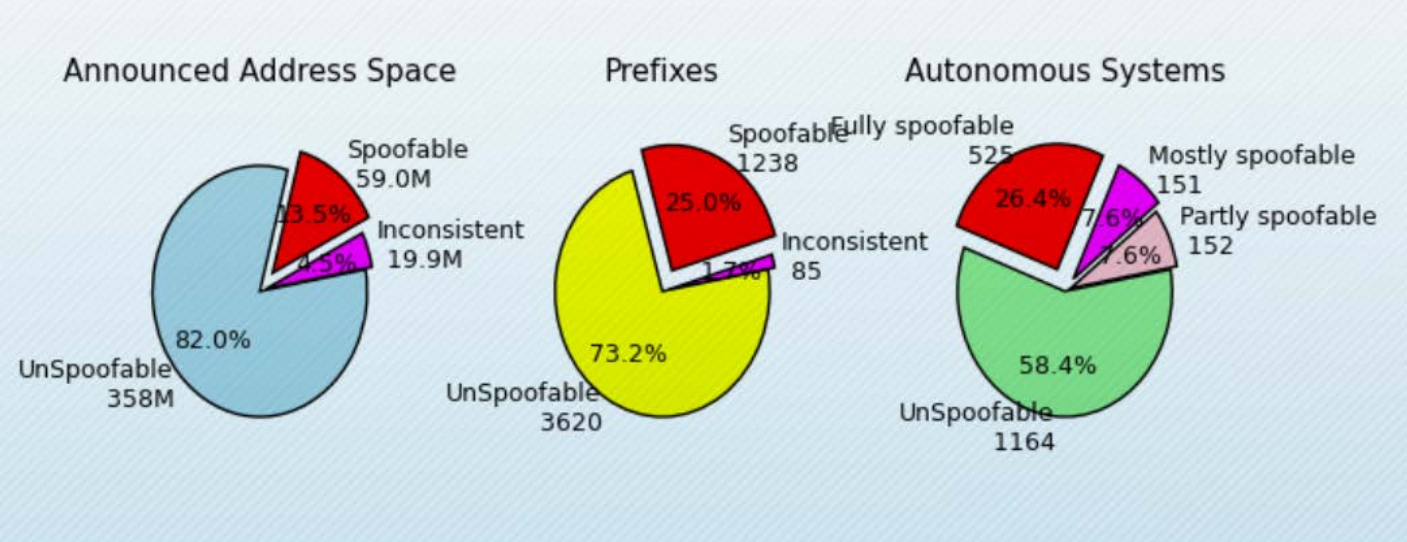
Для успешной координации необходимо хорошо знать своих соседей и иметь альтернативные способы общения с ними, т.к. электронная почта может не работать в такой ситуации.

Использование коммерческих продуктов и услуг по борьбе с атаками DDoS

Сегодня многие провайдеры облачных услуг хостинга включают противодействие атакам в свой пакет. Также существуют и специализированные услуги, например, от компании Akamai (например, Prolexic), Incapsula или «Лаборатории Касперского» (Kaspersky DDoS Prevention). Основой этих систем является распределенная высокопроизводительная сеть, позволяющая во время атаки перенаправлять на себя весь трафик атакуемой сети, анализировать и отфильтровывать атакующий трафик от полезного, передавая последний обратно в сеть клиента.

При достаточной производительности собственной сети можно использовать по-

Рис.5. Статистика открытых для спуфинга сетей (в процентах адресного пространства, анонсируемых префиксов и автономных систем). Источник: Проект Spoofer, http://spoofer.caida.org/



добные системы фильтрации в рамках собственной инфраструктуры и под большим собственным контролем. Примером такого решения является Pravail Availability Protection System (APS) от компании Arbor Networks.

Социально-экономические трудности

Решение проблемы распределенных атак и, в частности, рефлекторных атак с усилением, требует согласованных усилий практически всех участников экосистемы Интернета. Каждый, будь то сетевой оператор, провайдер услуг или даже пользователь, может пострадать от атаки, но также зачастую является и частью проблемы.

Посмотрим, например, на проблему спуфинга. Технические методу борьбы были опубликованы более десяти лет назад, однако спустя 11 лет ситуация далека от идеальной. Согласно статистике проекта Spoofer, предоставляющего пользователями возможность проверить, позволяет ли их сеть/провайдер спуфинг, около 23% сетей открыты (Рис. 5). Учитывая, что результаты Spoofer могут не вполне отражать реальность, поскольку в эксперименте как правило участвуют более технически образованные пользователи, возможно, имеющие больший контроль за своей сетью, это довольно широко открытая дверь для проведения рефлекторных атак.

Печальна ситуация и с открытыми рефлекторами. Это и открытые резолверы (15 М), и открытые серверы времени (1,5 М), и системы, поддерживающие SSDP (3,7 М). Причина в большей степени экономическая. Например, внедрение механизмов антиспуфинга означает затраты, требует более подготовленного персонала и включает определенные риски (например, ошибочную фильтрацию легитимного трафика), в то же время преимущества этих мер недостаточно ощутимы. Меры эти позволяют исключить возможности использования сети в качестве стартовой площадки, но для безопасности самой сети и защиты ее от внешних атак они мало что значат.

Многие открытые рефлекторы являются бесплатным приложением модемов и маршрутизаторов в домашних сетях – оконечных устройств в сетях широкополосного доступа.

Известный экономический принцип экстерналии в известной мере объясняет недостаточную степень внедрения достаточной защиты сервис-провайдерами и производителями оборудования. Например, в отношении спуфинга для изменения этой ситуации должна быть существенно уменьшена стоимость мер защиты и выявлены дополнительные преимущества.

Одним из путей изменения первой части этого уравнения является внесение отрицательной стоимости – «штрафования» за неиспользование антиспуфинга. Это может быть как вмешательство регулятора, так и давление со стороны индустриальных партнеров. Дополнительные преимущества также не обязательно должны лежать непосредственно в материальной сфере - вопросы репутации и индустриальная кооперация могут стимулировать применение этой практики, в результате которой экосистема в целом станет более защищенной и неприспособленной для этого типа атак. В этой ситуации, разумеется, выигрывают все положительные герои моей статьи.

Хочется заметить, что Интернет, с его высокой степенью связности и взаимозависимости, открывает новый аспект безопасности. Безопасность и устойчивость Интернета зависит не только от того, насколько хорошо удается управлять рисками, представляющими угрозу для организации и ее ресурсов, но также, что очень важно, от признания и управления рисками, которые представляет сама организация (в результате своих действий или бездействия) для экосистемы Интернета — так сказать, «исходящих» рисков. Этот аспект не всегда очевиден, особенно потому, что преимущества от снижения таких рисков неявны. Однако он является существенным условием фундаментального решения проблемы DDoS-атак в Интернете.

IT-конференции

Ольга Александрова-Мясина

В прошлом выпуске я рассказывала вам про IT-конференции, на которых мне довелось побывать, и закончила казанским ENOG, который состоялся в июне, а в этом выпуске расскажу, чем мне запомнилось второе полугодие

В начале июля Технический центр Интернет проводил вторую встречу DOMINO (Доменная Индустрия) для регистратур и ICANN-аккредитованных регистраторов. Мы придумали это мероприятие, чтобы коллеги могли и поработать (деловая часть), и отдохнуть. На DOMINO основное время посвящено профессиональному образованию, которое дается в игровой форме. В прошлом году участники снимали кино. Было предложено разбиться на команды и сделать короткий фильм о работе технических центров. Потом всем коллективом смотрели на то, что получилось, и очень смеялись. В этом же году для участников были проведены тренинг личностного роста от доцента и кандидата психологических наук **Зульфии Камалетдиновой** и мастер-класс по приготовлению шашлыков от **Кирилла Готовцева**. Мы же показали Кириллу мастер-класс по их поеданию.

С самого начала как-то всё пошло не так: накладка европейских мероприятий, сложная политическая обстановка и общее напряжение в атмосфере не позволяли делать все так, как задумывалось. Любое дело шло как по наждачной бумаге, да еще и с препятствиями. Во-первых, долго не могли выбрать подмосковный отель: то стоимость не подходила, то условия. Во-вторых, не складывалась деловая программа. Мы танцевали танцы с бубнами вокруг спикеров и пытались склеить темы, которые не склеивались. А в конце несколько человек, на которых мы рассчитывали, вообще отменили визит в Москву. Таким образом, пришлось корректировать сценарий почти на коленке, а время неумолимо двигалось к обозначенной дате К слову сказать, лето в этом году тоже не задалось, и пришлось загружать в машину свитера и куртки вместо платьев и панам. К ним же был погружен и мой друг этого лета – самокат.

Мероприятие началось в первый день с тренинга, а утром второго дня стартовала деловая часть.

Главная задача, которую ставят перед собой участники **DOMINO**, – это налаживание контактов между регистратурами и обсуждение вопросов взаимодействия регистратур национальных доменов и новых доменов верхнего уровня с backend-провайдерами. В прошлом году на первой встрече DOMINO эти вопросы уже поднимались, тогда же участники встречи поделились своим видением того, как в техническом плане должна быть организована поддержка как традиционных, так и новых доменов, и что регистратуры, собственно, ожидают получить от технического центра.

Через год требования к техцентру приобрели четкие формы. К традиционным требованиям по безопасности, надежности и скорости работы прибавилось требование юридической гибкости по отношению как к регистратурам, так и к их клиентам. А такой подход возможен только в большом профессиональном техническом центре, который работает с регистратурами разных стран. По оценке заместителя генерального директора Технического центра Интернет Марины Никеровой, сегодня на смену маленьким техцентрам, где поддерживался один домен верхнего уровня, приходят большие многопрофильные компании, которые готовы поддерживать десятки миллионов доменных имен и предоставлять самые разные услуги.

Мероприятие DOMINO ежегодное, формат думаем оставить прежним, будем менять только места. В общем, поживем - увидим.

В сентябре нас ждала конференция **TLDCON** (Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы) в Ереване.

Армения! Страна солнца и фруктов. С восточным гостеприимством и коньячным заводом. Как много я слышала об этом месте, и как непередаваемо с эффектом 5D эти рассказы друзей пришли в мою реальную жизнь. Наверное, как любой восточный город мира, столица Армении произвела на меня впечатление своим контрастом. Здесь на дороге можно встретить дорогущую иномарку и «копейку» с мешком овощей на крыше, стоящие рядом на светофоре. Или пожилую женщину в черной одежде, которая выгуливает козу, и модно одетую молодую девушку, которая что-то весело рассказывает по телефону. А еще, конечно, рынок!

Нам удалось побывать на том, что около вокзала, куда нас любезно отвезла Анна Караханян. Аня работает в ISOC и, помимо всего прочего, прекрасный и отзывчивый человек. Благодаря ей мы находили всё что угодно и сразу - в незнакомом городе. Ну а как можно пройти мимо гастрономического сумасшествия из мяса, фруктов и специй? Никак. Потому мы отправились на рынок, и когда уходили обратно, то еле могли тащить за собой огромные сумки с разнообразной едой. Я, конечно, уже плохо помню, но, по-моему, кто-то даже не удержался и купил пару-тройку килограммов картошки...

В первый день конференции в зале не работал WI-FI. С одной стороны – и хорошо! Посетители будут слушать доклады, а не сидеть в соцсетях – думала я. Но с другой стороны – вся наша жизнь и работа сейчас связана с Интернетом: ведение Twitter'а мероприятия, выкладывание новостей, фотографий и т.д. То есть - работать-то как? Что, можно возвращаться в номер и спать ложиться? Все эти мысли были в моей голове, с менеджерами отеля я старалась говорить конструктивно, при этом была злая,

хуже собаки, и на вопросы коллег отвечала односложно.

Менеджмент отеля где-то можно было понять. Естественно, на обычных мероприятиях участники пользуются Интернетом, но как-то в меру! Например, не все, или все, но не одновременно. У нас же если пришло 150 человек, то все одномоментно достают еще по три устройства - и на этом Интернет в отеле заканчивается. Самое главное, что я всё это уже проходила много раз, а тут как-то поверила заверениям о том, что всё хорошо, и не настояла на дополнительном и страховочном варианте.

Но, собственно, отсутствие Интернета – это не повод задерживать открытие конференции. Тем более что мероприятие этого года собрало рекордное число участников – 130 делегатов, представлявших национальные регистратуры и регистраторов из 20 стран мира. Конференцию мы проводили вместе с Техническим центром Интернет при поддержке ICANN, Общества Интернет Армении и Армянского форума по управлению Интернетом. Поэтому на открытии у нас выступал и вице-президент ICANN Михаил Якушев, и главный человек армянского Интернета – председатель ISOC Армении Игорь Мкртумян.

После открытия началась практическая работа всех участников. Главной темой первого дня работы стали новые домены верхнего уровня. Сегодня во всех новых общих доменах зарегистрировано почти 7 миллионов имен. Всего делегировано чуть меньше 700 доменов, и более чем в половине из них идет открытая регистрация. Отметку в 100 тысяч регистраций преодолели 10 доменов.

Оправдались ли ожидания новых регистратур, регистраторов и самой корпорации ICANN?

В конце июня организация ICANN сообщала, что показатели регистраций в новых общих доменах верхнего уровня оказались существенно ниже запланированных: в начале 2014 года корпорация прогнозировала 33 миллиона регистраций, результат середины 2015 года оказался почти в пять раз меньше. Примечательно, что в принятом бюджете ICANN на следующий финансовый год понятие «ожидаемое число регистраций» вообще отсутствует.

Но пессимизм ICANN разделяют далеко не все регистратуры и регистраторы. Например, представители двух российских регистраторов, RU-CENTER и «101 Домен», которые активно включились в программу New gTLD, оценивают первые результаты программы весьма позитивно. Их представители отметили, что для российских регистраторов новые домены верхнего уровня оправдали ожидания, а наиболее успешными оказались домены, регистратуры которых отличаются грамотным построением маркетинговой компании и хорошей организацией рекламы своих доменных зон. В отличие от российских коллег, европейская регистратура пока недовольна результатами программы. Одной из причин этого стала не всегда продуманная маркетинговая и рекламная программа отдельных регистратур, а также неполная готовность регистраторов. Крупные регистратуры типа Afilias или Donuts использовали все возможные ресурсы для продвижения «своих» новых доменов, и это дало результаты. Но подавляющее большинство остальных новых доменов оказалось в гораздо худшем положении.

Участники второй секции, посвященной новым доменам – «New gTLD vs вторичный рынок. Что выберут пользователи», – отметили, что увеличение числа доменов верхнего уровня практически не повлияло на общее число регистраций доменных имен: скорее, произошло перераспределение регистраций и некоторое их количество «мигрировало» в новые домены. Далеко не все компании, работающие на доменном рынке, удовлетворены ситуацией с новыми доменами.

Рост доменного пространства предъявляет новые требования и к компаниям, которые обеспечивают стабильность и надежность работы Интернета, занимаются строительством и эксплуатацией инфраструктуры сети, предоставляют услуги регистратурам и регистраторам. Участники секции «Новые бизнесы бэкенд-провайдеров» обсудили, как работают крупнейшие инфраструктурные компании в новых условиях и на какие вызовы им приходится оперативно реагировать. Например, для RIPE NCC серьезным вызовом стал «Интернет вещей», для которого уже в самое ближайшее время потребуются миллионы IP-адресов. Эту проблему с легкостью решает переход на IPv6, но, как оказалось, к использованию IPv6 не готовы конечные пользователи.

Еще одной темой секции стало обеспечение безопасности в доменном пространстве. Большую работу в этом направлении ведет Технический центр Интернет, уже давно сотрудничающий в этой области с рядом крупнейших российских компаний. На платформе ТЦИ уже три года работает проект «Нетоскоп». Это исследовательская платформа для агрегации информации о вредоносных ресурсах, в работе которой сегодня участвуют Group-IB, Координационный центр, «Лаборатория Касперского», Mail.ru, «Спутник» («Ростелеком»), RU-CERT, Технический центр Интернет, «Яндекс». Также в Интернете функционирует информационно-аналитический ресурс «Нетоскоп», на котором собраны самые свежие данные о распространении киберугроз в сети и о ходе борьбы с вредоносными ресурсами. Информация на этот ресурс поступает из базы данных проекта: ее поставляют компании, участвующие в работе платформы и обменивающиеся друг с другом данными о «зловредах».

Ну а после напряженного рабочего дня участников конференции ждал ужин в национальном стиле, который мы провели в одном из ресторанов Еревана. Такого единодушия, какое было на этом ужине, я давно не припомню. Было сыто, пьяно, душевно и жарко. Народ разбился на компании и обсуждал последние новости. Развлекали нас национальными песнями и танцами. Мне всегда было интересно; выбирает же себе кто-то такую профессию – петь национальные песни! Если вдуматься, то это же полный Lifestyle, так сказать. Вот стала бы я в детстве ходить на пение не раз в неделю и не прогуливала бы музыкальную школу, а

выучилась бы на певицу и каждый бы раз в ресторанах мой вечер начинался одинаково... песней «Во поле березка стояла»... Это сколько силы воли надо, чтобы не сбежать от такого призвания? Сколько надо терпения и тренировки стойкости? То есть снимаю шляпу, как говорится, перед такими людьми. Они – достойные всяческого уважения – не давали нам скучать до полуночи. В полночь мы отправились в отель, чтобы немного отдохнуть перед вторым днем.

Во второй день конференции я вела секцию о продвижении доменов: «За кем главная роль - регистратуры или регистраторы». Это был мой настоящий «День сурка»! Потому что ровно год назад в Баку, в 10 утра я открывала секцию второго дня с такой же тематикой. В зале было, как и в прошлом году, немноголюдно, потому что утро второго дня всегда неблагодарное время, и я на правах организатора забрала его себе, чтобы приглашенным спикерам было приятнее и комфортнее. Рассказывала я о маркетинговых программах ТЦИ для регистраторов, о том, что было сделано и какие дало результаты. Обязательно напишу об этом когда-нибудь отдельную статью!

Кибербезопасность стала одним из главных мировых трендов, этой теме стали уделять внимание даже организации, до недавнего времени не занимавшиеся вопросами информационной безопасности, например, ISOC. Другая крупнейшая международная организация – RIPE NCC – одним из важных направлений своей работы считает популяризацию DNSSEC, в связи с чем участникам секции было предложено поделиться своим видением работы сертификационных центров в современных условиях.

На конференции TLDCON ежегодно встречаются представители национальных регистратур, которые используют не только латинские национальные домены, но и домены на национальных алфавитах. Поэтому секция, посвященная IDN-доменам, всегда вызывает у участников особый интерес. На секции был представлен новый национальный домен Армении .հայ (“hye”), который не так давно был делегирован этой стране.

После окончания конференции мы поехали на коньячный завод. Это была экскурсия с дегустацией. Там были прослушаны истории о создании разных видов коньяка, а также мы посмотрели на бочки, заделанные в дни визитов президентов разных стран. Их не открывают, выдерживают, чтобы потом через много лет какие-то счастливые люди могли сесть у камина холодным зимним вечером и, открыв бутылочку коллекционного 20-летнего коньяка, выпить! К слову сказать, я совсем не эксперт в этом вопросе, хотя, скорее всего, смогу отличить хороший коньяк от плохого. Другое дело, что, кроме этих эпитетов других слов мне не подобрать. То есть коньяк для меня бываеттолько двух видов: хороший и плохой. А всё остальное - это происки маркетологов, которым както надо зарабатывать деньги, в том числе и на легендах. С другой стороны, если бы всё было так, то как тогда оправдать дверь в коньячное хранилище как в банке - с кодовым замком и пуленепробиваемыми стеклами? Возможно, те бочки, которые хранятся под такой защитой, действительно ценны, и кто-то готов выложить за их содержимое кругленькую сумму.

На этом оставляем прекрасный Ереван с горами, солнцем и озером Севан, которое заслуживает отдельного описания. Когда-нибудь я обязательно расскажу историю о нашей поездке на это озеро, где удалось попробовать вкуснейший кебаб из раков с холодным белым вином.

Сейчас надо спешить дальше, к следующему событию, достойному внимания, – ENOG-10 в Одессе.

К сожалению, по некоторым обстоятельствам непреодолимой силы я не смогла поехать в этот прекрасный курортный город, хотя легенды об Одессе мучают меня с детства, еще с тех самых шаланд, которые «полные кефали». Но удалось туда поехать моему коллеге Мише Анисимову, а мне удалось его подробно расспросить о том, что и как там было. Итак, это был уже десятый ENOG. Проводили его в одном из самых красивых отелей города – «Бристоле» (когда-то гостиница «Красная»). Мероприятие длилось два дня, но гости успели все: и обсудить все насущные проблемы развития Интернета, и в полной мере ощутить гостеприимство южного города.

Программа была насыщенной, так что времени на прогулки у Миши было крайне мало. За деловой частью шел прием, за ним – посиделки с коллегами за бокалом вина и жаркими спорами о судьбах Интернета, а на следующий день все сначала. И все равно с городом ему удалось познакомиться.

Одесса, конечно же, очень похожа на все рассказы о себе. Для большинства людей это советский и постсоветский фольклор, едкий юмор, яркий, ни с чем не сравнимый колорит и обаяние местных жителей. Все таксисты, официанты, да и просто прохожие мгновенно переходят на «ты» и общаются с тобой как с давним приятелем, делятся историями, показывают город и что-то рекомендуют. К сожалению, на знаменитый «Привоз» ему не удалось попасть.

Организаторы хорошо потрудились над программой – за два дня успели поговорить о безопасности, о новых совершенно сумасшедших скоростях доступа, о том, в каком состоянии находится внедрение IPv6, и как много доменов уже подписаны DNSSEC. Так, коллеги из домена .ua рассказали, что на сегодняшний день в .ua все шесть name-серверов поддерживают оба протокола: IPv4 и IPv6. Ко всем публичным доменам (.com.ua, .kyiv.ua) предъявляется обязательное требование: наличие минимум двух name-серверов с IPv6. В домене .ua зарегистрировано 562 тысячи доменных имен, из них делегировано 450 тысяч (80%). 18% делегированных доменных имен поддерживают протокол IPv6. Лидером же внедрения IPv6 является Бельгия – в этой стране почти 38% серверов поддерживают IPv6.

Украинские коллеги также рассказали, как они строят и развивают свои точки обмена трафиком и как борются с DDoS-атаками. Спикеры из RIPENCC и ICANN в очередной раз рассказали о том, как изменится мир после передачи сообществу функций IANA.

К сожалению, в октябре даже яркие и звучные приморские города теряют часть своего очарования – осень приглушает краски и смягчает колорит. Почти все время на улице шел дождь, пронизывающий морской ветер заставлял поднимать воротник и зябко ежиться редких туристов, зато многочисленные маленькие кафе домашней кухни были просто переполнены. Там шкварчит на решетке барабулька, приветливые официанты разносят посетителям пиво, и целые семьи отчаянно болеют за любимые футбольные команды. Одесса – город романтики и детства – провожала участников конференции домой улыбками прохожих.

Потом, 14 октября, настал черед партнерского завтрака в Новосибирске от MSK-IX. Это был завершающий аккорд серии семинаров, проводимых в этом году в разных городах России в честь 20-летия MSK-IX. На встречу с руководителями и экспертами MSK-IX пришли не только новосибирские клиенты и партнеры компании, но и участники рынка из Томска, Красноярска и других городов Сибири.

Александр Ильин, технический директор MSK-IX, и менеджер по региональному

развитию Константин Степанов представили участникам новую партнерскую программу MSK-IX. Они рассказали о планах по расширению и углублению взаимодействия с пиринг-партнерами региона и сделали краткий обзор услуг и продуктов, предлагаемых сегодня MSK-IX клиентам и партнерам. Особый интерес вызвала партнерская программа msk-ix и услуга media-ix на региональных точках обмена трафиком. Также на семинаре обсудили возможности открытия новых узлов в других городах.

Выступить на семинаре были приглашены и партнеры MSK-IX. Представители компании Extreme Networks Кирилл Жуков и Алексей Григорьев рассказали о том, как используется в коммутаторах Extreme язык программирования Python, а Тимур Кадараков, представлявший площадку «Синар» NSK-IX, в своем выступлении остановился на том, как в Новосибирске развиваются технические площадки «ЦентрИнформ».

Вообще, Новосибирск замечателен не только разницей во времени с Москвой (очень удобно возвращаться: сел утром в самолет – а по прилете все еще продолжается то же утро), но и советской архитектурой, которая очень заметна в городе: основа городского пейзажа - это бетонные сооружения, видавшие виды дома и, конечно, академический городок, откуда родом многие российские интернет-деятели. Добрые люди, приятные цены, вкусные молочные продукты – что еще надо путешественнику, чтобы сказать, что время проведено не зря.

А мы стремительно мчимся к трехдневной выставке-конференции RIW в Москве.

Неделя российского Интернета (RIW) – еще одно мероприятие, в котором мне довелось принять участие. Я бываю там каждый год и могу сравнивать, как изменяется и сама концепция мероприятия, и то, что происходит внутри, и состав участников. В этом году RIW шел три дня и проходил как всегда в московском Экспоцентре на Красной Пресне.

RIW второй год проходит в новом формате: это не только Интернет, но и телекоммуникации, и медиа. Поэтому количество мероприятий, проводимых здесь, с каждым годом все увеличивается, а аудитория становится все шире. В этом году была проведена **интересная конференция «Поколение NEXT «Школа новых технологий»**, на которую пришли не только профессионалы интернет-индустрии, но и школьники вместе со своими учителями. В итоге в залах конференции и на стендах участников выставки яблоку было негде упасть.

Но начнем по порядку. А сначала было открытие Недели российского Интернета, которое вел новый директор Координационного центра **Андрей Воробьев**. Он назвал RIW 2015 «репетицией подведения итогов года» и предложил проанализировать все то, что было сделано за прошедший год. Одним из важных событий, произошедших за предыдущие 12 месяцев, он назвал создание **Института развития Интернета - ИРИ**, которое было анонсировано год назад. Также на открытии RIW выступили министр связи и массовых коммуникаций РФ **Николай Никифоров**, руководитель Роскомнадзора Александр Жаров, председатель правления РОЦИТ, депутат Государственной Думы ФС РФ, председатель комитета по информационной политике, информационным технологиям и связи Леонид Левин, а еще Михаил Толкачев — заместитель генерального директора ЗАО «Экспоцентр», Герман Клименко — председатель совета ИРИ, Кирилл Варламов — директор ФРИИ, Юлиана Слащева — гендиректор «СТС Медиа», Александр Провоторов — гендиректор Tele2, Дмитрий Чернышенко — генеральный директор и член совета директоров АО «Газпром-Медиа Холдинг», Алексей Басов — вице-президент «Ростелекома», Руслан Ибрагимов — член правления МТС, Дэнни Перекальски — гендиректор Ozon.ru и Илья Массух — глава Фонда информационной демократии. Выступающих на открытии было так много, что для того, чтобы всех вспомнить, пришлось заниматься поиском в Интернете.

Также в первый день проходила закрытая секция проекта **«Нетоскоп»**, к которой я имела непосредственное отношение. Вернее, это была наша спонсорская секция в программе, и я-то размечталась уже, что приду в зал и буду с улыбкой встречать спикеров, но не тут-то было. Когда я двинулась от зала открытия в зал секции «Нетоскоп», то оказалось, что его вообще перенесли в другой павильон, и всех гостей, которые были приглашены и сориентированы, надо было теперь как-то собирать. Но это еще полбеды. Вход в этот самый новый неведомый зал был с торца непрофильного павильона, где проходила выставка «Таможенная служба-2015», и прекрасные девы в коротких юбках и в погонах пытались мне всучить всяких разных информационных листовок, пока я пробиралась в наш новый зал на третий этаж.

Каким чудом я нашла это помещение, уже не важно, важно другое. Когда я вошла внутрь, то руки похолодели, а сердце учащенно забилось. В зале не было ни стола, ни стульев для спикеров, ни проектора, ни микрофона, ни-че-го. То есть совсем ничего, что напоминало бы зал на таком мероприятии как RIW. Пришлось нам с коллегами двигать стулья, искать организаторов и что-то срочно придумывать. В итоге докладчики выступали с ноутбуками на коленках, что, естественно, мощно объединяло зал в общей проблеме. Зато потом был вкусный фуршет и охлажденное шампанское.

Что было во второй и третий день, можно почитать в новостях, так как я решила провести остаток недели в офисе, и что было дальше, доподлинно не знаю. Но известно, что в конференции приняли участие 803 человека, а также почти 600 школьников посетили выставку. Во время проведения конференции была организована аллея детских стартапов, детский пресс-центр, где юные журналисты брали интервью у представителей интернет-индустрии и освещали самые интересные факты и события.

Календарь событий: 2016 год

Международные события

15-26 февраля 2016
APRICOT2016/APNIC41,
Окленд, Новая Зеландия

APRICOT — крупнейшая ежегодная конференция по интернет-технологиям, собирающая более 800 участников азиатского региона и Океании. Здесь обсуждаются вопросы внедрения и использования интернет-технологий, технического администрирования сетей и инфраструктурных услуг Интернета. https://2016.apricot.net/

21-24 февраля 2016
Симпозиум NDSS,
Сан-Диего, Калифорния

Симпозиум NDSS - это ежегодная конференция, организуемая ISOC с целью способствования обмену информацией между исследователями и практиками по безопасности сетей и распределенных систем. https://www.internetsociety.org/events/ndss-symposium-2016

6-11 марта 2016
ICANN 55,
Маракеш, Марокко

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. https://meetings.icann.org/en/marrakech55

3-8 апреля 2016
IETF95,
Буэнос-Айрес, Аргентина

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF производится в могочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Совещания IETF хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке. https://www.ietf.org/meeting/95/

В России

19 февраля 2016
Россия,
Санкт-Петербург

III Бизнес-форум «Телеком двух столиц 2016. Эффективные пути повышения конкурентоспособности операторов связи в мегаполисах»
Крупнейшее отраслевое событие для операторского рынка Москвы и Санкт-Петербурга. Переформатирование рынка услуг связи: новые вызовы и тренды; стратегии и возможности развития операторов связи в текущих экономических условиях; актуальные проблемы операторского рынка Москвы и Санкт-Петербурга; демонстрация эффективных бизнес-моделей и инструментов для повышения конкурентоспособности операторов на насыщенном рынке. http://www.comnews-conferences.ru/tds2016

25-26 февраля 2016
Россия,
Казань

XX Форум «Безопасность и связь»
Научно-практическая Конференция и специализированные выставки. Автоматизированные системы связи и системы управления связью; системы и аппаратура телефонной, радио, спутниковой и космической связи; мобильные технологии; услуги сетей связи (местная, международная связь, представление выделенных каналов связи, IP-телефония, доступ в Интернет); локальные, корпоративные и глобальные сети (оборудование, технологии). http://www.exposecurity.ru/rus/

В Москве

26-28 января 2016,
ВЦ «Крокус Экспо»

18-я Международная Выставка и Форум CSTB Telecom&Media 2016
Текущее состояние коммуникационной отрасли и направления ее развития; новые технологии в индустрии Telecom&Media; роль телеком-операторов на медиарынке; перспективы развития рынка ШПД и БШПД.
http://www.cstb.ru/

4-5 февраля 2016,
Здание Правительства Москвы

18-й Национальный форум информационной безопасности «Инфофорум-2016»
Важнейшее ежегодное событие отрасли информационной безопасности в Российской Федерации. Более 1,5 тысяч практикующих специалистов из всех регионов России, ИТ-директора федеральных и региональных министерств и ведомств, крупных производственных предприятий и ИТ-компаний.
http://infoforum.ru/

3 марта 2016,
отель «Азимут Москва Олимпик»

II Федеральный форум
«Telecom QoS Russia 2016 – Качество телекоммуникационных услуг в России»
Открытый диалог участников ИКТ-отрасли о проблематике обеспечения качества связи в стране и обеспечение единого информационного пространства с высоким уровнем предоставления телекоммуникационных услуг.
http://www.comnews-conferences.ru/qos2016

10 марта 2016,
Москва

Конференция «Большие данные 2016»
Мероприятие представителей российского рынка: поставщиков решений в области больших данных и аналитики, а также представителей отделов ИТ из различных секторов бизнеса и госструктур.
http://www.events.cnews.ru/events/bolshie_dannye_2016.shtml

17-18 марта 2016,
отель «Холидей Инн Лесная»

VII Международная конференция «Transport Networks Russia 2016 - Развитие телекоммуникационных транспортных сетей в России и СНГ»
Крупнейшее ежегодное мероприятие, посвященное развитию рынка телекоммуникационных транспортных сетей в России и СНГ.
http://www.comconf.ru/tn2016?Itemid=2017

23 марта 2016,
EVENT-ХОЛЛ
«ИнфоПространство»

V Российский Форум BIG DATA 2016
В центре внимания форума тема Больших Данных как стратегического инструмента развития бизнеса, практический опыт использования технологий Больших Данных и продвинутой аналитики в российских компаниях.
http://www.osp.ru/iz/bigdata/event/about

12 апреля 2016,
Москва

Евразийский форум DataCloud & IoT 2016
Инновационные ИТ-решения для крупного бизнеса: всё о дата-центрах, облачных вычислениях и интернете вещей.
http://www.eurasiandatacloud.ru/

19-21 апреля 2016,
ВЦ ВДНХ, павильон 75

Международная выставка+форум перспективных информационных и коммуникационных технологий и решений «EXPO COMM Russia 2016»
Презентация инноваций высокотехнологичной отрасли, эффективная бизнес-площадка для деловых коммуникаций и профессионального обмена международным опытом.
http://www.expocomm.ru/

Светлой памяти Роба Блокзайла (1943 – 2015)

Интернет-сообщество понесло тяжелую утрату. Ушел из жизни человек, стоявший у истоков европейского Интернета, один из основателей сообщества RIPE и координационного центра RIPE NCC. Роб Блокзайл (Rob Blokzijl) скончался 1 декабря 2016 года в возрасте 72 лет.

С момента основания сообщества RIPE в 1989 году Роб являлся его бессменным председателем на протяжении 25 лет. За эти годы RIPE вырос в активное международное сообщество, вносящее существенный вклад в координацию и развитие Интернета в Европе и за ее пределами. Процессы принятия решений, основанные на принципах консенсуса, сотрудничества и управления снизу-вверх, явились эталоном для многих других групп.

Изначальной областью работы Роба была физика высоких энергий. Роб являлся сотрудником Института высоких энергий в Амстердаме, и позже – ЦЕРНа в Женеве. Здесь он активно способствовал строительству компьютерных сетей, которые требовались научному сообществу. Его опыт в этой области окажется незаменимым в работе по созданию сетевого сообщества в Европе.

В 1989 году Роб в соавторстве написал «конституцию» RIPE, где, в частности, говорилось: «Целью RIPE является обеспечение необходимой административной и технической координации для функционирования и развития пан-европейских IP-сетей».

Роб был ключевой фигурой в создании координационного центра RIPE NCC – первой в мире Региональной интернет-регистратуры, отвечающей за администрирование адресного пространства в Европе, на Ближнем Востоке и части Центральной Азии. Модель RIPE NCC была принята и стала основой глобальной системы администрирования номерных ресурсов (IP-адресов и номеров Автономных систем), насчитывающей сегодня пять РИРов.

Для многих в сообществе RIPE и за ее пределами Роб был ментором, другом, доверенным лицом и всегда – голосом разума. Его наследие простирается от физических сетей, составляющих Интернет, до сообщества, где мудрость Роба присутствует в основополагающих принципах. Это наследие останется с нами, вместе с развитием сообщества его участники будут часто спрашивать себя: **«А что бы сделал Роб?»**

Интернет изнутри

2015