Путевые заметки: IETF-84

Очередная конференция IETF состоялась с 29 июля по 3 августа в Ванкувере, Канада. Это недельное совещание, которое проводится три раза в год и собирает более тысячи участников из полусотни стран, как обычно, было посвящено разработке новых стандартов и вопросам технического развития Интернета. Сразу оговорюсь – разработка и обсуждение стандартов в IETF проводятся онлайн, в списках рассылки, а конференции помогают более широкому обмену мнениями, знакомству со смежными разработками и поиску общего мнения по сложным или спорным вопросам.

DANE – сертификаты в DNS

Я уже писал о работе DANE (DNS-based Authentication of Named Entities) в одной из моих предыдущих статей. Суть этой работы заключается в предоставлении возможности операторам серверов, например, веб-сайтов, опубликовать сертификат TLS (http://ru.wikipedia.org/wiki/TLS), или сертификат удостоверяющего центра (УЦ), выдавший сертификат TLS, в глобальной системе DNS. Этот сертификат может быть использован для обеспечения защищенной связи между клиентами-браузерами и веб-сервером.

Напомню, что сертификат TLS связывает открытый ключ и имя, например, доменное имя сервера. Связь эта удостоверяется электронной подписью другого, родительского ключа. Возможность проверки достоверности сертификата зависит от возможности проверки достоверности родительского ключа. Эта задача традиционно решается с помощью PKI (Public Key Infrastructure) - инфраструктуры открытых ключей, где для проверки подлинности всех сертификатов, выданных УЦ, "доверительные" отношения необходимо установить лишь с одним ключом, т.н. корневым или якорным ключом, принадлежащим этому УЦ.

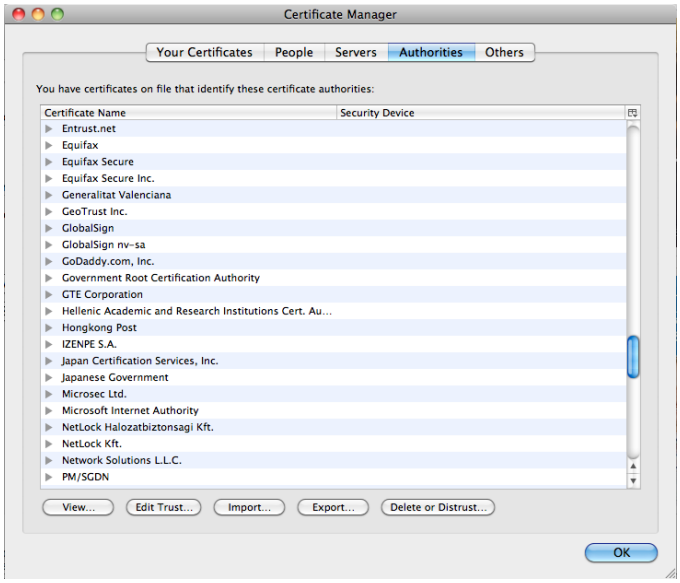

Рис. 1. Многообразие Удостоверяющих Центров, которым от нашего имени доверяет Mozilla Firefox

Проблема заключается в том, что системы PKI, используемые на практике, скажем Verisign, DigiCert, GoDaddy.com, Thawte, не имеют ничего общего со структурой и бизнес-отношениями в DNS, поэтому для установления подлинности владения доменным именем организации, предоставляющие эту услугу, прибегают к различным косвенным проверкам, например, проверке регистрационных записей

whois и т.п. Это усугубляется тем, что современные браузеры "доверяют" более чем сотне различных PKI, качество проверок которых сильно варьируется. А как известно, безопасность системы определяется ее слабым звеном.

Правда существует единственная система, напоминающая PKI, полностью конгруэнтная DNS - это DNSSEC (о протоколе DNSSEC я писал в статье «Как подписали корень» http://www.ripn.net/articles/dnssec/). DANE позволяет владельцу доменного имени опубликовать сертификат TLS или указатель на доверенную систему PKI, в которой такой сертификат находится, наряду с другими записями, связанными с именем - например, адресами или именами серверов, обслуживающих доменную зону и т.п. DNSSEC, в свою очередь, позволяет посредством электронной подписи установить подлинность этих записей, в том числе и сертификата TLS. Таким образом обеспечивается такая же криптографическая защита, как и в традиционных PKI, но цепочка доверия полностью соответствует доменной иерархии. Другими словами, DANE позволяет получить достоверный сертификат от самого владельца имени без посредников.

Эта часть работы DANE уже завершена: стандарт RFC6698 (http://datatracker.ietf.org/doc/rfc6698/) определяет протокол и новую запись DNS - TLSA, ассоциирующую сертификат или открытый ключ с доменным именем. Однако в процессе разработки находятся новые интересные предложения. Ведь этот подход можно использовать и для обеспечения безопасности и аутентичности почтовых серверов, для публикации сертификатов S/MIME, применяемых для шифрования и электронной подписи почтовых сообщений. Безопасность протоколов мгновенных сообщений XMPP или голосовой связи SIP также может быть значительно улучшена с помощью DANE.

Одна из проблем, решаемая в рамках этих задач, заключается в определении с каким именем ассоциировать сертификат. Например, если электронная почта для домена example.com обслуживается сервером mx.example.net, с каким именем следует связать запись TLSA? Подобные вопросы справедливы и для других протоколов.

Рассматриваемые проекты предлагают в качестве целевого имени использовать имя сервера, с которым и будет связан сертификат, а не доменное имя, почту которого этот сервер обслуживает. Пример использования DANE в приложении к электронной почте показан на рис 2.

```
; mail domain
  example.com.          MX     1 mx.example.net.
  example.com.          RRSIG  MX ...

  ; SMTP server host name
  mx.example.net.        A     192.0.2.1
  mx.example.net.        AAAA  2001:db8:212:8::e:1

  ; TLSA resource record
  _25._tcp.mx.example.net.  TLSA   ...
  _25._tcp.mx.example.net.  RRSIG  TLSA ...
...
```

Рис. 2. Фрагмент зоны DNS с использованием записей TLSA для указания сертификата почтового сервера

Электронная почта для адресатов домена example.com доставляется посредством протокола SMTP на сервер mx.example.net. Для установления защищенной связи с сервером с использованием TLS, клиенты получат сертификат, удостоверяющий имя mx.example.net.

Стандарты DANE предусматривают внедрение расширений безопасности DNSSEC, и можно сказать, что разработки DANE открыли новые важные приложения DNSSEC, что может послужить дополнительным стимулом для его внедрения.

Использование стандартов DANE позволит, в свою очередь, существенно улучшить защищенность критических приложений Интернета, таких как веб и электронная почта.

IPv6: 6 недель после запуска – полет нормальный

Во время конференций Internet Society традиционно организует дискуссии в формате круглого стола, посвященные технологиям и развитию Интернета. На этот раз круглый стол был посвящен Всемирному Запуску IPv6 (http://www.worldipv6launch.org/), прошедшему 6 июня этого года. Участники Запуска - веб-сайты, сетевые операторы и производители оконечного сетевого оборудования - в этот день включили поддержку IPv6 для своих сайтов, сетей и оборудования на постоянной основе, тем самым определив новую норму для всей отрасли.

Полтора месяца спустя ведущие участники Запуска собрались, чтобы обсудить предварительные итоги внедрения IPv6.

Собравшиеся отметили, что Запуск явился значительным событием и стимулом для многих к ускорению внедрения IPv6 в своих организациях. Хотя различия в масштабах внедрения существенны, все измерения показывают видимый скачок в использовании IPv6 в момент Запуска и затем продолжающийся рост. Показательным в этом смысле является график поддержки IPv6 среди 1000 наиболее популярных веб сайтов согласно рейтингу Alexa (http://www.alexa.com/). На сегодня четверть из них полностью поддерживает IPv6. Среди них флагманы провайдеров контента - Google, YouTube, Yahoo!, Facebook, Miscrosoft Bing, ВКонтакте, Netflix. Яндекс открыл IPv6-доступ к своему вторичному сайту www.yandex.com, номер 5852 в рейтинге Alexa. Приятно видеть, что многие лидеры российского контента серьезно подходят к вопросу внедрения IPv6, некоторые вошли в этот список.

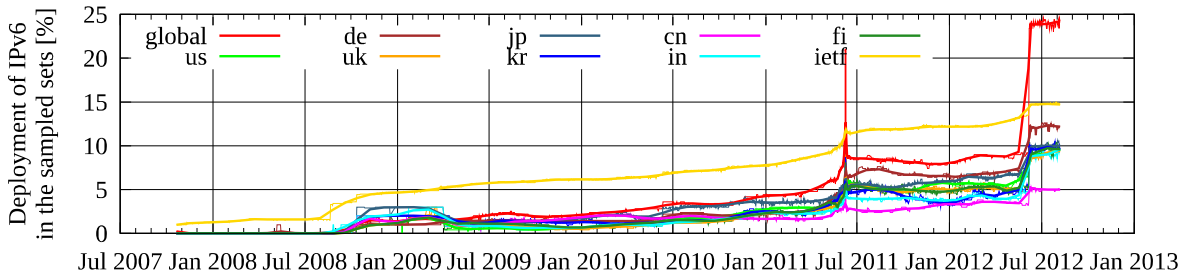

Рис. 3. Поддержка IPv6 ведущими веб-сайтами (источник: Lars Eggerthttp://eggert.org/meter/ipv6)

Одним из критических элементов Запуска явилось участие сетевых провайдеров. Год назад Internet Society организовала Всемирный День IPv6 (http://www.internetsociety.org/ipv6/archive-2011-world-ipv6-day), когда участники, в основном веб-сайты, "включили" IPv6, но только на 24 часа. Тогда это не вызвало заметного увеличения трафика IPv6, во многом вследствие неготовности сетевых операторов, и в первую очередь операторов широкополосного доступа.

Требованием для участия в Запуске для сетей являлось обеспечение использования IPv6 как минимум одним процентом всех своих пользователей. То есть не просто поддержка IPv6, а реальное использование и реальный трафик - проценты измерялись Google, Facebook и Yahoo! по "хитам" пользователей сетей-участников.

Хотя цифра 1% не кажется значительной, за ней стоят десятки процентов инфраструктуры, поддерживающей IPv6. Дело в том, что возможность использования IPv6 для доступа к контенту обусловлена выполнением следующих условий:

- контент должен быть доступен по IPv6;
- сетевая инфраструктура должна поддерживать IPv6, включая глобальную связность;
- абонентское оконечное оборудование - кабельные или ADSL-модемы и маршрутизаторы должны поддерживать IPv6;
- операционная система компьютера пользователя должна поддерживать IPv6.

Невыполнение хотя бы одного из этих условий означает отсутствие трафика. Задача многократно усложняется тем, что пользовательское оборудование – компьютеры, а иногда и маршрутизаторы и модемы - находится вне контроля провайдера. Поэтому для того чтобы получить статистический 1% использования IPv6, уровень внедрения должен быть гораздо выше. По оценкам Comcast и TimeWarnerCable – от 30 до 50%.

Но эти затраты окупаются по мере роста использования IPv6. По оценкам Джона Бржозовского (John Brzozowski), главного архитектора Comcast, процент трафика IPv6 в общем потоке составляет

меньше 1%, хотя и растет. И в то же время, в день открытия Олимпийских Игр 2012 в Лондоне, 6% трафика трансляции на YouTube составлял IPv6, а для IPv6-пользователей уровень трафика IPv6 может достигать 40%, в основном благодаря YouTube, Netflix и iTunes App Store.

Приятно отметить, что российский провайдер Starlink вошел в список 25 ведущих операторов, более 10% пользователей этого оператора используют IPv6 (http://www.worldipv6launch.org/measurements/).

В списке стран лидируют Румыния с 8% уровнем внедрения, за ней следует Франция (4,5%), Япония и США (1,85% и 1,35% соответственно). Россия находится в десятке сильнейших (0,48%), опережая большинство европейских стран. Эти данные представил Джорж Майклсон (George Michaelson), APNIC, по результатам измерений, проводимых с помощью рекламных объявлений со встроенным кодом, которые были размещены на различных сайтах (более подробно - http://labs.apnic.net/index.shtml).

С ростом внедрения и использования IPv6 растет и число атак, и других происшествий, связанных с компьютерной безопасностью. В этом отношении IPv6 мало отличается от своего предшественника. Как было отмечено участниками, политика безопасности оператора должна быть одинаково строгой как для IPv4, так и для IPv6. Было отмечено, что в пятницу накануне конференции веб-сайт IETF www.ietf.org был частично недоступен вследствие атаки DDoS. Любопытно, что весь трафик атаки был исключительно IPv6. Возможно, это является еще одной из метрик уровня внедрения этого протокола.

Лоренцо Колитти (Lorenzo Colitti), Google, представил график роста использования IPv6 (рис. 4). За последний год степень внедрения выросла в 2,5 раза, и это на фоне быстрого роста трафика IPv4. На сегодня эта цифра выглядит еще весьма скромно – чуть меньше 0,8%, но такими темпами через 6 лет уже 50% пользователей Интернета будут иметь IPv6, а спустя еще пару лет Интернет полностью перейдет на IPv6. Стоит задуматься тем, чьи долгосрочные планы основаны на IPv4!

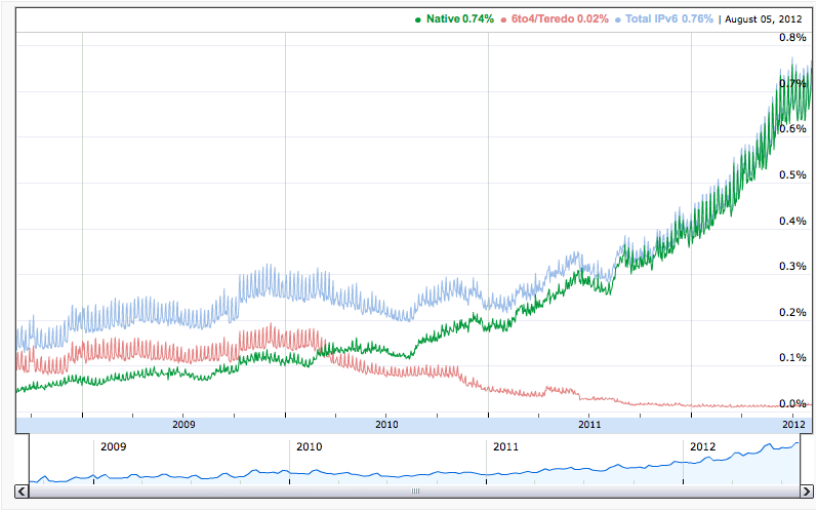

Рис. 4. Процент использования протокола IPv6 по отношению к IPv4
(источник: http://www.google.com/intl/en/ipv6/statistics.html)

Защита системы межсетевой маршрутизации: вопросы внедрения

Рабочая группа IETF по безопасности междоменной маршрутизации (читай – BGP), SIDR (http://datatracker.ietf.org/wg/sidr/), движется семимильными шагами к достижению поставленной цели – разработке стандартов и технологий – «строительных блоков» - для обеспечения защиты уязвимых мест сегодняшней глобальной системы маршрутизации. Об этой работе я писал в статьях «Сертификация Адресных Интернет-Ресурсов" (http://www.ripn.net/articles/certification/) и «Пять препятствий на пути к безопасности глобальной системы маршрутизации" (http://www.ripn.net/articles/secrout2012/).

В основе этих технологий лежит система сертификации номерных ресурсов (сетевых блоков и номеров автономных систем), базирующаяся на инфраструктуре открытых ключей PKI со специальными расширениями, описанными в RFC3779 "X.509 Extensions for IP Addresses and AS Identifiers" (http://datatracker.ietf.org/doc/rfc3779/), - RPKI.

Работа по стандартизации элементов системы и связанных с ней протоколов завершена. В начале этого года рабочая группа SIDR опубликовала 17 RFC, описывающих работу RPKI и определяющих необходимые протоколы. Более того, все Региональные Интернет Регистратуры (РИРы), за исключением североамериканской – ARIN, имеют работающие системы, позволяющие своим членам создавать сертификаты распределенных ресурсов и дополнительные объекты, имеющие непосредственное отношение к маршрутизации – например, ROA (Route Origin Authorization), указывающие на список автономных систем, которые могут являться источником определенного маршрута.

Хотя работа SIDR в настоящее время сфокусирована на разработке расширений BGPSEC, призванных решить задачу защиты пути, по которому распространяются анонсы маршрутов, внеочередное заседание SIDR, которое прошло за два дня до конференции IETF84, было полностью посвящено проблемам внедрения RPKI.

Очевидно, что для использования этой системы сетевыми операторами, RPKI должна демонстрировать высокий уровень надежности, производительности и масштабируемости. На практике же пока что мы можем говорить скорее о тестовых испытаниях, чем о полноценной системе.

Основная проблема заключается в репозиториях – открытых базах данных, в которых хранятся все объекты RPKI – сертификаты, списки отозванных сертификатов (Certificate Revocation List, CRL), ROA и манифесты (списки всех объектов, находящихся в репозитории, заверенные цифровой подписью). Замечу, что в RPKI каждый участник (держатель номерных ресурсов - IANA, РИР, сетевой оператор) является Удостоверяющим центром (УЦ), а каждый УЦ имеет свой репозиторий. На практике, правда, РИРы предлагают т.н. услуги хостинга УЦ, когда все операции выполняются через пользовательский интерфейс, но на инфраструктуре РИРа. Включая и репозиторий, т.е. объединенный репозиторий РИРа содержит все репозитории подчиненных УЦ, за исключением единичных операторов, которые обслуживают свой УЦ собственными силами.

Хотя число объектов в этих репозиториях пока невелико – самое большое число у RIPE NCC –почти 4000, - производительность системы вызывает некоторые опасения. Например, для синхронизации локального кэша с репозиторием сегодня требуется порядка 40 минут. Учитывая, что число членов RIPE NCC около 8000, плюс порядка 25 тысяч держателей т.н. PI -блоков, число объектов в репозитории, в случае полного внедрения в регионе RIPE, превысит 100 тысяч. Даже при линейной масштабируемости системы синхронизация для одного клиента только для региона RIPE займет около 16 часов! Такая производительность, безусловно, неприемлема.

Для решения этих проблем разработчики экспериментируют с новыми моделями синхронизации с данными репозиториев. В качестве альтернатив существующего протокола rsync (http://ru.wikipedia.org/wiki/Rsync) предлагается использовать http (http://ru.wikipedia.org/wiki/Http) и даже bittorrent (http://ru.wikipedia.org/wiki/BitTorrent). Протокол http , по мнению разработчиков RIPE NCC , является наиболее перспективным направлением. Этот протокол является стандартом (в отличие от rsync), обладает требуемой масштабируемостью, а распространенность этого протокола, как в приложениях, так и в программных библиотеках, повсеместна. Использование http позволяет также применять технологии распределения контента, такие как, например, CDN (http://ru.wikipedia.org/wiki/Content_Delivery_Network).

Правда на сегодня, основная проблема все же не в производительности системы, а в недостаточном ее использовании, далеком от критической массы, когда преимущества становятся очевидными. Пока что ведутся эксперименты и осторожное тестирование некоторыми операторами, однако все согласны, что многие вопросы производительности, защищенности и надежности системы, которые стоят в ряду причин недоверия операторов, должны быть решены уже сейчас.

Андрей Робачевский, Менеджер по программам Internet Society

Мнения, представленные в статье, не обязательно отражают официальную позицию Internet Society