Технический анализ инфраструктуры открытых ключей ресурсов (RPKI)

Офис технического директора ICANN

Алан Дуран (Alain Durand)
OCTO-014
2 сентября 2020

ICANN

СОДЕРЖАНИЕ

ОСНОВНЫЕ ПОЛОЖЕНИЯ 3

ЗАКЛЮЧЕНИЕ 4

БЛАГОДАРНОСТЬ 5

Настоящий документ входит в серию документов OCTO. Перечень всех документов серии см. на странице публикаций OCTO.
Вопросы или предложения по любому из этих документов принимаются по адресу octo@icann.org.

Основные положения

Протокол граничного шлюза (BGP) – это протокол маршрутизации в интернете, который используется интернет-провайдерами (ISP). Он существует с начала 1990-х годов. Инциденты с маршрутизацией BGP, например, широко известная утечка маршрута YouTube по вине компании Pakistan Telecom в 2008 году, называются утечками маршрутов и могут приводить к перенаправлению трафика во всем интернете. Сегодня они происходят ежедневно и серьезно сказываются на работе интернет-провайдеров. Перенаправление может быть связано с ошибками конфигурации, программного обеспечения или активных атак. Основная причина этих проблем – отсутствие встроенной защиты в протоколе BGP.

Трудная работа по модернизации защищенности началась давно, но она все еще не завершена. Наиболее перспективное решение, которое сейчас доступно для внедрения, называется проверкой источника RPKI. При проверке источника RPKI используется инфраструктура открытых ключей ресурсов (PKI ресурсов или RPKI), иерархическая структура взаимосвязанных сертификатов открытых ключей X.509, с якорями доверия в региональных интернет-регистратурах (RIR). Цель состоит в подтверждении того, что являющиеся источником интернет-маршрутов интернет-провайдеры уполномочены выполнять эту роль владельцем соответствующих блоков IP-адресов. Процедура проверки источника RPKI существует с 2011 года. Сейчас она приобретает популярность благодаря нескольким факторам, в число которых входит многолетняя работа RIR по продвижению этой проверки и обучению инженеров ее использованию; усилия Общества интернета по разработке взаимосогласованных норм защиты маршрутизации (MANRS); финансирование разработки программного обеспечения RPKI Министерством национальной безопасности США. Это, а также растущее раздражение на утечки маршрутов, которые наводят на мысль о том, что «надо что-то предпринять», плюс пример нескольких крупных провайдеров (таких как Cloudflare и NTT), сделало вопрос проверки источника RPKI животрепещущим в 2020 году.

Надо отметить, что эта технология еще недостаточно развита. Есть серьезные проблемы с масштабированием, которые приводят к задержкам передачи информации о маршрутах, снижающим гибкость реагирования интернет-провайдеров на чрезвычайные ситуации и повышающим уязвимость системы. Может быть атакована сама система RPKI. Возможны трудности в обнаружении сценария катастрофического отказа и еще большие трудности при восстановлении после него. Эти риски усугубляются особенностями модели развертывания, где используются пять якорей доверия, что открывает возможность несогласованности данных и создает предпосылки для создания еще большего числа якорей доверия. Стороны, которые вообще не используют RPKI, также могут стать случайными жертвами взлома любого из якорей доверия. Американская регистратура интернет-регистрации (ARIN) считает связанные с этими сценариями риски с точки зрения ответственности настолько высокими, что требует от всех сторон, использующих ее данные RPKI, признать, что RIR не несет за это ответственности. Эта система сделала RIR активными участниками повседневной работы интернета и, как показали некоторые недавние инциденты, неизвестно, насколько хорошо они подходят для выполнения этой роли.

Еще важнее то, что при ограничении области применения процедуры проверки источника RPKI источником анонсов о маршрутах, обеспечивается защита только от самых простых

атак на систему маршрутизации. Надежная система защиты маршрутизации требует проверки всего пути, хотя это намного сложнее.

Ряд интернет-провайдеров, точек обмена интернет-трафиком (IXP) и облачных провайдеров считает, что улучшение качества работы системы, которое достигается за счет предотвращения утечек маршрутов из-за неправильной конфигурации и ошибок программного обеспечения с помощью проверки источника RPKI, оправдывает затраты на развертывание этой достаточно сложной системы. При этом любой, кто рассматривает возможность внедрения процедуры проверки источника RPKI, должен знать о текущих проблемах зрелости и связанных с ней операционных рисках. Защита инфраструктуры маршрутизации (пока) не является простым вопросом развертывания программного обеспечения. Необходимо тщательно изучить компромисс между безопасностью протокола и сложностью эксплуатации.

См. полный текст Публикации OCTO 014 (на английском языке).

Заключение

Наблюдается значительный интерес к RPKI, движущей силой которого являются RIR и сетевые операторы, как крупные, так и мелкие. По мнению многих сторон, есть достаточное количество легких способов воспользоваться положительными аспектами RPKI, позволяющих окупить инвестиции. Процесс подписания ROA настолько упростился, что теперь им воспользоваться может практически любой владелец IP-адреса. При этом проверка источника RPKI обеспечивает защиту от ошибок ввода, а также ошибок конфигурации и программном обеспечении. Хотя проверка источника RPKI не защищает от изощренных атак на систему маршрутизации, с точки зрения оператора как атаки на систему маршрутизации, так и утечки маршрутов из-за ошибок ввода приводят к появлению жалоб, требующих рассмотрения. Несомненно, многие интернет-провайдеры будут рады помощи, которую в этой области удастся получить благодаря проверке источника RPKI.

Однако система в целом, построенная на базе сертификатов X.509, сложна. Эта сложность сопряжена с риском появления новых ошибок и опечаток в самой RPKI. Наличие у организации большого опыта и знаний в области управления криптографическими системами скорее всего останется обязательным условием включения ROV. Некоторые проблемы наблюдаются и в самой RPKI. На передачу информации о маршрутах может уходить до 24 часов, что усугубляется отсутствием повсеместного систематического мониторинга и, соответственно, может стать большой эксплуатационной проблемой. Также следует отметить, что помимо неспособности устранить все проблемы защиты маршрутизации, проверка источника RPKI может создать новые угрозы для системы маршрутизации, например, в случае атак на репозитории RPKI, а также на различные сертификаты или системы распределения ROA. На данный момент ROV для проверки источника RPKI развернута только в ограниченном объеме. Без ответа по-прежнему остаются вопросы, касающиеся масштабируемости всей системы.

В конечном итоге, решать, стоит ли польза от обеспечения целостности маршрутизации затрат, связанных с развертыванием достаточно разветвленной инфраструктуры и

операционной сложности процедуры проверки источника RPKI, предстоит сетевым операторам. Некоторые сетевые операторы, которые волнуются об отрицательных последствиях утечек маршрутов (связанных с неправильной конфигурацией) на их деятельность, безусловно убеждены в пользе этих затрат, а некоторые, которые волнуются о защите маршрутизации, еще сомневаются. Пожалуй, еще важнее тот факт, что RPKI подразумевает определенные изменения критически важных операционных структур интернета в целом. Пока неясно, осознают ли участвующие или затрагиваемые сообщества все последствия этих изменений. Ясно, что необходимо продолжать информировать о важности RPKI.

Благодарность

Хотя все мнения, изложенные в настоящем докладе, принадлежат его автору, нам хотелось бы поблагодарить следующих лиц, которые на этапе составления доклада представили свои комментарии, отзывы или критические замечания:

- Ален Айна (Alain Aina), WACREN
- Роб Остин (Rob Austein), Hacntr
- Джон Курран (John Curran), ARIN
- Ким Дейвис (Kim Davies), ICANN (IANA)
- Джефф Хьюстон (Geoff Huston), APNIC
- Фредрик Корсбэк (Fredrik Korsback), Amazon
- Натали Кюннейк-Тренаман (Nathalie Künnake-Trenaman), RIPE NCC
- Мартин Леви (Martin Levy), CloudFlare
- Ди Ма (Di Ma), ZDNS
- Терри Мэндерсон (Terry Manderson), ICANN (DNS и проектирование сетей)
- Карлос Мартинес (Carlos Martinez), LACNIC
- Кристофер Моррoy (Christopher Morrow), Google
- Рикардо Патара (Ricardo Patara), NIC Бразилии
- Амреш Фокир (Amreesh Phokeer), AFRINIC
- Андрей Робачевский, ISOC
- Джоб Снийдерс (Job Snijders), NTT
- Билл Вудкок (Bill Woodcock), PCH

Выражаем особую благодарность Дэвиду Хуберману (David Huberman) из ICANN за постоянную поддержку и готовность выступать в качестве референта во время подготовки настоящего документа.