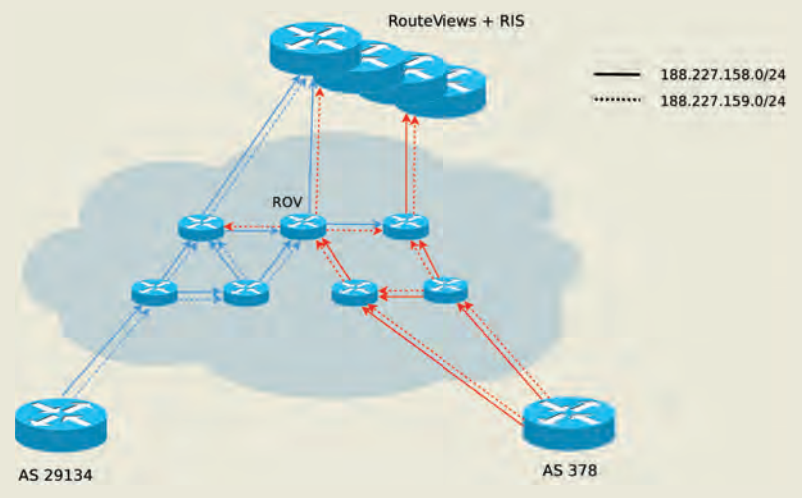


Obrázek 1: Oboustranně symetrický experiment.

cování platných ROA by v současnosti teoreticky ochránilo jen kolem 10 % prefixů a až 1 % by bylo neprávem odpojeno.

Otázka počtu sítí, které validují a vynucují ROA, byla donedávna předmětem spekulací a převládal názor, že jde o marginální počet omezený zejména na výzkumné sítě a experimentální nasazení.

Měření nasazení ROV

Změřit, kolik autonomních systémů v internetu vytvořilo a zveřejnilo ROA pro své prefixy, a spočítat, kolik prefixů je chráněných, je jednoduché. Vezme-li se ROA dostupná na úložištích regionálních registrů (RIR), dospěje se k uvedenému číslu kolem 10 % prefixů, pokrytých příslušnými ROA.

Z toho je určitá část, až 1 %, podezřelá, že obsahuje zastaralé anebo chybné informace. Detailní analýza konfliktů mezi BGP a RPKI je dostupná na webu NIST.

Naproti tomu je komplikované najít a kvantifikovat v internetu sítě, které validují ROA a skutečně aplikují výsledky ROV na routing, tedy zahazují prefixy, pro něž existují konfliktní ROA, a neexistuje ROA povolující daný pár prefix a origin (tj. autonomní systém, který prefix oznamuje).

Aktivní experiment

Prezentovaná metoda, která umožňuje otestovat omezený vzorek sítí v internetu, zjistit, zda validují ROA, a tyto výsledky následně zobecnit a usuzovat podle nich o rozšíření ROV v celém internetu, je závislá na aktivním experimentu.

Jeho podstatou je, že se řízeně vyvolá konflikt mezi prefixy oznámenými v BGP a příslušnými ROA a následně se sondují vzdálené sítě, zda je v nich daný prefix dostupný.

Tato metoda je sama o sobě velmi nespolehlivá kvůli náhodným fluktuacím v routingu, nedostupným sítím a ztrátám provozu. Spolehlivost i citlivost však lze zvýšit tím, že se připraví diferenciální experiment: oznámené jsou dvě sítě, z toho jedna s platným ROA a druhá v konfliktu s příslušným ROA. Pak lze sledovat rozdíly v šíření těchto dvou prefixů v DFZ.

To samo o sobě ale pořád nestačí, protože výsledkem ROV může být nejen zahození konfliktního prefixu, ale i pouhé snížení jeho priority. Proto je potřeba k nevalidnímu prefixu nabídnout i validní alternativu, která by ovšem byla bez ROV méně prioritní. Proto se připravil oboustranně symetrický experiment, jak ukazuje obrázek 1.

Aktivního experimentu se účastnily dva autonomní systémy (AS) ve dvou různých geograficky vzdálených lokalitách – AS29134 v ČR a AS378 v Izraeli. Z obou zmíněných AS se oznamovaly dva prefixy 188.227.158.0/24 a 188.227.159.0/24, přičemž pro první prefix se zveřejnilo ROA autorizující jeho oznámení z AS29134 a pro druhý prefix pak ROA autorizující oznámení z AS378.

Oba spolupracující AS zajistily průchod prefixů filtry svých upstreamů a vytvořily příslušné route objekty v RIPE DB (oba AS patří do servisního regionu RIPE NCC).

[Změřit, kolik autonomních systémů v internetu vytvořilo a zveřejnilo ROA pro své prefixy, a spočítat, kolik prefixů je chráněných, je jednoduché.]

Rozpoznání ROV a kvantifikace

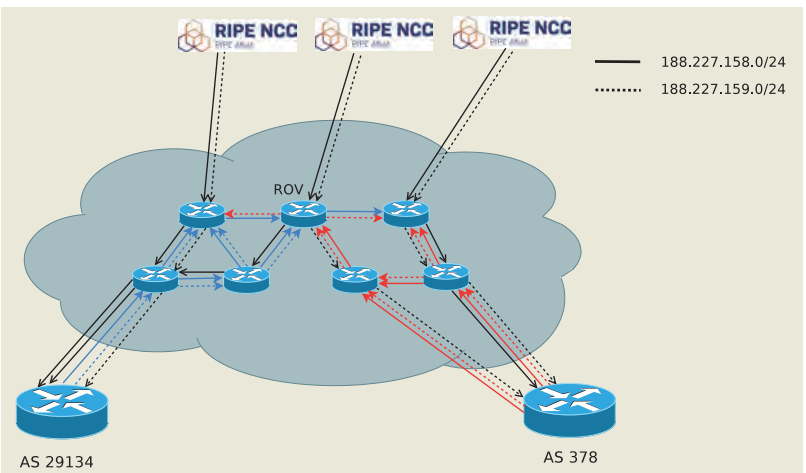
Druhá část experimentu měla zjistit, ve kterých autonomních systémech byl konfliktní prefix potlačen, zatímco validní prefix procházel. Pro to je potřeba získat informace o routingu.

První metoda, naznačená v obrázku 1, využívá RouteViews a RIPE RIS, což jsou služby, které stahují a dlouhodobě uchovávají obsahy BGP tabulek a celou historii změn v BGP z několika stovek autonomních systémů, jež poskytují data ze svých routerů těmto projektům.

V těchto datech lze snadno dohledat cesty, kde validní prefix prošel, zatímco nevalidní byl cestou ztracen. A s trochou kombinování získaných znalostí lze s různou mírou pravděpodobnosti dovodit to, které autonomní systémy potlačují nevalidní prefixy. Problémem této metody však je pouze malý rozsah tohoto experimentu.

Jinou možností, jak získat obdobná data, avšak z mnohem větší a rozmanitější množiny bodů v síti, je použít RIPE Atlas. Tato síť malých a centrálně ovládaných sond umožňuje vykonávat aktivní měření pro výzkumné i provozní účely a jednou z funkcí, které poskytuje, je vzdálené spuštění traceroute na vybraný cíl.

V našem případě se ze všech sond RIPE Atlasu spustil traceroute na jednu z IP adres uvnitř každého z námi injektovaných experimentálních prefixů, jak ukazuje obrázek 2. Výsledek traceroute lze s velkou mírou pravděpodobnosti převést na předchozí případ.



Obrázek 2: Použití RIPE Atlas sond pro získání dat z aktivního experimentu.