Přestože se povedlo získat díky RIPE Atlasu data z bezmála 9 000 sond, pořád tento experiment trpí omezeným rozsahem měření. Posledním krokem bylo škálovat experiment do rozměrů, které umožní zobecnění výsledků s velkou mírou jistoty pro celý internet.

Pro toto zobecnění je však zapotřebí slevit z požadavku na objevení konkrétních autonomních systémů, které vykonávají ROV – místo toho se položila otázka: Jaké procento komunikace či přesněji jaké procento cest v internetu je chráněných ROV?

Tato otázka umožňuje použít aktivní experiment k měření na (skoro) všechny aktivní IP adresy v internetu tím způsobem, že se do sítě injektují dva datagramy pro každou vzdálenou adresu, jejíž zabezpečení se testuje. První bude mít zdrojovou adresu z prvního injektovaného prefixu a testovaná adresa bude cílovou adresou.

Druhý datagram bude mít odlišnou pouze zdrojovou adresu, která bude tentokrát z druhého prefixu. V obou případech je potřeba vytvořit takový datagram, na který vzdálená adresa odpoví.

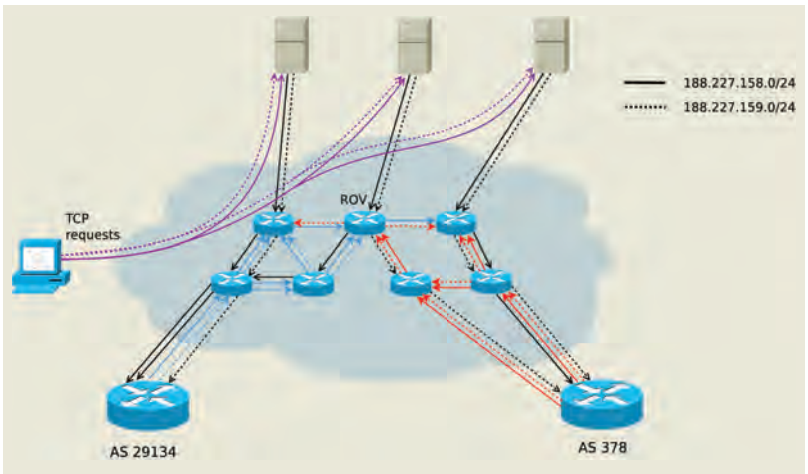
Následně stačí zachytit odpovědi, které dorazí buď do AS29134, anebo do AS378.

Pokud obě odpovědi dojdou do stejného AS, nedošlo k jejich ovlivnění ROV. Jestliže dorazí každá do jiného AS, je možné, anebo dokonce pravděpodobné, že je testovaná adresa chráněná.

Pokud ale dojde odpověď jen na jednu nebo na žádnou ze sond, je situace složitější, nicméně v některých případech stále řešitelná. Metodu ilustruje obrázek 3. V našem případě jsme vybrali nakonec jako metodu posílání TCP segmentů navazujících spojení na HTTP servery z Alexa rankingu, který byl zredukován na 700 000 adres.

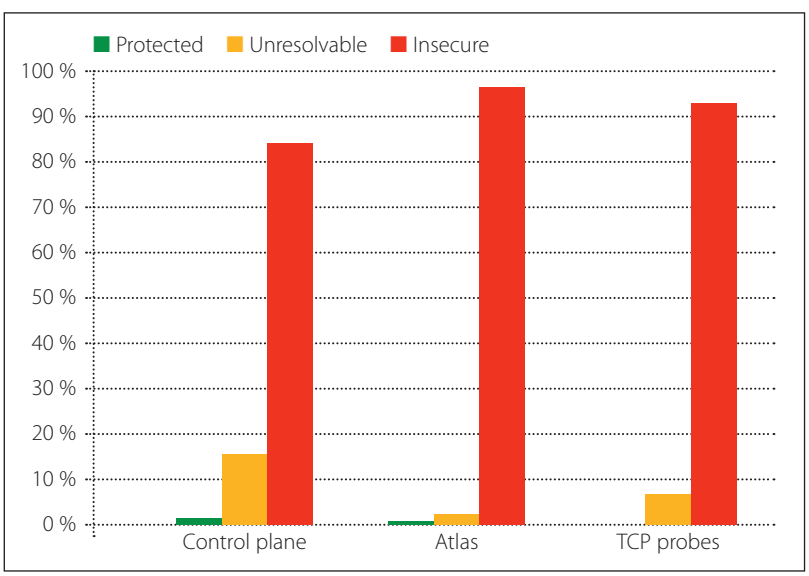
Všechny tři zhruba popsané metody akvizice dat z jednoho společného aktivního experimentu jsou přirozeně komplikovanější z hlediska postprocessingu získaných dat, protože je nutné odfiltrovat náhodné chyby při doručování datagramů přes internet, nestandardní směrovací rozhodnutí, zejména náhodné vlivy ECMP, změny routingu v průběhu měření a další nepredikovatelné vlivy.

Tyto vlivy lze odstranit statistickými úvahami a několikanásobným opakováním měření. Detaily akvizice a zpracování těchto dat jsou popsány v příspěvku Methodologies for Measuring Route Origin Validation.



Obrázek 3: Testování ochrany vzdálených sítí pomocí TCP sond.

[Hlavním výsledkem je potvrzení dlouho existující domněnky, že ROV je opravdu marginálním jevem.]



Obrázek 4: Porovnání výsledků tří metod akvizice dat z aktivního experimentu.

Výsledky

Hlavním výsledkem je potvrzení dlouho existující domněnky, že ROV je opravdu marginálním jevem. Validaci vykonává jen několik málo sítí, zejména akademických, výzkumných anebo nějakým způsobem zainteresovaných na propagaci standardu RPKI.

Obrázek 4 ukazuje procentuální výsledky všech tří experimentů.

1 RouteViews a RIPE RIS experiment:
Nevalidující autonomní systémy: 250 (84,5 %)
Možná validace (horní hranice, autonomní systémy bez negativních výsledků): 46 (15,5 %)
Pravděpodobně validující AS: 4 (1,35 %)

2 RIPE Atlas experiment:
Nevalidující autonomní systémy: 2043 (97,0 %)
Možná validace (horní hranice, autonomní systémy bez negativních výsledků): 49 (2,3 %)
Prokázaná validace (spodní hranice): 2 (0,1 %)
Pravděpodobně validující AS: 12 (0,5 %)

3 Odražené odpovědi od HTTP serverů:
Nechráněné adresy: 632570 (93,30 %)
Pravděpodobně chráněné: 201 (0,03 %)
Ochranu nelze určit: 45163 (6,66 %)

Zabezpečení routingu

Z uvedených výsledků je zřejmé, že původní domněnku o zanedbatelném nasazení ROV, a tedy prakticky neexistujícím dopadu na zabezpečení internetu, lze považovat za prokázanou.

Se zvyšujícím se počtem otestovaných sítí klesá počet zabezpečených cest, a proto se dá očekávat, že skutečné procento bude opravdu mizivé. Na druhou stranu se objevily, a dokonce ověřily dva případy AS, které ROV vykonávají jako součást běžného provozu AS, což dokazuje, že to v současnosti je technicky i provozně možné. ■

Důsledkem tohoto výzkumu bylo rozpracování metodiky měření ROV v internetu.

Autor je bezpečnostním expertem společnosti CZ.NIC