Internet ve víru Route Origin Validation

Route Origin Validation (ROV) je komplementárním mechanismem k vydávání Route Origin Authorization (ROA) – dohromady pak tvoří bezpečnostní mechanismus Resource Public Key Infrastructure (RPKI), který má ambice potírat anebo přinejmenším zmírnit následky chybně oznámených prefixů protokolem BGP. Nasazení mechanismu RPKI je pomalé, a to i navzdory jeho technologické vyspělosti, existenci všech potřebných standardů, softwaru i detailní dokumentaci či propagaci standardu ze strany RIPE NCC.

TOMÁŠ HLAVÁČEK

Procedury propojování autonomních systémů se v internetu vyvíjejí, avšak nezávislost autonomních systémů a provoz internetu bez centrálních autorit přetrvaly. Nebývalá svoboda a s ní související absence jakékoliv byrokracie umožnily rychlý rozvoj internetu a přinesly technologickou revoluci.

Technika i provozní postupy internetu prokázaly, že samoregulace je statisticky skvěle fungující model i pro celosvětovou síť, jejíž spolehlivost je v současnosti kritická. Samoregulace v současné podobě však nezaručuje odolnost proti občasným útokům a chybám.

Jeden z nejznámějších případů se stal v únoru 2008, kdy autonomní systém s číslem 17557 (tedy Pakistan Telecom) začal oznamovat svým sousedům nový prefix 208. 65. 153.0/24. Tento prefix byl součástí méně specifického prefixu, který byl přidělený YouTube a byl používán pro servery, jež byly tou dobou zcela klíčové pro doručování obsahu a tedy pro přehrávání videa z YouTube.

Kvůli fundamentálnímu pravidlu směrování protokolu TCP/IP, že specifičtější cesta vždy vyhrává, tedy AS17557 přetáhl veškerý provoz z celého světa směrovaný na klíčové body YouTube do své sítě a tam tento provoz potichu zahodil.

Celá příhoda se vysvětlila jako konfigurační chyba na straně AS17557, který ve snaze splnit příkaz vlády k omezení přístupu k YouTube ve vlastní síti injektoval slepou cestu do své sítě a nedopatřením došlo k redistribuci do protokolu BGP a k oznámení cesty všem sousedům.

Selhali i sousedé, zejména upstreamy, od kterých se očekává ochrana proti podobným konfiguračním chybám v podobě ručně nastavených filtrů. Celý incident se zanalyzoval a popsal na webu RIPE NCC.

Vznik RPKI

Nejen tento incident, ale desítky dalších podobných úniků, útoků a nehod akcelerovaly vývoj automatických preventivních opatření. Návrhem, který uspěl v diskuzi internetové komunity a v procesu vývoje standardů, byl systém RPKI.

K jeho standardizaci došlo v roce 2013 v dokumentu RFC 6480 a v dalších návazných standardech. Jde o hierarchický systém, který staví na kryptografickém potvrzování transferu autority nad částmi adresního prostoru, a proto byla klíčová podpora RIR, tedy mezinárodních koordinátorů užití adresního prostoru.

Z hlediska Evropy přišla podpora RPKI od RIPE NCC velmi brzy po standardizaci a plnému nasazení RPKI už několik let vlastně nic nebrání.

Celý systém RPKI není příliš složitý, jeho návrh je přiměřeně elegantní a software realizující tento systém je k dispozici v produkční kvalitě i s dokumentací a s možností bezplatných školení ze strany RIPE NCC.

Z hlediska jednotlivého provozovatele sítě – autonomního systému lze RPKI implementovat i se skromnými prostředky a časem. Nicméně už během standardizace se objevily výhrady proti hierarchické podobě RPKI, která efektivně umožní výše postaveným uzlům v RPKI stromu kdykoliv revokovat certifikáty pro nižší uzly, a ve výsledku tak odpojit anebo omezit konektivitu závislým sítím.

Sluší se však říci, že to není vedlejší účinek, ale prakticky to je prostředek i cíl RPKI.

[Technika i provozní postupy internetu prokázaly, že samoregulace je statisticky skvěle fungující model i pro celosvětovou síť.]

[Bezpodmínečné nasazení RPKI by bylo bezpochyby obrovskou změnou organizace internetu.]

Přijetí RPKI a nasazení

Bezpodmínečné nasazení RPKI by bylo bezpochyby obrovskou změnou organizace internetu. V současnosti nad tím, co kdo oznámí protokolem BGP svým sousedům, není žádná centrální kontrola, a veškerá zodpovědnost tak padá na zdroj oznámení cesty a částečně na jeho bezprostřední sousedy.

V mnoha případech není kvůli počtu oznamovaných prefixů a frekvenci změn reálné všechna příchozí oznámení ručně kontrolovat, a proto je mnohde ve filtrech vše povoleno stejně jako v případě Pakistan Telecomu a jeho upstreamů.

RPKI by pravomoc rozhodovat o příchozích oznámeních přeneslo ve prospěch automatického systému. Správci by stále mohli ručně zasáhnout, ale stejně jako dnes od určitého množství není ruční kontrola únosná, vše zůstává povoleno a správci ručně zasahují až po důrazném upozornění.

V případě automatizace kontroly pomocí RPKI by tedy v drtivé většině případů rozhodovaly hierarchicky vydávané certifikáty, a to se všemi důsledky pro omezení decentralizace internetu.

V současnosti je prefixů, které jsou pokryté příslušným ROA, zatím jen kolem 10 % celkového počtu a růst množství takto chráněných sítí neslibuje všeobecné přijetí v nejbližší budoucnosti.

Mimo to je 0,5–1 % celkového počtu prefixů pravděpodobně pokryté chybným ROA. Validace a vynu-