Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-189 wer. 1.0

30 października 2023

Odporność wymiany ruchu międzydomenowego - bezpieczeństwo BGP i ograniczanie DDoS

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

Niniejsza publikacja **NSC 800-189**, *Odporność wymiany ruchu międzydomenowego - bezpieczeństwo BGP i ograniczanie DDoS*, opracowana została za zgodą National Institute of Science and Technology na podstawie specjalnej publikacji NIST SP 800-189, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation.*

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w poradniku źródłowym, na podstawie którego powstały niniejsze zalecenia. W przypadku, gdy tożsame pojęcie zostało zdefiniowane również w powszechnie obowiązujących aktach prawnych lub normatywnych, a ich definicja różni się od tej zamieszczonej w niniejszej publikacji, wówczas należy stosować sformułowania zawarte w tych aktach/w obiegu prawnym.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim.[1] Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

[1] Kluczowi uczestnicy zarządzania ryzykiem - patrz NSC 800-18; NSC 800-37, NSC 7298.

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[2]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

[2] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:


Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.


+48222455922


sekretariat.dc@cyfra.gov.pl

ABSTRAKT

W ostatnich latach, liczne anomalie w warstwie sterowania routingiem, takie jak przechwytywanie (*ang. hijacking*) prefiksów protokołu BGP (*ang. Border Gateway Protocol*) i wycieki tras, powodowało odmowę świadczenia usługi (*ang. denial-of-service - DoS*), niepożądane zmiany ruchu danych i spadki wydajności. Częste były również wielkoskalowe rozproszone ataki odmowy usług (*ang. distributed denial-of-service - DDoS*) na serwery przy użyciu fałszywych adresów IP i ataki typu „odbicie-wzmocnienie" (*ang. reflection-amplification)* w płaszczyźnie danych, co powodowało znaczne zakłócenia usług i szkody. Niniejsza publikacja na temat odporności wymiany ruchu międzydomenowego (*ang. Resilient Interdomain Traffic Exchange - RITE*) zawiera podstawowe wskazówki dotyczące bezpieczeństwa sterowania ruchem międzydomenowym, zapobiegania spoofingowi adresów IP oraz niektórych aspektów wykrywania i ograniczania ataków DoS/DDoS.

Wiele zaleceń zawartych w niniejszej publikacji dotyczy protokołu BGP. BGP jest protokołem sterującym, służącym do przydzielania i obliczania ścieżek pomiędzy dziesiątkami tysięcy sieci autonomicznych składających się na Internet. Technologie zalecane w niniejszym dokumencie dla zabezpieczenia ruchu związanego ze sterowaniem routingem międzydomenowym zawierają zasoby infrastruktury klucza publicznego (*ang. Resource Public Key Infrastructure - RPKI*), sprawdzanie poprawności pochodzenia BGP (*ang. BGP Origin Validation - BGP-OV*) i filtrowanie prefiksów. Dodatkowo, technologie zalecane do ograniczania ataków DoS/DDoS skupiają się na zapobieganiu spoofingowi adresów IP przy użyciu funkcji sprawdzania poprawności adresu źródłowego (*ang. source address validation - SAV*) z listami kontroli dostępu (*ang. access control list - ACL*) i mechanizmu uRPF (*ang. unicast Reverse Path Forwarding).* Inne technologie (w tym niektóre metody płaszczyzny aplikacyjnej), takie jak zdalnie wyzwalany blackholing (*ang. remotely triggered black hole - RTBH filtering*), specyfikacja przepływu (*ang. flow specification -Flowspec*) i ograniczenie współczynnika odpowiedzi (*ang. response rate limiting - RRL*) są również zalecane jako część ogólnego mechanizmu bezpieczeństwa.

SŁOWA KLUCZOWE

Bezpieczeństwo i niezawodność routingu (*ang. routing security and robustness*); bezpieczeństwo infrastruktury internetowej (*ang. Internet infrastructure security*); bezpieczeństwo protokołu BGP; przechwycenie prefiksu (*ang. prefix hijacks*); spoofing adresów IP (*ang. IP address spoofing*); rozproszona odmowa usługi (*ang. distributed denial-of-service - DDoS*); zasoby infrastruktury klucza publicznego (*ang. Resource Public Key Infrastructure - RPKI*); sprawdzanie poprawności pochodzenia BGP (*ang. BGP origin validation - BGP-OV*); filtrowanie prefiksów; sprawdzanie poprawności ścieżki BGP (*ang. BGP path validation - BGP-PV*);protokół BGP z rozszerzeniami bezpieczeństwa (*ang. Broder Gateway Protocol with Security Extensions – BGPsec)*; wycieki trasy (*ang. route leaks*); sprawdzanie poprawności adresu źródłowego (*ang. source address validation - SAV*); unicast ścieżek zwrotnych (*ang. unicast Reverse Path Forwarding - uRPF*); zdalnie wyzwalany blackholing (*ang. remotely triggered black hole RTBH filtering*); specyfikacja przepływu (*ang. filtering; flow specification Flowspec*).

ODBIORCY

Niniejszy dokument zawiera wskazówki techniczne i zalecenia dotyczące odporności wymiany ruchu międzydomenowego. Głównymi odbiorcami jest personel ds. bezpieczeństwa informacji i menedżerowie sieci organizacyjnych. Zalecenia mają zastosowanie do usług sieciowych dostawców usług hostingowych (np. aplikacje i hosting usług w chmurze) oraz dostawców usług internetowych (*ang. Internet service provider - ISP*). Mogą być również przydatne także dla operatorów sieci i dostawców sprzętu.

Oczekuje się, że wytyczne i stosowne zalecenia zawarte w niniejszej publikacji zostaną włączone do planów bezpieczeństwa i procesów operacyjnych sieci organizacyjnych.

Przewiduje się również, że stosowne zalecenia zostaną włączone do treści umów o świadczenie usług w ramach zamówień na hostowane usługi aplikacji i usługi tranzytu internetowego.

INFORMACJE NA TEMAT ZNAKÓW HANDLOWYCH

Wszystkie znaki handlowe należą odpowiednio do ich organizacji.

INFORMACJA O UJAWNIENIU PATENTU

INFORMACJA: Laboratorium technologii informacyjnych (Information Technology Laboratory - ITL) zwróciło się do posiadaczy zastrzeżeń patentowych, których zastosowanie może być konieczne dla zapewnienia zgodności z wytycznymi lub wymogami niniejszej publikacji, o przedstawienie ITL takich zastrzeżeń patentowych. Posiadacze patentów nie są jednak zobowiązani do odpowiedzi na to wezwanie ITL, a ITL nie przeprowadziło kwerendy patentowej w celu ustalenia, które patenty mogą mieć zastosowanie do niniejszej publikacji.

Na dzień publikacji i po wezwaniu do wskazania zastrzeżeń patentowych, których wykorzystanie może być wymagane dla zgodności z wytycznymi lub wymogami niniejszej publikacji, żadne takie zastrzeżenie patentowe nie zostało wskazane ITL.

ITL nie oświadcza ani nie sugeruje, że przy korzystaniu z niniejszej publikacji nie są wymagane licencje dla uniknięcia naruszenia patentu.

STRESZCZENIE

W ostatnich latach nastąpiło wiele incydentów związanych z anomaliami dotyczącymi płaszczyzny sterowania routingem, takich jak przejmowanie prefiksów protokołu BGP, wycieki tras i inne formy błędnego kierowania ruchu powodujące odmowę świadczenia usługi (DoS), niechciane obejścia ruchu danych i spadek wydajności. Częste były również wielkoskalowe rozproszone ataki odmowy usług (DDoS) na serwery przy użyciu fałszywych adresów IP i ataki typu „odbicie-wzmocnienie" w płaszczyźnie danych, co powodowało znaczne zakłócenia usług i wyrządzało szkody.

Niniejszy dokument podaje wskazówki techniczne i zalecenia dla technologii podnoszących odporność wymiany ruchu międzydomenowego (RITE). Głównym obiektem tych zaleceń są punkty wzajemnych połączeń między sieciami organizacji lub dostawcami usług hostingowych a publiczną siecią internetową — innymi słowy, między tak zwanymi sieciami „szczątkowymi"[3] (*ang. „stub" network)* a sieciami tranzytowymi (tzn. sieciami, które służą do łączenia i przekazywania ruchu między sieciami „stub" i innymi sieciami tranzytowymi). Często takie punkty wzajemnych połączeń między sieciami szczątkowymi i tranzytowymi są określane jako „krawędź Internetu" (*ang. „internet's edge*") Zwykle istnieje stosunek umowny między sieciami tranzytowymi i obsługiwanymi przez nie sieciami szczątkowymi, a szereg procedur technicznych i zasad określonych w ramach tego stosunku jest powszechnie nazywany „polityką partnerską" (*ang. peering policy*).

Wiele zaleceń zawartych w niniejszym dokumencie dotyczy również punktów styku między dwiema sieciami tranzytowymi. Istnieją przypadki, w których zalecenia dotyczące wymiany ruchu międzydomenowego między sieciami tranzytowymi będą się różnić od tych dotyczących wymiany między sieciami „stub" i tranzytowymi.

[3] Sieci, które zapewniają jedynie łączność ze swoimi systemami końcowymi. Sieć typu „stub" lub „pocket", jest nieco swobodnym terminem opisującym sieć komputerową lub część sieci internetowej, bez wiedzy o innych sieciach, która zazwyczaj wysyła większość lub cały swój ruch nielokalny przez pojedynczą ścieżkę, przy czym sieć zna tylko domyślną trasę do nielokalnych miejsc docelowych.

Podane zalecenia zmniejszają ryzyko przypadkowych ataków (spowodowanych przez błędną konfigurację) i złośliwych ataków w płaszczyźnie sterowania routingu, a także pomagają wykrywać i zapobiegać spoofingowi adresów IP i wynikającym z niego atakom DoS/DDoS. Niniejsze zalecenia przede wszystkim obejmują technologie (w celu zapewnienia bezpieczeństwa i niezawodności), które mają być stosowane w routerach granicznych[4] (*ang. border router*), które obsługują Border Gateway Protocol (powszechnie zwanymi routerami BGP). Jednak obejmują one również inne systemy wspierające osiągalność w Internecie (np. repozytoria RPKI, DNS, inne otwarte usługi internetowe).

Oczekuje się, że wytyczne i obowiązujące zalecenia na podstawie niniejszej publikacji zostaną włączone do planów bezpieczeństwa i procesów operacyjnych sieci organizacyjnych. Oczekuje się również, że odpowiednie zalecenia zostaną włączone do umów na usługi w ramach zamówień dotyczących usług hostowanych aplikacji i usług tranzytu internetowego.

Technologie zalecane w niniejszym dokumencie dla zabezpieczenia ruchu związanego z kontrolą trasowania ruchu międzydomenowego obejmują zasoby infrastruktury klucza publicznego (RPKI), sprawdzanie poprawności pochodzenia BGP-OV i filtrowanie prefiksów. Ponadto technologie zalecane do ograniczania ataków DoS/DDoS obejmują zapobieganie spoofingowi adresów IP przy użyciu sprawdzania poprawności adresu źródłowego (SAV) z listami kontroli dostępu (ACL) i mechanizmu uRPF. Inne technologie (w tym niektóre metody płaszczyzny aplikacyjnej), takie jak zdalnie wyzwalany blackholing (RTBH filtering), specyfikacja przepływu (Flowspec) i ograniczenie współczynnika odpowiedzi (RRL) są również zalecane jako część ogólnego mechanizmu bezpieczeństwa.

[4] Router graniczny - router, który ma co najmniej jedno połączenie z innym systemem autonomicznym.

Spis treści

Spis ilustracji

Spis tabel

1. WSTĘP

1.1. Zawartość przewodnika

Przewodnik zawiera techniczne wskazówki i zalecenia dotyczące wdrażania protokołów i technologii, które poprawiają bezpieczeństwo wymiany ruchu międzydomenowego. Zalecenia niniejsze zmniejszają ryzyko przypadkowych ataków (spowodowanych błędną konfiguracją) i złośliwych ataków w płaszczyźnie sterowania routingiem, a także pomagają wykrywać i zapobiegać spoofingowi adresów IP i wynikającym z niego atakom DoS/DDoS. Zalecenia obejmują przede wszystkim protokoły i techniki do stosowania w routerach BGP. Jednakże, częściowo obejmują one również inne systemy wspierające osiągalność w Internecie (np. repozytoria RPKI, DNS i inne otwarte usługi internetowe).

Technologie zalecane w tym dokumencie w celu zabezpieczania sterowania ruchem międzydomenowym obejmują RPKI, sprawdzanie pochodzenia BGP (BGP-OV) oraz filtrowanie prefiksów. Ponadto technologie zalecane do ograniczania ataków DoS/DDoS obejmują zapobieganie spoofingowi adresów IP przy użyciu sprawdzania poprawności adresu źródłowego (SAV) z listami kontroli dostępu (ACL) i mechanizmu uRPF (unicast Reverse Path Forwarding). Inne technologie (w tym niektóre metody płaszczyzny aplikacyjnej), takie jak zdalnie wyzwalany blackholing (RTBH filtering), specyfikacja przepływu (Flowspec) i ograniczenie współczynnika odpowiedzi (RRL, są również zalecane jako część ogólnego mechanizmu bezpieczeństwa.

Niniejszy dokument odnosi się do wielu z problemów wskazanych w [CSRIC6-WG3] dotyczących podatności BGP i ataków DoS/DDoS, ale zawiera bardziej techniczne informacje przy opisie mechanizmów bezpieczeństwa opartych na standardach i podawaniu konkretnych zaleceń dotyczących bezpieczeństwa.

1.2. Czego niniejszy przewodnik nie zawiera

Sprawdzanie pochodzenia BGP opiera się na globalnym systemie RPKI (np. organy certyfikacji, repozytoria publikacji itp.) jako źródle zaufanych informacji o posiadaczach adresów internetowych i ich oświadczeniach o autoryzacji pochodzenia tras. Każdy regionalny rejestr internetowy (*ang. Regional Internet Registry*

– *RIR*) prowadzi zaufany główny urząd certyfikacji (*ang. certificate authority - CA*) w systemie RPKI i publikuje zasady postępowania dotyczące certyfikatów (*ang. Certificate Practice Statement*) [RFC7382] opisujące właściwości każdej implementacji w zakresie bezpieczeństwa i niezawodności. Każdy CA RPKI posiada mechanizmy integralności i uwierzytelniania na potrzeby tworzenia, przechowywania i transmisji danych. Niemniej, naruszenie zasad ochrony podstawowych serwerów i/lub usług rejestru jest nadal potencjalnym, jeśli mało prawdopodobnym, zagrożeniem. Przygotowanie zaleceń dotyczących bezpieczeństwa w celu ograniczenia takich zagrożeń nie wchodzi w zakres niniejszego dokumentu.

Bezpieczeństwo warstwy transportowej jest kluczem do integralności wiadomości przekazywanych w sesjach BGP. Sformułowanie zaleceń dotyczących bezpieczeństwa dla bazowej warstwy transportowej również nie wchodzi w zakres niniejszego dokumentu.

Ataki DDoS wykorzystują sfałszowane adresy IP do wykorzystania bezpołączeniowych usług typu „zapytanie-odpowiedź” (*ang. „query-response*”), np. DNS, Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP) w celu „odbijania” i „wzmacniania” wpływu na wybrane cele. Niniejszy dokument dotyczy niektórych, ale nie wszystkich, aspektów zabezpieczenia serwerów wykorzystywanych do ataku typu reflection/amplification.

Środki bezpieczeństwa, takie jak ograniczanie współczynnika pakietów z nietypowych adresów źródłowych, połączeń IP lub SYN-proxy, mogą być skutecznie stosowane na serwerach używanych do odbijania i wzmacniania ataków DoS/DDoS, ale niniejszy dokument ich nie obejmuje.

1.3. Struktura dokumentu

Pozostała część dokumentu przedstawiona jest następująco:

- **Rozdział 2:** Opisuje ataki w płaszczyźnie sterowania routingu (np. przechwytywanie prefiksu BGP, modyfikacja ścieżki systemu autonomicznego (AS) i wycieki tras).
- **Rozdział 3:** Opisuje ataki w płaszczyźnie danych obejmujące spoofing źródłowego adresu IP i atak typu reflection-amplification.

- **Rozdział 4:** Przedstawia rozwiązania i formułuje zalecenia dotyczące bezpieczeństwa płaszczyzny sterowania routingiem/BGP. Omawiane technologie rozwiązań obejmują RPKI, sprawdzanie pochodzenia BGP (BGP-OV), filtrowanie prefiksów, sprawdzanie ścieżki BGP (BGP-PV), uogólniony mechanizm zabezpieczenia TTL (*ang. Generalized TTL Security Mechanism - GTSM*) oraz wykrywanie i ograniczanie wycieków tras.
- **Rozdział 5:** Przedstawia rozwiązania i formułuje zalecenia dotyczące zabezpieczeń w celu wykrywania i ograniczania skutków spoofingu źródłowych adresów IP i ataków typu reflection-amplification. Omawiane technologie rozwiązań obejmują listy ACL, różne metody uRPF, ograniczanie współczynnika odpowiedzi (RRL), RTBH i Flowspec.

1.4. Konwencje zastosowane w przewodniku

W niniejszym przewodniku stosuje się następujące konwencje formatów do oznaczania tekstu specjalnego zastosowania:

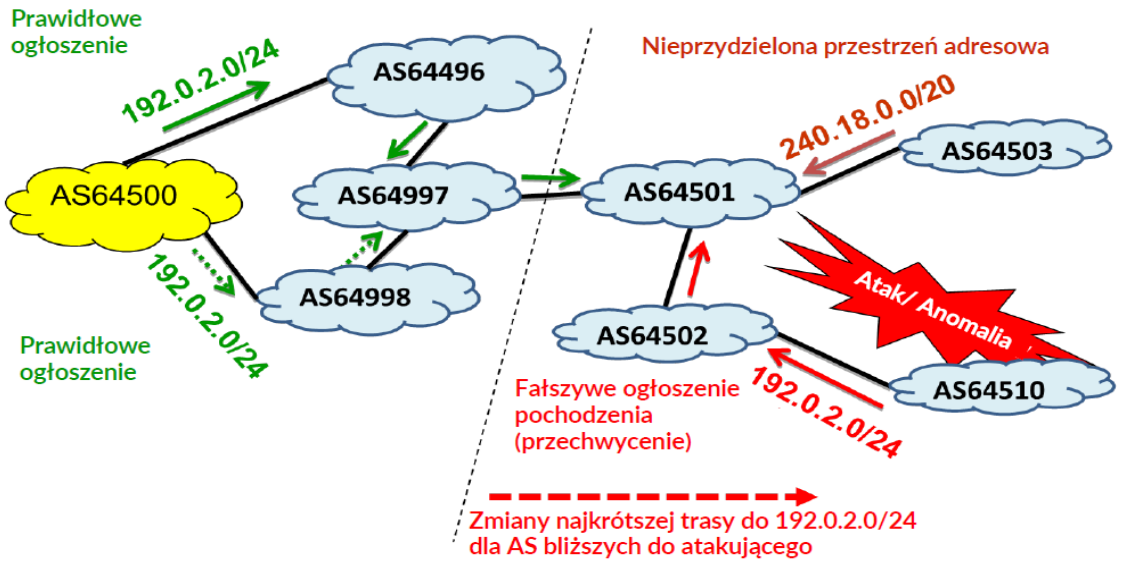
„**Zalecenie dotyczące bezpieczeństwa**” oznacza zalecenie, które powinno być uwzględnione w planach bezpieczeństwa, praktykach operacyjnych i umowach dotyczących zamówionych usług.

W tekście i odesłaniach podane są adresy URL, aby pokierować czytelników do danej strony internetowej lub narzędzia online zaprojektowanego w celu pomocy administratorom. Nie ma to na celu rekomendowania strony internetowej lub jakiegokolwiek produktu czy usługi oferowanej przez wydawcę witryny. Przyjmuje się, że wszystkie adresy URL są prawidłowe na moment opracowywania niniejszego dokumentu.

2. PODATNOŚCI PŁASZCZYZNY STEROWANIA/BGP

2.1. Przechwytywanie prefiksów i rozgłaszanie nieprzydzielonej przestrzeni adresowej

Przejęcie prefiksu BGP następuje, gdy system autonomiczny (*ang. autonomous system - AS*) przypadkowo lub złośliwie inicjuje prefiks, do którego utworzenia nie jest upoważniony (przez właściciela prefiksu). Jest to również znane jako fałszywe zainicjowanie/ rozgłoszenie. W przeciwieństwie do tego, jeśli AS jest upoważniony do zainicjowania/ rozgłoszenia prefiksu przez właściciela prefiksu, wówczas takie zainicjowanie/ rozgłoszenie trasy nazywa się legalnym. W przykładzie zilustrowanym na rys. 1, prefiks 192.0.2.0/24 jest prawidłowo zainicjowany przez AS64500, ale AS64510 inicjuje go fałszywie. Ścieżka do prefiksu przez AS fałszywego pochodzenia będzie krótsza dla podzbioru systemów AS w Internecie, a ten podzbiór systemów AS zainstaluje fałszywą trasę w swojej tablicy trasowania (*ang. routing table*) lub tablicy przekazywania (*ang. forwarding information base - FIB*). Oznacza to, że AS-y, dla których AS64510 jest bliżej (tj. posiadają krótszą ścieżkę do tego AS) wybiorą fałszywe ogłoszenie, a zatem ruch danych od klientów w tych AS przeznaczonych dla sieci 192.0.2/24 zostanie błędnie przekierowany do AS64510.



Niekorzystne skutki: odmowa usługi, nieprawidłowe pokierowanie ruchu, nieautoryzowany routing

Rysunek 1: Przechwytywanie prefiksów i rozgłaszanie nieprzydzielonej przestrzeni adresowej

Reguły wyboru trasy IP w Internecie zawsze preferują najbardziej szczegółowy (tj. najdłuższy) wpis w tabeli FIB routera. Gdy system autonomiczny naruszający reguły błędnie ogłasza prefiks bardziej szczegółowy (niż prefiks ogłaszany przez autoryzowany AS), ten dłuższy, nieautoryzowany prefiks zostanie powszechnie zaakceptowany i użyty do przesyłania danych. Rys. 1 ilustruje również przykład nieautoryzowanego zainicjowania nieprzydzielonej (zarezerwowanej) przestrzeni adresowej 240.18.0.0/20. Obecnie adres 240.0.0.0/8 jest zarezerwowany do użytku w przyszłości [IANA-v4-r]. Podobnie system autonomiczny może również fałszywie zainicjować przydzieloną, ale obecnie nieużywaną przestrzeń adresową. Określa się to jako „prefix squatting”[5]. Jest to sytuacja, w której nieużywany prefiks kogoś innego jest tymczasowo ogłaszany i używany do wysyłania spamu lub w innym złośliwym celu.

Różne typy nieautoryzowanych inicjacji prefiksów opisane powyżej nazywane są przejęciami prefiksów lub fałszywymi ogłoszeniami o ich pochodzeniu. Nieautoryzowane rozgłoszenie prefiksu dłuższego niż uprawnione ogłoszenie jest nazywane przechwyceniem subprefiksu (*ang. sub-prefix hijack*). Konsekwencje takich szkodliwych działań mogą być poważne i obejmować odmowę usługi, podsłuchiwanie, przekierowywanie do fałszywych serwerów (w celu kradzieży poświadczeń logowania lub wprowadzenia złośliwego oprogramowania) lub przełamanie systemów reputacji IP w celu uruchomienia wiadomości e-mail zawierającej spam. W ostatnich latach miały miejsce liczne incydenty związane z przechwytywaniem prefiksów. Istnieje kilka komercyjnych usług i projektów badawczych, które śledzą i rejestrują nieprawidłowości w globalnym systemie routingu BGP [BGPmon], [ThousandEyes], [BGPStream], [ARTEMIS]. Wiele z tych referencji zawiera szczegółowe analizy śledczo-informatyczne zaobserwowanych scenariuszy ataków.

2.2. Modyfikacja ścieżki AS

Komunikaty BGP zawierają sekwencję numerów AS, która wskazuje „ścieżkę” wzajemnie połączonych sieci, przez które będą przepływać dane. Te dane „AS_PATH” [RFC4271] są często używane do realizowania polityk routingu odzwierciedlających

[5] Prefiks przydzielony „na dziko”.

umowy biznesowe i zasady komunikacji równorzędnej wynegocjowane między sieciami. BGP jest również podatny na modyfikację informacji AS_PATH, które przekazuje. Na przykład złośliwy AS, który otrzymuje aktualizację BGP, może bezprawnie usunąć niektóre z poprzednich systemów AS w atrybucie AS_PATH aktualizacji w taki sposób, aby długość ścieżki wydawała się krótsza. Kiedy zmodyfikowana w ten sposób aktualizacja zostanie rozpropagowana, strumienie wychodzące (*ang. upstream*) systemów autonomicznych AS mogą zostać oszukane, że ścieżka do prefiksu ogłaszanego przez wrogi AS jest krótsza. W ten sposób wrogi AS może próbować bezprawnie zwiększyć swoje korzyści od swoich klientów lub może podsłuchiwać ruch, który w innym przypadku nie przechodziłby przez jego AS.

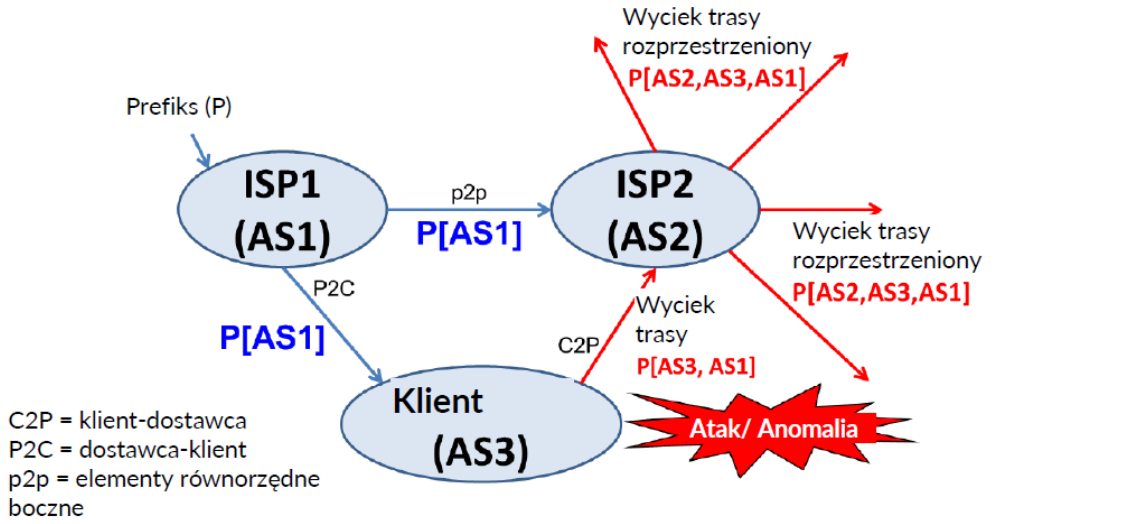
Innym przykładem złośliwej modyfikacji aktualizacji BGP jest sytuacja, w której wrogi AS zastępuje prefiks w odbieranej aktualizacji bardziej specyficznym prefiksem (podciągniętym pod ten prefiks), a następnie przekazuje aktualizację do sąsiadów. Ten atak jest znany jako atak Kapeli-Pilosova [Kapela-Pilosov]. Tylko prefiks jest zastępowany bardziej specyficznym prefiksem, ale ścieżka AS nie jest zmieniana. Przy wyborze ścieżki BGP ogłoszenie bardziej specyficznego prefiksu wygrywa z ogłoszeniem mniej specyficznego prefiksu. Oznacza to, że systemy autonomiczne w Internecie szeroko akceptowałyby i wykorzystywały rozgłoszenie bardziej szczegółowego prefiksu dokonane przez wrogi AS. Wyjątkiem są systemy autonomiczne znajdujące się na ścieżce AS od atakującego do prefiksu. Te stanowiące wyjątek systemy AS odrzucają wszelkie ogłoszenia, jakie mogą otrzymać dla bardziej specyficznego prefiksu, ponieważ wykrywają swój własny numer AS w ścieżce AS. Nazywa się to unikanie wykrycia pętli i jest standardową praktyką w BGP. W ten sposób ścieżka danych z wrogiego AS do prefiksu (tj. rozważanej sieci) pozostaje nienaruszona (tj. nie ma na nią wpływu bardziej specyficzne złośliwe rozgłoszenie). Efekt sieciowy tego ataku jest bardzo poważny. Atakujący byłby w stanie wymusić przez swój AS przekierowanie prawie całego ruchu do bardziej specyficznego prefiksu. W ten sposób mogą podsłuchiwać dane (przeznaczone dla bardziej specyficznego prefiksu), kierując je z powrotem do legalnego miejsca docelowego, aby uniknąć wykrycia.

2.3. Wycieki tras

Jak wyżej zauważono, wzajemne połączenia sieci w Internecie są podyktowane umownymi relacjami biznesowymi, które wyrażają polityki i procedury wymiany ruchu sterowania i danych w każdym punkcie wzajemnego połączenia. Takie polityki komunikacji równorzędnej (*ang. peering*) często określają limity dotyczące tego, jakie rozgłoszenia routingu będą akceptowane przez każdą ze stron. Często polityki te odzwierciedlają relacje biznesowe pomiędzy sieciami - klient, dostawca tranzytu i/lub lateralnymi sieciami równorzędnymi (*ang. lateral peer*).

Definicje stosunków komunikacji równorzędnej, stożek klientów (ang. customer cone):
Definicje te są przydatne w przypadku wycieków tras (opisanych tutaj i w dziale 4.9), a także w przypadku BGP-OV (dział 4.3), filtrowania prefiksów (działy 4.4 i 4.5), oraz SAV/uRPF (działy 5.1 i 5.2). Dostawca tranzytowy zazwyczaj świadczy usługi w celu podłączenia swoich klientów do globalnego Internetu. AS lub sieć klienta może być typu „single-homed” dla jednego dostawcy tranzytowego lub typu „multi-homed” dla więcej niż jednego dostawcy tranzytowego. AS klienta typu „stub” nie ma własnych systemów AS klienta lub lateralnych równorzędnych AS (*ang. lateral peer AS*). Klient typu „liść” (*ang. leaf customer*) jest klientem stub o charakterze single-homed, połączonym z jednym dostawcą tranzytowym i nie połączonym z żadnym innym AS. Relacje równorzędne rozważane w niniejszym dokumencie to relacje dostawca-klient (*ang. provider-to-customer - P2C*), klient-dostawca (*ang. customer-to-provider - C2P*) i relacje równorzędne (*ang. peer-to-peer - p2p*). Określenie „dostawca” oznacza tu dostawcę tranzytowego. Pierwsze dwa, to stosunki tranzytowe. Element równorzędny (peer) połączony p2p jest określany jako lateral peer - element równorzędny boczny (nietranzytowy). Stożek klientów (*ang. customer cone*) systemu autonomicznego AS A jest definiowany jako AS A plus wszystkie systemy autonomiczne możliwe do osiągnięcia z A tylko po łączach P2C [Luckie]. Termin „prefiksy stożków klientów” systemu autonomicznego (AS) odnosi się do związku prefiksów otrzymanych od wszystkich bezpośrednio powiązanych klientów i prefiksów pochodzących od samego AS. Oczywiście zestaw ten cyklicznie obejmuje rozgłoszenia prefiksów klientów (w dół hierarchii). Systemy AS, które mają relację równorzędną boczną (tj. p2p),

zazwyczaj ogłaszają swoje prefiksy stożków klientów sobie nawzajem, a następnie ogłaszają prefiksy stożków klientów elementów równorzędnych bocznych odpowiednio ich klientom, ale nie innym elementom równorzędnym bocznym lub dostawcom tranzytowym.



Rysunek 2: Ilustracja podstawowego rozumienia wycieku

Zależności te są istotne, ponieważ większość operacji globalnego Internetu jest zaprojektowana w taki sposób, by stub AS lub AS klienta nigdy nie był użyty do wyznaczania trasy pomiędzy dwoma tranzytowymi systemami AS. Polityka ta jest realizowana poprzez zapewnienie, że stub AS lub AS klienta nie przekaże informacji routingowej BGP otrzymanej od jednego dostawcy tranzytowego innemu. Rys. 2 ilustruje zwykłą postać wycieku trasy, która występuje, gdy AS typu multi-homed klienta (taki jak AS3 na rys. 2) dowiaduje się o aktualizacji prefiksu od jednego dostawcy tranzytowego (ISP1) i dokonuje „przecieku" aktualizacji do innego dostawcy tranzytowego (ISP2) z naruszeniem zamierzonych zasad routingu, a drugi dostawca tranzytowy nie wykrywa wycieku i propaguje taką aktualizację do swoich klientów, bocznych elementów równorzędnych i ISP tranzytowych [RFC7908]. Przykłady ostatnich incydentów związanych z wyciekiem tras obejmują: 1) wyciek prefiksów Google przez MainOne (nigeryjskiego ISP), który spowodował przerwę w działaniu usług Google przez ponad godzinę w listopadzie 2018 roku [Naik]; 2) incydent

Dodo-Telstra w marcu 2012 roku, który spowodował ogólnokrajową przerwę w działaniu usług internetowych w Australii [Huston2012]; oraz 3) masowe wycieki tras Telekom Malaysia, które Level3 z kolei zaakceptował i rozpropagował [Toonk-B].

Ogólnie rzecz biorąc, zgodnie z definicją zawartą w [RFC7908], wyciek trasy to propagacja ogłoszeń o trasach poza ich zamierzonym zakresem. Oznacza to, że ogłoszenie przez AS poznanej trasy BGP do innego AS narusza zamierzone polityki odbiorcy, nadawcy i/lub jednego z AS wzdłuż poprzedzającej ścieżki AS.

W [RFC7908] wymieniono i opisano kilka rodzajów wycieków tras wraz z przykładami ostatnich incydentów. Rezultatem wycieku tras może być przekierowanie ruchu przez niezamierzoną ścieżkę, co może umożliwić podsłuch lub złośliwą analizę ruchu. Kiedy jednocześnie wycieka duża liczba tras, szkodliwy AS jest często przeciążony wynikającym z tego nieoczekiwanym ruchem danych i porzuca dużą część obsługiwanego ruchu [Huston2012], [Toonk-A], [Naik], [Zmijewski]. Powoduje to „czarną dziurę (*ang. blackhole*)[6] i odmowę usługi dla zaatakowanych prefiksów (*ang. blackholing*)[7]. Wycieki tras mogą być przypadkowe lub złośliwe, ale najczęściej powstają w wyniku przypadkowych błędnych konfiguracji.

[6] Czarna dziura – w sieciach komputerowych pojęcie to odnosi się do miejsca w sieci, w którym ruch sieciowy jest przerywany, ale bez informowania o tym źródła. Podczas sprawdzania topologii sieci czarne dziury są niewidoczne. Można je wykryć tylko przez monitorowanie ruchu sieciowego.

[7] Blackholing to technika antyspamowa, w której dostawca usług internetowych (ISP) blokuje pakiety pochodzące z określonej domeny lub adresu. Blackholing może również odnosić się do osoby, która ustawia podobną barierę dla swojej sieci osobistej. Blackholing określonych domen może zapobiegać niektórym rodzajom złośliwego oprogramowania i atakom typu denial of service.

3. SPOOFING ADRESÓW IP I ATAKI TYPU REFLECTION-AMPLIFICATION

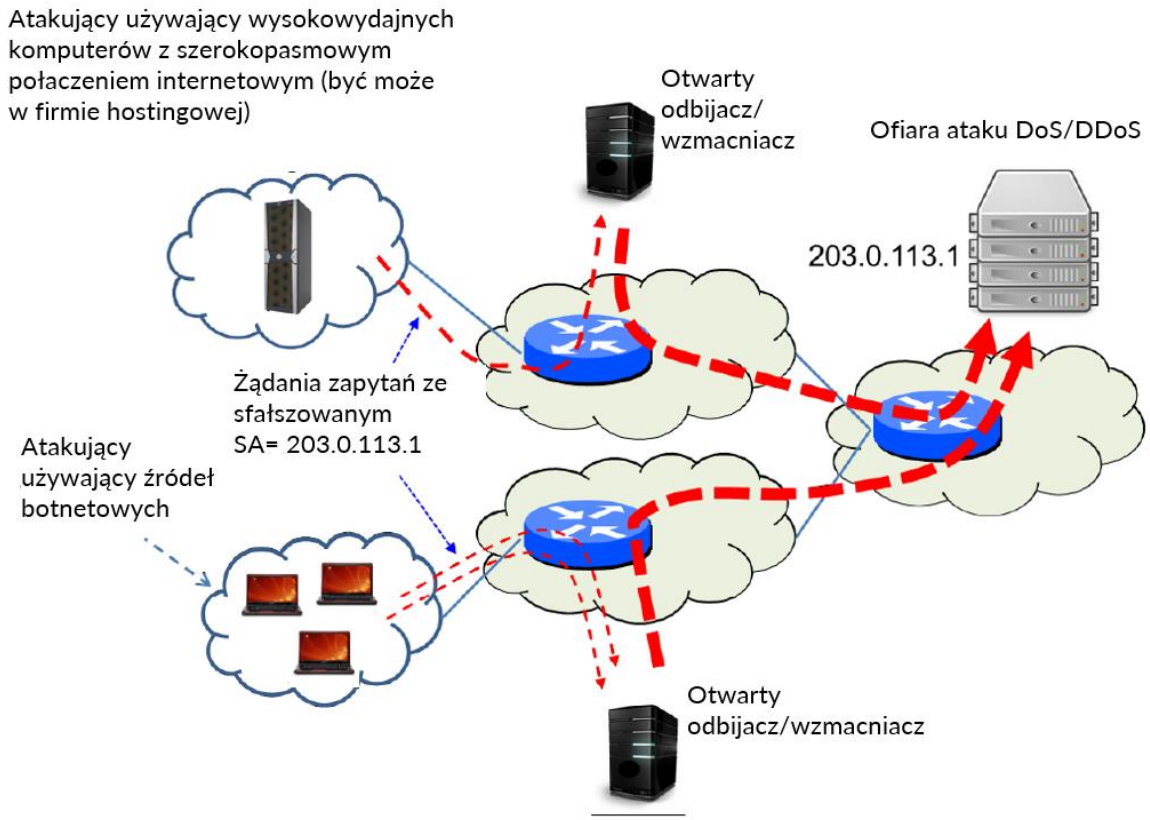
3.1. Sfałszowane adresy źródłowe

Rozproszona odmowa usługi (DDoS) jest postacią ataku, w którym ruch ataku jest generowany z wielu rozproszonych źródeł w celu osiągnięcia intensywności ataku i skierowany na wybraną ofiarę (tj. system lub serwer) [Arbor], [Arbor2], [ISOC], [Huston2016], [Mirai1]. Aby przeprowadzić bezpośredni atak DDoS, atakujący zazwyczaj korzysta z kilku wysokowydajnych komputerów lub ogromnej liczby zainfekowanych urządzeń nieświadomych osób trzecich (np. laptopów, tabletów, telefonów komórkowych, urządzeń Internetu rzeczy (IoT) itp.). Ten ostatni scenariusz jest często realizowany za pomocą botnetów [Arbor], [Huston2016], [DOC-Botnet]. W wielu atakach DDoS adresy źródłowe IP w wiadomościach ataku są „sfałszowane" (*ang. „spoofed"*), aby uniemożliwić ich prześledzenie [Arbor]. Niektóre ataki DDoS są uruchamiane bez użycia fałszywych adresów źródłowych. Na przykład w atakach Mirai [Mirai1], [Mirai2], [Winward], [TA16-288A] bardzo duża liczba zainfekowanych botów (urządzeń IoT) wysyłających ruch ataku korzystała z normalnych źródłowych adresów IP urządzeń IoT. Ponadto adresy źródłowe mogą również należeć do przechwyconego prefiksu z zamiarem oszukania walidacji adresu źródłowego (SAV) [BCP38], [BCP84] (patrz również dział 5.1.7). Jeśli używany jest przechwycony prefiks, adresy źródłowe pojawiające się w pakietach ataku DDoS są czasami losowo wybierane z tego prefiksu.

3.2. Ataki typu „odbicie-wzmocnienie"

Spoofing adresów źródłowych jest często łączony z atakiem „odbicie-wzmocnienie" ze źle zarządzanych otwartych serwerów internetowych (np. DNS, NTP) aby zwielokrotnić objętość ruchu ataku o współczynnik 50 lub większy [TA14-017A], [ISOC]. Sposób jego działania można wyjaśnić na ilustracji pokazanej na rys. 3. Osoba atakująca może użyć wydajnego komputera z łączem internetowym o dużej przepustowości lub botnetu składającego się z wielu zainfekowanych urządzeń do wysyłania żądań zapytań (*ang. query requests*) do serwerów internetowych o wysokiej wydajności. Atakujące systemy wykorzystują fałszowanie adresu źródłowego, które wstawia adres IP celu (203.0.113.1) jako adres źródłowy w żądaniach. W przypadku usług internetowych

korzystających z protokołu pakietów użytkownika (*ang. User Datagram Protocol - UDP*), np. DNS, NTP, zapytanie i odpowiedź są zawarte w jednym pakiecie, a wymiana nie wymaga ustanowienia połączenia między źródłem a serwerem (w przeciwieństwie do protokołu sterowania transmisją (*ang. Transmission Control Protocol - TCP*). Odpowiedzi z takich otwartych serwerów internetowych są kierowane do celu ataku, ponieważ adres IP celu został sfałszowany jako pole adresu źródłowego komunikatów żądań. Często odpowiedź serwera na adres docelowy jest znacznie większa niż samo zapytanie, co wzmacnia efekt ataku DoS (patrz Tabela 1 w dziale 5.4). Takie ataki typu „odbicie-wzmocnienie" mogą skutkować masowymi atakami DDoS o wolumenie ataków rzędu setek Gbps [Symantec], [ISTR-2015], [ISTR-2016], [ISTR-2017], [ISOC], [Verisign1], [Verisign2], [Bjarnason]. W I kwartale 2018 r. nastąpił wzrost o 100% licząc kwartał do kwartału i 700% rok do roku w przypadku ataków „wzmocnienie" DNS (*ang. DNS amplification*) [HelpNet]. Liczba ataków może nadal znacznie wzrosnąć, jeśli ataki w skali Mirai zostaną połączone z atakami typu „odbicie-wzmocnienie".



Rysunek 3: DDoS poprzez spoofing źródłowych adresów IP i atak typu „odbicie-wzmocnienie"

4. PŁASZCZYZNA STEROWANIA/BEZPIECZEŃSTWO BGP - ROZWIĄZANIA I ZALECENIA

Podatności w zakresie bezpieczeństwa BGP i techniki ograniczania od kilku lat cieszą się zainteresowaniem środowiska osób związanych z sieciami (np. [IETF-SIDR], [RFC7454], [NANOG], [Murphy], [MANRS], [MANRS2], [ENISA], [Quilt], [Levy1], [CSRIC4-WG6], [CSRIC6-WG3], [RFC6811], [RFC8205], [NSA-BGP], [CSDE], [Chung], [Wishnick], [Yoo]). W niniejszym rozdziale omówiono kluczowe technologie zabezpieczeń BGP, które powstały w wyniku tych starań oraz przedstawiono związane z nimi zalecenia dotyczące zabezpieczeń. Wiele omawianych tutaj technologii rozwiązań zostało opracowanych i znormalizowanych w Internet Engineering Task Force (IETF) [IETF-SIDR], [IETF-SIDROPS], [IETF-IDR], [IETF-OPSEC], [IETF-GROW]. Dokument [MANRS] można uznać za uzupełniający niniejszą publikację, ponieważ zawiera on wskazówki dotyczące implementacji niektórych technologii rozwiązań opisanych w niniejszym dziale i rozdziale 5. Niniejszy dokument odnosi się do wielu takich samych problemów dotyczących podatności BGP i ataków DoS/DDoS wskazanych w [CSRIC6-WG3], ale w sposób bardziej szczegółowy pod względem technicznym opisuje oparte na standardach i dostępne na rynku mechanizmy bezpieczeństwa oraz podaje konkretne zalecenia dotyczące bezpieczeństwa.

4.1. Rejestracja obiektów tras w internetowych rejestrach tras

Dane deklaratywne dotyczące alokacji zasobów internetowych oraz polityki trasowania tradycyjnie dostępne są w regionalnych rejestrach internetowych (*ang. regional internet registries - RIR*) oraz rejestrach routingu internetowego (*ang. internet routing registries - IRR*). Dane RIR są utrzymywane regionalnie przez ARIN w Ameryce Północnej, RIPE w Europie, LACNIC w Ameryce Łacińskiej, APNIC w Azji i Pacyfiku oraz AfriNIC w Afryce. IRR są utrzymywane przez RIR (RIPE NCC, APNIC, AfriNIC i ARIN) oraz niektórych głównych dostawców usług internetowych (ISP). Dodatkowo, Merit's Routing Assets Database (RADb) [Merit-RADb] i inne podobne podmioty zapewniają zbiorczą bazę informacji o trasach, składającą się z danych zarejestrowanych (u nich), jak również dublowanych (z IRR). Obiekty tras dostępne

w IRR dostarczają informacji o trasach deklarowanych przez operatorów sieci. W szczególności obiekty tras zawierają informacje dotyczące inicjowania prefiksów (tj. skojarzenia pomiędzy prefiksami a AS, które mogą je inicjować). Routing Policy Specification Language (RPSL) [RFC4012], [RFC7909] oraz Shared Whois Project (SWIP) [SWIP] to dwa formaty, w których prezentowane są dane w RIRs/IRRs. ARIN przeważnie używa SWIP, ale niektórzy używają także RPSL. LACNIC również korzysta z SWIP. Pozostałe RIR i IRR dostawców usług internetowych stosują wyłącznie RPSL.

Kompletność, poprawność, aktualność i spójność danych pochodzących z tych źródeł jest bardzo zróżnicowana, a dane nie zawsze są wiarygodne. Prowadzone są jednak działania mające na celu uczynienie danych kompletnymi i wiarygodnymi [RFC7909]. Operatorzy sieci często uzyskują informacje o obiektach tras z IRR i/lub RADb, i mogą wykorzystać te dane przy tworzeniu filtrów prefiksów (patrz działy 4.4 i 4.5) w swoich routerach BGP.

Warto zauważyć, że RIPE NCC, APNIC i AfriNIC prowadzą internetowe rejestry routingu (IRR), które są zintegrowane z danymi alokacji regionalnych rejestrów internetowych (RIR), co ułatwia stosowanie silniejszych schematów uwierzytelniania. Są one udokumentowane w [RFC2725]. W przypadku rejestracji bloku adresowego (NetRange) w ARIN, dozwolone jest uwzględnienie źródłowego autonomicznego systemu (*ang. origin AS*)[8].

Chociaż zachęca się do podejmowania wysiłków w celu stworzenia kompletnych i dokładnych danych IRR zgodnie z aktualną rzeczywistością operacyjną, należy dołożyć jeszcze większych wysiłków do tworzenia autoryzacji źródła trasy (*ang. route origin authorizations - ROA*), patrz dział 4.3, ponieważ RPKI zapewnia silniejsze ramy uwierzytelniania i walidacji dla operatorów sieci niż IRR.

[8] Zob. https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0.

Zalecenie dot. bezpieczeństwa[9]**1**: Wszystkie internetowe zasoby numerów (np. bloki adresowe i numery AS) powinny być objęte odpowiednią umową o świadczenie usług rejestracyjnych z RIR, a wszystkie informacje dotyczące punktów kontaktowych (*ang. point of contact - POC*) powinny być aktualne. Szczegółowość takich rejestracji powinna odzwierciedlać wszystkie subalokacje do podmiotów (np. jednostek w ramach organizacji macierzystej, oddziałów), które obsługują własne usługi sieciowe (np. dostęp do Internetu, DNS).

Zalecenie dot. bezpieczeństwa 2: W przypadku rejestracji bloku adresowego (NetRange) w ARIN należy uwzględnić inicjujący system autonomiczny (origin AS)[10].

Zalecenie dot. bezpieczeństwa 3: Obiekty tras odpowiadające trasom BGP pochodzącym z AS powinny być rejestrowane i aktywnie utrzymywane w IRR odpowiednim dla RIR. Przedsiębiorstwa powinny zapewnić istnienie odpowiednich informacji IRR dla całej przestrzeni adresowej IP wykorzystywanej bezpośrednio oraz przez ich systemy i usługi informatyczne zlecane na zewnątrz.

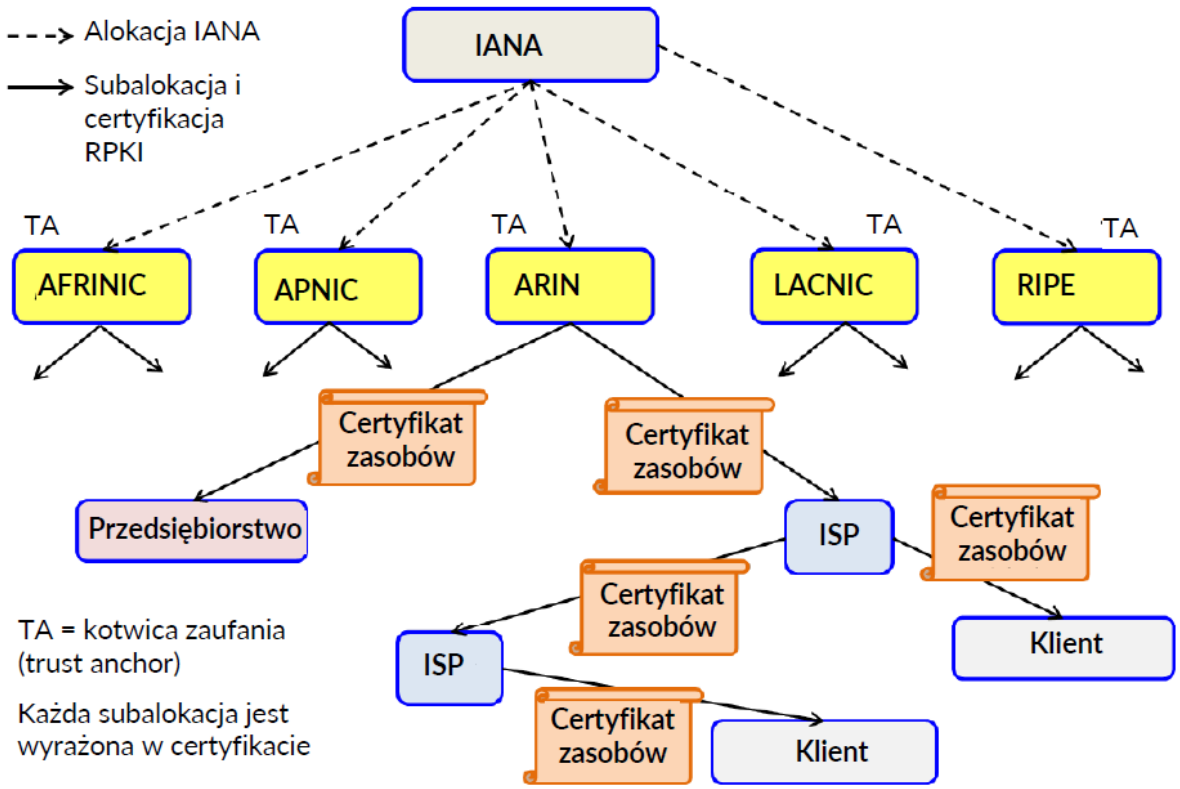
4.2. Certyfikacja środków w zasobach infrastruktury klucza publicznego

Zasób infrastruktury klucza publicznego (*ang. Resource Public Key Infrastructure - RPKI*) jest opartym na standardach podejściem do zapewnienia kryptograficznie zabezpieczonych rejestrów zasobów internetowych i autoryzacji routingowych [RFC6480], [RFC6482], [NANOG], [Murphy]. Przydzielanie adresów IPv4/IPv6 i numerów AS odbywa się według hierarchii. Internet Assigned Numbers Authority (IANA) przydziela zasoby regionalnym rejestrom internetowym (RIR) (np. ARIN, RIPE itp.), a RIR-y przydzielają zasoby dostawcom usług internetowych i organizacjom. Dostawcy usług internetowych mogą dalej subalokować zasoby innym dostawcom usług internetowych i organizacjom. W niektórych regionach RIR-y subalokują lokalnym rejestrom internetowym (LIR), które z kolei subalokują dostawcom usług internetowych i organizacjom. RPKI jest globalnym urzędem certyfikacji

[9] Pewne zalecenia bezpieczeństwa dotyczą różnych ról (ISP, enterprise, serwery otwarte) i informacja ta jest widoczna we wszystkich zaleceniach bezpieczeństwa i podana w tabeli w Załączniku A.

[10] Zob. https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0.

(*ang. certificate authority - CA*) i usługą rejestrową oferowaną przez wszystkie regionalne rejestry internetowe (RIR). Łańcuch certyfikacji RPKI przebiega według tej samej hierarchii alokacji (zob. rys. 4). Chociaż certyfikaty RPKI są przedstawione na rys. 4, tylko w ramach ARIN, podobny schemat występuje we wszystkich innych RIR. W idealnym przypadku na szczycie hierarchii powinien znajdować się pojedynczy root lub kotwica zaufania (*ang. trust anchor - TA*), ale obecnie każdy z pięciu RIR (AFRINIC, APNIC, ARIN, LACNIC i RIPE) utrzymuje niezależną TA dla usług certyfikacyjnych RPKI w swoim regionie. W ten sposób globalna RPKI działa obecnie z pięcioma TA (patrz [ARIN1], [ARIN2], [RIPE1]). Istnieją różne otwarte narzędzia programowe dla stron ufających, służące do przeprowadzania walidacji RPKI [RIPE2], [Routinator], [OctoRPKI], [FORT], [Phuntsho]. Analiza postrzeganych barier prawnych dla przyjęcia i wykorzystania usług RPKI w regionie północnoamerykańskim została przeprowadzona w referencjach [Wishnick], [Yoo].



Rysunek 4: Ilustracja alokacji zasobów i łańcucha certyfikatów w RPKI

RPKI opiera się na standardzie X.509 z rozszerzeniami RFC 3779 opisującymi specjalne profile certyfikatów dla zasobów numerów internetowych (prefiksy i numery AS) [RFC5280], [RFC6487], [RFC3779]. Jak pokazano na rys. 4, RIR wydają certyfikaty zasobów (tj. certyfikaty urzędu certyfikacji (CA)) dostawcom usług internetowych i organizacjom z zarejestrowanymi alokacjami i przydziałami zasobów numerów. Istnieją dwa modele certyfikacji zasobów: hostowane i delegowane [ARIN1], [RIPE1]. W modelu hostowanym RIR przechowuje i zarządza kluczami oraz wykonuje operacje RPKI na swoich serwerach. W modelu delegowanym posiadacz zasobu (ISP lub organizacja) otrzymuje certyfikat CA od swojego RIR, hostuje własny CA i wykonuje operacje RPKI (np. podpisuje autoryzacje źródła trasy (zob. dział 4.3), wydaje pochodne certyfikaty zasobów swoim klientom).

Zalecenie dot. bezpieczeństwa 4: Posiadacze zasobów numerów internetowych z prefiksami IPv4/IPv6 i/lub numerami AS (*ang. AS number - AN*) powinni uzyskać dla swoich zasobów certyfikat(y) RPKI.

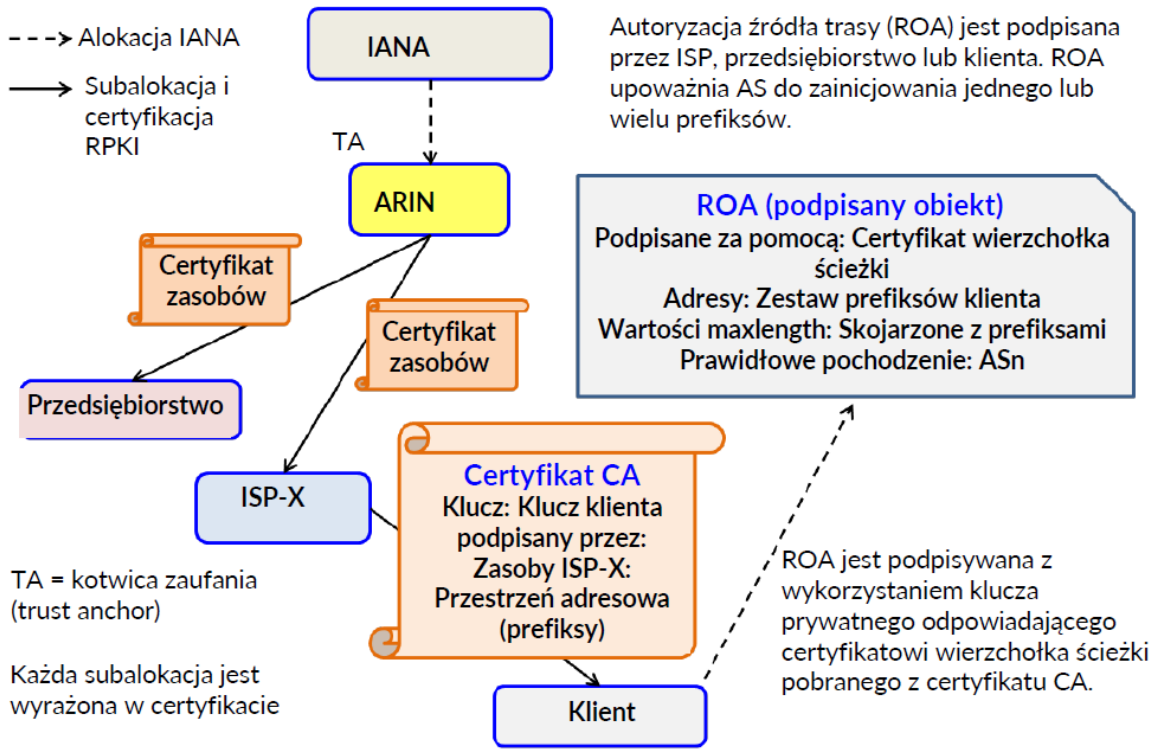
Zalecenie dot. bezpieczeństwa 5: Dostawcy tranzytowi powinni świadczyć usługi, w ramach których tworzą, publikują i zarządzają podrzędnymi certyfikatami zasobów dla przestrzeni adresowej i/lub numerów ASN (*ang. AS number – ASN*) przydzielonych ich klientom[11].

4.3. Sprawdzanie pochodzenia BGP (BGP-OV)

Gdy właściciel prefiksu adresu uzyska certyfikat urzędu certyfikacji (CA), może wygenerować certyfikat wierzchołka ścieżki (*ang. end-entity - EE*) i użyć klucza prywatnego powiązanego z certyfikatem EE do cyfrowego podpisania autoryzacji źródła trasy (ROA) [RFC6482], [RFC6811]. ROA deklaruje określony AS jako autoryzowanego inicjatora ogłoszeń BGP dla prefiksu (zob. rys. 5). Określa jeden lub więcej prefiksów (opcjonalnie maksymalna długość na prefiks (*ang. maxlength per prefix*) i pojedynczy numer AS. Jeśli wartość *maxlength* jest określona dla prefiksu w ROA, to wszelkie bardziej specyficzne (tj. dłuższe) prefiksy (podciągnięte pod ten prefiks)

[11] Obecnie usługi RPKI oparte na modelu hostowanym i oferowane przez RIR występują powszechnie. Zalecenie dot. bezpieczeństwa 5 może być wdrożone w modelu hostowanym lub delegowanym w oparciu o umowy usług z klientami.

o długości nieprzekraczającej maksymalnej długości mogą pochodzić z określonego AS. W przypadku braku określonej wartości *maxlength*, wartość ta jest równa długości samego prefiksu. Jeśli właściciel zasobu ma certyfikat zasobu zawierający wiele prefiksów, może utworzyć jedno ROA, w którym wymienione są niektóre lub wszystkie te prefiksy. Alternatywnie, może utworzyć jedno ROA na prefiks.

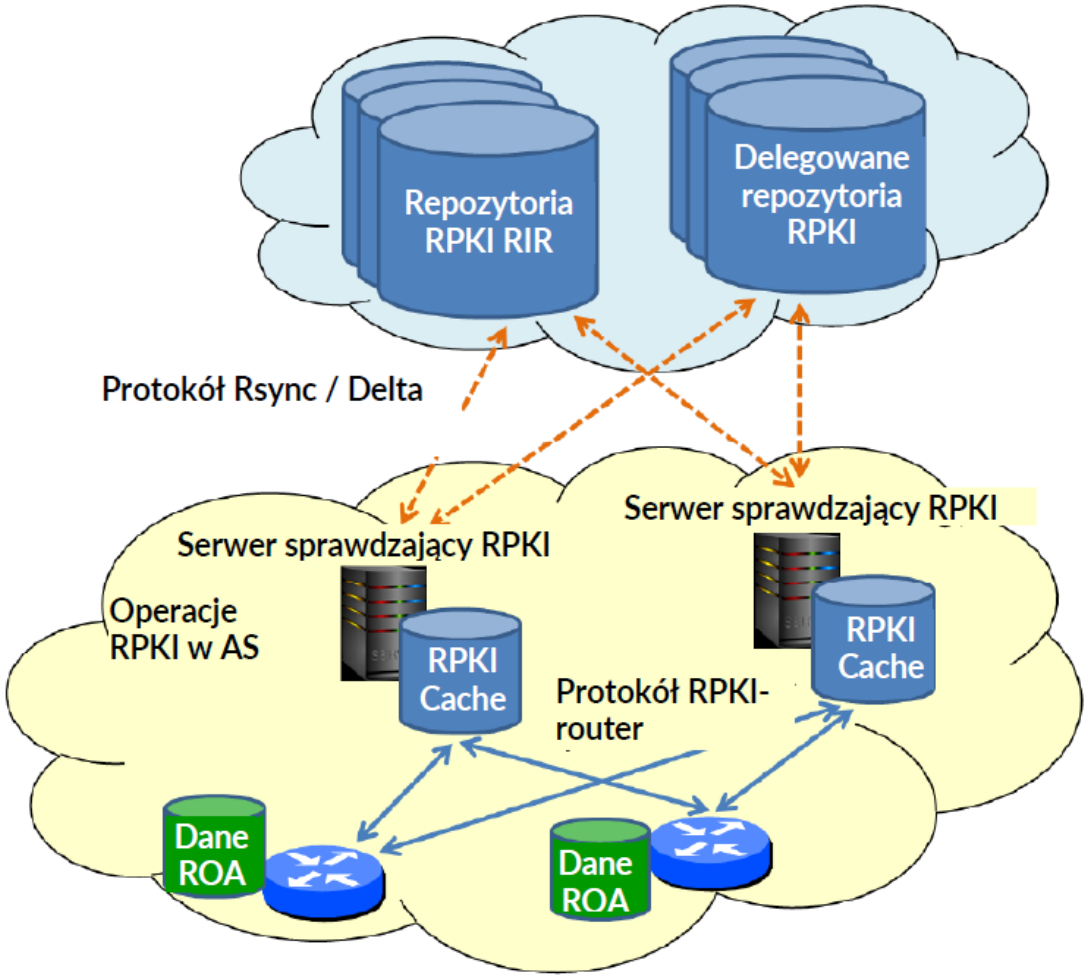


Rysunek 5: Tworzenie autoryzacji źródła trasy (ROA) przez właściciela prefiksu

ROA mogą być również tworzone (podpisywane) przez dostawcę usług internetowych (dostawcę tranzytowego) w imieniu jego klienta na podstawie umowy serwisowej, pod warunkiem, że dostawca usług internetowych przydzielił przestrzeń adresową klientowi. Dostawca usług internetowych może oferować swoim klientom usługę, w ramach której tworzy i obsługuje certyfikaty urzędu certyfikacji dla zasobów klientów oraz ROA dla prefiksów klientów.

Po utworzeniu dane RPKI są używane w Internecie przez strony ufające (RP). RP, takie jak serwery sprawdzające RPKI, mogą uzyskiwać dostęp do danych RPKI z repozytoriów (patrz rys. 6) za pomocą protokołu rsync [Rsync], [Rsync-RPKI] lub

protokołu RPKI Repository Delta Protocol (RRDP) [RFC8182]. Protokół RRDP jest często skrótowo nazywany „protokołem delta". Router BGP zazwyczaj uzyskuje dostęp do wymaganych danych ROA z jednego lub więcej serwerów pamięci podręcznej RPKI, które są obsługiwane przez jego AS. Jak pokazano na rys. 6, protokół RPKI-router (*ang. RPKI-to-router Protocol*) jest używany do komunikacji między serwerem pamięci podręcznej RPKI a routerem [RFC6810], [RFC8210]. Bardziej szczegółowe informacje dotyczące bezpiecznej architektury routingu opartej na RPKI znajdują się w [RFC6480].

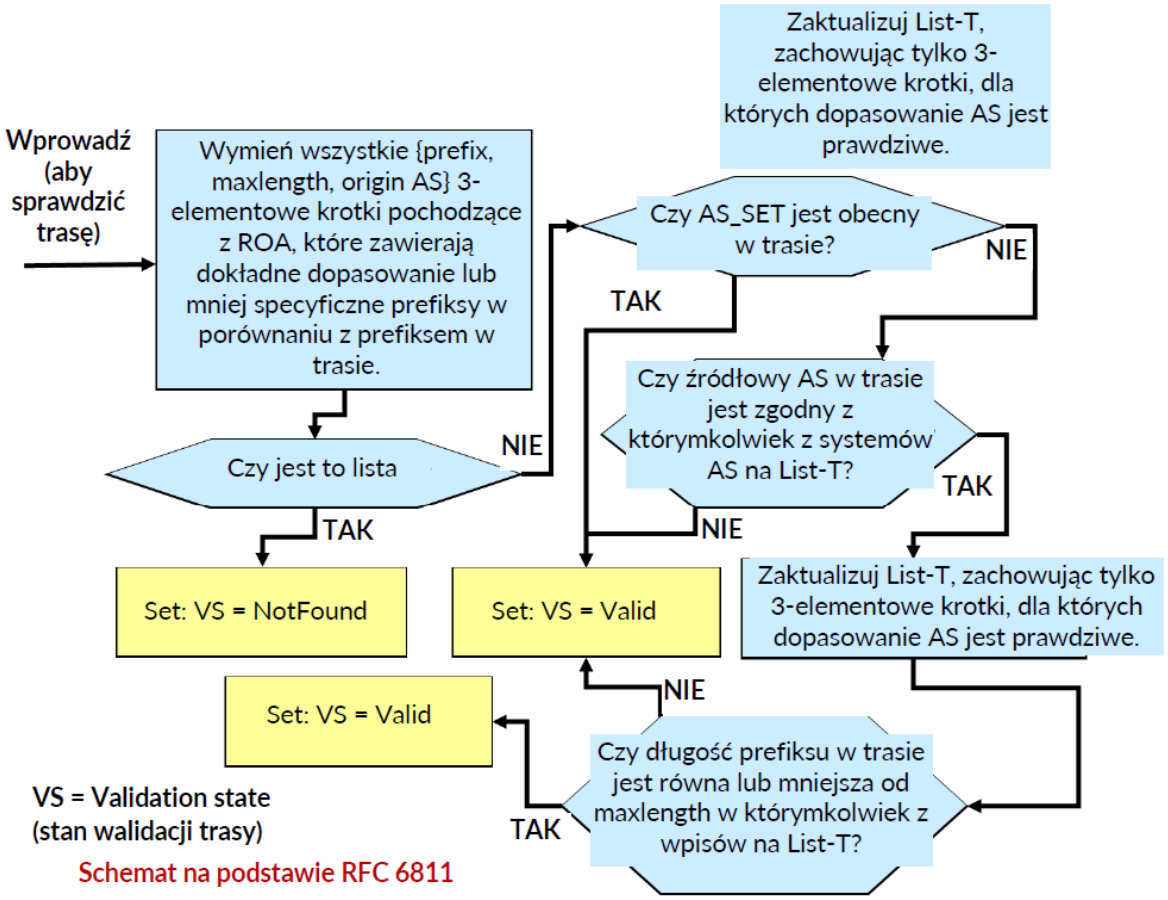


Rysunek 6: Pobieranie, buforowanie i propagacja danych RPKI do routerów

Router BGP może użyć informacji ROA pobranych z serwera pamięci podręcznej RPKI, aby zmniejszyć ryzyko przechwyceń prefiksów i niektórych form wycieków

tras w ogłaszanych trasach. Router BGP zwykle otrzyma sprawdzoną listę krotek[12] {prefix, maxlength, origin AS} (pochodzących z prawidłowych ROA) z jednego lub kilku serwerów pamięci podręcznej RPKI. Lista ta może być określana jako biała lista. Router korzysta z tej listy w procesie sprawdzania pochodzenia BGP (BGP-OV) przedstawionym na rys. 7 w celu określenia stanu walidacji ogłaszanej trasy [RFC6811]. Uznaje się, że trasa BGP ma „prawidłowe" pochodzenie, jeśli para {prefix, origin AS} w ogłaszanej trasie może zostać potwierdzona listą (tj. para jest dozwolona zgodnie z co najmniej jedną ROA; szczegóły na rys. 7). Trasa jest uznawana za nieprawidłową („Invalid"), jeśli występuje niezgodność z listą (tzn. numer systemu autonomicznego nie pasuje lub długość prefiksu przekracza wartość *maxlength*; więcej informacji można znaleźć na rys. 7). Ponadto trasa jest uważana za nieodnalezioną („NotFound"), jeśli ogłoszony prefiks nie jest objęty żadnym prefiksem z białej listy (tzn. nie istnieje ROA, która zawiera prefiks równy lub obejmujący prefiks ogłoszony). Gdy w aktualizacji BGP występuje AS_SET [RFC4271], nie jest możliwe jednoznaczne określenie AS pochodzenia na podstawie AS_PATH [RFC6811]. Dlatego aktualizacja zawierająca AS_SET w swojej AS_PATH nigdy nie może otrzymać oceny „Valid" w procesie sprawdzania pochodzenia (patrz rys. 7). W BCP 172 [RFC6472] nie zaleca się używania AS_SET w aktualizacjach BGP. Sprawdzanie pochodzenia w oparciu o RPKI można uzupełnić sprawdzaniem opartym na danych IRR (zob. dział 4.1).

[12] Krotka (*ang. tuple*) – struktura danych będąca odzwierciedleniem matematycznej „n-ki", tj. uporządkowanego ciągu wartości.



Rysunek 7: Algorytm sprawdzania pochodzenia (na podstawie RFC 6811)

Istnieje kilka implementacji BGP OV opartych na RPKI zarówno na sprzętowych, jak i programowych platformach routerów [Juniper1], [Cisco1], [Patel], [Scudder], [NIST-SRx], [Parsons2], [goBGP], [RTRlib]. Wskazówki dotyczące wdrażania i konfigurowania dla wielu z tych implementacji są dostępne z kilku źródeł, w tym [NCCoE-sidr], [RIPE1], [MANRS]. Choć BGP-OV jest już zaimplementowany w komercyjnych routerach BGP, aktywacja i wszechobecne wykorzystanie RPKI i BGP-OV w routerach BGP wymaga motywacji i zaangażowania ze strony operatorów sieci.

Zalecenie dot. bezpieczeństwa 6: Posiadacze zasobów powinni rejestrować ROA w globalnej RPKI dla wszystkich prefiksów, które są ogłaszane lub mają być ogłaszane w publicznym Internecie.

Zalecenie dot. bezpieczeństwa 7: Każdy dostawca usługi tranzytowej powinien świadczyć usługę, w której tworzy, publikuje i utrzymuje ROA dla prefiksów przydzielonych swoim klientom. Alternatywnie, w ramach usługi, klienci mogą tworzyć, publikować i utrzymywać swoje ROA w repozytorium prowadzonym przez dostawcę tranzytowego[13].

Zalecenie dot. bezpieczeństwa 8: Jeśli prefiks, który jest ogłoszony (lub który ma być ogłoszony) jest typu multi-homed i pochodzi z wielu systemów autonomicznych, wówczas dla tego prefiksu należy zarejestrować jedną ROA na każdy inicjujący system autonomiczny (ewentualnie w połączeniu z innymi prefiksami, które również pochodzą z tego samego systemu autonomicznego).

Zalecenie dot. bezpieczeństwa 9: Gdy dostawca usług internetowych lub organizacja posiada wiele prefiksów, które obejmują prefiksy mniej i bardziej specyficzne, powinien przed utworzeniem ROA dla podciągnięcia prefiksów mniej specyficznych upewnić się, że bardziej specyficzne prefiksy mają ROA.

Zalecenie dot. bezpieczeństwa 10: Dostawca usług internetowych powinien upewnić się, że bardziej specyficzne prefiksy ogłoszone z jego stożka klientów mają ROA przed utworzeniem własnych ROA w celu podciągnięcia mniej specyficznych prefiksów.

AS0 to specjalny numer AS, który nie jest przypisany żadnemu systemowi autonomicznemu. AS0 nie jest również dozwolone na trasach ogłaszanych w BGP. ROA AS0 to ROA zawierająca AS0 dla inicjującego AS [RFC6483], [APNIC1]. Właściciel zasobu adresowego może utworzyć ROA AS0 dla swojego prefiksu, aby zadeklarować zamiar, aby prefiks lub jakikolwiek bardziej specyficzny prefiks podciągnięty pod niego nie był ogłaszany, dopóki nie będzie zwykłej ROA jednocześnie dla tego prefiksu lub bardziej specyficznego prefiksu.

Zalecenie dot. bezpieczeństwa 11: Dostawca usług internetowych lub organizacja powinno stworzyć ROA AS0 dla każdego prefiksu, który obecnie nie jest ogłaszany w publicznym Internecie. Jednak należy to zrobić dopiero po upewnieniu się, że ROA

[13] Zalecenie dot. bezpieczeństwa 7 może być implementowane według modelu hostowanego lub delegowanego na podstawie umów o świadczenie usług z klientami.

istnieją dla wszelkich bardziej specyficznych prefiksów podciągniętych pod ten prefiks, które są rozgłaszane lub mają być ogłaszane.

Zalecenie dot. bezpieczeństwa 12: Router BGP nie powinien wysyłać aktualizacji zawierających AS_SET lub AS_CONFED_SET (zgodnie z BCP 172 [RFC6472]).

Zalecenie dot. bezpieczeństwa 13: Dostawcy usług internetowych i organizacje obsługujące routery BGP powinny również obsługiwać jeden lub więcej pamięci podręcznych sprawdzających RPKI.

Zalecenie dot. bezpieczeństwa 14: Router BGP powinien utrzymywać aktualną białą listę składającą się z {prefix, maxlength, origin ASN}, która pochodzi z ważnych ROA w globalnej RPKI. Router powinien wykonywać BGP-OV.

Co się tyczy Zalecenia dot. bezpieczeństwa 14, BGP-OV jest zaimplementowane przez większość głównych dostawców routerów. Biała lista trójelementowych krotek {prefix, maxlength, origin ASN} jest zazwyczaj uzyskiwana i okresowo odświeżana przez router z lokalnego serwera pamięci podręcznej RPKI. Jak wspomniano wcześniej, do tej komunikacji wykorzystywany jest protokół RPKI-to-router [RFC6810], [RFC8210].

Zalecenie dot. bezpieczeństwa 15: W sytuacji częściowego/stopniowego wdrożenia RPKI, dopuszczalne pary {prefix, origin ASN} do przeprowadzenia BGP-OV powinny być generowane poprzez przyjęcie zestawienia takich danych uzyskanych z ROA, danych IRR oraz umów z klientami.

Zalecenie dot. bezpieczeństwa 16: Wyniki BGP-OV powinny być włączone do lokalnych decyzji dotyczących polityki w zakresie wyboru najlepszych ścieżek BGP.

W odniesieniu do zalecenia dot. bezpieczeństwa 16, dokładnie to, w jaki sposób wyniki BGP-OV są wykorzystywane w wyborze ścieżek, jest ściśle lokalną decyzją dotyczącą zasad dla każdego operatora sieci. Typowe wybory dotyczące zasad obejmują:

- Tag-Only - Wyniki BGP-OV są używane tylko do oznaczania/rejestrowania danych o trasach BGP w celach diagnostycznych.

- Prefer-Valid - Użycie lokalnych ustawień preferencji dla nadania priorytetu ważnym trasom. Należy zauważyć, że jest to tylko preferencja do rozstrzygania sytuacji równoważności (remisów) pomiędzy trasami z dokładnie tym samym prefiksem.
- Drop-Invalid - zastosowanie lokalnej polityki do ignorowania nieważnych tras w procesie decyzyjnym BGP.

Należy starannie zaplanować i przemyśleć stosowanie takiej polityki. Ogólnie rzecz biorąc, ważne jest, aby lokalna polityka BGP-OV była spójna w całym AS, zarówno pod względem tego, na jakich sesjach równorzędnych BGP-OV jest włączona, jak i sposobu wykorzystania wyników do wpływania na proces decydowania BGP. Zaleca się, aby operatorzy sieci kontynuowali proces stopniowego wdrażania, polegający na przyjmowaniu coraz bardziej rygorystycznych polityk po zdobyciu doświadczenia i zaufania do systemu. Trzy powyższe przykładowe polityki można postrzegać jako zalecane etapy planu stopniowego wdrożenia.

Organizacje powinny wymagać od swoich dostawców usług hostowanych - np. hostowanych systemów chmurowych, sieci dostarczania zawartości (*ang. content delivery network – CDN*), e-mail, DNS - przestrzegania zaleceń bezpieczeństwa określonych w niniejszym rozdziale, dotyczących certyfikacji zasobów i tworzenia ROA dla prefiksów używanych do świadczenia usług hostowanych i należących do dostawców. Organizacja może to zrobić samodzielnie, jeżeli dostawca usług hostowanych wykorzystuje własną przestrzeń adresową organizacji dla usług hostowanych.

4.3.1. Przechwycenia ze sfałszowanym pochodzeniem — jak je zminimalizować

Nawet dzięki tylko sprawdzaniu pochodzenia opartemu na ROA można zapobiec przypadkowemu błędnemu przypisaniu pochodzenia. Jednak umyślnie złośliwy przechwytujący może sfałszować pochodzenie AS w dowolnej aktualizacji, dostawiając numer AS znaleziony w ROA dla docelowego prefiksu do własnego nieautoryzowanego ogłoszenia BGP. Aby uzyskać większy efekt, w połączeniu z fałszowaniem pochodzenia, atakujący może zastąpić prefiks w trasie bardziej specyficznym prefiksem (podciągniętym pod ogłoszony prefiks), którego długość nie przekracza maksymalnej długości (maxlength) w ROA.

Poniższe zalecenia dotyczące bezpieczeństwa są przydatne do minimalizowania ataków ze sfałszowanym źródłem[14].

Zalecenie dot. bezpieczeństwa 17: Zapewnia pewien stopień odporności na ataki ze sfałszowanym pochodzeniem. Wartość maxlength w ROA nie powinna przekraczać długości najbardziej specyficznego prefiksu (objętego rozważanym prefiksem), który jest zainicjowany lub ma być zainicjowany z AS wymienionego w ROA.

Zalecenie dot. bezpieczeństwa 18: Zapewnia jeszcze większy stopień odporności na ataki ze sfałszowanym pochodzeniem. Jeśli prefiks i określone przez niego bardziej specyficzne prefiksy są ogłaszane lub mają być ogłaszane, to zamiast określać maxlength, prefiks i określone przez niego bardziej specyficzne prefiksy powinny być wyraźnie wymienione w wielu ROA (tj. jedna ROA na prefiks lub określony przez niego bardziej specyficzny prefiks)[15].

4.4. Kategorie filtrów prefiksów

Filtrowanie prefiksów BGP (znane również jako filtrowanie tras) jest najbardziej podstawowym mechanizmem ochrony routerów BGP przed przypadkowym lub złośliwym zakłóceniem [RFC7454]. Filtrowanie prefiksów różni się od BGP-OV tym, że akceptowane są tylko prefiksy oczekiwane w relacji równorzędnej (np. klient), a nieoczekiwane — w tym bogony[16] i nieprzydzielone — są odrzucane. Ponadto weryfikacja pochodzenia nie wchodzi w skład tradycyjnego filtrowania prefiksów, ale jest uzupełnieniem. Należy zaimplementować możliwości filtrowania zarówno prefiksów przychodzących (*ang. inbound prefix filtering*), jak i wychodzących (*ang. outbound prefix filtering*). Filtry tras są zazwyczaj definiowane przy użyciu składni podobnej do składni stosowanej w przypadku list kontroli dostępu. Jedną z opcji jest wyświetlenie zakresów prefiksów IP, które mają być odrzucane, a następnie

[14] Sprawdzanie ścieżki BGP (tzn. BGPsec [RFC8205]) opisane w dziale 4.7 jest wymagane do pełnej ochrony przed modyfikacją prefiksu i/lub ścieżki.

[15] Ogólnie rzecz biorąc, należy unikać stosowania maxlength, chyba że wszystkie lub prawie wszystkie bardziej specyficzne prefiksy wartości maxlength są ogłaszane lub mają być ogłaszane [maxlength].

[16] Bogon – nieformalna nazwa pakietu o takim adresie źródłowym, który nie powinien istnieć w danej sieci. Przestrzeń adresowa, z której nie powinien przychodzić żaden ruch nazywamy adresową przestrzenią bogonową.

dopuszczenie wszystkich pozostałych. Alternatywnie można określić zakresy dozwolonych prefiksów, a pozostałe można odrzucić. Wybór podejścia zależy od praktycznych uwarunkowań określonych przez administratorów systemu. Zazwyczaj elementy równorzędne BGP powinny mieć zgodne filtry prefiksów (tzn. filtry prefiksów wychodzących systemu autonomicznego powinny być dopasowane do filtrów prefiksów elementów równorzędnych, z którymi komunikuje się ten system). Na przykład, jeśli AS 64496 filtruje swoje wychodzące prefiksy w kierunku elementu równorzędnego AS 64500, zezwalając tylko tym ze zbioru *P*, wówczas AS 64500 ustanawia przychodzące filtry prefiksowe w celu zapewnienia, by prefiksy, które akceptuje z AS 64496 były tylko tymi ze zbioru *P*.

W dalszej części działu 4.4, opisano różne rodzaje filtrów prefiksowych, a ich zastosowanie przedstawiono w kontekście różnych relacji równorzędnych w dziale 4.5.

4.4.1. Nieprzydzielone prefiksy

Internet Assigned Numbers Authority (IANA) przydziela przestrzeń adresową rejestrom RIR. Cała przestrzeń adresowa IPv4 (lub prefiksy), z wyjątkiem niektórych zarezerwowanych do przyszłego użytku, została przydzielona przez IANA [IANA-v4-r]. RIR również prawie całkowicie przydzieliły swoją przestrzeń adresową IPv4 [IANA-v4-r][17]. Przestrzeń adresowa IPv6 jest znacznie większa niż IPv4 i, co zrozumiałe, spora jej część jest nieprzydzielona. Dlatego dobrą praktyką jest akceptowanie tylko tych rozgłoszeń prefiksów IPv6, które zostały przydzielone przez IANA [IANA-v6-r]. Operatorzy sieci powinni zapewnić regularną aktualizację filtrów prefiksów IPv6 (zwykle w ciągu kilku tygodni po każdej zmianie w alokacji prefiksów IPv6). W przypadku braku takich regularnych procesów aktualizacyjnych lepiej nie konfigurować filtrów w oparciu o przydzielone prefiksy. Team Cymru[18] udostępnia usługę aktualizacji list prefiksów bogon dla IPv4 i IPv6 [Cymru-bogon].

[17] Niektóre z prefiksów są przeznaczone do celów specjalnych, co opisano w dziale 4.4.2.

[18] Od 2005 r. misją Team Cymru jest ratowanie i poprawa jakości życia poprzez współpracę z zespołami bezpieczeństwa na całym świecie, umożliwiając im śledzenie i eliminowanie najbardziej zaawansowanych szkodliwych podmiotów i złośliwych infrastruktur.

Zalecenie dot. bezpieczeństwa 19: Trasy IPv6 powinny być filtrowane tak, aby dopuszczały tylko przydzielone prefiksy IPv6. Operatorzy sieci powinni regularnie aktualizować filtry prefiksów IPv6, aby uwzględnić wszelkie nowo przydzielone prefiksy.

Jeśli właściciele zasobów prefiksowych regularnie rejestrują ROA AS0 (patrz dział 4.3) dla przydzielonych (ale prawdopodobnie obecnie nieużywanych) prefiksów, wówczas te ROA mogłyby być uzupełniającym źródłem aktualizacji filtrów prefiksowych.

4.4.2. Prefiksy specjalnego przeznaczenia

IANA utrzymuje rejestry dla adresów specjalnego przeznaczenia IPv4 i IPv6 [IANA-v4-sp], [IANA-v6-sp]. Rejestry te zawierają również specyfikację zakresu routingu prefiksów specjalnego przeznaczenia.

Zalecenie dot. bezpieczeństwa 20: Prefiksy, które są oznaczone jako „False" w kolumnie „Global" [IANA-v4-sp], [IANA-v6-sp] są zabronione do routingu w globalnym Internecie i powinny być odrzucone, jeśli zostaną odebrane od zewnętrznego elementu równorzędnego BGP (eBGP).

4.4.3. Prefiksy posiadane przez AS

AS może inicjować jeden lub wiele prefiksów. W kierunku przychodzącym AS powinien (w większości przypadków) odrzucać trasy dla prefiksów (podsieci), które inicjuje, jeśli zostały otrzymane od któregokolwiek z jego elementów równorzędnych eBGP (*ang. eBGR peers*) - dostawcy tranzytowego, klienta lub elementu lateral peer. Ogólnie rzecz biorąc, ruch danych przeznaczony dla tych prefiksów powinien pozostać lokalny i nie powinien przeciekać do zewnętrznej komunikacji równorzędnej (*ang. external peering*). Jeśli jednak operator AS nie ma pewności czy prefiks, który inicjuje jest single-homed czy multi-homed, powinien zaakceptować ogłoszenie prefiksu od elementu równorzędnego eBGP (i przypisać niższą wartość preferencji lokalnej), aby zachować pożądaną nadmiarowość.

Zalecenie dot. bezpieczeństwa 21: W przypadku prefiksów single-homed (podsieci), które są własnością systemu AS i są przez niego zainicjowane, wszelkie trasy dla tych prefiksów otrzymanych w tym AS od elementów równorzędnych eBGP powinny zostać odrzucone.

4.4.4. Prefiksy wykraczające poza limit specyficzności

Zazwyczaj dostawcy usług internetowych nie ogłaszają ani nie akceptują tras dla prefiksów, które są bardziej specyficzne niż określony poziom specyficzności. Na przykład maksymalne dopuszczalne długości prefiksów są wymienione w istniejących praktykach jako /24 dla IPv4 [RIP-399] i /48 dla IPv6 [RIPE-532]. Poziom specyficzności, który jest akceptowalny, jest określany przez każdego operatora AS i komunikowany z elementami równorzędnymi. W przypadkach, gdy Flowspec (zob. dział 5.5) [RFC5575], [RFC5575bis], [Ryburn] jest stosowany między sąsiadującymi ze sobą systemami autonomicznymi do ograniczania DDoS, oba systemy autonomiczne mogą się wzajemnie zgodzić na akceptowanie dłuższych długości prefiksów (np. /32 dla IPv4), ale tylko dla niektórych uprzednio uzgodnionych prefiksów. Oznacza to, że ogłoszony bardziej specyficzny prefiks musi być zawarty w uprzednio uzgodnionym prefiksie.

Zalecenie dot. bezpieczeństwa 22: Zaleca się, aby router eBGP określał limit specyficzności dla każdego elementu równorzędnego eBGP i odrzucał prefiksy, które przekraczają limit specyficzności dla każdego elementu równorzędnego[19].

Niektórzy operatorzy mogą wybrać odrzucanie ogłoszeń prefiksów, które są mniej specyficzne niż /8 i /11 odpowiednio dla IPv4 i IPv6.

4.4.5. Trasa domyślna

Trasa dla prefiksu 0.0.0.0/0 jest znana jako trasa domyślna w IPv4, a trasa dla ::/0 jest znana jako trasa domyślna w IPv6. Trasa domyślna jest ogłaszana lub akceptowana tylko w określonych relacjach równorzędnych klient-dostawca. Na przykład dostawca tranzytowy i klient, który jest siecią typu stub lub leaf, mogą zawrzeć między sobą

[19] Limit specyficzności może być taki sam dla wszystkich elementów równorzędnych (np. /24 dla IPv4 i /48 dla IPv6).

umowę, zgodnie z którą klient akceptuje domyślną trasę od dostawcy zamiast pełnej tabeli routingu. Ogólnie rzecz biorąc, zaleca się filtrowanie trasy domyślnej, z wyjątkiem sytuacji, gdy istnieje specjalna umowa komunikacji równorzędnej.

Zalecenie dot. bezpieczeństwa 23: Trasa domyślna (0.0.0.0/0 w IPv4 i ::/0 w IPv6) powinna zostać odrzucona, chyba że istnieje specjalna umowa komunikacji równorzędnej, która zezwala na jej zaakceptowanie.

4.4.6. Prefiksy IXP LAN

Zazwyczaj istnieje potrzeba, aby klienci w punkcie wymiany ruchu internetowego (IXP) posiadali wiedzę na temat prefiksu IP używanego dla IXP LAN, co ułatwia komunikację równorzędną pomiędzy klientami.

Zalecenie dot. bezpieczeństwa 24: Punkt wymiany ruchu internetowego (*ang. internet exchange point - IXP*) powinien ogłaszać — ze swojego serwera tras do wszystkich swoich systemów autonomicznych — swój prefiks sieci LAN lub cały prefiks, który byłby taki sam lub mniej specyficzny niż prefiks sieci LAN. Każdy AS należący do IXP powinien z kolei akceptować ten prefiks i odrzucać wszelkie bardziej specyficzne prefiksy (od prefiksu ogłoszonego przez IXP) od któregokolwiek ze swoich elementów równorzędnych eBGP.

Wdrożenie Zalecenia dot. bezpieczeństwa nr 24 zapewni osiągalność prefiksu IXP LAN dla każdego z członków IXP. Zapewni również, że wykrycie rozmiaru maksymalnego rozmiaru jednostki transmisji ścieżki (*ang. Path Maximum Transmission Unit Discovery - PMTUD*)[20] będzie działać między członkami nawet w obecności unicast Reverse Path Forwarding (uRPF). Dzieje się tak dlatego, że komunikaty „packet too big” Internet Control Message Protocol (ICMP) wysyłane przez routery członków IXP mogą być pozyskiwane przy użyciu adresu IP z prefiksu IXP LAN. Więcej szczegółów na ten temat można znaleźć w dokumencie [RFC7454].

[20] Path MTU Discovery (PMTUD) to znormalizowana technika w sieciach komputerowych służąca do określania maksymalnego rozmiaru jednostki transmisji (MTU) na ścieżce sieciowej między dwoma hostami protokołu internetowego (IP), zwykle w celu uniknięcia fragmentacji IP.

4.5. Filtrowanie prefiksów dla różnych typów elementów równorzędnych

Zalecenia dotyczące filtrowania prefiksów przychodzących i wychodzących różnią się w zależności od typu relacji komunikacji równorzędnej (peeringu) istniejącej między sieciami: element równorzędny boczny, dostawca tranzytowy, klient lub klient typu leaf (zobacz definicje w dziale 2.3). Różne mające zastosowanie typy filtrów pochodzą z listy opisanej w działach od 4.4.1 do 4.4.6.

Poniższe zalecenia dotyczące bezpieczeństwa mają zastosowanie do organizacji, które mają komunikację równorzędną eBGP (eBGP peering) z sąsiednimi systemami autonomicznymi. Gdy organizacja nabywa usługi tranzytowe od dostawcy usług internetowych lub usługi hostowane (np. hostowane instancje w chmurze, CDN, DNS, poczta e-mail) od dostawców usług hostowanych, zalecenia dotyczące bezpieczeństwa powinny być zawarte w odpowiednich umowach o świadczenie usług.

4.5.1. Filtrowanie prefiksu z lateral peer

Zalecenie dot. bezpieczeństwa 25: Filtrowanie prefiksów przychodzących w połączeniach lateral peer — w kierunku przychodzącym należy zastosować następujące filtry prefiksów:

- nieprzydzielone prefiksy,
- prefiksy specjalnego przeznaczenia,
- prefiksy inicjowane przez AS,
- prefiksy wykraczające poza limit specyficzności,
- trasa domyślna,
- prefiksy IXP LAN.

Zalecenie dot. bezpieczeństwa 26: Filtrowanie prefiksów wychodzących w połączeniach lateral peer —odpowiednie prefiksy wychodzące to te, które zostały zainicjowane przez dany AS, oraz te, które zostały zainicjowane przez podrzędne (*ang. downstream*) systemy AS (tj. systemy autonomiczne w jego stożku klientów – customer cone). Następujące filtry prefiksów powinny być stosowane w kierunku wychodzącym:

- nieprzydzielone prefiksy[21],
- prefiksy specjalnego przeznaczenia,
- prefiksy wykraczające poza limit specyficzności,
- trasa domyślna,
- prefiksy IXP LAN,
- prefiksy uzyskane od innych elementów równorzędnych bocznych systemu autonomicznego (zob. Zalecenia dot. bezpieczeństwa w Dziale 4.9),
- prefiksy uzyskane od dostawców tranzytowych systemu autonomicznego (zob. Zalecenia dot. bezpieczeństwa w Dziale 4.9).

4.5.2. Filtrowanie prefiksu z dostawcą tranzytowym

Zalecenie dot. bezpieczeństwa 27: **Filtrowanie prefiksów przychodzących od strony dostawcy tranzytowego** - Przypadek 1 (pełna tablica routingu): Ogólnie rzecz biorąc, gdy od dostawcy tranzytowego wymagana jest pełna tablica routingu, na kierunku wejściowym należy zastosować następujące filtry prefiksowe[22]:

- nieprzydzielone prefiksy,
- prefiksy specjalnego przeznaczenia,
- prefiksy inicjowane przez AS,
- prefiksy wykraczające poza limit specyficzności,
- prefiksy IXP LAN.

[21] Nieprzydzielone prefiksy mogą zostać pominięte, jeśli istnieje pewność, że filtry prefiksów przychodzących nie wpuszczą ich.

[22] Lista nie zawiera trasy domyślnej. W niektórych przypadkach sieć klienta chce otrzymywać od dostawcy tranzytowego trasę domyślną obok pełnej tablicy routingu.

Zalecenie dot. bezpieczeństwa 28: **Filtrowanie prefiksów przychodzących od strony dostawcy tranzytowego** - Przypadek 2 (trasa domyślna): Jeśli router graniczny jest skonfigurowany tylko dla trasy domyślnej, wówczas od dostawcy tranzytu powinna być akceptowana wyłącznie ta trasa domyślna.

Zalecenie dot. bezpieczeństwa 29: **Filtrowanie prefiksów wychodzących do dostawcy tranzytowego**: Należy zastosować te same filtry prefiksów wychodzących, co w przypadku bocznego elementu równorzędnego (patrz dział 4.5.1), z tym, że ostatnie dwa punktory modyfikuje się w następujący sposób[23]:

- prefiksy uzyskane od równorzędnego systemu autonomicznego AS lateral (zob. zalecenia dot. bezpieczeństwa w dziale 4.9),
- prefiksy uzyskane od innych dostawców tranzytowych systemu autonomicznego AS (zob. Zalecenia dot. bezpieczeństwa w dziale 4.9).

4.5.3. Filtrowanie prefiksów z klientem

Filtrowanie prefiksów przychodzących: Istnieją dwa scenariusze do rozważenia. **Scenariusz 1** to pełna widoczność klienta i jego stożka klientów (jeśli istnieje) oraz znajomość prefiksów zainicjowanych od takiego klienta i jego stożka. Znajomość prefiksów może opierać się na bezpośredniej wiedzy klienta, danych IRR i/lub danych RPKI (jeśli wiadomo, że dane te są kompletne i dobrze utrzymane w przypadku tego klienta i jego stożka klientów). Takie znane prefiksy dotyczące klienta i jego stożka klientów są wymienione w konfiguracji danego routera eBGP.

Zalecenie dot. bezpieczeństwa 30: Filtrowanie prefiksów przychodzących od klienta w Scenariuszu 1 — należy akceptować tylko prefiksy, o których wiadomo, że pochodzą od klienta i jego stożka klientów, a wszystkie inne ogłoszenia dotyczące tras należy odrzucić.

[23] W związku z Zaleceniem dot. bezpieczeństwa 29, niektóre zasady można też zastosować, jeśli nie zamówiono (lub wybrano) dostawcy tranzytowego do świadczenia tranzytu dla pewnego podzbioru prefiksów wychodzących.

Scenariusz 2 występuje, gdy brak jest wiarygodnej wiedzy o wszystkich prefiksach pochodzących od klienta i jego stożka klientów.

Zalecenie dot. bezpieczeństwa 31: Filtrowanie prefiksów przychodzących od klienta w Scenariuszu 2 — należy zastosować ten sam zestaw filtrów prefiksów przychodzących jak dla lateral peer (patrz dział 4.5.1).

Zalecenie dot. bezpieczeństwa 32: Filtrowanie prefiksów wychodzących do klienta — filtry stosowane w tym przypadku będą się różnić w zależności od tego, czy klient chce otrzymać tylko trasę domyślną, czy też pełną tablicę routingu. Jeśli to pierwsze, to należy ogłosić tylko trasę domyślną i nic więcej. W tym drugim przypadku należy zastosować następujące filtry prefiksów wychodzących[24]:

- prefiksy specjalnego przeznaczenia,
- prefiksy wykraczające poza limit specyficzności.

4.5.4. Filtrowanie prefiksów prowadzone w sieci klienta typu leaf

Sieć klienta typu leaf to sieć o charakterze single-homed połączona z dostawcą tranzytowym i nie posiadająca downstreamu do lateral peerów lub systemów AS klienta.

Zalecenie dot. bezpieczeństwa 33: Filtrowanie prefiksów typu leaf przychodzących do klienta od dostawcy tranzytowego- Klient leaf może zażądać tylko domyślnej trasy od swojego dostawcy tranzytowego. W tym przypadku, powinna być zaakceptowana tylko domyślna trasa i nic więcej. Jeśli klient typu leaf wymaga pełnej tablicy routingu od dostawcy tranzytowego, wtedy powinien zastosować następujące filtry prefiksów przychodzących:

- nieprzydzielone prefiksy,
- prefiksy specjalnego przeznaczenia,
- prefiksy inicjowane przez AS (tzn. klienta typu leaf),
- prefiksy wykraczające poza limit specyficzności,
- trasa domyślna.

[24] Filtr trasy domyślnej może zostać dodany, jeżeli klient żąda pełnej tablicy routingu, ale bez trasy domyślnej.

Zalecenie dot. bezpieczeństwa 34: Filtrowanie prefiksów typu leaf przychodzących od klienta do dostawcy tranzytowego- Sieć klienta typu leaf powinna stosować bardzo prostą politykę ruchu wychodzącego polegającą na ogłaszaniu tylko prefiksów przez nią inicjowanych. Jednak może dodatkowo zastosować te same filtry prefiksów wychodzących, jak dla lateral peer (patrz dział 4.5.1), aby zachować dodatkową ostrożność.

4.6. Rola RPKI w filtrowaniu prefiksów

Dostawca usług internetowych (ISP) może pobrać (z rejestrów RPKI) wszystkie dostępne autoryzacje źródła trasy (ROA) odpowiadające systemom autonomicznym (AS), o których wiadomo, że należą do jego stożka klientów (patrz definicja w dziale 2.3)[25]. Na podstawie dostępnych ROA można określić prefiksy, które mogą być inicjowane z systemów autonomicznych w stożku klientów. W miarę jak rejestry RPKI będą zyskiwały dojrzałość wraz z rosnącym stopniem przyjęcia, listy prefiksów uzyskane z ROA staną się przydatne do filtrowania prefiksów. Nawet na wczesnych etapach przyjęcia RPKI, listy prefiksów (z ROA) mogą pomóc w sprawdzeniu krzyżowym i/lub uzupełnieniu list filtrów prefiksów, które dostawca usług internetowych tworzy w inny sposób.

Zalecenie dot. bezpieczeństwa 35: Dane ROA (dostępne z rejestrów RPKI) powinny być wykorzystywane do konstruowania i/lub rozszerzania list filtrów prefiksowych dla interfejsów klienta[26,27].

[25] Listę systemów autonomicznych w stożku klientów danego systemu autonomicznego można ustalić przez utworzenie listy systemów autonomicznych o unikalnym pochodzeniu we wszystkich otrzymanych ogłoszeniach BGP (tzn. obecnie w Adj-RIB-ins [RFC4271]) na wszystkich interfejsach klienta w rozważanym AS (zob. etap 3 w dziale 3.4 w [EFP-uRPF]). Można tego dokonać w systemie zarządzania siecią (poza routerem).

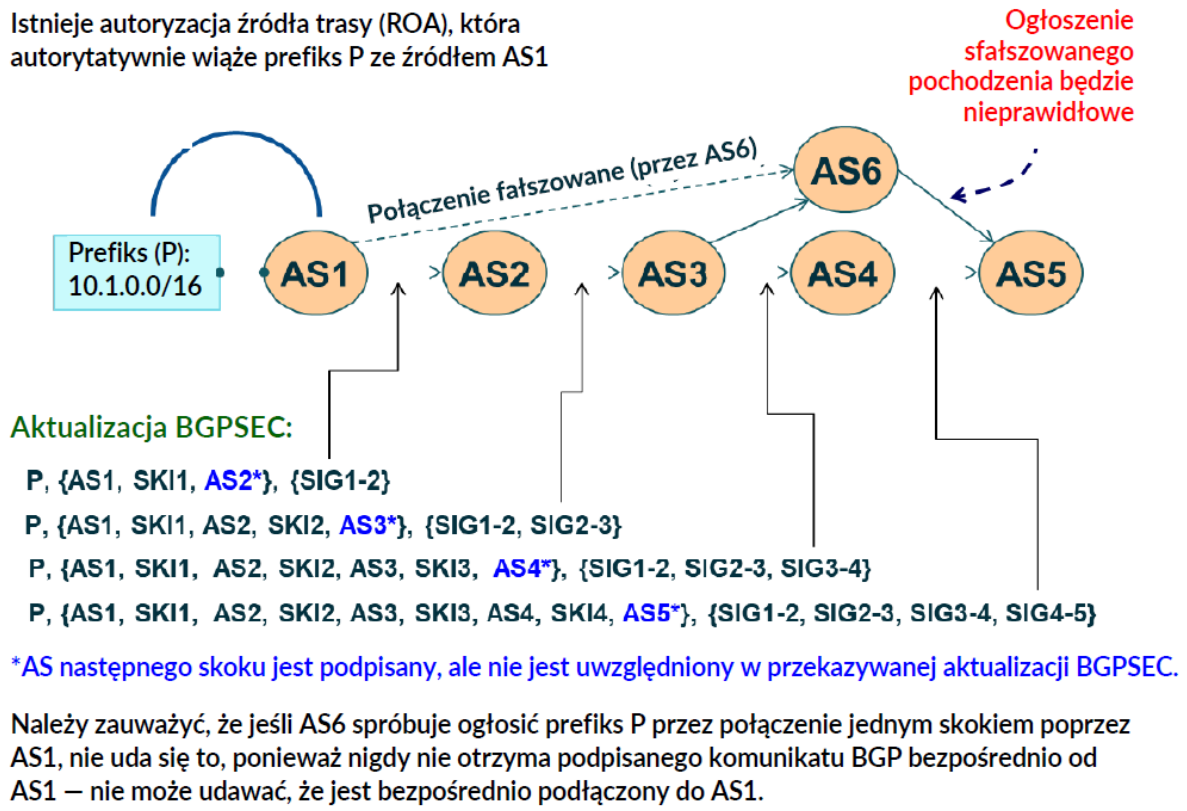
[26] Zalecenie dot. bezpieczeństwa nr 35 jest być może lepiej przystające do mniejszych ISP które mają lepszą widoczność swojego stożka klientów. Większe ISP zwykle nie dysponują taką widocznością.

[27] Ogólnie nie jest wykonalne zastosowanie tego na interfejsach elementów równorzędnych (*ang. peer interfaces*) ponieważ dokładna znajomość stożka klientów elementu równorzędnego (*ang. peer's customer cone*) nie jest możliwa. Oczywiście BGP OV (patrz dział 4.3) w celu wykrywania nieprawidłowych ogłoszeń jest stosowane na wszystkich interfejsach.

4.7. Sprawdzanie ścieżki AS (tworzona/w przyszłości)

Standard IETF dla walidacji ścieżki BGP (BGP-PV), mianowicie BGPsec [RFC8205], jest dostępny, ale komercyjne implementacje dostawców na chwilę opracowywania tej publikacji nie są obecnie oferowane. Dlatego też w niniejszym dziale krótko opisano technologię i standardy, ale nie przedstawiono żadnych zaleceń dotyczących bezpieczeństwa BGP-PV.

Jak zauważono w działach 4.3 i 4.3.1, sprawdzanie pochodzenia BGP (BGP-OV) jest konieczne, ale samo w sobie nie wystarcza do pełnego zabezpieczenia prefiksu i ścieżki AS w ogłoszeniach BGP. Sprawdzanie ścieżki BGP (BGP-PV) jest dodatkowo wymagane do ochrony przed modyfikacjami prefiksów i atakami w oparciu o sfałszowane pochodzenie (patrz dział 4.3.1), jak również innymi atakami na ścieżkę AS, takimi jak skracanie ścieżki i ataki Kapeli-Pilosova (patrz dział 2.2). W środowisku specjalistów sieciowych istnieje duże zainteresowanie zabezpieczeniem ścieżki AS w aktualizacjach BGP, tak aby można było zapewnić bardziej kompleksową ochronę aktualizacji BGP [RFC8205], [RFC8608], [RFC7353], [Huston2011], [RFC8374]. RFC 8205 jest standardem IETF, który określa protokół BGPsec (tj. protokół do sprawdzania poprawności ścieżki BGP). Dostępne są prototypowe implementacje open-source BGP-PV [NIST-SRx], [Parsons2], [Adalier2].



Rysunek 8: Podstawowa zasada podpisywania/sprawdzania ścieżek AS w aktualizacjach BGP

Podstawowe zasady protokołu BGP-PV przedstawiono na rys. 8[28]. ROA podpisana przez właściciela prefiksu 10.1.0.0/16 potwierdza, że AS1 jest autoryzowany do zainicjowania prefiksu. Ponadto każdy operator sieci, który wdrożył BGP-PV, otrzymuje certyfikat zasobu dla swojego numeru systemu autonomicznego, a routery BGP-PV w systemie autonomicznym otrzymują certyfikaty routera i klucze prywatne do podpisywania aktualizacji. Certyfikaty wszystkich routerów BGP-PV są pobierane przez wszystkie uczestniczące systemy autonomiczne, a klucze publiczne wszystkich routerów BGP-PV powinny być dostępne na każdym routerze BGP-PV. Na rys. 8, system AS1 używa klucza prywatnego do wygenerowania swojego podpisu, SIG1-2, potwierdzającego wysłanie trasy dla 10.1.0.0/16 do systemu AS2. Docelowy system autonomiczny jest uwzględniony w danych, które będą podpisane. Podobnie AS2 podpisuje trasę do AS3 i tak dalej. Każdy system autonomiczny dodaje swój podpis

[28] Zob. szczegółową specyfikację protokołu w [RFC8205].

podczas propagowania aktualizacji do swoich sąsiadów. Aktualizacja zawiera identyfikator klucza (*ang. subject key identifier - SKI*) dla klucza publicznego każdego systemu autonomicznego w ścieżce (tj. klucz publiczny routera BGP-PV w systemie autonomicznym). AS5 otrzymuje aktualizację z czterema podpisami (po jednym na każdy skok). Jeśli wszystkie podpisy poprawnie weryfikują AS5, a sprawdzanie poprawności pochodzenia również jest pomyślne, wówczas AS5 może mieć pewność, że odebrana aktualizacja dla 10.1.0.0/16 ze ścieżką systemu autonomicznego [AS1 (origin), AS2, AS3, AS4] jest prawidłowa (tj. nie jest uszkodzona przez modyfikację prefiksu lub ścieżki po drodze). Przykładowo, na rys. 8, AS6 nie uda się, gdyby próbował, sfałszować połączenie z AS1 i ogłosić do AS5 podpisaną aktualizację BGPsec (z krótszą ścieżką i sfałszowanym pochodzeniem AS1). Wynika to z faktu, że AS6 nie ma aktualizacji podpisanej bezpośrednio z AS1.

Algorytm ECDSA-P256 jest obecnie zalecany do podpisywania aktualizacji BGPsec między systemami autonomicznymi, które wzajemnie się ze sobą komunikują równorzędnie [RFC8608]. Aktualizacje będą miały większy rozmiar ze względu na dodanie 64-bajtowego podpisu ECDSA P-256 dla każdego skoku. Ponadto procesory tras w routerach BGP-PV będą musiały wykonać dodatkowe przetwarzanie z powodu podpisywania i weryfikacji podpisów ścieżek. W [Sriram1] podano charakterystykę wydajności BGP-PV w zakresie kwantyfikacji rozmiaru bazy informacji o routingu (*ang. routing information base - RIB*) oraz czas konwergencji routingu. Dostępne są wysokowydajne implementacje operacji kryptograficznych (podpisywanie i weryfikacje ECC) skojarzonych z przetwarzaniem aktualizacji BGPsec [Adalier1], [Adalier2], [NIST-SRx]. Algorytmy optymalizacji dla przetwarzania aktualizacji BGPsec zostały zaproponowane i przeanalizowane w [Sriram2].

Aby zmniejszyć koszty aktualizacji i zachęcić do szybszego wdrażania, system autonomiczny typu leaf lub stub może zaufać nadrzędnemu systemowi autonomicznemu i negocjować odbieranie niepodpisanych aktualizacji podczas wysyłania podpisanych aktualizacji do nadrzędnego (*ang. upstream*) systemu autonomicznego [RFC8205].

Standardy BGP-PV są udokumentowane w publikacjach IETF RFC: 8205, 8206, 8207, 8209, 8210, i 8608. Gdy implementacje oparte na tych standardach staną się

dostępne w produktach komercyjnych, ten dokument może zostać zaktualizowany w celu rekomendacji BGP-PV.

4.8. Sprawdzanie ścieżki AS pod kątem niedopuszczonych numerów AS

Ścieżka AS w aktualizacji otrzymanej w eBGP jest sprawdzana, aby upewnić się, że nie ma pętli AS [RFC4271]. Odbywa się to poprzez sprawdzenie czy numer AS systemu lokalnego nie pojawia się w odebranej ścieżce AS. Ścieżka AS jest również sprawdzana, aby upewnić się, że numery AS przeznaczone do celów specjalnych [IANA-ASN-sp] nie są obecne. Należy zauważyć, że specjalny numer ASN 23456 jest przydzielony dla AS_TRANS [RFC6793] i może być obecny w AS_PATH w połączeniu z AS4_PATH [RFC 6793] w aktualizacji.

Zalecenie dot. bezpieczeństwa 36: Należy sprawdzić ścieżkę AS w aktualizacji otrzymanej w eBGP, aby upewnić się, że lokalny numer AS nie jest obecny. Należy również sprawdzić ścieżkę AS, aby upewnić się, że nie ma numerów AS przeznaczonych do celów specjalnych [IANA-ASN-sp][29]. W przypadku naruszenia, aktualizacja powinna zostać odrzucona.

4.9. Rozwiązanie w zakresie wycieków tras

W dziale 2.3 opisano przestrzeń problemową wycieków tras i wskazano, że w dokumencie RFC 7908 [RFC7908] wymieniono różne rodzaje wycieków tras. Zdefiniowano również kilka podstawowych terminów używanych w dyskusjach na temat wycieków tras. Rozwiązania dot. wycieków tras dzielą się na dwie kategorie: wewnątrz systemu autonomicznego (*ang. intra-AS*) i między systemami autonomicznymi (*ang. inter-AS*) - w przeskokach AS. Wielu operatorów korzysta obecnie z rozwiązania intra-AS, które jest realizowane poprzez tagowanie aktualizacji BGP od wejścia do wyjścia (w AS) za pomocą BGP community[30] [NANOG-list].

[29] Należy zauważyć, że specjalny numer ASN 23456 jest przydzielony dla AS_TRANS [RFC6793] i może być obecny w AS_PATH w połączeniu z AS4_PATH [RFC 6793] podczas aktualizacji.

[30] Community to "dodatkowe informacje", które można dodać do jednego lub więcej prefiksów, które są rozgłaszane do sąsiednich BGP. Te dodatkowe informacje mogą być wykorzystywane do takich rzeczy, jak inżynieria ruchu lub dynamiczne zasady routingu.

Użyty BGP community jest nieprzechodni, ponieważ nie propaguje w eBGP (między systemami autonomicznymi). Każda aktualizacja BGP jest oznaczana na wejściu celem wskazania, że została odebrana w eBGP od klienta, lateralnego elementu równorzędnego lub dostawcy tranzytowego. Ponadto trasa, która pochodzi z AS jest oznaczana tak samo. W punkcie wyjściowym router wysyłający stosuje zasady ruchu wychodzącego, które wykorzystują oznaczanie (tagowanie). Trasy, które są odbierane od klienta, mogą być przekazywane na wyjściu do dowolnego typu elementu równorzędnego (np. klienta, elementu równorzędnego bocznego lub dostawcy tranzytowego). Jednak trasy otrzymane od bocznego elementu równorzędnego lub dostawcy tranzytowego są przekazywane tylko do klientów (tj. nie można ich przekazywać do bocznego elementu równorzędnego lub dostawcy tranzytowego). Te zasady ruchu przychodzącego i wychodzącego są kluczowe dla zapobiegania wyciekom tras wewnątrz AS (intra-AS).

Zalecenie dot. bezpieczeństwa 37: Operator AS powinien mieć politykę dotyczącą ruchu przychodzącego, aby wewnętrznie (lokalnie w AS) oznaczać trasy w celu komunikowania od wejścia do wyjścia co do typu elementu równorzędnego (klient, boczny peer lub dostawca tranzytu), od którego otrzymano trasę.

Zalecenie dot. bezpieczeństwa 38: Operator AS powinien mieć politykę ruchu wychodzącego w zakresie wykorzystywania oznakowanych informacji (jak w Zaleceniu dot. bezpieczeństwa 37), aby zapobiec wyciekom tras, gdy trasy są przekazywane na wyjściu. AS nie powinien przekazywać tras otrzymanych od dostawcy tranzytowego do innego dostawcy tranzytowego lub elementu równorzędnego bocznego. Ponadto AS nie powinien przekazywać tras otrzymanych od elementu równorzędnego bocznego innemu elementowi równorzędnemu bocznemu lub dostawcy tranzytowemu.

Powyższe rozwiązanie intra-AS służące zapobieganiu wyciekom tras można również zaimplementować przy użyciu BGP attribute (zamiast BGP community). Zaletą rozwiązania opartego na atrybutach [RouteLeak2] jest to, że można je udostępnić w komercyjnych routerach jako standardową funkcję, co z kolei minimalizuje ręczne działania operatora sieci. Jednak takie rozwiązanie wiąże się z aktualizacją protokołu

BGP [RFC4271] i wymaga standaryzacji, co wymaga czasu i jest obecnie w toku w IETF [RouteLeak2].
Drugi typ rozwiązania, inter-AS, jest przeznaczony do pracy w eBGP w skokach AS. Dzięki rozwiązaniu inter-AS, punkt ciężkości przesuwa się na wykrywanie i ograniczanie wycieku tras, który już wystąpił i zaczął się rozprzestrzeniać. Jeśli wyciek rzeczywiście rozchodzi się poza AS, wówczas równorzędny AS lub dowolny AS na następnej ścieżce AS powinien być w stanie go wykryć i zatrzymać. W IETF [RouteLeak1], [RouteLeak3] trwają również prace nad rozwiązaniem do wykrywania i ograniczania wycieków tras między AS.

Dla zapewnienia solidności infrastruktury routingu internetowego, oprócz wewnątrzsystemowych (intra-AS) zdolności zapobiegania konieczne będzie również wdrożenie międzysystemowej (inter-AS) zdolności wykrywania i ograniczania wycieków tras. Gdy mechanizmy zdolności wykrywania i ograniczania wycieków tras zostaną ustandaryzowane i staną się dostępne w produktach, niniejszy dokument zostanie zaktualizowany w celu uwzględnienia odpowiednich zaleceń dotyczących bezpieczeństwa odzwierciedlających ten fakt.

4.10. Uogólniony mechanizm zabezpieczenia TTL (Generalized TTL Security Mechanism - GTSM)

Czas życia pakietu (*ang. Time to Live - TTL*) jest 8-bitowym polem w każdym pakiecie IP i jest dekrementowany o jeden przy każdym skoku. Generalized TTL Security Mechanism (GTSM) [RFC5082] wykorzystuje TTL do zapewnienia dodatkowego mechanizmu bezpieczeństwa dla komunikatów BGP. Zazwyczaj sesja BGP przebiega pomiędzy sąsiadującymi routerami BGP, co oznacza, że komunikaty BGP pochodzą z odległości jednego skoku. W ramach takiej sesji BGP, router wysyłający ustawia TTL na 255 przy każdym komunikacie BGP, a router odbierający oczekuje, że przychodzący TTL będzie wynosić 255 i odrzuca wszelkie wiadomości BGP, które mają przychodzące TTL < 255. Oczekiwana wartość TTL w GTSM może być stosowana na zasadzie per-peer dla każdej sesji BGP. W rzadkich przypadkach, jeśli wiadomo, że sesja BGP z określonym elementem równorzędnym przebiega przez „n” skoków, wówczas oczekiwane TTL dla tej sesji może być dostosowane do

odpowiedniej wartości (w tym przypadku 255-n+1) zgodnie z liczbą skoków. W ten sposób GTSM pomaga wykryć i odrzucić sfałszowane komunikaty BGP, które mogą pochodzić od atakującego. Dodatkowe szczegóły dotyczące działania GTSM można znaleźć w [RFC5082].

Zalecenie dot. bezpieczeństwa 39: Generalized TTL Security Mechanism (GTSM) [RFC5082], [RFC5082] powinien być stosowany na zasadzie per-peer, aby zapewnić ochronę przed sfałszowanymi komunikatami BGP.

4.11. Domyślne zachowanie zewnętrznej propagacji tras BGP bez zastosowania polityk

RFC 8212 podkreśla jak ważne jest jednoznaczne skonfigurowanie polityk importu i eksportu w eBGP. Następujące domyślne zachowania są określone w [RFC8212]:

- Trasy zawarte w Adj-RIB-In związanego z elementem równorzędnym eBGP, NIE MOGĄ być uznane za dopuszczalne w Procesie Decyzyjnym, jeśli nie zastosowano jednoznacznej Polityki Importu.
- Trasy NIE MOGĄ być dodawane do Adj-RIB-Out związanego z elementem równorzędnym eBGP, jeżeli nie zastosowano jednoznacznej Polityki Eksportu.

Po osiągnięciu znacznego postępu w zakresie wdrażania i doświadczeń operacyjnych z zaleceniami RFC 8212, zostanie rozważone włączenie tych zaleceń do rekomendacji dotyczących bezpieczeństwa w niniejszym dokumencie (w przyszłej wersji).

5. ZABEZPIECZANIE PRZECIWKO ATAKOM DDOS ORAZ „ODBICIE-WZMOCNIENIE" - ROZWIĄZANIA I ZALECENIA[31]

Istnieją różne techniki i zalecenia dotyczące odstraszania przed atakami DDoS z wykorzystaniem sfałszowanych adresów [BCP38], [BCP84], [NABCOP], [CSRIC4-WG5]. Sprawdzanie poprawności adresu źródłowego (*ang. source address validation - SAV*) pakietów protokołu internetowego (IP) jest skuteczną techniką zapobiegającą spoofingowi [BCP38], [BCP84]. Istnieją również pewne techniki stosowane do zapobiegania atakom „odbicie-wzmocnienie" [RRL], [TA14-017A] wykorzystywanym do zwiększenia intensywności ataków DDoS. Zastosowanie kombinacji tych technik prewencyjnych w routerach granicznych organizacji i dostawców usług internetowych, sieciach dostawców usług hostowanych, otwartych serwerach DNS/NTP/innych, szerokopasmowych i bezprzewodowych sieciach dostępowych oraz centrach danych zapewnia niezbędną ochronę przed atakami DDoS. Projekt Spoofer [Spoofer], [Luckie2] ocenia i raportuje wdrażanie SAV w wielu wymiarach w: czasie, systemach autonomicznych, krajach i według wersji IP.

5.1. Techniki sprawdzania poprawności adresów źródłowych

Sprawdzanie poprawności adresu źródłowego (*ang. source address validation - SAV*) jest przeprowadzane w urządzeniach brzegowych sieci (*ang. network edge device*), takich jak routery graniczne, systemy zakończenia modemów kablowych (CMTS) [RFC4036], cyfrowe multipleksery dostępu do linii abonenckiej (*ang. digital subscriber line access multiplexers - DSLAM*) i bramy sieciowe danych pakietowych (*ang. packet data network gateways - PDN-GW*) w sieciach mobilnych [Firmin]. Listy kontroli dostępu do ruchu przychodzącego/wychodzącego (ACL) i unicast Reverse Path Forwarding (uRPF) to techniki stosowane do implementacji SAV [BCP38], [BCP84], [ISOC], [RFC6092; REC-5, REC-6]. SAV ruchu przychodzącego ma zastosowanie do pakietów przychodzących (odbieranych), a SAV ruchu wychodzącego ma zastosowanie do pakietów wychodzących (transmitowanych).

[31] Fragmenty materiału w niniejszym dziale odnoszące się do przeglądu istniejącej technologii SAV/uRPF brzmią jak odpowiadające im części w [EFP-uRPF], ponieważ autorzy pracowali nad obydwoma dokumentami równolegle i uznali za zasadne użycie tego samego lub podobnego materiału przeglądowego w obu miejscach. Ogólną zasadą IETF jest zachowanie praw autorskich przez oryginalnych autorów. Zob. https://trustee.ietf.org/reproduction-rfcs-faq.html.

Definicje terminów użytych w niniejszym dziale, takich jak dostawca tranzytowy, boczny element równorzędny, relacja komunikacji równorzędnej (C2P, p2p) i stożek klientów, podano w dziale 2.3. Ponadto lista Reverse Path Forwarding (*ang. RPF list*) jest definiowana jako lista dopuszczalnych prefiksów adresów źródłowych dla przychodzących pakietów danych na danym interfejsie.

5.1.1. Sprawdzanie poprawności adresu źródłowego (SAV)z wykorzystaniem list kontroli dostępu (ACL)

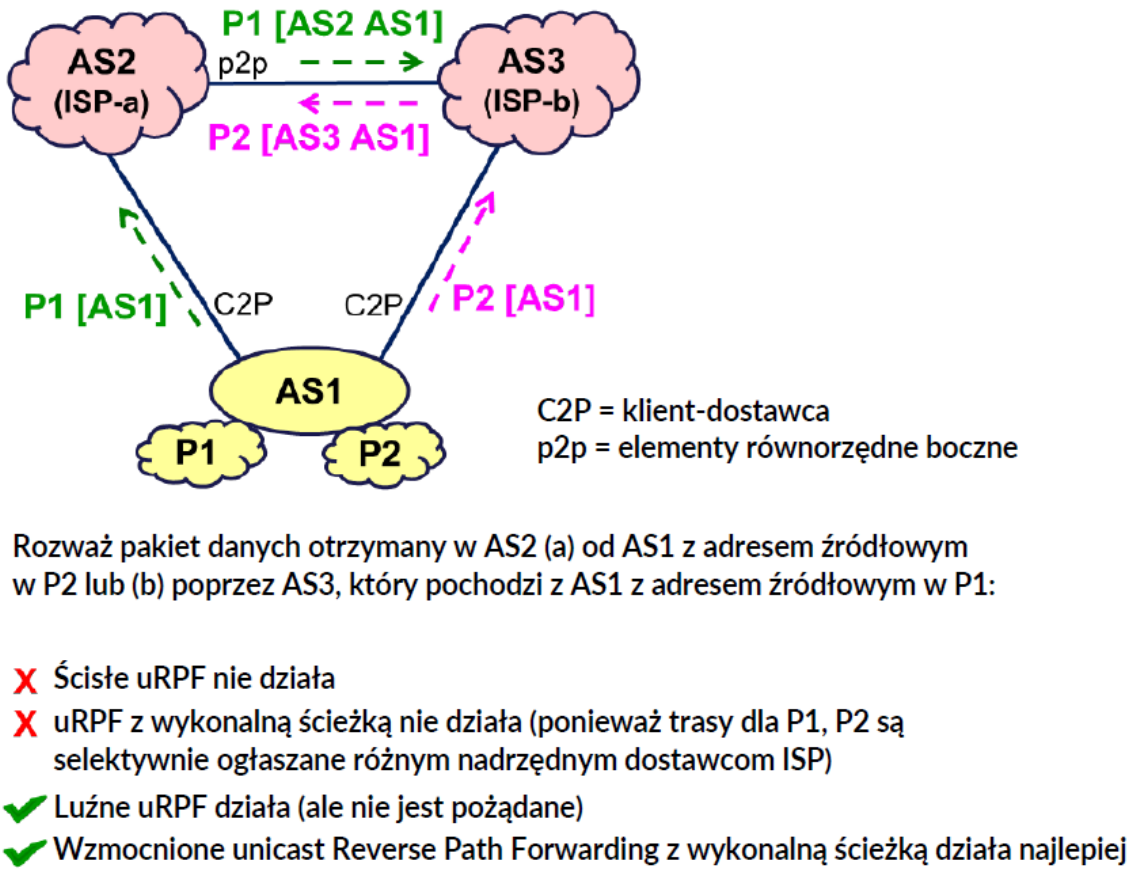
Listy kontroli dostępu (*ang. access control lists*, *ACL*) ruchu przychodzącego/ wychodzącego są utrzymywane wraz z listą akceptowanych (lub alternatywnie, niedopuszczalnych) prefiksów adresów źródłowych w przychodzących/wychodzących pakietach IP. Każdy pakiet z adresem źródłowym nie pasującym do filtru jest odrzucany. Należy utrzymywać aktualność listy ACL dla filtrów wejściowych/ wyjściowych. W związku z tym, metoda ta może być operacyjnie trudna lub niewykonalna w dynamicznych środowiskach, na przykład, gdy sieć klienta jest typu multi-homed, ma alokacje przestrzeni adresowej od wielu dostawców usług internetowych lub dynamicznie zmienia swoje ogłoszenia BGP (tj. routing) do celów inżynierii ruchu.

Zazwyczaj wyjściowe listy ACL w urządzeniach agregujących dostęp (np. CMTS, DSLAM, PDN-GW) zezwalają na adresy źródłowe tylko z przestrzeni adresowych (prefiksów) skojarzonych z interfejsem, z którym połączona jest sieć klienta. Listy kontroli dostępu ruchu przychodzącego są zwykle wdrażane na routerach granicznych i odrzucają pakiety przychodzące, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów — prefiksów oznaczonych jako „False” w kolumnie „Global” [IANA-v4-sp], [IANA-v6-sp], własnych prefiksów organizacji lub prefiksów tylko do użytku wewnętrznego usługodawcy internetowego).

5.1.2. Sprawdzanie poprawności adresu źródłowego (SAV) z wykorzystaniem ścisłego Unicast Reverse Path Forwarding (uRPF)

Terminologia: Na rysunkach (scenariuszach) w niniejszym dziale i kolejnych działach użyto następującej terminologii: „źle działa” oznacza odrzucanie pakietów

z prawidłowymi adresami źródłowymi; „działa (ale nie w sposób pożądany)" oznacza przekazywanie wszystkich pakietów z prawidłowymi adresami źródłowymi, ale bez wskazania kierunku; „działa najlepiej" oznacza przekazywanie wszystkich pakietów z prawidłowymi adresami źródłowymi bez (lub minimalnie) naruszenia kierunkowości. Ponadto zapis Pi [ASn ASm ...] oznacza aktualizację BGP z prefiksem Pi i AS_PATH, jak pokazano w nawiasach kwadratowych.



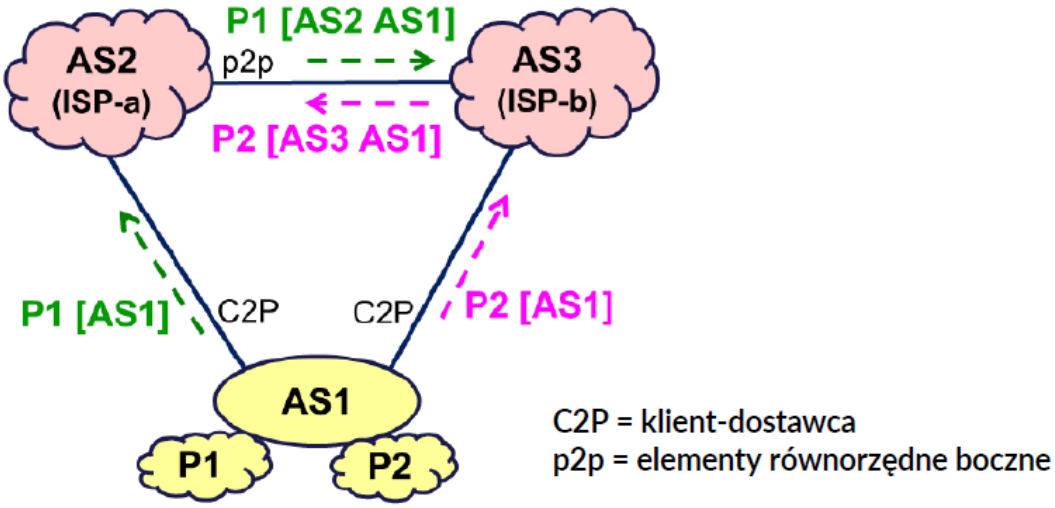
Rysunek 9: Scenariusz 1 do zilustrowania skuteczności schematów uRPF

W metodzie ścisłego unicast Reverse Path Forwarding (*ang. strict uRPF*), pakiet wejściowy na interfejsie routera granicznego jest akceptowany tylko wtedy, gdy baza informacji o przekazywaniu (*ang. forwarding information base - FIB*) zawiera prefiks, który obejmuje adres źródłowy i przekazywanie pakietów dla danego prefiksu wskazuje na dany interfejs. Innymi słowy, wybrana najlepsza ścieżka routingu do tego adresu źródłowego (jeśli był używany jako adres docelowy) powinna wskazywać na dany interfejs. Metoda ta ma pewne ograniczenia, gdy sieć lub system autonomiczny

jest typu multi-homed, trasy nie są symetrycznie ogłaszane wszystkim dostawcom tranzytowym, oraz występuje routing asymetryczny pakietów danych. Na przykład routing asymetryczny ma miejsce (zob. rys. 9, Scenariusz 1), gdy system autonomiczny klienta ogłasza jeden prefiks (P1) jednemu dostawcy tranzytowemu (ISP-a), a inny prefiks (P2) innemu dostawcy tranzytowemu (ISP-b), ale przesyła pakiety danych z adresami źródłowymi w drugim prefiksie (P2) do pierwszego dostawcy tranzytowego (ISP-a) lub odwrotnie. Następnie pakiety danych z adresem źródłowym w prefiksie P2, które są odbierane w AS2 bezpośrednio z AS1, zostaną odrzucone. Ponadto pakiety danych z adresem źródłowym w prefiksie P1, które pochodzą z AS1 i przechodzą przez AS3 do AS2, również zostaną odrzucone w AS2.

5.1.3. Sprawdzanie poprawności adresu źródłowego (SAV) z wykorzystaniem unicast Reverse Path Forwarding z wykonalną ścieżką

uRPF z wykonalną ścieżką (*ang. feasible-path uRPF*) pomaga częściowo przezwyciężyć problem związany ze ścisłym uRPF w przypadku multi-homingu. uRPF z wykonalną ścieżką jest podobny do ścisłego uRPF, ale oprócz wstawienia prefiksu najlepszej ścieżki, na liście RPF są również uwzględnione dodatkowe prefiksy z alternatywnych ogłoszonych tras (na rozważanym interfejsie) - patrz definicja na początku działu 5.1. Ta metoda opiera się albo na (a) ogłoszeniach dla tych samych prefiksów (chociaż niektóre mogą zostać dodane na początku, aby wpłynąć na niższe preferencje) propagujących do wszystkich dostawców tranzytowych wykonujących kontrole uRPF z wykonalną ścieżką, albo (b) ogłoszeniu zagregowanego, mniej specyficznego prefiksu wszystkim dostawcom tranzytowym, ogłaszając bardziej specyficzne prefiksy (objęte mniej specyficznym prefiksem) różnym dostawcom tranzytowym, zgodnie z potrzebami inżynierii ruchu. Na przykład w scenariuszu multi-homing (patrz rys. 10, scenariusz 2), jeśli AS klienta ogłasza trasy dla obu prefiksów (P1, P2) obu dostawcom tranzytowym (z odpowiednimi przedrostkami, jeśli są potrzebne do inżynierii ruchu), wówczas metoda uRPF z wykonalną ścieżką działa. uRPF z wykonalną ścieżką działa w tym scenariuszu tylko wtedy, gdy trasy klienta są preferowane w AS2 i AS3 zamiast krótszej trasy innej niż trasa klienta.



Rozważ pakiet danych otrzymany w AS2 (a) od AS1 z adresem źródłowym w P2 lub (b) poprzez AS3, który pochodzi z AS1 z adresem źródłowym w P1:

- ✗ Ścisłe uRPF nie działa
- ✗ uRPF z wykonalną ścieżką nie działa (ponieważ trasy dla P1, P2 są selektywnie ogłaszane różnym nadrzędnym dostawcom ISP)
- ✓ Luźne uRPF działa (ale nie jest pożądane)
- ✓ Wzmocnione unicast Reverse Path Forwarding z wykonalną ścieżką działa najlepiej

Rysunek 10: Scenariusz 2 do zilustrowania skuteczności schematów uRPF

Jednak metoda uRPF z wykonalną ścieżką ma również ograniczenia. Jedna forma ograniczenia występuje naturalnie, gdy zalecenie propagowania tych samych prefiksów (lub połączonej przestrzeni adresowej) do wszystkich routerów nie jest uwzględnione. Inną formę ograniczenia można opisać w następujący sposób: w Scenariuszu 2 (zilustrowanym na rys. 10) możliwe jest, że kolejny dostawca tranzytowy AS3 (ISP-b) nie propaguje trasy dostawionej z przodu (tj. P1 [AS1 AS1 AS1]) do pierwszego dostawcy tranzytowego AS2 (ISP-a). Wynika to z faktu, że polityka decyzyjna ISP-b zezwala na nadanie pierwszeństwa krótszej trasie do prefiksu P1 przez ISP-a w stosunku do dłuższej trasy uzyskanej bezpośrednio od klienta (AS1). W takim scenariuszu AS3 (ISP-b) nie wysyłałby żadnego ogłoszenia trasy dla prefiksu P1 do AS2 (ISP-a). Następnie pakiet danych pochodzący z AS1 z adresem źródłowym w prefiksie P1, który przechodzi przez AS3 (ISP-b), zostanie odrzucony w AS2 (ISP-a).

5.1.4. Sprawdzanie poprawności adresu źródłowego (SAV) z wykorzystaniem luźnego unicast Reverse Path Forwarding

W metodzie luźnego unicast Reverse Path Forwarding (*ang. loose uRPF*), pakiet wchodzący na router graniczny jest akceptowany tylko wtedy, gdy w FIB znajduje się jeden lub więcej prefiksów obejmujących adres źródłowy. Oznacza to, że pakiet jest odrzucany, jeśli w FIB nie ma trasy dla adresu źródłowego. Luźne uRPF rezygnuje z kierunkowości. Metoda ta nie jest zbyt efektywna w zapobieganiu spoofingu adresów. Odrzuca ona pakiety tylko wtedy, gdy sfałszowany adres jest nierutowalny (np. należy do ewidentnie niedozwolonych bloków prefiksów — prefiksów oznaczonych jako „False" w kolumnie „Global" [IANA-v4-sp], [IANA-v6-sp], jest nieprzydzielony lub przydzielony, ale obecnie nierutowany). Można zauważyć, że metoda ta wydawałaby się bardziej przydatna dla IPv6 niż IPv4.

5.1.5. Sprawdzanie poprawności adresu źródłowego (SAV) z wykorzystaniem tablicy VRF

Technologia wirtualnego routingu i przekierowywania (*ang. Virtual routing and forwarding - VRF*) [RFC4364], [Juniper5] pozwala utrzymywać w routerze wiele instancji tablicy routingu odrębnych od globalnej bazy informacji o routingu (*ang. routing information base - RIB*). Zewnętrzne sesje peeringowe BGP (*ang. external BGP - eBGP*) wysyłają określone trasy, które mają być przechowywane w dedykowanej tablicy VRF. Proces uRPF odpytuje tabelę VRF (zamiast FIB) w celu weryfikacji adresu źródłowego. Tabela VRF może być dedykowana dla każdego elementu równorzędnego eBGP i używana do uRPF tylko dla tego elementu równorzędnego, co skutkuje działaniem w trybie ścisłym. W celu wdrożenia luźnego uRPF na interfejsie, odpowiednia tabela VRF byłaby globalna (tzn. zawierałaby te same trasy co w FIB).

5.1.6. Sprawdzanie poprawności adresu źródłowego (SAV) z wykorzystaniem wzmocnionego unicast Reverse Path Forwarding z wykonalną ścieżką (powstające/przyszłe)

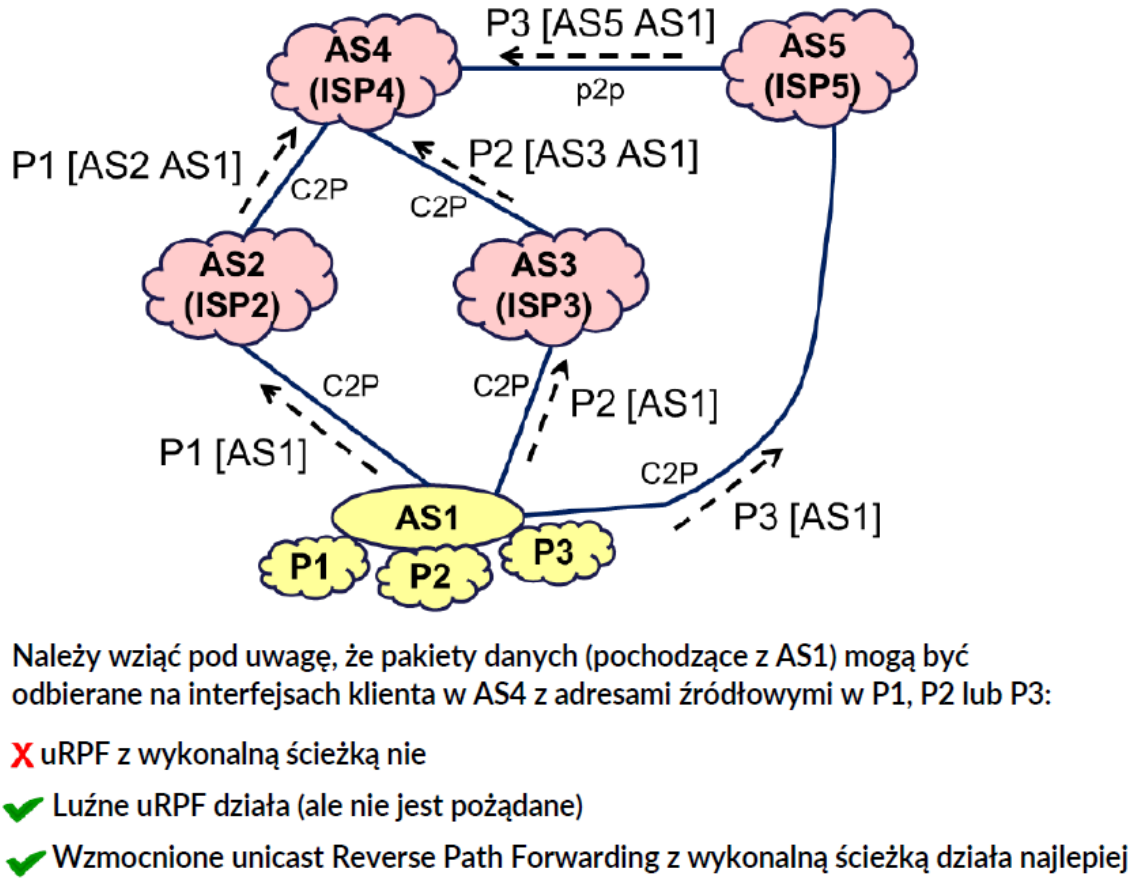
Metoda wzmocnionego uRPF z wykonalną ścieżką (*ang. enhanced feasible-path uRPF - EFP-uRPF*) jest obecnie w trakcie opracowywania (jako standard RFC) w IETF [EFP-

uRPF]. Daje nadzieje na zapewnienie znacznej poprawy skuteczności i możliwości wdrażania w stosunku do uRPF z wykonalną ścieżką. Niniejszy dział pokrótce opisuje prace związane z technologią i standardami, ale nie zawiera zaleceń dotyczących bezpieczeństwa w zakresie korzystania z EFP-uRPF w tym momencie.

EFP-uRPF zapewnia większą elastyczność i dokładność operacji uRPF niż istniejące metody uRPF omówione w działach od 5.1.2 do 5.1.5. Podstawowa zasada metody EFP-uRPF zwiększająca efektywność w scenariuszach multi-homing i asymetrycznego routingu jest następująca: jeśli trasa dla prefiksu P1 jest odbierana na interfejsie klienta X i ma pochodzenie AS1, a trasy dla P2 i P3 są odbierane na inne interfejsy komunikacji równorzędnej Y i Z, ale mają to samo pochodzenie AS1, to należy dopuścić elastyczność, że pakiety danych z adresem źródłowym w dowolnym z tych trzech prefiksów (P1, P2, P3) mogą być legalnie odbierane na interfejsie klienta X. Zatem zgodnie z zasadą wspólnego pochodzenia AS, lista prefiksów dla dozwolonych adresów źródłowych w pakietach danych (tj. lista RPF) jest rozszerzana o wszystkie trzy prefiksy (P1, P2, P3) dla interfejsu klienta X. Ponadto ta sama zasada jest stosowana do określanie listy prefiksów dla dopuszczalnych adresów źródłowych dla każdego interfejsu klienta i ewentualnie interfejsów bocznych elementów równorzędnych.

Jak pokazano w scenariuszach 1 i 2 (rys. 9 i rys. 10), EFP-uRPF zapewnia porównywalną lub lepszą wydajność niż inne metody uRPF w tych scenariuszach. Scenariusz 3 (rys. 11) dodatkowo ilustruje, że metoda EFP-uRPF działa najlepiej nawet w znacznie bardziej złożonych scenariuszach routingu asymetrycznego. Scenariusz 3 (rys. 11) koncentruje się na odbieraniu przez AS4 pakietów danych z adresem źródłowym w {P1, P2, P3}. Jeżeli metoda EFP-uRPF (jak opisano powyżej) jest użyta w AS4, wówczas {P1, P2, P3} zostaną uwzględnione na listach RPF odpowiadających interfejsom klienta skierowanym do AS2 i AS3. Ponadto, jeżeli EFP-uRPF jest również użyty w AS4 w kierunku do AS5 elementu równorzędnego, wówczas {P1, P2, P3} zostaną uwzględnione na liście RPF odpowiadającej interfejsowi elementu równorzędnego skierowanemu w stronę AS5. W ten sposób operator (w AS4) może być pewny, że jego SAV będzie działał efektywnie, a żaden z pakietów danych pochodzący z AS1 (i odbierany poprzez sąsiednie AS2, AS3

lub AS5) z adresami źródłowymi w {P1, P2, P3} nie zostanie odrzucony ze względu na SAV. Zatem metoda EFP-uRPF ma na celu wyeliminowanie lub znaczne zmniejszenie fałszywych alarmów dotyczących nieprawidłowego wykrywania w SAV w porównaniu z innymi metodami uRPF. Szczegóły dotyczące EFP-uRPF można znaleźć w [EFP-uRPF]. Ponieważ wciąż trwają prace, nie przedstawiono tutaj żadnych zaleceń dotyczących bezpieczeństwa dotyczących EFP-uRPF.

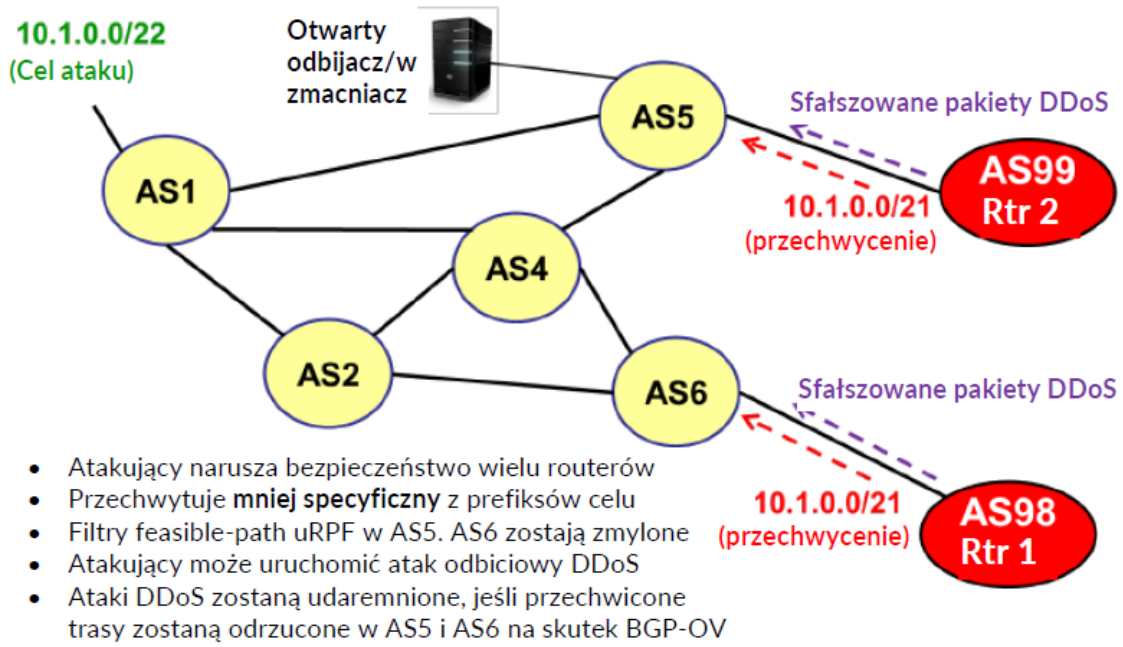


Rysunek 11: Scenariusz 3 do zilustrowania skuteczności schematów uRPF

5.1.7. Skuteczniejsze ograniczanie poprzez łączne zastosowanie sprawdzania pochodzenia (BGP-OV) i poprawności adresu źródłowego (SAV)

Dzięki połączeniu omówionych powyżej technik sprawdzania pochodzenia BGP (*ang. BGP origin validation - BGP-OV*) - patrz dział 4.3 i SAV (uRPF) - możliwa jest lepsza ochrona przed spoofingiem adresów i atakami DDoS. Zdeterminowany atakujący DDoS może naruszyć dowolną z metod uRPF, przechwytując prefiks, a następnie

fałszując adres źródłowy, jak pokazano na rys. 12. W scenariuszu przedstawionym na rys. 12. atakujący najpierw kompromituje routery (lub może niektóre z nich są jego własnościami) w systemach AS98 i AS99, a następnie fałszywie ogłasza mniej specyficzny prefiks (np. 10.1.0.0/21) obejmujący prefiks celu (np. 10.1.0.0/22). Zakłada się, że brak jest w tym momencie prawidłowego ogłoszenia mniej specyficznego prefiksu (10.1.0.0/21). Filtry uRPF (FP- uRPF) z wykonalną ścieżką w AS5 i AS6 są skutecznie zmylone, a atakujący prawdopodobnie pozostaje niewykryty, ponieważ przechwycony prefiks jest mniej specyficznym prefiksem. Atakujący będzie wtedy w stanie skutecznie wykonać spoofing adresów i atak DDoS wraz z odbiciem i wzmocnieniem Aby chronić się przed tego typu atakami wielowątkowymi, należy zastosować kombinację BGP-OV (aby zapobiec przechwyceniu) i FP-uRPF lub EFP-uRPF (aby zapobiec fałszowaniu adresu). Aby to zadziałało, właściciele prefiksów (10.1.0.0/22 i 10.1.0.0/21) powinni utworzyć ROA, a wszystkie systemy autonomiczne (zwłaszcza AS5 i AS6) na rys. 12 powinny wykonać BGP-OV oprócz użycia SAV z wykorzystaniem metody FP-uRPF/EFP-uRPF.



Rysunek 12: Ilustracja sposobu, w jaki sprawdzanie pochodzenia uzupełnia SAV

5.2. Zalecenia dotyczące sprawdzania poprawności adresu źródłowego (SAV) dla różnych rodzajów sieci

Uwzględniono tutaj trzy typy scenariuszy sieciowych, a dla każdego scenariusza podano zalecenia dotyczące zabezpieczeń SAV. Te typy scenariuszy to: 1) sieci, które mają klientów z bezpośrednio połączoną przydzieloną przestrzenią adresową, takich jak dostawcy usług szerokopasmowych i bezprzewodowych; 2) sieci organizacyjne; oraz 3) dostawcy usług internetowych (ISP).

Gdy instytucja publiczna lub przedsiębiorstwo zamawia usługi dostawcy usług hostowanych lub tranzytowego dostawcy usług internetowych, należy rozważyć uwzględnienie w umowach o świadczenie usług zaleceń dotyczących bezpieczeństwa odpowiednio wymienionych w niniejszym dokumencie.

5.2.1. Klient z bezpośrednio przydzieloną przestrzenią adresową: Dostawcy usług szerokopasmowych i bezprzewodowych

Technika SAV z listami ACL jest stosunkowo łatwa, gdy sieć obsługiwana przez urządzenie brzegowe dostawcy usług internetowych (np. router graniczny, CMTS, DSLAM, PDN-GW) jest bezpośrednio podłączona i korzysta z przestrzeni adresowej IP, która jest podzielona przez dostawcę usług internetowych. W związku z tym, w takich przypadkach należy zawsze stosować SAV przy użyciu metody ACL. W przypadku pakietów przychodzących (tj. pakietów przechodzących przez urządzenie brzegowe do Internetu) adres źródłowy musi mieścić się w przydzielonej przestrzeni. Przykładowo, standard Data Over Cable Service Interface Specification 3.1 (DOCSIS 3.1) dla CMTS zawiera już ten test bezpieczeństwa [DOCSIS], [Comcast], [RFC4036].

Zalecenie dot. bezpieczeństwa 40: Routery BGP, które bezpośrednio połączyły klientów z subalokowaną przestrzenią adresową, CMTS (lub odpowiednik) w szerokopasmowych sieciach dostępowych oraz PDN-GW (lub odpowiednik) w sieciach mobilnych, powinny implementować SAV za pomocą list ACL (dział 5.1.1). Routery BGP mogą alternatywnie stosować metodę ścisłego uRPF (dział 5.1.2).

5.2.2. Routery graniczne organizacji

Zalecenia dot. bezpieczeństwa SAV dla routerów granicznych organizacji różnią się w zależności od charakteru wejścia/wyjścia pakietów danych. Poniżej znajdują się również zalecenia dotyczące płaszczyzny sterującej routingiem (aktualizacji BGP).

Zalecenie dot. bezpieczeństwa 41: Router graniczny organizacji, typu multi-homed, powinien zawsze ogłaszać całą swoją przestrzeń adresową do każdego ze swoich nadrzędnych (upstream) dostawców tranzytowych. Można to zrobić na jeden z dwóch sposobów: 1) ogłaszać zagregowany mniej specyficzny prefiks wszystkim dostawcom tranzytowych oraz bardziej specyficzne prefiksy (objęte mniej specyficznym prefiksem) różnym dostawcom tranzytowym, zgodnie z potrzebami inżynierii ruchu, lub 2) ogłaszać takie prefiksy każdemu dostawcy tranzytowemu (aczkolwiek z odpowiednim dostawianiem na początku dla celów inżynierii ruchu)[32].

Zalecenie dot. bezpieczeństwa 42: Jest to wyjątkowy przypadek, gdy router graniczny organizacji nie wypełnia Zalecenia dot. bezpieczeństwa 41 i zamiast tego selektywnie ogłasza niektóre prefiksy jednemu tranzytowemu dostawcy usług internetowych na kierunku upstream, a inne prefiksy innemu tranzytowemu dostawcy usług internetowych upstream. W tym przypadku organizacja powinna kierować dane (poprzez odpowiedni wewnętrzny routing) w taki sposób, aby adresy źródłowe w pakietach danych w kierunku każdego tranzytowego dostawcy usług internetowych upstream należały do prefiksu lub prefiksów ogłoszonych temu dostawcy.

Zalecenie dot. bezpieczeństwa 43: Po stronie wejścia (tj. dla pakietów danych otrzymywanych od tranzytowego dostawcy usług internetowych) routery graniczne organizacji powinny wdrożyć luźne uRPF (dział 5.1.4) i/lub ACL (dział 5.1.1) w celu odrzucenia pakietów, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów — prefiksów oznaczonych jako „False” w kolumnie „Global” [IANA- v4-sp], [IANA-v6-sp] oraz własnych prefiksów organizacji).

[32] Postępując zgodnie z Zaleceniem dot. bezpieczeństwa 41, router graniczny organizacji zapewnia, by routery graniczne tranzytowych dostawców usług internetowych odrzucały (ze względu na uRPF) tylko te pakiety danych z organizacji, które nie mają adresów źródłowych należących do żadnego z ogłoszonych prefiksów organizacji. W ten sposób zapewnia również, że pakiety danych z organizacji, które mają adresy źródłowe należące do dowolnego z ogłoszonych prefiksów organizacji, nigdy nie są odrzucane.

Zalecenie dot. bezpieczeństwa 44: Organizacja (tj. AS typu leaf z multihomingiem lub bez) powinna dopuszczać po stronie wyjściowej (tj. dla pakietów danych wysyłanych do tranzytowego ISP) tylko te pakiety z adresami źródłowymi, które należą do ich własnych prefiksów.

5.2.3. Dostawcy usług internetowych

Zalecenia dotyczące bezpieczeństwa SAV dla dostawców usług internetowych (ISPs) różnią się w zależności od ruchu wejściowego/wyjściowego pakietów oraz relacji z elementem równorzędnym (np. klient, lateralny element równorzędny, dostawca tranzytowy).

Zalecenie dot. bezpieczeństwa 45: W przypadku interfejsów skierowanych do klienta mniejsi dostawcy usług internetowych[33] powinni przeprowadzać SAV na pakietach wejściowych, wdrażając uRPF z wykonalną ścieżką (zob. dział 5.1.3). Powinni unikać stosowania ścisłego lub luźnego uRPF, ponieważ nie są one skuteczne. Przyjmuje się, że więksi dostawcy usług internetowych mogą korzystać z luźnego uRPF w interfejsach klientów[34].

Zalecenie dot. bezpieczeństwa 46: Aby uRPF z wykonalną ścieżką działało właściwie, mniejszy dostawca usług internetowych (zwłaszcza ten, który znajduje się w pobliżu krawędzi Internetu) powinien propagować całą swoją ogłaszaną przestrzeń adresową do każdego ze swoich upstreamowych dostawców tranzytowych. Można to zrobić na jeden z dwóch sposobów: 1) ogłaszać zagregowany mniej specyficzny prefiks wszystkim dostawcom tranzytowym i ogłaszać bardziej specyficzne prefiksy (objęte mniej specyficznym prefiksem) różnym dostawcom tranzytu, w miarę potrzeby inżynierii ruchu, lub 2) ogłaszać te same prefiksy każdemu dostawcy tranzytowemu (choć z odpowiednim prefiksem dla celów inżynierii ruchu).

[33] Mniejsi dostawcy usług internetowych są zwykle usytuowani bliżej krawędzi internetu gdzie SAV jest skuteczniejsze. Zazwyczaj mają dokładny wgląd w swój stożek klientów. Mieliby znikome prawdopodobieństwo fałszywych alarmów z nieprawidłowym wykryciem w SAV z FP-uRPF.

[34] W przyszłości ulepszony uRPF ze ścieżką wykonalności [EFP-uRPF] może być rozważany dla SAV dla pakietów wejściowych na interfejsach klienta (u wszystkich dostawców usług internetowych)w oparciu o dostępność komercyjnej implementacji (zob. dział 5.1.6).

Zalecenie dot. bezpieczeństwa 47: Dostawcy usług internetowych powinni preferować trasy klientów w stosunku do innych (tj. dostawcy tranzytu lub elementów równorzędnych bocznych) tras. W większości przypadków jest to również normalna polityka ISP[35].

Zalecenie dot. bezpieczeństwa 48: W przypadku interfejsów z lateralnymi (tj. nietranzytowymi) elementami równorzędnymi, mniejsi dostawcy usług internetowych (w pobliżu krawędzi Internetu) powinni wykonywać SAV na pakietach wejściowych, wdrażając uRPF z wykonalną ścieżką (zob. dział 5.1.3). Powinni unikać stosowania ścisłego lub luźnego uRPF, ponieważ nie są one zbyt skuteczne dla SAV na interfejsach bocznych elementów równorzędnych.

Uznaje się, że więksi dostawcy usług internetowych mogą stosować luźne uRPF na interfejsach z bocznymi elementami równorzędnymi[36].

Zalecenie dot. bezpieczeństwa 49: W przypadku interfejsów z dostawcami tranzytowymi, dostawcy usług internetowych powinni wykonywać SAV na pakietach przychodzących, wdrażając luźne uRPF (patrz dział 5.1.4) i/lub ACL (patrz dział 5.1.1), w celu odrzucania pakietów, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów – prefiksów oznaczonych jako „False" w kolumnie „Global" [IANA- v4-sp], [IANA-v6-sp] i prefiksów ISP tylko do użytku wewnętrznego).

Zalecenie dot. bezpieczeństwa 50: Po stronie wychodzącej w kierunku klientów, elementów równorzędnych bocznych (tj. nietranzytowych) i dostawców tranzytowych, routery graniczne dostawcy usług internetowych powinny wdrożyć listy kontroli dostępu (patrz dział 5.1.1), aby odrzucać pakiety, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów - prefiksów oznaczonych jako „False" w kolumnie „Global" [IANA- v4-sp], [IANA-v6-sp] i prefiksów ISP tylko do użytku wewnętrznego).

---

[35] Przestrzeganie Zalecenia dot. bezpieczeństwa 47 ułatwia przestrzeganie Zalecenia dot. bezpieczeństwa 45. Jest to także jeden z warunków stabilności polityki BGP dla zapewnienia stabilnej konwergencji informacji o routingu [Gao-Rexford].

[36] W przyszłości może być rozważony wzmocniony uRPF z wykonalną ścieżką [EFP-uRPF] dla SAV dla pakietów wejściowych na interfejsach klienta (u wszystkich ISP) w oparciu o dostępność komercyjnej implementacji (zob. dział 5.1.6).

5.3. Rola RPKI w sprawdzaniu adresów źródłowych

W dziale 4.6 opisano metodę, jak dostawcy usług internetowych mogą używać ROA w rejestrach RPKI, by pomóc w budowie filtrów prefiksów. Ta sama technika może być zastosowana do konstruowania list ACL dla SAV na każdym interfejsie skierowanym do klienta. Te listy ACL mogą być używane do krzyżowego sprawdzania i/lub rozszerzania wpisów na listach RPF odpowiadających każdemu interfejsowi skierowanemu do klienta.

Zalecenie dot. bezpieczeństwa 51: Dostawcy usług internetowych powinni używać danych ROA (dostępnych z rejestrów RPKI) do tworzenia i/lub rozszerzania list ACL/RPF do celów SAV dla pakietów przychodzących na interfejsach klienta[37].

5.4. Monitorowanie portów UDP/TCP z aplikacjami wrażliwymi i stosowanie filtrowania ruchu

Zagrożenia DDoS związane z wrażliwymi aplikacjami korzystającymi z różnych portów UDP/TCP i urządzeń IoT stale ewoluują i są zróżnicowane (np. ataki odbiciowe memcached DDoS i dyfrakcja SSDP, itp. [Bjarnason], [Arbor2]). W związku z tym metody filtrowania ruchu wymienione w niniejszym dziale nie są wyczerpujące.

Monitorowanie i filtrowanie ruchu w oparciu o określone porty User Datagram Protocol (UDP) i Transmission Control Protocol (TCP) jest prowadzone w celu zablokowania ruchu określonego typu aplikacji, które nie są spodziewane na danym interfejsie [TA14-017A], [Acunetix], [ISC2]. W niektórych przypadkach aplikacje mogą być prawidłowe, ale obserwowane natężenie ruchu może być podejrzanie wysokie. W takim przypadku stosowane jest ograniczenie wskaźnika odpowiedzi (*ang. response rate limiting - RRL*) [Redbarn], [ISC1].

W przypadku DNS (UDP/Port 53 i TCP/Port 53) organizacyjny wewnętrzny program rozpoznawania nazw z systemu nazw domen (*ang. resolver DNS*) może ograniczyć zakres klientów, od których będzie akceptował żądania. Klienci zwykle pochodzą z tej samej sieci organizacyjnej, w której znajduje się resolver DNS. W związku z tym

[37] Zalecenie dot. bezpieczeństwa 51 jest być może lepiej przystające do mniejszych ISP którzy mają lepszą widoczność swojego stożka klientów. Więksi ISP zwykle nie dysponują taką widocznością.

rekursywny resolver DNS może utrzymywać listy dostępu w konfiguracji, dzięki czemu otwarty resolver DNS może zostać skutecznie „zamknięty" [ISOC]. Innym skutecznym środkiem jest monitorowanie przez autorytatywne resolvery DNS wskaźnika zapytań na adres źródłowy i stosowanie ograniczania wskaźnika odpowiedzi (RRL), co zmniejsza wskaźnik, z jakim autorytatywne serwery odpowiadają na dużą liczbę złośliwych zapytań [Redbarn], [ISC1].

Poniższa Tabela 1 zawiera listę protokołów warstwy aplikacji i ich numerów portów [TA14-017A], [Akamai]. Aplikacje oparte na UDP zostały zidentyfikowane jako podatne na ataki reflection/amplification. W Tabeli 1 współczynnik wzmocnienia wymieniony dla każdego protokołu to mnożnik natężenia ruchu, który można osiągnąć, wykorzystując efekt odbicia/wzmocnienia tego protokołu uruchomionego na UDP [TA14-017A], [Akamai]. Status przypisania portu jest nazwany „Official", jeśli został oficjalnie nadany przez IANA; w przeciwnym razie jest to „Unofficial" [port TCP-UDP].

Tabela 1: Zwykłe aplikacje i ich numery portów TCP/UDP

Protokół aplikacji	**Współczynnik wzmocnienia pasma**	**Nr portu**	**Status przypisania portu**
Domain Name System (DNS)	28 do 54	53, 853, 953	Official
Network Time Protocol (NTP)	557	123	Official
Simple Network Management Protocol (SNMP), SNMPv2	6	161	Official
NetBIOS Name/Datagram/Session	4	137/138/139	Official
Simple Service Discovery Protocol (SSDP); discovery of UPnP devices	31	1900	Official

Protokół aplikacji	**Współczynnik wzmocnienia pasma**	**Nr portu**	**Status przypisania portu**
Character Generation Protocol (CharGEN)	359	19	Official
Quote of the Day (QOTD)	140	17	Official
BitTorrent	4	6881-6887; 6889-90; 6891-6900; itd. różne zakresy	Unofficial
Kad Network (Kademlia P2P overlay protocol)	16	6419, 6429	Unofficial
Quake Network Protocol	64	15, 28, 27500-27900, 27901-27910, 27950, 27952, 27960-27969 itd.	Unofficial
Protokoły strumieniowe (np. QuickTime)		6970-9999 itd.	Unofficial
Real-Time Streaming Protocol (RTSP); ms-streaming		554, 1755	Official
Routing Information Protocol (RIP, RIPng)	131	520, 521	Official
Multicast DNS (mDNS)	2 do 10	5353	Official
Portmap/Remote Procedure Call (RPC)RPC	7 do 28	111, 369	Official
Lightweight Directory Access Protocol (LDAP); Connectionless LDAP (CLDAP)	70	389	Official

Poniższy zestaw zaleceń dotyczących bezpieczeństwa dotyczy aplikacji wrażliwych, takich jak wymienione w Tabeli 1:

Zalecenie dot. bezpieczeństwa 52: W routerach BGP zezwalaj elementom równorzędnym na łączenie się tylko z portem 179. Standardowym portem do odbierania komunikatów OPEN sesji BGP jest port 179, więc próby dotarcia przez elementy równorzędne BGP do innych portów mogą wskazywać na wadliwą konfigurację lub potencjalną działalność złośliwą.

Zalecenie dot. bezpieczeństwa 53: Wyłącz aplikacje lub usługi, które są niepożądane w danej sieci lub systemie.

Zalecenie dot. bezpieczeństwa 54: Odmawiaj ruchu dla wszystkich portów TCP/UDP, dla których dana sieć lub system nie obsługuje odpowiednich aplikacji. W niektórych przypadkach aplikacja lub usługa jest obsługiwana przez niektóre interfejsy (np. interfejsy skierowane do klienta lub do wewnątrz), ale nie przez inne (np. interfejsy skierowane do Internetu). W takich przypadkach należy odmówić ruchu z ID portu właściwym dla rozpatrywanej aplikacji na interfejsach, na których ta aplikacja nie jest obsługiwana.

Zalecenie dot. bezpieczeństwa 55: Zalecenie to ma na celu wykrycie przeciążeń ruchu i zastosowania działań ograniczających. Odpowiednie techniki ograniczania to response rate limiting (RRL) [ISC1], [Redbarn] oraz uruchomione filtrowanie source-based remotely triggered black hole (S/RTBH) z Flowspec (zob. dział 5.5) [RFC5575], [RFC5575bis]. Techniki te mają zastosowanie do otwartych usług/protokołów, takich jak wymienione w Tabeli 1, które same są podatne na ataki DOS/DDoS lub mogą być wykorzystywane do ataku typu reflection/amplification. Zalecenie składa się z kilku następujących etapów [TA14-017A]:

- Monitoruj współczynnik zapytań/żądań na adres źródłowy i wykrywaj, czy nienormalnie duża liczba odpowiedzi zmierza do tego samego miejsca docelowego (tj. tego samego adresu IP).

- Zastosuj technikę ograniczania współczynnika odpowiedzi (RRL), aby ograniczyć atak[38].
- Korzystając z komunikatów BGP (Flowspec), utwórz filtr source-based remotely triggered black hole (S/RTBH). Można to skoordynować z dostawcą usług internetowych wyższego szczebla (upstream).
- Zachowuj awaryjne informacje kontaktowe dla dostawcy nadrzędnego (upstream), aby koordynować reakcję na atak.
- Dostawca usług internetowych szczebla nadrzędnego (upstream) powinien aktywnie koordynować reakcje z klientami podrzędnymi (downstream).

Poniższe zalecenia dotyczące bezpieczeństwa są charakterystyczne dla NTP i DNS:

Zalecenie dot. bezpieczeństwa 56: Całkowicie odmawiaj ruchu żądań NTP monlist (wyłączając polecenie monlist) lub wymuszaj, aby żądania pochodziły z prawidłowych (dozwolonych) adresów źródłowych.

Zalecenie dot. bezpieczeństwa 57: Aby ograniczyć wykorzystanie luk, wewnętrzny rekursywny resolver DNS organizacji powinien ograniczać zakres klientów, od których akceptuje żądania. Klienci zwykle pochodzą z tej samej sieci organizacyjnej, w której znajduje się resolver DNS. W związku z tym rekursywny resolver DNS może utrzymywać listy dostępowe w konfiguracji, tak aby nie była otwarta dla całego Internetu [ISOC], [TA14-017A].

Zalecenie dot. bezpieczeństwa 58: Organizacja powinna zablokować protokoły UDP/Port 53 i TCP/Port 53 dla ruchu wchodzącego i wychodzącego na granicy sieci; wyjątki[39] obejmują wyznaczone organizacyjne rekursywne resolvery organizacji, które muszą wysyłać zapytania, oraz wyznaczone autorytatywne serwery organizacji, które muszą wysłuchiwać zapytań.

[38] Technika RRL jest powszechnie stosowana w DNS, tłumiąc współczynnik, z jakim autorytatywne serwery odpowiadają na dużą liczbę złośliwych zapytań. Może być również stosowany w innych aplikacjach (wskazanych w Tabeli 1) do tłumienia współczynnika odpowiedzi.

[39] Na przykład Google 8.8.8.8, Cloudflare 1.1.1.1 itd.

Jeśli chodzi o Zalecenie dot. bezpieczeństwa 58, celem blokowania ruchu wychodzącego jest zablokowanie możliwości wysyłania do Internetu własnych zapytań przez resolvery stub (na hostach), a zamiast tego zapewnienie, że używają one rekursywnego resolvera organizacji. Podobnie, celem blokowania ruchu wejściowego jest zablokowanie ataków lub „podstępnych" (*ang. „rogue")* rekursywnych resolverów przed użyciem w atakach poprzez zablokowanie ruchu przed dotarciem do nich.

Protokoły DNS, LDAP i inne otwarte protokoły usług używane w amplifikacji DDoS generują znaczne ilości ruchu fragmentów UDP. Istnieje możliwość zmniejszenia wpływu ruchu związanego z amplifikacją DDoS poprzez ograniczenie współczynnika nieinicjowanych fragmentów UDP na krawędziach komunikacji równorzędnej ISP. Są to pakiety UDP, w których przesunięcie fragmentu jest większe niż 0.

Zalecenie dot. bezpieczeństwa 59: Dostawca usług internetowych powinien prowadzić ograniczanie współczynnika dla nieinicjowanych fragmentów UDP na routerach brzegowych[40] (*ang. edge router*) skierowanych do klientów i bocznych elementów równorzędnych.

5.5. Specyfikacja przepływu BGP (Flowspec)

Jako techniki ograniczania DDoS wykorzystano zdalnie wyzwalana „czarna dziura"[41](ang. blackholing) oparta na adresach docelowych (*ang. destination-based remotely triggered black-holing*, *D/RTBH*) [RFC3882], [RFC7999] oraz zdalnie wyzwalany blackholing oparty na adresach źródłowych[42] (*ang. source-based remotely triggered black-holing*, *S/RTBH*) [RFC5635]. Jednak dzięki standaryzacji i obsłudze przez dostawcę Flowspec [RFC5575], [RFC7674], [RFC5575bis], [Ryburn], [Cisco4], [Juniper4] podstawowe zasady D/RTBH i S/RTBH są znacznie ulepszone i mogą być operacyjnie wdrażane w precyzyjny, dynamiczny i wydajny sposób. Doświadczenie operacyjne z Flowspec w zakresie ograniczania DDoS zostało zgłoszone w [Levy2], [Compton], [Hinze].

[40] Router brzegowy - router, który znajduje się na krawędzi sieci i może zezwalać na nowy ruch w sieci. Obejmuje to routery graniczne, ale także routery, które akceptują ruch z urządzeń klienckich.

[41] Czarna dziura – w sieciach komputerowych pojęcie to odnosi się do miejsca w sieci, w którym ruch sieciowy jest przerywany, ale bez informowania o tym źródła. Podczas sprawdzania topologii sieci czarne dziury są niewidoczne. Można je wykryć tylko przez monitorowanie ruchu sieciowego.

[42] W połączeniu z uRPF.

W D/RTBH wysyłany jest komunikat BGP wyzwalający routery brzegowe dostawcy (*ang. provider edge - PE*) tranzytowego (w systemie autonomicznym ofiary lub w systemie autonomicznym jej dostawcy tranzytowego) w celu zablokowania ruchu przychodzącego na określony adres IP, na którym znajduje się dany serwer.
W S/RTBH wysyłany jest komunikat BGP wyzwalający routery brzegowe dostawcy PE tranzytowego (w systemie autonomicznym ofiary lub w systemie autonomicznym jej dostawcy tranzytowego) w celu zablokowania ruchu przychodzącego z określonego adresu IP, który jest adresem źródłowym używanym przez atakującego. W przypadku S/RTBH, do filtrowania ruchu z określonego adresu źródłowego jest używany luźny uRPF. W mechanizmie Flowspec BGP zdefiniowano i użyto specyfikację przepływu NLRI służącą do przekazywania informacji o regułach filtrowania ruchu, który powinien zostać odrzucony [RFC5575], [RFC5575bis]. Mechanizm ten umożliwia systemowi autonomicznemu nadrzędnemu (upstream) filtrowanie ruchu przychodzącego w routerach brzegowych, który dany system podrzędny (downstream) chce odrzucić. Tabela 2 przedstawia informacje, które można uwzględnić w BGP Flowspec [RFC5575], [RFC5575bis].

Tabela 2: Typy BGP Flowspec

Typ 1	Prefiks docelowy (*ang. Destination Prefix*)
Typ 2	Prefiks źródłowy (*ang. Source Prefix*)
Typ 3	Protokół IP (*ang. IP Protocol*)
Typ 4	Port źródłowy lub docelowy (*ang. Source or Destination Port*)
Typ 5	Port docelowy (*ang. Destination Port*)
Typ 6	Port źródłowy (*ang. Source Port*)
Typ 7	Typ ICMP (*ang. ICMP Type*)
Typ 8	Kod ICMP (*ang. ICMP Code*)
Typ 9	Flagi TCP (*ang. TCP flags*)
Typ 10	Długość pakietu (*ang. Packet length*)

Typ 11	DSCP
Typ 12	Kodowanie fragmentów (*ang. Fragment Encoding*)

Tabela 3 pokazuje rozszerzone wartości community zdefiniowane w celu określenia różnych typów działań [RFC5575] [RFC5575bis] wymaganych w systemie AS wyższego rzędu (upstream AS).

Tabela 3: Wartości rozszerzonego community zdefiniowane we Flowspec dla wskazania różnych rodzajów działania

Typ	Rozszerzone community	Kodowanie
0x8006	Traffic-rate (ustawienie na 0 do odrzucenia całego ruchu)	2-bajtowe as#, 4-bajtowe float
0x8007	Traffic-action (sampling)	Bitmask
0x8008	Redirect to VRF (route target)	6-bajtowy cel trasy
0x8009	Traffic-marking	Wartość DsCp

W powyższej tabeli VRF oznacza wirtualny routing i przekierowywanie (*ang. virtual routing and forwarding*), a DSCP oznacza punkt kodowy różnicowania usług (*ang. differentiated services code point*). Flowspec ułatwia elastyczną specyfikację i komunikację (przez downstream AS) reguł i działań ograniczających DDoS, które mają być wykonywane na routerach brzegowych w upstream AS.

Zalecenie dot. bezpieczeństwa 60: Routery brzegowe powinny być wyposażone w funkcję filtrowania zdalnie wyzwalanym blackholingiem w oparciu o adres docelowy (D/RTBH) i filtrowania zdalnie wyzwalanym blackholingiem w oparciu o adres źródłowy (S/RTBH).

Zalecenie dot. bezpieczeństwa 61: Routery brzegowe powinny być przystosowane do korzystania ze specyfikacji przepływu BGP (Flowspec) w celu ułatwienia ograniczania ataków DoS/DDoS (w koordynacji między autonomicznymi systemami upstream i downstream).

Zalecenie dot. Bezpieczeństwa 62: Routery brzegowe w systemie autonomicznym zapewniające filtrowanie RTBH powinny mieć politykę ruchu wejściowego w kierunku klientów RTBH, akceptującą trasy bardziej specyficzne niż /24 w IPv4 i /48 w IPv6. Ponadto routery brzegowe powinny akceptować bardziej specyficzną trasę (w przypadku D/RTBH) tylko wtedy, gdy jest ona podciągnięta pod mniej specyficzną trasę, którą klient może ogłosić jako standardową politykę (tj. mniej specyficzna trasa ma zarejestrowany wpis IRR i/lub ROA). Ponadto routery brzegowe nie powinny odrzucać bardziej specyficznych ogłoszeń tras związanych z RTBH od klientów, nawet jeśli sprawdzanie pochodzenia BGP może oznaczać je jako „Invalid".

Zalecenie dot. Bezpieczeństwa 63: AS klienta powinien zapewnić, że trasy zgłoszone do filtrowania RTBH mają community: NO_EXPORT, NO_ADVERTISE lub podobne.

Zalecenie dot. Bezpieczeństwa 64: Dostawca usług internetowych świadczący klientom usługę filtrowania RTBH musi mieć politykę ruchu wychodzącego, która odrzuca trasy z tagami community i przeznaczonymi do wyzwalania filtrowania RTBH. Jest to dodatkowe zabezpieczenie na wypadek niepowodzenia tagowania NO_EXPORT, NO_ADVERTISE lub podobnego.

Zalecenie dot. Bezpieczeństwa 65: Dostawca usług internetowych świadczący klientom usługę filtrowania RTBH musi mieć politykę ruchu wychodzącego odrzucającą prefiksy dłuższe niż spodziewane. Zapewnia to dodatkowe bezpieczeństwo w przypadku niepowodzenia tagowania NO_EXPORT, NO_ADVERTISE lub podobnego.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[43]	
NSC199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[43] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

PUBLIKACJE ANGLOJĘZYCZNE[44]	
[Acunetix]	"Prevention of NTP Reflection DDoS attacks based on CVE-2013-5211," Acunetix blog, September 2014. http://www.acunetix.com/blog/articles/ntp-reflection-ddos-attacks/
[Adalier1]	M. Adalier, K. Sriram, O. Borchert, K. Lee, and D. Montgomery, "High Performance BGP Security: Algorithms and Architectures", North American Network Operators Group (NANOG 69), Washington D.C, February 2017. https://archive.nanog.org/sites/default/files/1_Sriram_High_Performance_Bgp_v1.pdf (slides) https://www.youtube.com/watch?v=Yp03po5WJP0 (video)
[Adalier2]	M. Adalier, "Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256," NIST Workshop on ECC Standards, June 2015. http://csrc.nist.gov/groups/ST/ecc-workshop-2015/papers/session6-adalier-mehmet.pdf
[Akamai]	J. Artega and W. Mejia, "CLDAP Reflection DDoS," Akamai Threat Advisory, April 2017. https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf
[APNIC1]	G. Michaelson, "MyAPNIC RPKI service now supports AS0 ROA creation," APNIC technical note online, November 2018. https://blog.apnic.net/2018/11/09/myapnic-rpki-service-now-supports-as0-roa-creation/
[Arbor]	"NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report" (2018). https://pages.arbornetworks.com/rs/082-KNA-087/images/f3th_Worldwide_Infrastructure_Security_Report.pdf

[44] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

[Arbor2]	"NETSCOUT Arbor's 14th Annual Worldwide Infrastructure Security Report" (2019). https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf
[ARIN1]	"Using RPKI at ARIN to certify resources," ARIN online. https://www.arin.net/resources/rpki/using_rpki.html#hosted
[ARIN2]	M. Kosters, "ARIN Provisioning in RPKI," NANOG 67, June 2016. https://archive.nanog.org/sites/default/files/Kosters.pdf
[ARTEMIS]	Automatic and Real-Time dEtection and Mitigation (ARTEMIS) http://www.inspire.edu.gr/artemis/
[BCP38]	P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," BCP 38 (RFC 2827), May 2000. https://tools.ietf.org/html/bcp38
[BCP84]	F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," BCP 84 (RFC 3704), March 2004, https://tools.ietf.org/html/bcp84
[BGPmon]	BGPmon: https://bgpmon.net/
[BGPStream]	BGPStream: https://bgpstream.caida.org/
[Bjarnason]	S. Bjarnason, "Withstanding the Infinite: DDoS Defense in the Terabit Era," Presentation at NANOG-74, October 2018. https://pc.nanog.org/static/published/meetings/NANOG74/1789/20181001_Bjarnason_WithstandingThe_Infinite_v1.pdf
[Botnet-Roadmap]	"A Road Map Toward Resilience Against Botnets," Joint US DOC/DHS report, November 2018. https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[Chung]	T. Chung, et al., "RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins," Proceedings of the Internet Measurement Conference, Pages 406-419, October 2019. https://dl.acm.org/citation.cfm?id=3355596
[Cisco1]	"BGP—Origin AS Validation," http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/irg-origin-as.pdf
[Cisco2]	"Understanding Unicast Reverse Path Forwarding," Cisco blog, http://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html
[Cisco3]	"Unicast reverse path forwarding enhancements for the internet service provider—internet service provider network edge," Cisco WP, http://www.cisco.com/c/dam/en_us/about/security/intelligence/urpf.pdf
[Cisco4]	"Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide, Release 5.2.x - Chapter: Implementing BGP Flowspec," http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html
[Comcast]	"Comcast network management: Preventing Network Spoofing," March 2014, http://networkmanagement.xfinity.com/index.php/faqs-on-preventing-network-spoofing
[Compton]	R. Compton, T. Bowlby, T. Harris, P. Lotia, "eBGP Flowspec Peering for DDoS Mitigation," NANOG 75, February 2019. https://pc.nanog.org/static/published/meetings/NANOG75/1887/20190219_Compton_Ebgp_Flowspec_Peering_v1.pdf
[CSDE]	"Cyber Crisis: Foundations of Multi-Stakeholder Coordination," Council for Secure Digital Economy (CSDE) report (2019). https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf

[CSRIC4-WG5]	"Remediation of Server-Based DDoS Attacks," CSRIC IV Working Group 5 final report, September 2014. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V_11.pdf
[CSRIC4-WG6]	"Long-Term Core Internet Protocol Improvements," CSRIC IV Working Group 6 presentation, September 2014. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG6_Presentation_09242014.pdf
[CSRIC6-WG3]	"Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols," CSRIC VI Working Group 3 final report, March 2019. https://www.fcc.gov/files/csric6wg3finalreport030819pdf
[CVE-2013-5211]	"Vulnerability summary for CVE-2013-5211," (for vulnerability related to monlist feature in NTP), National Vulnerability Database, September 27, 2016. https://nvd.nist. gov/vuln/detail/CVE-2013-5211
[Cymru-bogon]	"Bogon route server project: Bogons via BGP" http://www.team-cymru.org/bogon-reference-bgp.html
[Cymru-UTRS]	Unwanted traffic removal service (UTRS), Team Cymru blog, http://www.team-cymru.com/utrs.html
[DOC-Botnet]	U.S. Department of Commerce, U.S. Department of Homeland Security, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," May 22, 2018. https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final
[DOCSIS]	"DOCSIS® 3,1 Technology", CableLabs, https://www.cablelabs.com/technologies/docsis-3-1.

[EFP-uRPF]	K. Sriram, D. Montgomery, and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Filtering," IETF Internet Draft (soon to be RFC), August 2019. https://datatracker.ietf.org/doc/draft-ietf-opsec-urpf-improvements/
[ENISA]	"7 Steps to shore up the Border Gateway Protocol (BGP)", the EU Cybersecurity Agency, May 2019.
[Firmin]	F. Firmin, "The Evolved Packet Core," 3GPP The Mobile Broadband Standard.https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core
[FISMA2002]	Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat. 2946. http://www. gpo. gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.
FISMA	Federal Information Security Modernization Act L. 113-283, 128 Stat. 3073. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.
[FORT]	FORT RPKI validator. https://github.com/NICMx/FORT-validator
[Gao-Rexford]	Freedman, M., „Interdomain Routing Policy", Princeton University COS 461 Lecture Notes; Slides 25-27, Spring 2011, http://www. cs.princeton.edu/courses/archive/ spr11/cos461/docs/ lec17-bgp-policy.ppt
[goBGP]	Use of Resource Public Key Infrastructure (RPKI) server to do Origin AS Validation in goBGP. https://github.com/osrg/gobgp/blob/master/docs/sources/rpki.md
[HelpNet]	"DNS amplification attacks double in Q1 2018," Help Net Security blog, June 2018. https://www.helpnetsecurity.com/2018/06/14/dns-amplification-attacks-q1-2018/

[Hinze]	N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T.C. Schmidt, M. Wahlisch, „On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources: ISP and IXP," In: Proc. of ACM SIGCOMM. Poster Session, pp. 57--59, New York, NY, USA: ACM, August 2018. http://www.caida.org/publications/papers/2018/potential_bgp_flowspec/potential_bgp_flowspec.pdf
[Huston2011]	G. Huston and R. Bush, "Securing BGP," The Internet Protocol Journal, Volume 14, No. 2, June 2011. http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-52/142-bgp.html
[Huston2012]	G. Huston, "Leaking Routes," Asia Pacific Network Information Centre (APNIC) Blog, March 2012, http://labs.apnic.net/blabs/?p=139/
[Huston2016]	G. Huston, "Taking a Closer Look at the Recent DDoS Attacks and What It Means for the DNS," CircleID Blog, October 2016. http://www.circleid.com/posts/20161026_closer_look_at_recent_ddos_attacks_and_what_it_means_for_dns/
[IANA-ASN-sp]	"Special-Purpose Autonomous System (AS) Numbers" IANA web page. https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml
[IANA-v4-r]	"IANA IPv4 Address Space Registry," IANA web page. http://www.iana.org/assignments/ipv4-address-space
[IANA-v6-r]	"Internet Protocol Version 6 Address Space," IANA web page. http://www.iana.org/assignments/ipv6-address-space
[IANA-v4-sp]	"IANA IPv4 Special-Purpose Address Registry," IANA web page. https://www.iana.org/assignments/iana-ipv4-special-registry
[IANA-v6-sp]	"IANA IPv6 Special-Purpose Address Registry," IANA web page. http://www.iana.org/assignments/iana-ipv6-special-registry

[IETF-GROW]	IETF Global Routing Operations (GROW) Working Group https://datatracker.ietf.org/wg/grow/documents/
[IETF-IDR]	IETF Inter-Domain Routing (IDR) Working Group https://datatracker.ietf.org/wg/idr/documents/
[IETF-OPSEC]	IETF Operational Security Capabilities for IP Network Infrastructure (OPSEC) Working Group https://datatracker.ietf.org/wg/opsec/documents/
[IETF-SIDR]	IETF Secure Inter-Domain Routing (SIDR) Working Group https://datatracker.ietf.org/wg/sidr/documents/
[IETF-SIDROPS]	IETF Secure Inter-Domain Routing Operations (SIDROPS) Working Group https://datatracker.ietf.org/wg/sidrops/documents/
[ISC1]	"A Quick Introduction to Response Rate Limiting," ISC Knowledge Base blog. https://kb.isc.org/article/AA-01000/0/A-Quick-Introduction-to-Response-Rate-Limiting.html
[ISC2]	"A Chargen-base DDoS? Chargen still a thing?" ISC blog, https://isc.sans.edu/forums/diary/A+Chargenbased+DDoS+Chargen+is+still+a+thing/15647
[ISOC]	P. Vixie (Ed.), "Addressing the challenge of IP spoofing," ISOC report, September 2015. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf
[ISTR-2015]	*Internet Security Threat Report 2015*, *Volume 20*, Symantec Corporation, Mountain View, CA, April 2015. https://www.symantec.com/content/en/us/entergrise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

[ISTR-2016]	*Internet Security Threat Report 2016, Volume 21*, Symantec Corporation, Mountain View, CA, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-en.pdf
[ISTR-2017]	*Internet Security Threat Report 2017, Volume 22*, Symantec Corporation, Mountain View, CA, April 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-en.pdf
[Juniper1]	"Example: Configuring Origin Validation for BGP," Juniper blog, http://www.juniper.net/techpubs/en_US/junos12.2/topics/topic-map/bgp-origin-as-validation. html
[Juniper2]	"Configuring Unicast RPF," Juniper blog, https://www.juniper.net/documentation/en_US/junos14.2/topics/usage-guidelines/interfaces-configuring-unicast-rpf.html
[Juniper3]	"Example: Configuring Unicast Reverse-Path-Forwarding Check," Juniper blog, http://www.juniper.net/documentation/en_US/junos15.1/topics/topic-map/unicast-rpf.html
[Juniper4]	"Example: Enabling BGP to Carry Flow-Specification Routes," Juniper TechLibrary. https://www.juniper.net/documentation/en_US/junos12.3/topics/example/routing-bgp-flow-specification-routes.html
[Juniper5]	"Creating Unique VPN Routes Using VRF Tables," May 2019 https://www.juniper.net/documentation/en_US/junos/topics/topic-map/l3-vpns-routes-vrf-tables.html#id-understanding-virtual-routing-and-forwarding-tables

[Kapela-Pilosov]	A. Pilosov and T. Kapela, „Stealing the Internet: An Internet-Scale Man in the Middle Attack", 16th Defcon Conference, August 2008, https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf.
[Levy1]	M. Levy, "RPKI - The required cryptographic upgrade to BGP routing," Cloudflare blog, September 2018. https://blog.cloudflare.com/rpki/
[Levy2]	N. Levy, D. Smith, and J. Schiel, "Bi-Lateral Security Management Framework (a.k.a. DDoS peering)," NANOG 71, October 2017. https://pc.nanog.org/static/published/meetings/NANOG71/1447/20171003_Levy_Operationalizing_Isp_v2.pdf
[Luckie]	M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy, "AS Relationships, Customer Cones, and Validation," Proceedings of the 2013 ACM Internet Measurement Conference (IMC), DOI 10.1145/2504730.2504735, October 2013. http://www.caida.org/~amogh/papers/asrank-IMC13.pdf
[Luckie2]	M. Luckie, R. Beverly, R. Koga, K. Keys, J. Kroll, and k. claffy, „Network Hygiene, Incentives, and Regulation: Deployment of source address validation in the Internet", in ACM Computer and Communications Security (CCS), Nov 2019. https://dl.acm.org/citation.cfm?id=3354232
[MANRS]	"Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide," Published by the Internet Society (ISOC), retrieved October 2019. https://www.manrs.org/isps/guide/
[MANRS2]	"MANRS Observatory," Monitoring data published by Internet Society (ISOC), retrieved October 2019. https://observatory.manrs.org/#/overview
[maxlength]	Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, and B. Maddison, "The use of maxlength in the RPKI," IETF Internet Draft, April 2019. https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpkimaxlen/
[Merit-RADb]	„Merit RADb" (Merit Network Inc.) http://www.radb.net

[Mirai1] "Mirai: what you need to know about the botnet behind recent major DDoS attacks," Symantec Security Response, October 27, 2016. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

[Mirai2] "Dyn Analysis Summary of Friday October 21 Attack," Dyn Company News, October 26, 2016.https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[Murphy] S. Murphy, "RPKI Tutorial: Routing Security and RPKI", NANOG on the Road (NOTR), St. Louis, MO, November, 2015 https://www.nanog.org/sites/default/files/04-Murphy-StLouis.pdf

[NABCOP] "DDoS-DoS-attack-BCOP," North American BCOP, http://nabcop.org/index.php/DDoS-DoS-attack-BCOP

[Naik] A. Naik, "Internet Vulnerability Takes Down Google," ThousandEyes report, November 2018.https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/

[NANOG] "Practical BGP Origin Validation using RPKI: Vendor Support, Signing and Validation Services, and Operational Experience,"," NANOG Track (multiple presentations) at NANOG 67, Chicago, IL, June 2016. https://archive.nanog.org/meetings/nanog67/agenda

[NANOG-list] "Intra-AS messaging for route leak prevention," NANOG Email List - Discussion Thread, June 2016. http://mailman.nanog.org/pipermail/nanog/2016-June/thread.html#86348

[NCCoE-sidr] W. Haag, D. Montgomery, W.C. Barker, A. Tan, "Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation, Volume B," NIST Special Publication (SP) 1800-14B, August 2018.https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800- 14b-draft.pdf

[NIST-CSF]	Cybersecurity Framework, National Institute of Standards and Technology [Web site],http://www.nist.gov/cyberframework/
[NIST-RIDR]	"Robust Inter-Domain Routing," NIST RIDR project. https://www.nist.gov/programs-projects/robust-inter-domain-routing
[NIST-RPKI]	"RPKI Deployment Monitor," NIST's online monitor with Global and Regional views. https://rpki-monitor.antd.nist.gov/
[NIST-SRx]	BGP Secure Routing Extension (BGP-SRx): Open source Origin Validation and BGPsec Path Validation implementations in Quagga. https://www-x.antd.nist.gov/bgpsrx/
[NSA-BGP]	"A guide to Border Gateway Protocol (BGP) Best Practices," NSA Technical Report, September 2018. https://apps.nsa.gov/iaarchive/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm
[OctoRPKI]	OctoRPKI: Cloudflare's RPKI Validator. https://github.com/cloudflare/cfrpki#octorpki
[Parsons1]	"Secure Your Routing Infrastructure," Parsons blog. http://www.securerouting.net/
[Parsons2]	Open source Origin Validation and BGPsec Path Validation implementations in BIRD, Parsons blog. http://www.securerouting.net/tools/bird/
[Patel]	K. Patel, "Cisco's Origin Validation Implementation," NANOG 67, June 2016. https://www.nanog.org/sites/default/files/Patel.pdf
[PEO-13800]	U.S. Presidential Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[Phuntsho]	T. Phuntsho, "How to install an RPKI validator," RIPE NCC blog. https://labs.ripe.net/Members/tashi_phuntsho_3/how-to-install-an-rpki-validator
[Quilt]	"The Quilt security cookbook," published by the Quilt community, https://www.nitrd.gov/nitrdgroups/images/d/db/Quilt-Network-Security-Cookbook-v7.pdf
[Redbarn]	"Response Rate Limiting in the Domain Name System (DNS RRL)," Redbarn blog. http://www.redbarn.org/dns/ratelimits
[RFC2725]	C. Villamizar, C. Alaettinoglu, D. Meyer, S. Murphy, "Routing Policy System Security," IETF RFC 2725, December 1999. https://tools.ietf.org/html/rfc2725
[RFC3882]	D. Turk, "Configuring BGP to Block Denial-of-Service Attacks," IETF RFC 3882, September 2004 https
[RFC4012]	L. Blunk, J. Damas, F. Parent, and A. Robachevsky, "Routing Policy Specification Language next generation (RPSLng)," IETF RFC 4012, March 2005 https
[RFC4036]	W. Sawyer, "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modem Termination Systems for Subscriber Management", RFC 4036, DOI 10.17487/RFC4036, April 2005 https
[RFC4271]	Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF RFC 4271, January 2006 https
[RFC4364]	E. Rosen and Y. Rekhter, „BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006. https://www.rfc-editor.org/info/rfc4364

[RFC5280]	D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile," IETF RFC 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt.
[RFC5575]	P. Marques et al., "Dissemination of Flow Specification Rules," IETF RFC 5575, August 2009 https
[RFC5575bis]	C. Loibl, S. Hares, R. Raszuk, D. McPherson, and M. Bacher, "Dissemination of Flow Specification Rules," IETF I.D. draft-ietf-idr- rfc5575bis (work in progress), November 2019. https://datatracker. ietf. org/doc/draft-ietf-idr-rfc5575bis/
[RFC5635]	W. Kumari and D. McPherson, „Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, DOI 10.17487/RFC5635, August 2009 https
[RFC5802]	V. Gill, J. Heasley, D. Meyer, P. Savola, Ed., C. Pignataro, "The Generalized TTL Security Mechanism, GTSM)," IETF RFC 5082, October 2007. https://tools.ietf.org/html/rfc5082
[RFC6092]	J. Woodyatt, "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service," IETF RFC 6092, January 2011. https://tools.ietf.org/html/rfc6092
[RFC6472]	W. Kumari and K. Sriram, "Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP," BCP 172 (RFC 6472), December 2011. https://tools.ietf.org/html/rfc6472
[RFC6480]	M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," RFC6480, February 2012. https://tools.ietf.org/html/rfc6480
[RFC6481]	G. Huston, R. Loomans, and G. Michaelson, „A Profile for Resource Certificate Repository Structure", RFC 6481, February 2012. https://tools.ietf.org/html/rfc6481

[RFC6482]	M. Lepinski, S. Kent, and D. Kong, „A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012. https://tools.ietf.org/html/rfc6482
[RFC6483]	G. Huston and G. Michaelson, „Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs) „, RFC 6483, February 2012. https://tools.ietf.org/html/rfc6483
[RFC6487]	G. Huston, G. Michaelson, and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," RFC 6487, February 2012. https://tools.ietf.org/html/rfc6487
[RFC6492]	G. Huston, R. Loomans, B. Ellacott, and R. Austein, "A Protocol for Provisioning Resource Certificates," RFC 6492, February 2012. https://tools.ietf.org/html/rfc6492
[RFC6810]	R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," RFC 6810, January 2013. https://tools.ietf.org/html/rfc6810
[RFC6811]	P. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein, "BGP Prefix Origin Validation," IETF RFC 6811, January 2013. https://tools.ietf.org/pdf/rfc6811.pdf
[RFC7318]	A. Newton and G. Huston, "Policy Qualifiers in Resource Public Key Infrastructure (RPKI) Certificates," RFC 7318, July 2014. https://tools.ietf.org/html/rfc7318
[RFC7353]	S. Bellovin, R. Bush, and D. Ward, "Security Requirements for BGP Path Validation," IETF RFC 7353, August 2014. https://tools.ietf.org/html/rfc7353
[RFC7382]	S. Kent, D. Kong, and K. Seo, "Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)," IETF RFC 7382, April https://tools.ietf.org/html/rfc7382

[RFC7454]	J. Durand, I. Pepelnjak, and G. Doering, "BGP Operations and Security," IETF RFC 7454, February 2015. https://tools.ietf. org/html/rfc7454
[RFC7674]	J. Haas, "Clarification of the Flowspec Redirect Extended Community," IETF RFC 7674, October 2015. https://tools.ietf.org/html/rfc7674
[RFC7908]	K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, and B. Dickson, „Problem Definition and Classification of BGP Route Leaks", RFC 7908, June 2016. https://tools.ietf.org/html/rfc7908
[RFC7909]	R. Kisteleki and B. Haberman, "Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures," IETF RFC 7909, June 2016. https://tools.ietf.org/html/rfc7909
[RFC7935]	G. Huston and G. Michaelson, "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure," IETF RFC 7935, August 2016. https://tools.ietf.org/html/rfc7935
[RFC7999]	T. King, et al., "BLACKHOLE Community," IETF RFC 7999, October https://tools.ietf.org/html/rfc7999
[RFC8182]	T. Bruijnzeels, O. Muravskiy, B. Webre, and R. Austein, "RPKI Repository Delta Protocol (RRDP)," IETF RFC 8182, July 2017. https://tools.ietf.org/html/rfc8182
[RFC8205]	M. Lepinski (Ed.) and K. Sriram (Ed.), "BGPsec Protocol Specification," IETF RFC 8205, September 2017. https://tools.ietf.org/html/rfc8205
[RFC8210]	R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1," IETF RFC 8210, September 2017. https://tools.ietf.org/html/rfc8210
[RFC8212]	J. Mauch, J. Snijders, and G. Hankins, "Default External BGP (EBGP) Route Propagation Behavior without Policies", IETF RFC 8212, DOI 10.17487/RFC8212, July 2017. https://www.rfc-editor.org/info/rfc8212

[RFC8374]	K. Sriram (Ed.), "BGPsec Design Choices and Summary of Supporting Discussions," IETF RFC 8374, April 2018. https://tools.ietf.org/html/rfc8374
[RFC8608]	S. Turner and O. Borchert, "BGPsec Algorithms, Key Formats, & Signature Formats," IETF RFC 8608, September 2017. https://tools.ietf.org/html/rfc8608
[RIPE1]	RIPE NCC Resource Certification: Using the RPKI System, https://www.ripe.net/manage-ips-and-asns/resource-management/certification/using-the-rpki-system
[RIPE2]	RIPE NCC RPKI Validator,https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
[RIPE3]	"Router Configuration with JunOS and Cisco IOS," RIPE NCC blog, https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration
[RIPE-399]	P. Smith, R. Evans, and M. Hughes, „RIPE-399 - RIPE Routing Working Group Recommendations on Route Aggregation", December 2006. https://www.ripe.net/publications/docs/ripe-399
[RIPE-532]	P. Smith and R. Evans, „RIPE-532 - RIPE Routing Working Group Recommendations on IPv6 Route Aggregation", November 2011. https://www.ripe.net/publications/docs/ripe-532
[RouteLeak1]	K. Sriram (Ed.) and A. Azimov (Ed.), "Methods for Detection and Mitigation of BGP Route Leaks", IETF Internet Draft, July 2019. https://datatracker.ietf.org/doc/draft-ietf-grow-route-leak-detection-mitigation/
[RouteLeak2]	A. Azimov, E. Bogomazov, R. Bush, K. Patel, and K. Sriram, „Route Leak Prevention using Roles in Update and Open Messages", IETF Internet Draft, July 2019. https://datatracker.ietf.org/doc/draft-ietf-idr-bgp-open-policy/

[RouteLeak3]	K. Sriram (Ed.), "Design Discussion of Route Leaks Solution Methods", IETF Internet Draft, August 2019. https://datatracker.ietf.org/doc/draft-sriram-idr-route-leak-solution-discussion/
[Routinator]	Routinator: NLNetLabs' RPKI validator. https://nlnetlabs.nl/projects/rpki/routinator/
[Rsync]	Wiki page on the Rsync protocol. https://en.wikipedia.org/wiki/Rsync
[Rsync-RPKI]	S. Kent and K. Sriram, „RPKI Rsync Download Delay Modeling," Presented at the IETF-86, IETF SIDR WG Meeting, March 2013. https://www.ietf.org/proceedings/86/slides/slides-86-sidr-1.pdf
[RTRlib]	"An open-source C implementation of the RPKI/Router Protocol client," https://github.com/rtrlib and http://www.mi.fu-berlin.de/en/inf/groups/ilab/software/index.html
[Ryburn]	J. Ryburn, "DDoS Mitigation using BGP Flowspec," NANOG 63, February 2015. https://archive.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf
[Scudder]	J. Scudder, "RPKI on Juniper Routers," NANOG 67, June 2016. https://www.nanog.org/sites/default/files/Scudder.pdf
[SP800-53]	Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) 800-53 Revision 4, April 2013 (includes updates as of 01-22-2015). https://doi.org/10.6028/NIST.SP.800-53r4
[SP800-54]	Kuhn DR, Sriram K, Montgomery D (2007) Border Gateway Protocol Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-54. https://doi.org/10.6028/NIST.SP.800-54

[Spoofer]	CAIDA Spoofer Project: Assessment and reporting on the deployment of source address validation (SAV) best anti-spoofing practices. https://www.caida.org/projects/spoofer/
[Sriram1]	K. Sriram, D. Montgomery, and R. Bush, "RIB Size and CPU Workload Estimation for BGPSEC," Presentation at the IETF-91 Joint IDR/SIDR WG Meeting, November 2014. http://www.ietf.org/proceedings/91/slides/slides-91-idr-17.pdf
[Sriram2]	V.K. Sriram and D. Montgomery, "Design and analysis of optimization algorithms to minimize cryptographic processing in BGP security protocols," Computer Communications, volume 106, pages 75-85, July https://doi.org/10.1016/j.comcom.2017.03.007
[SWIP]	S. Whipple, "The SWIP Template Tutorial," ARIN VII, April 2001. https://www.arin.net/vault/participate/meetings/reports/ARIN_VII/PDF/tutorials/swip_arin.pdf
[Symantec]	C. Wueest, "Denial-of-service attacks - short but strong: DDoS amplification attacks continue to increase as attackers experiment with new protocols," Symantec Blog, October 2014. http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong
[TA14-017A]	"UDP-Based Amplification Attacks," US-CERT alert TA14-017A, January 17, 2014. https://www.us-cert.gov/ncas/alerts/TA14-017A
[TA16-288A]	"Heightened DDoS Threat Posed by Mirai and Other Botnets," US-CERT alert TA16-288A, November 30, 2016. https://www.us-cert.gov/ncas/alerts/TA16-288A
[TCP-UDP-port]	"List of TCP and UDP ports," https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.
[ThousandEyes]	ThousandEyes: BGP Route Monitoring https://www.thousandeyes.com/solutions/bgp-and-route-monitoring

[Toonk-A]	Toonk, A., „What caused the Google service interruption", BGPMON Blog, March 2015, http://www.bgpmon.net/what-caused-the-google-service-interruption/.
[Toonk-B]	Toonk, A., „Massive route leak causes Internet slowdown", BGPMON Blog, June 2015,http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/.
[Verisign1]	"Verisign Releases Q4 2016 DDoS Trends Report: 167% Increase in Average Peak Attack from 2015 to 2016," CircleID blog post, February 2017. http://www.circleid.com/posts/20170214_verisign_releases_q4_2016_ddos_trends_report_167_increase/
[Verisign2]	"Distributed Denial of Service Trends Report" by Verisign, Published quarterly.http://www.verisign.com/en_US/security-services/ddos-protection/ddo s-report/index.xhtml
[Winward]	R. Winward, "Mirai - Inside of an IoT Botnet," NANOG 69, February 2017. https://www.nanog.org/sites/default/files/1_Winward_Mirai_The_Rise.pdf
[Wishnick]	D. Wishnick and C. Yoo, "Overcoming Legal Barriers to RPKI Adoption," Presented at NANOG 74, October 2018. https://pc.nanog.org/static/published/meetings//NANOG74/daily/day_2.html#talk_1767
[White]	R. White, "Rethinking Path Validation," NANOG 66, February 2016. https://www.nanog.org/sites/default/files/White Rethinking Bgp Path.pdf
[Yoo]	C. Yoo and D. Wishnick, "Lowering Legal Barriers to RPKI Adoption," University of Pennsylvania Law School publication, January 2019. https://scholarship.law.upenn.edu/faculty_scholarship/2035/
[Zmijewski]	E. Zmijewski, „Indonesia Hijacks the World", Dyn Research/Renesys Blog, April 2014, http://research. dyn.com/2014/04/indonesia-hijacks-world

ZAŁĄCZNIK A — JEDNOLITA LISTA REKOMENDACJI W ZAKRESIE. BEZPIECZEŃSTWA INFORMACJI

Tabela 4 przedstawia wykaz rekomendacji dotyczących bezpieczeństwa zawartych w różnych działach dokumentu NSC 800-189. Jeśli zaznaczona jest kolumna „Organizacja", oznacza to, że zalecenia dotyczące bezpieczeństwa powinny być brane pod uwagę przy implementacji w systemach autonomicznych (AS) organizacji i dostawcy usług hostowanych — w niektórych przypadkach działanie (działania) do wykonania przez operatora AS, a w innych przypadkach funkcja (funkcje), które powinny być dostępne w routerach BGP. Podobne stwierdzenie ma zastosowanie do dostawców usług internetowych, gdy zaznaczona jest kolumna „ISP". Kolumna „Serwery otwarte" dotyczy dostawców otwartych usług internetowych, takich jak DNS, DNSSEC lub NTP. Gdy organizacja zleca usługi na zewnątrz, wówczas funkcja/usługa odpowiadająca zaleceniu dotyczącego bezpieczeństwa, które ma do nich zastosowanie, miałaby z kolei zastosowanie do jego dostawcy usług hostowanych. Organizacja powinna zawsze rozważyć (w swojej umowie serwisowej), czy jego tranzytowy ISP spełnia zalecenia bezpieczeństwa, które są sprawdzane w kolumnie ISP. W Tabeli 4 nie ma kolumny odpowiadającej internetowemu punktowi wymiany (*ang. internet exchange point - IXP*), ale zalecenia dotyczące bezpieczeństwa BGP (płaszczyzna sterowania) dla ISP mają również zastosowanie do nieprzezroczystych IXP (tj. IXP, które wprowadzają swoje ASN do ścieżki AS i obsługują BGP).

Tabela 4: Jednolita lista zaleceń dot. bezpieczeństwa

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Sprawdzanie pochodzenia BGP (BGP-OV)			
Zalecenie dot. bezpieczeństwa 1: Wszystkie internetowe zasoby numerów (np. bloki adresowe i numery AS) powinny być objęte odpowiednią umową o świadczenie usług rejestracyjnych z RIR, a wszystkie informacje dotyczące punktów kontaktowych (PoC) powinny być aktualne. Szczegółowość takich rejestracji powinna odzwierciedlać wszystkie subalokacje do podmiotów (np. jednostek w ramach organizacji macierzystej, oddziałów), które obsługują własne usługi sieciowe (np. dostęp do Internetu, DNS).	X	X	
Zalecenie dot. bezpieczeństwa 2: W przypadku rejestracji bloku adresowego (NetRange) w ARIN, powinien być uwzględniony źródłowy system autonomiczny (origin AS). Zob. https://whois.arin.net/rest/net/NET-128-3-0-0-1/pft?s=128.3.0.	X	X	
Zalecenie dot. bezpieczeństwa 3: Obiekty tras odpowiadające trasom BGP pochodzącym z AS powinny być rejestrowane i aktywnie utrzymywane w IRR odpowiednim dla RIR. Organizacje powinny zapewnić istnienie odpowiednich informacji IRR dla całej przestrzeni adresowej IP wykorzystywanej bezpośrednio oraz przez ich systemy i usługi IT zlecane na zewnątrz.	X	X	
Zalecenie dot. bezpieczeństwa 4: Posiadacze zasobów numerów internetowych z prefiksami IPv4/IPv6 i/lub numerami AS (ASN) powinni uzyskać dla swoich zasobów certyfikat(y) RPKI.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 5: Dostawcy tranzytowi powinni świadczyć usługi, za pomocą której tworzą, publikują i zarządzają podrzędnymi certyfikatami zasobów dla przestrzeni adresowej i/lub numerów ASN przydzielonych ich klientom. Uwaga: Obecnie usługi RPKI oparte na modelu hostowanym i oferowane przez RIR występują powszechnie. To zalecenie dot. bezpieczeństwa może być wdrożone w modelu hostowanym lub delegowanym w oparciu o umowy usług z klientami.		X	
Zalecenie dot. bezpieczeństwa 6: Posiadacze zasobów powinni rejestrować ROA w globalnej RPKI dla wszystkich prefiksów, które są ogłaszane lub mają być rozgłaszane w publicznym Internecie.	X	X	
Zalecenie dot. bezpieczeństwa 7: Każdy dostawca usługi tranzytowej powinien świadczyć usługę, w której tworzy, publikuje i utrzymuje ROA dla prefiksów przydzielonych swoim klientom. Alternatywnie, w ramach usługi, klienci mogą tworzyć, publikować i utrzymywać swoje ROA w repozytorium prowadzonym przez dostawcę tranzytowego. Uwaga: To zalecenie dot. bezpieczeństwa może być wdrożone w modelu hostowanym lub delegowanym w oparciu o umowy usług z klientami.		X	
Zalecenie dot. bezpieczeństwa 8: Dla prefiksu, który jest ogłoszony (lub który ma być ogłoszony) jest typu multi-homed i pochodzi z wielu systemów autonomicznych, należy zarejestrować jedną ROA na każdy inicjujący system autonomiczny (ewentualnie w połączeniu z innymi prefiksami, które również pochodzą z tego samego systemu autonomicznego).	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 9: Gdy dostawca usług internetowych lub organizacja posiada wiele prefiksów, które obejmują prefiksy mniej i bardziej specyficzne, powinien przed utworzeniem ROA dla podciągnięcia prefiksów mniej specyficznych upewnić się, że bardziej specyficzne prefiksy mają ROA.	X	X	
Zalecenie dot. bezpieczeństwa 10: Dostawca usług internetowych powinien upewnić się, że bardziej specyficzne prefiksy ogłoszone z jego stożka klientów mają ROA przed utworzeniem własnych ROA w celu podciągnięcia mniej specyficznych prefiksów.		X	
Zalecenie dot. bezpieczeństwa 11: Dostawca usług internetowych lub organizacja powinien stworzyć ROA AS0 dla każdego prefiksu, który obecnie nie jest ogłaszany w publicznym Internecie. Jednak należy to zrobić dopiero po upewnieniu się, że ROA istnieją dla wszelkich bardziej specyficznych prefiksów podciągniętych pod ten prefiks, które są ogłaszane lub mają być ogłaszane.	X	X	
Zalecenie dot. bezpieczeństwa 12: Router BGP nie powinien wysyłać aktualizacji zawierających AS_SET lub AS_CONFED_SET (zgodnie z BCP 172 [RFC6472]).	X	X	
Zalecenie dot. bezpieczeństwa 13: Dostawcy usług internetowych i organizacje obsługujące routery BGP powinny również obsługiwać jedną lub więcej pamięci podręcznych sprawdzających RPKI.	X	X	
Zalecenie dot. bezpieczeństwa 14: Router BGP powinien utrzymywać aktualną białą listę składającą się z {prefix, maxlength, origin ASN}, która pochodzi z ważnych ROA w globalnej RPKI. Router powinien wykonywać BGP-OV.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 15: W sytuacji częściowego/stopniowego wdrożenia RPKI, dopuszczalne pary {prefix, origin ASN} do przeprowadzenia BGP-OV powinny być generowane poprzez przyjęcie zestawienia takich danych uzyskanych z ROA, danych IRR oraz umów z klientami.	X	X	
Zalecenie dot. bezpieczeństwa 16: Wyniki BGP-OV powinny być włączone do lokalnych decyzji dotyczących polityki w zakresie wyboru najlepszych ścieżek BGP. Uwaga: Dokładnie to, w jaki sposób wyniki BGP-OV są wykorzystywane w wyborze ścieżek, jest ściśle lokalną decyzją w zakresie polityki dla każdego operatora sieci. Typowe wybory dotyczące zasad obejmują: • Tag-Only - Wyniki BGP-OV są używane tylko do oznaczania/rejestrowania danych o trasach BGP w celach diagnostycznych. • Prefer-Valid - Użycie lokalnych ustawień preferencji dla nadania priorytetu ważnym trasom. Należy zauważyć, że jest to tylko preferencja do rozstrzygania sytuacji równoważności (równości) pomiędzy trasami z dokładnie tym samym prefiksem. • Drop-Invalid - zastosowanie lokalnej polityki do ignorowania nieważnych tras w procesie decyzyjnym BGP.	X	X	
Zalecenie dot. bezpieczeństwa 17: Wartość maxlength w ROA nie powinna przekraczać długości najbardziej specyficznego prefiksu (podciągniętego pod rozważany prefiks), który jest zainicjowany lub ma być zainicjowany z AS wymienionego w ROA.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 18: Jeśli prefiks i wybrane bardziej specyficzne prefiksy podciągnięte pod niego są ogłaszane lub mają być ogłaszane, to zamiast określać maxlength, prefiks i bardziej specyficzne prefiksy powinny być wyraźnie wymienione w wielu ROA (tj. jedna ROA na prefiks lub bardziej specyficzny prefiks). Uwaga: Ogólnie rzecz biorąc, należy unikać stosowania maxlength, chyba że wszystkie lub prawie wszystkie bardziej specyficzne prefiksy o wartości do maxlength są ogłaszane lub mają być ogłaszane [maxlength].	X	X	
Filtrowanie prefiksów (tras):			
Zalecenie dot. bezpieczeństwa 19: Trasy IPv6 powinny być filtrowane tak, aby dopuszczały tylko przydzielone prefiksy IPv6. Operatorzy sieci powinni regularnie aktualizować filtry prefiksów IPv6, aby uwzględnić wszelkie nowo przydzielone prefiksy. Uwaga: Jeśli właściciele zasobów prefiksowych regularnie rejestrują ROA AS0 (patrz dział 4.3) dla przydzielonych (ale prawdopodobnie obecnie nieużywanych) prefiksów, wówczas te ROA mogłyby być uzupełniającym źródłem aktualizacji filtrów prefiksowych.	X	X	
Zalecenie dot. bezpieczeństwa 20: Prefiksy, które są oznaczone jako „False” w kolumnie „Global” [IANA-v4-sp], [IANA-v6-sp] są zabronione do routingu w globalnym Internecie i powinny być odrzucone, jeśli zostaną odebrane od zewnętrznego elementu równorzędnego BGP (eBGP).	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 21: W przypadku prefiksów single-homed (podsieci), które są własnością systemu AS i są przez niego zainicjowane, wszelkie trasy dla tych prefiksów otrzymanych w tym AS od elementów równorzędnych eBGP powinny zostać odrzucone.	X	X	
Zalecenie dot. bezpieczeństwa 22: Zaleca się, aby router eBGP określał limit specyficzności dla każdego elementu równorzędnego eBGP i odrzucał prefiksy, które przekraczają limit specyficzności na zasadzie per-peer. Uwaga: Limit specyficzności może być taki sam dla wszystkich elementów równorzędnych (np. /24 dla IPv4 i /48 dla IPv6).	X	X	
Zalecenie dot. bezpieczeństwa 23: Trasa domyślna (0.0.0.0/0 w IPv4 i ::/0 w IPv6) powinna zostać odrzucona, chyba że istnieje specjalna umowa komunikacji równorzędnej, która zezwala na jej zaakceptowanie.	X	X	
Zalecenie dot. bezpieczeństwa 24: Punkt wymiany ruchu internetowego (IXP) powinien ogłaszać — ze swojego serwera tras do wszystkich swoich systemów autonomicznych — swój prefiks sieci LAN lub cały prefiks, który byłby taki sam lub mniej specyficzny niż prefiks sieci LAN. Każdy AS należący do IXP powinien z kolei akceptować ten prefiks i odrzucać wszelkie bardziej specyficzne prefiksy (od prefiksu ogłoszonego przez IXP) od któregokolwiek ze swoich elementów równorzędnych eBGP.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 25: Filtrowanie prefiksów przychodzących w połączeniach lateral peer— w kierunku przychodzącym należy zastosować następujące filtry prefiksów: • nieprzydzielone prefiksy, • prefiksy specjalnego przeznaczenia, • prefiksy inicjowane przez AS, • prefiksy wykraczające poza limit specyficzności, • trasa domyślna, • prefiksy IXP LAN.	X	X	
Zalecenie dot. bezpieczeństwa 26: Filtrowanie prefiksów wychodzących w połączeniach lateral peer —odpowiednie prefiksy wychodzące to te, które zostały zainicjowane przez dany AS, oraz te, które zostały zainicjowane przez podrzędne (downstream) systemy AS (tj. systemy autonomiczne w jego stożku klientów). Następujące filtry prefiksów powinny być stosowane w kierunku wychodzącym: • nieprzydzielone prefiksy, • prefiksy specjalnego przeznaczenia, • prefiksy wykraczające poza limit specyficzności, • trasa domyślna, • prefiksy IXP LAN, • prefiksy uzyskane od innych elementów równorzędnych bocznych systemu autonomicznego, • prefiksy uzyskane od dostawców tranzytowych systemu autonomicznego.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 27: Filtrowanie prefiksów przychodzących od strony dostawcy tranzytowego - Przypadek 1 (pełna tablica routingu): Ogólnie rzecz biorąc, gdy od dostawcy tranzytowego wymagana jest pełna tablica routingu, na kierunku wejściowym należy zastosować następujące filtry prefiksowe: • nieprzydzielone prefiksy, • prefiksy specjalnego przeznaczenia, • prefiksy inicjowane przez AS, • prefiksy wykraczające poza limit specyficzności, • prefiksy IXP LAN.	X	X	
Zalecenie dot. bezpieczeństwa 28: Filtrowanie prefiksów przychodzących od strony dostawcy tranzytowego - Przypadek 2 (trasa domyślna): Jeśli router graniczny jest skonfigurowany tylko dla trasy domyślnej, wówczas od dostawcy tranzytowego powinna być akceptowana wyłącznie ta trasa domyślna.	X	X	
Zalecenie dot. bezpieczeństwa 29: Filtrowanie prefiksów wychodzących do dostawcy tranzytowego: Należy zastosować te same filtry prefiksów wychodzących, co w przypadku bocznego elementu równorzędnego (patrz dział 4.5.1), z tym że ostatnie dwa punktory modyfikuje się w następujący sposób: • prefiksy uzyskane od bocznych elementów równorzędnych systemu autonomicznego, • prefiksy uzyskane od innych dostawców tranzytowych systemu autonomicznego.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Uwaga: W związku z zaleceniem dotyczącym filtrowania wychodzących prefiksów, niektóre polityki można też zastosować, jeśli nie zamówiono (lub wybrano) dostawcy tranzytowego do świadczenia tranzytu dla pewnego podzbioru prefiksów wychodzących.			
Zalecenie dot. bezpieczeństwa 30: Filtrowanie prefiksów przychodzących od klienta w Scenariuszu 1 (zob. dział 4.5.3) — należy akceptować tylko prefiksy, o których wiadomo, że pochodzą od klienta i jego stożka klientów, a wszystkie inne ogłoszenia tras należy odrzucić.		X	
Zalecenie dot. bezpieczeństwa 31: Filtrowanie prefiksów przychodzących od klienta w Scenariuszu 2 (patrz dział 4.5.3) - należy zastosować ten sam zestaw filtrów prefiksów przychodzących, jak w przypadku lateral peer (patrz dział 4.5.1).		X	
Zalecenie dot. bezpieczeństwa 32: Filtrowanie prefiksów wychodzących do klienta: Filtry stosowane w tym przypadku będą się różnić w zależności od tego, czy klient chce otrzymać tylko trasę domyślną, czy też pełną tablicę routingu. Jeśli to pierwsze, to należy ogłosić tylko trasę domyślną i nic więcej. Jeśli drugie, należy zastosować poniższe filtry prefiksów wychodzących: • prefiksy specjalnego przeznaczenia, • prefiksy wykraczające poza limit specyficzności, Uwaga: Filtr trasy domyślnej może zostać dodany, jeżeli klient żąda pełnej tablicy routingu, ale bez trasy domyślnej.		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 33: Filtrowanie prefiksów typu leaf przychodzących do klienta od dostawcy tranzytowego - Klient leaf może zażądać tylko domyślnej trasy od swojego dostawcy tranzytowego. W tym przypadku, powinna być zaakceptowana tylko domyślna trasa i nic więcej. Jeśli klient typu leaf wymaga pełnej tablicy routingu od dostawcy tranzytowego, wtedy powinien zastosować następujące filtry prefiksów przychodzących: • nieprzydzielone prefiksy, • prefiksy specjalnego przeznaczenia, • prefiksy inicjowane przez AS (tzn. klienta typu leaf), • prefiksy wykraczające poza limit specyficzności, • trasa domyślna.	X		
Zalecenie dot. bezpieczeństwa 34: Filtrowanie prefiksów typu leaf przychodzących od klienta do dostawcy tranzytowego- Sieć klienta typu leaf powinna stosować bardzo prostą politykę ruchu wychodzącego polegającą na ogłaszaniu tylko prefiksów przez nią inicjowanych. Jednak może dodatkowo zastosować te same filtry prefiksów wychodzących, jak dla lateral peer (patrz dział 4.5.1), aby zachować dodatkową ostrożność.	X		
Zalecenie dot. bezpieczeństwa 35: Dane ROA (dostępne z rejestrów RPKI) powinny być wykorzystywane do konstruowania i/lub rozszerzania list filtrów prefiksowych dla interfejsów klienta. Uwaga: To zalecenie dot. bezpieczeństwa jest być może lepiej przystające do mniejszych ISP które mają lepszą widoczność swojego stożka klientów. Większe ISP zwykle nie dysponują taką widocznością.		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Sprawdzanie ścieżki AS dla niedopuszczonych numerów AS			
Zalecenie dot. bezpieczeństwa 36: Należy sprawdzić ścieżkę AS w aktualizacji otrzymanej w eBGP, aby upewnić się, że lokalny numer AS nie jest obecny. Ścieżka AS powinna być również sprawdzana, aby upewnić się, że numery AS przeznaczone do celów specjalnych [IANA-ASN-sp] nie są obecne. W przypadku naruszenia, aktualizacja powinna zostać odrzucona. Uwaga: Specjalny numer ASN 23456 jest przydzielony dla AS_TRANS [RFC6793] i może być obecny w AS_PATH w połączeniu z AS4_PATH [RFC 6793] w aktualizacji.	X	X	
Ograniczanie wycieków tras:			
Zalecenie dot. bezpieczeństwa 37: Operator AS powinien posiadać politykę dotyczącą ruchu przychodzącego, aby wewnętrznie (lokalnie w AS) oznaczać trasy w celu komunikowania od wejścia do wyjścia co do typu elementu równorzędnego (klient, boczny peer lub dostawca tranzytu), od którego otrzymano trasę.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 38: Operator AS powinien mieć politykę ruchu wychodzącego w zakresie wykorzystywania oznakowanych informacji (w Zaleceniu dot. bezpieczeństwa 37), aby zapobiec wyciekom tras, gdy trasy są przekazywane na wyjściu. AS nie powinien przekazywać tras otrzymanych od dostawcy tranzytowego do innego dostawcy tranzytu lub elementu równorzędnego bocznego. Ponadto AS nie powinien przekazywać tras otrzymanych od elementu równorzędnego bocznego innemu elementowi równorzędnemu bocznemu lub dostawcy tranzytowemu.	X	X	
Uogólniony mechanizm zabezpieczeń TTL (GTSM)			
Zalecenie dot. bezpieczeństwa 39: Generalized TTL Security Mechanism (GTSM) [RFC5082], [RFC5082] powinien być stosowany na zasadzie per-peer, aby zapewnić ochronę przed sfałszowanymi komunikatami BGP.	X	X	
Mitygacja DDoS (antyspoofing):			
Zalecenie dot. bezpieczeństwa 40: Routery BGP, które bezpośrednio połączyły klientów z subalokowaną przestrzenią adresową, CMTS (lub odpowiednikiem) w szerokopasmowych sieciach dostępowych oraz PDN-GW (lub odpowiednikiem) w sieciach komórkowych, powinny implementować SAV za pomocą list ACL (dział 5.1.1). Routery BGP w tym kontekście mogą alternatywnie stosować metodę ścisłego uRPF (dział 5.1.2).		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 41: Router graniczny organizacji, typu multi-homed, powinien zawsze ogłaszać całą swoją przestrzeń adresową do każdego ze swoich dostawców tranzytowych położonych upstream. Można to zrobić na jeden z dwóch sposobów: 1) ogłaszać zagregowany mniej specyficzny prefiks wszystkim dostawcom tranzytowym oraz bardziej specyficzne prefiksy (objęte mniej specyficznym prefiksem) różnym dostawcom tranzytowym, zgodnie z potrzebami inżynierii ruchu, lub 2) ogłaszać takie prefiksy każdemu dostawcy tranzytowemu (aczkolwiek z odpowiednim dostawianiem na początku dla celów inżynierii ruchu).	X		
Zalecenie dot. bezpieczeństwa 42: Jest to wyjątkowy przypadek, gdy router graniczny organizacji nie wypełnia Zalecenia dot. bezpieczeństwa 41 i zamiast tego selektywnie ogłasza niektóre prefiksy jednemu tranzytowemu dostawcy usług internetowych na kierunku upstream, a inne prefiksy innemu tranzytowemu dostawcy usług internetowych upstream. W tym przypadku organizacja powinna kierować dane (poprzez odpowiedni wewnętrzny routing) w taki sposób, aby adresy źródłowe w pakietach danych w kierunku każdego tranzytowego dostawcy usług internetowych upstream, należały do prefiksu lub prefiksów ogłoszonych temu dostawcy.	X		
Zalecenie dot. bezpieczeństwa 43: Po stronie wejścia (tj. dla pakietów danych otrzymywanych od tranzytowego dostawcy usług internetowych) routery graniczne organizacji powinny wdrożyć luźne uRPF (dział 5.1.4) i/lub ACL (dział 5.1.1) w celu odrzucenia pakietów, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów — prefiksów oznaczonych jako „False”	X		

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
w kolumnie „Global" [IANA- v4-sp], [IANA-v6-sp] oraz własnych prefiksów organizacji).			
Zalecenie dot. bezpieczeństwa 44: Organizacja (tj. AS typu leaf z multihomingiem lub bez) powinno dopuszczać po stronie wyjściowej (tj. dla pakietów danych wysyłanych do tranzytowego ISP) tylko te pakiety z adresami źródłowymi, które należą do ich własnych prefiksów.	X		
Zalecenie dot. bezpieczeństwa 45: W przypadku interfejsów skierowanych do klienta mniejsi dostawcy usług internetowych powinni przeprowadzać SAV na pakietach wejściowych, wdrażając uRPF z wykonalną ścieżką (zob. dział 5.1.3). Powinni unikać stosowania ścisłego lub luźnego uRPF, ponieważ nie są one skuteczne zwłaszcza w przypadku klientów typu multi-homed. Przyjmuje się, że więksi dostawcy usług internetowych mogą korzystać z luźnego uRPF na interfejsach klientów.		X	
Zalecenie dot. bezpieczeństwa 46: Aby uRPF z wykonalną ścieżką działało właściwie, mniejszy dostawca usług internetowych (zwłaszcza ten, który znajduje się w pobliżu krawędzi internetu) powinien propagować całą swoją ogłaszaną przestrzeń adresową do każdego ze swoich dostawców tranzytowych upstream. Można to zrobić na jeden z dwóch sposobów: 1) ogłaszać zagregowany mniej specyficzny prefiks wszystkim dostawcom tranzytowym i ogłaszać bardziej specyficzne prefiksy (objęte mniej specyficznym prefiksem) różnym dostawcom tranzytu, w miarę potrzeby inżynierii ruchu, lub 2) ogłaszać te same prefiksy każdemu dostawcy tranzytowemu (choć z odpowiednim prefiksem dla celów inżynierii ruchu).		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 47: Dostawcy usług internetowych powinni preferować trasy klientów w stosunku do innych (tj. dostawcy tranzytu lub elementów równorzędnych bocznych) tras. W większości przypadków jest to również normalna polityka ISP. Uwaga: Przestrzeganie tego zalecenia ułatwia przestrzeganie Zalecenia dot. bezpieczeństwa 45. Jest to także jeden z warunków stabilności polityki BGP dla zapewnienia stabilnej konwergencji informacji o routingu [Gao-Rexford].		X	
Zalecenie dot. bezpieczeństwa 48: W przypadku interfejsów skierowanych do klienta mniejsi dostawcy usług internetowych powinni przeprowadzać SAV na pakietach wejściowych, wdrażając uRPF z wykonalną ścieżką (zob. dział 5.1.3). Powinni unikać stosowania ścisłego lub luźnego uRPF, ponieważ nie są one zbyt skuteczne dla SAV na interfejsach bocznych elementów równorzędnych. Uznaje się, że więksi dostawcy usług internetowych mogą stosować luźne uRPF na interfejsach z bocznymi elementami równorzędnymi.		X	
Zalecenie dot. bezpieczeństwa 49: Po stronie wejścia (tj. dla pakietów danych otrzymywanych od tranzytowego dostawcy usług internetowych) routery graniczne organizacji powinny wdrożyć luźne uRPF (dział 5.1.4) i/lub ACL (dział 5.1.1) w celu odrzucenia pakietów, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów — prefiksów oznaczonych jako „False” w kolumnie „Global” [IANA- v4-sp], [IANA-v6-sp] oraz własnych prefiksów organizacji).		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 50: Po stronie wychodzącej w kierunku klientów, elementów równorzędnych bocznych (tj. nietranzytowych) i dostawców tranzytowych, routery graniczne dostawcy usług internetowych powinny wdrożyć listy kontroli dostępu (patrz dział 5.1.1), aby odrzucać pakiety, gdy adres źródłowy jest sfałszowany (tj. należy do oczywiście niedozwolonych bloków prefiksów - prefiksów oznaczonych jako „False” w kolumnie „Global” [IANA- v4-sp], [IANA-v6-sp] i prefiksów ISP tylko do użytku wewnętrznego).		X	
Zalecenie dot. bezpieczeństwa 51: Dostawcy usług internetowych powinni używać danych ROA (dostępnych z rejestrów RPKI) do tworzenia i/lub rozszerzania list ACL/RPF do celów SAV dla pakietów przychodzących na interfejsach klienta. Uwaga: To zalecenie dot. bezpieczeństwa jest być może lepiej przystające do mniejszych ISP które mają lepszą widoczność swojego stożka klientów. Większe ISP zwykle nie dysponują taką widocznością.		X	
Filtrowanie ruchu (Monitorowanie portów UDP/TCP z aplikacjami podatnymi)			
Zalecenie dot. bezpieczeństwa 52: W routerach BGP zezwalaj elementom równorzędnym na łączenie się tylko z portem 179. Standardowym portem do odbierania komunikatów OPEN sesji BGP jest port 179, więc próby dotarcia przez elementy równorzędne BGP do innych portów mogą wskazywać na wadliwą konfigurację lub potencjalną działalność złośliwą.	X	X	
Zalecenie dot. bezpieczeństwa 53: Wyłącz aplikacje lub usługi, które są niepożądane w danej sieci lub systemie.	X		X

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 54: Odmawiaj ruchu dla wszystkich portów TCP/UDP, dla których dana sieć lub system nie obsługuje odpowiednich aplikacji. W niektórych przypadkach aplikacja lub usługa jest obsługiwana przez niektóre interfejsy (np. interfejsy skierowane do klienta lub do wewnątrz), ale nie przez inne (np. interfejsy skierowane do internetu). W takich przypadkach należy odmówić ruchu z ID portu właściwym dla rozpatrywanej aplikacji na interfejsach, na których ta aplikacja nie jest obsługiwana.	X		X
Zalecenie dot. bezpieczeństwa 55: Zalecenie to ma na celu wykrycie przeciążeń ruchu i wprowadzenia działa ograniczających. Odpowiednie techniki ograniczania to response rate limiting (RRL) [ISC1], [Redbarn] oraz uruchomione filtrowanie source-based remotely triggered black hole (S/RTBH) z Flowspec (zob. dział 5.5) [RFC5575], [RFC5575bis]. Techniki te mają zastosowanie do otwartych usług/protokołów, takich jak wymienione w Tabeli 1, które same są podatne na ataki DoS/DDoS lub mogą być wykorzystywane do ataku typu reflection/amplification. Zalecenie składa się z kilku następujących kroków [TA14- 017A]: • Monitorowanie współczynnika zapytań/żądań na adres źródłowy i wykrywania, czy nienormalnie duża liczba odpowiedzi zmierza do tego samego miejsca docelowego (tj. tego samego adresu IP). • Zastosowania techniki ograniczania współczynnika odpowiedzi (RRL), aby ograniczyć atak. • Korzystania z komunikatów BGP (Flowspec), w celu utworzenia filtru source-based remotely triggered black hole (S/RTBH). Można to skoordynować z dostawcą usług internetowych wyższego szczebla (upstream).			X

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
• Utrzymywania danych kontaktowych w nagłych wypadkach do dostawcy nadrzędnego (upstream), aby koordynować reakcję na atak. • Aktywnego koordynowania odpowiedzi pomiędzy dostawcami usług internetowych wyższego poziomu (upstream) z klientami niższego szczebla (downstream).			
Zalecenie dot. bezpieczeństwa 56: Odmawiaj ruchu żądań NTP monlist (wyłączając polecenie monlist) w ogóle lub wymuszaj, aby żądania pochodziły z prawidłowych (dozwolonych) adresów źródłowych.			X
Zalecenie dot. bezpieczeństwa 57: Aby ograniczyć wykorzystanie luk, wewnętrzny rekursywny resolver DNS organizacji powinien ograniczać zakres klientów, od których akceptuje żądania. Klienci zwykle pochodzą z tej samej sieci organizacyjnej, w której znajduje się resolver DNS. W związku z tym rekursywny resolver DNS może utrzymywać listy dostępowe w konfiguracji, tak aby nie była otwarta dla całego Internetu [ISOC], [TA14-017A].	X		X
Zalecenie dot. bezpieczeństwa 58: Organizacja powinna zablokować protokoły UDP/Port 53 i TCP/Port 53 dla ruchu wchodzącego i wychodzącego na granicy sieci; wyjątki obejmują wyznaczone rekursywne resolvery organizacji, które muszą wysyłać zapytania, oraz wyznaczone autorytatywne serwery organizacji, które muszą wysłuchiwać zapytań. (zob. objaśnienie w dziale 5.4.).	X		X
Zalecenie dot. bezpieczeństwa 59: Dostawca usług internetowych powinien prowadzić ograniczanie współczynnika dla niepoczątkowych fragmentów UDP na routerach brzegowych skierowanych do klientów i bocznych elementów równorzędnych.		X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Ograniczanie DDoS Mitigation (filtrowanie Remote Triggered Black Hole, specyfikacja przepływu):			
Zalecenie dot. bezpieczeństwa 60: Routery brzegowe powinny być wyposażone w funkcję filtrowania zdalnie wyzwalanym blackholingiem w oparciu o adres docelowy (D/RTBH) i filtrowania zdalnie wyzwalanym blackholingiem w oparciu o adres źródłowy (S/RTBH).	X	X	
Zalecenie dot. bezpieczeństwa 61: Routery brzegowe powinny być przystosowane do korzystania ze specyfikacji przepływu BGP (Flowspec) w celu ułatwienia ograniczania ataków DoS/DDoS (w koordynacji między autonomicznymi systemami upstream i downstream).	X	X	
Zalecenie dot. bezpieczeństwa 62: Routery brzegowe w systemie autonomicznym zapewniające filtrowanie RTBH powinny mieć politykę ruchu wejściowego w kierunku klientów RTBH, akceptującą trasy bardziej specyficzne niż /24 w IPv4 i /48 w IPv6. Ponadto routery brzegowe powinny akceptować bardziej specyficzną trasę (w przypadku D/RTBH) tylko wtedy, gdy jest ona podciągnięta pod mniej specyficznej trasę, którą klient może ogłosić jako standardową politykę (tj. mniej specyficzna trasa ma zarejestrowany wpis IRR i/lub ROA). Ponadto routery brzegowe nie powinny odrzucać bardziej specyficznych ogłoszeń tras związanych z RTBH od klientów, nawet jeśli sprawdzanie pochodzenia BGP może oznaczać je jako „Invalid”.		X	
Zalecenie dot. bezpieczeństwa 63: AS klienta powinien upewnić się, że trasy zgłoszone do filtrowania RTBH mają community: NO_EXPORT, NO_ADVERTISE lub podobne.	X	X	

	Dotyczy		
Zalecenie dot. bezpieczeństwa	**Organizacja**	**ISP**	**Serwery otwarte (Open Servers)**
Zalecenie dot. bezpieczeństwa 64: Dostawca usług internetowych świadczący klientom usługę filtrowania RTBH musi mieć politykę ruchu wychodzącego, która odrzuca trasy z tagami community przeznaczonymi do wyzwalania filtrowania RTBH. Jest to dodatkowe zabezpieczenie na wypadek niepowodzenia tagowania NO_EXPORT, NO_ADVERTISE lub podobnego.		X	
Zalecenie dot. bezpieczeństwa 65: Dostawca usług internetowych świadczący klientom usługę filtrowania RTBH musi posiadać politykę ruchu wychodzącego odrzucającą prefiksy dłuższe niż spodziewane. Zapewnia to dodatkowe bezpieczeństwo w przypadku niepowodzenia tagowania NO_EXPORT, NO_ADVERTISE lub podobnego.		X	

ZAŁĄCZNIK B — AKRONIMY

Poniżej zdefiniowano akronimy i skróty użyte w niniejszym dokumencie.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

Akronim	Terminologia angielska	Terminologia polska
ACL	Access Control List	Lista kontroli dostępu
AfriNIC	African Network Information Center	Afrykańskie centrum informacji sieciowych
APNIC	Asia-Pacific Network Information Centre	Centrum Informacji Sieciowych Azji i Pacyfiku
ARIN	American Registry for Internet Numbers	Amerykański rejestr numerów internetowych
AS	Autonomous System	System autonomiczny
BGP	Border Gateway Protocol	Protokół trasowania (routingu)
BGP-OV	BGP Origin Validation	Sprawdzanie poprawności pochodzenia BGP
BGP-PV	BGP Path Validation	Sprawdzanie poprawności ścieżki BGP
BGPsec	Border Gateway Protocol with Security Extensions	Protokół trasowania z rozszerzeniami bezpieczeństwa
DA	Destination Address	Adres docelowy
DSCP	Differentiated Services Code Point	Punkt kodowy różnicowania usług

DHS	Department of Homeland Security	Departament Bezpieczeństwa Krajowego (USA)
DoS	Denial of Service	Odmowa świadczenia usługi
DDoS	Distributed Denial of Service	Atak typu rozproszona odmowa usługi
DNS	Domain Name System	System nazw domenowych
DNSSEC	Domain Name System Security Extensions	Rozszerzenia bezpieczeństwa systemu nazw domenowych
eBGP	External BGP	Zewnętrzny BGP
EFP-uRPF	Enhanced Feasible Path Unicast Reverse Path Forwarding	Wzmocniony unicast ścieżek zwrotnych z wykonalną ścieżką
FIB	Forwarding Information Base	Tablica przekazywania
FISMA	Federal Information Security Modernization Act	Federalna ustawa o modernizacji bezpieczeństwa informacyjnego
Flowspec	Flow Specification	Specyfikacja przepływu
FP-uRPF	Feasible Path Unicast Reverse Path Forwarding	Unicast ścieżek zwrotnych z wykonalną ścieżką
GTSM	Generalized TTL Security Mechanism	Uogólniony mechanizm zabezpieczenia TTL
IANA	Internet Assigned Numbers Authority	Instytucja zarządzająca domenami najwyższego poziomu oraz sprawująca ogólny nadzór nad działaniem mechanizmu DNS

iBGP	Internal BGP	Protokół wewnętrzny BGP
ICMP	Internet Control Message Protocol	Internetowy protokół komunikatów kontrolnych
IETF	Internet Engineering Task Force	Zespół zadaniowy inżynierii internetowej
IGP	Internal Gateway Protocol	Protokół trasowania bramy wewnętrznej
IRR	Internet Routing Registry	Rejestr Trasowania w Internecie
ISP	Internet Service Provider	Dostawca usług internetowych
IXP	Internet Exchange Point	Punkt wymiany ruchu internetowego
LACNIC	Latin America and Caribbean Network Information Centre	Centrum Informacji Sieciowych Ameryki Łacińskiej i Karaibów
maxlength	Maximum allowed length of a prefix specified in RAO	Maksymalna dopuszczalna długość prefiksu określona w RAO
NCCoE	National Cybersecurity Center of Excellence	Narodowe Centrum Doskonalenia Cyberbezpieczeństwa
NIST SP	NIST Special Publication	Publikacja specjalna NIST
NLRI	Network Layer Routing Information (synonymous with prefix)	Informacja routingowa warstwy sieciowej (synonim prefiksu)

NTP	Network Time Protocol	Protokół synchronizacji sieciowej
RFC	Request for Comments (IETF standards document)	Dokument standardów IETF
RFD	Route Flap Damping	Tłumienie flappingu trasy
RIB	Routing Information Base	Baza informacji o routingu
RIPE	Reseaux IP Europeens	Europejska sieć IP
RIR	Regional Internet Registry	Regionalny rejestr internetowy
RITE	Resilient Interdomain Traffic Exchange	Odporna wymiana ruchu międzydomenowego
ROA	Route Origin Authorization	Autoryzacja źródła trasy
RPKI	Resource Public Key Infrastructure	Zasób infrastruktury klucza publicznego
RPKI-to-router protocol	RPKI cache to router protocol	Protokół RPKI cache-router
RLP	Route Leak Protection	Ochrona trasy przed wyciekiem
RRDP	RPKI Repository Delta Protocol	Protokół Delta repozytorium RPKI
RTBH	Remotely Triggered Black-Holing	Zdalnie wyzwalany blackholing
D/RTBH	Destination-based Remotely Triggered Black-Holing	Zdalnie wyzwalany blackholing oparty na adresach docelowych
S/RTBH	Source-based Remotely Triggered Black-Holing	Zdalnie wyzwalany blackholing oparty na adresach źródłowych

SA	Source Address	Adres źródłowy
SAV	Source Address Validation	Sprawdzanie poprawności adresu źródłowego
SIDR	Secure Inter-Domain Routing	Bezpieczny routing międzydomenowy
SIDR WG	Secure Inter-Domain Routing Working Group (in the IETF)	Grupa Robocza ds. Bezpiecznego Routingu Miedzydomenowego (w IETF)
SSDP	Simple Service Discovery Protocol	Prosty protokół wykrywania usług
TCP	Transmission Control Protocol	Protokół sterowania transmisją
TLS	Transport Layer Security	Standard komunikacyjnego protokołu kryptograficznego
UDP	User Datagram Protocol	Protokół pakietów użytkownika
UPnP	Universal Plug and Play	Protokół Universal Plug and Play („podłącz i działa”)
uRPF	Unicast Reverse Path Forwarding	Mechanizm analizy ruchu unicast pod kątem zgodności z ścieżką zwrotną routingu