Aspetti di sicurezza di BGP e Routing in Internet - parte II

Author : Andrea Pasquinucci

Date : 17 Marzo 2020

Nella prima parte di questo articolo è stata fatta una breve rassegna dei principali aspetti di sicurezza relativi al Routing BGP in Internet. In questa seconda parte sono descritte in maggior dettaglio le problematiche di sicurezza di BGP-4 e le misure di sicurezza adottate e in corso di valutazione.

Modalità di attacco a BGP-4

Il modo più semplice per effettuare un attacco al Routing BGP-4 o “BGP Hijacking”, è quello di accedere ad un router BGP di un Internet Provider o Carrier, attraverso credenziali rubate o vulnerabilità di sistemi. Una volta avuto accesso ad un router BGP, si possono modificare gli annunci BGP inviati ai Peer in modo da bloccare o dirottare il traffico di interesse. **Il protocollo BGP-4 non prevede meccanismi espliciti di controllo o sicurezza:** in linea di principio ogni router ripone completa fiducia negli annunci che riceve dai propri Peer. Quindi, se un router BGP invia annunci errati o malevoli, questi possono essere accettati senza alcun controllo dagli altri router BGP.

Un altro modo per modificare le tabelle di Routing è quello di intercettare e modificare il traffico dati tra due router BGP e quindi gli annunci che i due router si scambiano. Di base il traffico tra due router BGP è costituito da sessioni TCP non autenticate e non protette da cifratura o altre misure di sicurezza, sono verificati solo gli indirizzi IP dei due router. In alcune situazioni è pertanto possibile, anche se non del tutto facile, inserire o modificare i dati scambiati tra due router BGP.

È anche possibile inserire volontariamente (o per errore) nei propri router BGP degli “annunci” allo scopo di deviare o bloccare il traffico verso alcuni Prefissi. Gli effetti di questi annunci malevoli sono tipicamente locali, ma in alcuni casi particolari possono estendersi a livello globale (come già visto per alcuni incidenti descritti nella prima parte di questo articolo).

Infine, come indicato ad esempio dalla frode “3ve” precedentemente descritta, è possibile attaccare i processi formali e burocratici di assegnazione di AS e Prefissi alle organizzazioni per

ottenerne un uso formalmente valido. Ad esempio, “3ve” utilizzò, tra gli altri, gli indirizzi IP del Prefisso 192.73.128.0/18 assegnato ma non utilizzato dall'Aeronautica Militare Americana (United States Air Force); questo annuncio BGP fu accettato globalmente sino a quando non fu mostrato che l'Aeronautica Militare Americana non aveva autorizzato ad utilizzare i propri indirizzi IP una sconosciuta azienda Ucraina sospettata di gestire reti e servizi criminali.

Prime misure di sicurezza

La prima misura di sicurezza pratica applicabile agli annunci BGP consiste nell'applicare dei **filtri** (Rif. 1). Il primo tipo di filtri è quello che va genericamente sotto il nome di “Bogon Filtering”[1] ovvero filtri di rotte invalide. La comunità degli operatori mantiene delle liste basate principalmente sui documenti ufficiali di IANA e delle RIR di AS e Prefissi non allocati e che quindi non devono comparire in alcun annuncio BGP (Rif. 2). Sta però a chi configura e mantiene i router BGP applicare filtri agli annunci sia ricevuti che inviati ai Peer per impedire che questi AS e Prefissi compaiano nella tavola di Routing dei propri router e che vengano inviati ai Peer. Configurando in questo modo i propri router BGP, un AS impedisce che annunci e traffico invalido possano transitare sulle proprie reti.

Il secondo tipo di filtri su AS e Prefissi è invece specifico per ogni Peer. Infatti a seconda del tipo di accordo contrattuale in essere con un Peer, è norma di sicurezza, anche per il rispetto delle clausole contrattuali, configurare dei filtri che accettino e inviino solo gli annunci previsti dagli accordi. Ad esempio si consideri il caso di un'organizzazione con proprio AS che ha come Peer alcuni Internet Provider e Carrier che le forniscono accesso ad Internet. L'organizzazione configura sui propri router BGP dei filtri sugli annunci inviati ai fornitori che permettono l'invio solo del proprio AS e dei propri Prefissi. In questo modo l'organizzazione impedisce di diventare un nodo di transito del traffico tra i fornitori. L'organizzazione può poi mettere dei filtri sugli annunci che riceve in modo ad esempio di utilizzare un fornitore solo per il traffico in uscita verso una particolare regione geografica, e comunque sempre in accordo con gli accordi contrattuali. Specularmente i Peer dell'organizzazione configurano dei filtri BGP in modo da accettare solo gli annunci dell'AS e dei Prefissi dell'organizzazione. Questo impedisce ad esempio che anche solo per errore, l'organizzazione invii annunci di AS e Prefissi non propri e che diventi un nodo di transito di traffico verso altre AS. Infine i Peer possono configurare filtri sugli annunci che inviano all'organizzazione basati sugli accordi contrattuali in essere.[2]

Un altro tipo di filtro, da applicare non agli annunci BGP ma al traffico stesso, è quello sugli indirizzi IP sorgenti di ogni pacchetto IP. Il routing BGP considera solo gli indirizzi di destinazione ed il problema di consegnare al corretto destinatario i pacchetti IP. Molti attacchi in rete, in particolare di Denial of Service, sfruttano però la possibilità di inviare un pacchetto IP indicando un indirizzo sorgente diverso da quello reale. L'effetto è che chi riceve il pacchetto IP non sa chi è il vero mittente e nel caso invia il pacchetto IP di risposta ad un altro sistema. Questo meccanismo è stato spesso utilizzato per attacchi di Distributed (Reflected and Amplified) Denial of Service, in cui moltissimi sistemi attaccanti inviano contemporaneamente richieste a servizi quali DNS o NTP indicando come sorgente lo stesso indirizzo IP, che viene quindi subissato dalle risposte. Per contrastare questo attacco, si può applicare sui router il “Ingress Filtering” (Rif. 3) ma solo quando si conoscono esattamente i Prefissi IP da cui proviene il traffico. Tipicamente questo è il caso descritto precedentemente di

un'organizzazione che si connette a Internet tramite alcuni Peer: visto che i Peer ricevono da una certa connessione solo il traffico originato dall'organizzazione, possono inserire filtri sugli indirizzi IP sorgenti per limitarli a quelli dei Prefissi annunciati dall'organizzazione. In generale però, quando un AS od un Peering è di transito, ovvero scambia qualunque traffico IP, non è possibile filtrare gli indirizzi IP sorgenti, se non eliminando i Prefissi Bogon, che comunque non sono raggiungibili. È importante notare che nel routing BGP il percorso di andata di un pacchetto può essere diverso dal percorso di ritorno, pertanto anche i filtri su “reverse-path”, ovvero che il pacchetto di ritorno segua la stessa strada di quello d'andata, vanno applicati con cura e solo ove possibile.

I filtri appena descritti, se implementati da tutti ed in maniera completa, avrebbero impedito molti degli incidenti descritti precedentemente.

È anche possibile mettere in sicurezza la comunicazione BGP tra due Peer. Benché il protocollo BGP originale non lo prevedesse, un'estensione di BGP-4 permette di garantire l'integrità dei pacchetti scambiati tra i due Peer aggiungendo ad ognuno di essi un HMAC (“Hash-based Message Authentication Code”), ovvero un codice d'impronta del pacchetto BGP basato su di una chiave segreta condivisa tra i due router (Rif. 4).

Un'altra soluzione è quella di stabilire un tunnel IPSEC tra i due router BGP e instradare il traffico BGP attraverso questo tunnel. Visto che le informazioni scambiate sono comunque pubbliche, non è tipicamente necessario che siano cifrate a protezione della confidenzialità, quindi possono essere utilizzati tunnel IPSEC AH invece di IPSEC ESP. Questa soluzione è ormai disponibile nella maggior parte dei router in quanto IPSEC vi è in buona parte implementato in Hardware con circuiti dedicati. Al contempo però va valutato se la presenza di un tunnel IPSEC può comportare maggiori rischi di instabilità degli annunci. Infatti in caso di caduta del tunnel IPSEC tutti gli annunci ricevuti dal Peer vengono cancellati ed il traffico con il Peer bloccato, anche se il problema sia da addebitare al tunnel IPSEC e non alla linea tra i due router.

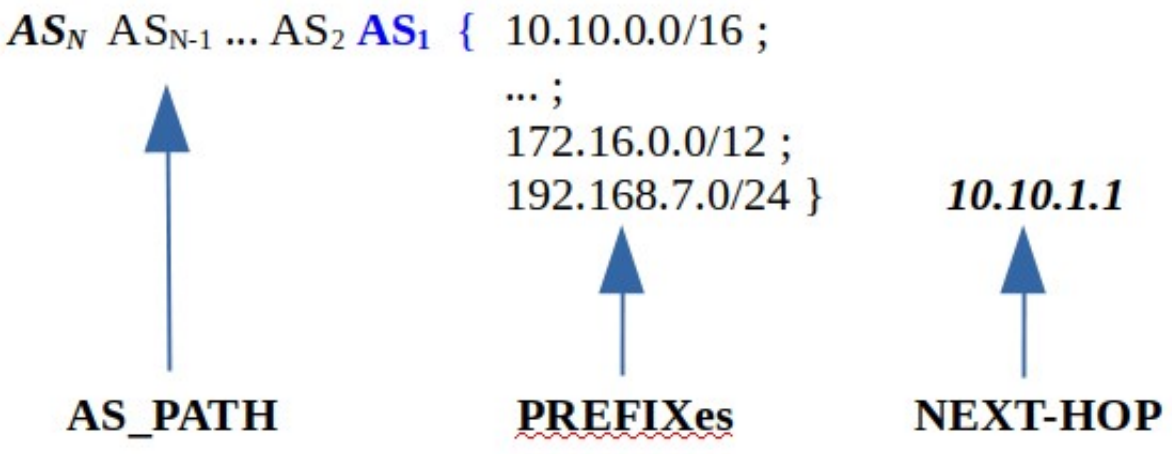

Fig. 1. Principali informazioni presenti in un annuncio BGP

Ulteriori problemi di sicurezza di BGP-4

Le misure di sicurezza appena descritte aiutano, ma non risolvono i problemi di sicurezza di BGP-4.
Sempre facendo riferimento alla Fig. 1, è possibile identificare le seguenti due principali problematiche di sicurezza:

1. garantire e dare la possibilità di verifica che AS_1 sia autorizzato ad annunciare i Prefissi indicati;
2. garantire e dare la possibilità di verifica che la AS_PATH non sia stata manipolata.

Il primo è principalmente un problema di autenticazione chiamato anche Origin Authentication (“OA”), mentre il secondo si può accostare a un problema di integrità, anche se non completamente.

Sin dagli anni '90 sono state proposte e studiate molte possibili soluzioni per queste problematiche di sicurezza di BGP-4. Queste proposte possono essere organizzate in tre categorie:

a) nuovi protocolli di Routing che sostituiscono completamente BGP-4;
b) nuove versioni di BGP che estendono il protocollo includendo anche le necessarie misure di sicurezza;
c) protocolli paralleli ma indipendenti da BGP-4 e che possono essere facilmente integrati con questo;

per una rassegna, si veda ad esempio Rif. 5, in particolare la tabella II.

La quasi totalità delle soluzioni proposte prevede l'utilizzo di algoritmi crittografici principalmente per firmare gli annunci e/o i dati relativi agli annunci BGP. Ben poche però di queste proposte hanno avuto anche un minimo successo. Negli ultimi anni, due proposte sono state sviluppate ed ora sono in fase di valutazione e possibile adozione: BGPSec (Rif. 6) e RPKI (Rif. 7).

BGPSec e RPKI

BGPSec è una nuova versione di BGP-4 che si propone di affrontare il problema dell'integrità di AS_PATH. L'idea di base del protocollo è quella di firmare digitalmente ogni “annuncio” sostituendo la AS_PATH con una BGPSEC_PATH che contiene sia i dati dell'AS_PATH ma anche il numero di AS a cui l'annuncio è inviato e la firma digitale dell'annuncio. In questo modo non solo l'annuncio è firmato, ma ogni annuncio è specifico tra due Peer. Un router BGP che riceve un annuncio firmato deve recuperare usando RPKI, discusso di seguito, le chiavi pubbliche di tutti i router delle AS presenti in un BGPSEC_PATH e verificare tutte le firme presenti. Allo stesso tempo, un router BGP che invia annunci BGPSec deve firmare singolarmente ogni annuncio inviato ad ogni Peer. E' chiaro che BGPSec richiede molte più risorse di BGP-4 ma non è chiaro quanto questo sia compatibile con l'hardware attuale dei router BGP. Inoltre l'utilizzo di BGPSec è opzionale rispetto a BGP-4, per cui se un router BGP

nella rotta non supporta BGPSec, da quel punto in avanti non saranno più presenti le firme digitali ma solo la AS_PATH tradizionale.

Si può porre la situazione di ricevere da due Peer distinti per lo stesso Prefisso una AS_PATH BGP-4 e una BGPSEC_PATH, come deve procedere il router BGP nella scelta dell'annuncio? Deve scegliere BGPSEC_PATH solo perché firmato digitalmente anche se la rotta non sarebbe conveniente rispetto a tutti gli altri parametri di scelta ed alla propria "Politica di Routing"? Va anche considerato che la firma digitale degli annunci, anche se fosse implementata da tutti i router BGP, non coprirebbe tutti gli scenari di attacco discussi: ad esempio annunci dovuti ad errori involontari di configurazione o ad intrusioni nei router BGP e perfino ad azioni volontarie, sarebbero comunque firmati digitalmente. Non è chiaro quindi se e come il fatto di firmare digitalmente a catena gli annunci BGP possa fornire il livello di integrità e "assurance" in grado di contrastare efficacemente le problematiche di sicurezza relative alla gestione delle AS_PATH. Vi sono parecchie voci discordi sull'adozione di BGPSec, e nel prossimo futuro vedremo se avrà fortuna o farà parte delle tante soluzioni proposte ma non adottate.

Nel frattempo in assenza di BGPSec, si può monitorare, anche attraverso servizi pubblici quali BGP Route Servers e Looking Glass Servers, lo stato degli "annunci" e delle AS_PATH ed implementare tecniche di baselining, analytics e visualizzazione per identificare modifiche e possibili anomalie sulle quali poi nel caso intervenire anche manualmente.

Se BGPSec è una proposta formalmente del 2017 anche se basata su idee già avanzate anche 20 anni prima, RPKI, ovvero "Resource Public Key Infrastructure" ha una storia ancora più lunga e culminata nella sua formalizzazione nel 2012/2013.

Prima di RPKI è necessario partire da quello che comunemente è chiamato WHOIS. La necessità di creare una base dati di assegnatari di AS e Prefissi, nomi ed indirizzi, risale ai primi anni '70 in ARPANET, prima ancora di Internet, ed una delle prime formalizzazioni è in Rif. 8. Sono stati creati quindi degli archivi che permettono di raccogliere in modo più o meno strutturato, tra l'altro, le informazioni sull'assegnazione di AS, Prefissi, nomi a dominio ecc. Queste basi dati sono oggi chiamate "Internet Routing Registries" (IRR), sono gestite da varie organizzazioni e le principali sono in carico alle RIR (e LIR), mentre una famosa base dati che risale ai primi anni '90 è Merit RADb (https://www.radb.net/). È procedura comune di molti Internet Provider e Carrier di permettere un Peering BGP solo se i corrispondenti dati di AS e Prefissi sono presenti nelle basi dati IRR / Whois. Ma oltre ai problemi di Privacy e conformità al GDPR, che non sono qui discussi, molte di queste basi dati contengono informazioni non aggiornate ed in alcuni casi del tutto errate. In generale queste basi dati sono di difficile manutenzione in quanto spesso la responsabilità di gestione è destrutturata e assegnata diversamente a seconda della nazione in cui opera chi mantiene la base dati. È opinione comune che queste basi dati siano sì utili ma solo a livello informativo, più o meno come un elenco telefonico non troppo aggiornato di cui ci si può fidare sino ad un certo punto. Ad esempio, nel 2014 il "Expert Working Group on gTLD Directory Services" di ICANN (Rif. 9) ha caldamente suggerito di rimuovere del tutto i servizi IRR / Whois perché ritenuti inaffidabili, e di sostituirli completamente con nuovi servizi di registrazione. Malgrado ciò, ancora oggi le informazioni presenti nelle basi dati IRR / Whois sono utilizzate quotidianamente anche per validare gli annunci BGP-4.

Nel frattempo però, a partire dal 2013, è stata introdotta la "Resource Public Key Infrastructure" (RPKI). Questa è una forma di PKI simile a quella a cui siamo ben abituati dalle Certification Authorities (CA) e dai certificati della navigazione Web. Invece di CA, la RPKI è basata su Trust Anchors (TA) che sono state individuate nelle cinque RIR. Ogni RIR genera i propri certificati X.509 "Trust" (ovvero "root") con i quali firma altri certificati, inclusi in caso quelli delle LIR, e le "Route Origination Authorizations" (ROAs). Un ROA è un documento firmato digitalmente che attesta che un AS è autorizzato ad annunciare un Prefisso con una massima lunghezza in bit: ad esempio AS_1 può annunciare 10.1.0.0/16 con lunghezza massima /22. Quindi AS_1 può annunciare 10.1.0.0/16 o 10.1.64.0/18 ma non 10.1.9.0/24. Ogni certificato ed ogni ROA ha una definita validità temporale, entro il quale deve essere nel caso rinnovato.

Le RIR hanno anche implementato delle basi dati pubbliche che contengono tutti i certificati pubblici necessari per verificare le firme, e tutti i ROA di competenza di quella RIR. Per verificare che gli annunci dei Prefissi siano corretti e autorizzati, un operatore BGP tipicamente allestisce dei server RPKI che interrogano le basi dati dei RIR, scaricano i certificati ed i ROA e verificano le firme svolgendo così la parte più onerosa dei calcoli. Le versioni più recenti dei router BGP di tutti i vendor permettono di interrogare server RPKI per verificare l'autorizzazione di un AS ad annunciare un prefisso. Il protocollo RPKI prevede solo tre possibili risposte alla domanda "AS_1 è autorizzato ad annunciare il Prefisso X ?":

1. **valido**: è stato trovato un ROA con firma valida che autorizza AS_1 all'annuncio del Prefisso;
2. **non valido**: è stato trovato un ROA per il Prefisso con firma valida ma per un altro AS, oppure l'AS è corretto ma la lunghezza del Prefisso supera il massimo previsto nel ROA;
3. **sconosciuto**: tutti gli altri casi, in particolare quando per il Prefisso non è stato trovato alcun ROA valido.

Si noti che vi è almeno un caso di difficile gestione: ritornando all'esempio precedente si supponga che AS_1 annunci 10.1.0.0/16, con risultato Valido, e AS_2 annunci 10.1.9.0/24, con risultato Sconosciuto in quanto non c'è un ROA valido per 10.1.9.0/24. Il router BGP deve accettare l'annuncio 10.1.9.0/24? In realtà no, in quanto il ROA di 10.1.0.0/16 ha lunghezza massima /22 ed assumendo che non vi siano altri ROA per 10.1.0.0/16 con altre AS, questo annuncio non dovrebbe essere accettato. Questo però è lasciato alla "Politica di Routing" decisa dall'operatore ed alle relative configurazioni dei router BGP.

Sinora abbiamo silentemente assunto che un Prefisso possa essere annunciato solo da un AS. In realtà questo non è vero in quanto più AS possono annunciare lo stesso prefisso e questo capita in particolare per grandi fornitori di connettività e servizi Internet (si veda ad esempio Rif. 10 per alcune statistiche sui Prefissi annunciati da più AS). L'esempio precedente, anche se come caso limite, può essere pertanto riformulato in maniera più generale: come bisogna comportarsi se un Prefisso ed un suo sotto-Prefisso sono annunciati da due AS uno con RPKI Valido e uno con RPKI Sconosciuto? Come prima, la risposta è lasciata alla "Politica di Routing" decisa dall'operatore.

La fig. 2 mostra il livello di adozione attuale di RPKI, quasi il 20% di Prefissi è autorizzato tramite un ROA mentre l'80% circa dei Prefissi non è descritto da alcun ROA. L'adozione di

RPKI comunque prosegue, ad esempio nel corso del 2019 il numero di Prefissi descritti da ROA è aumentato di almeno il 50%.

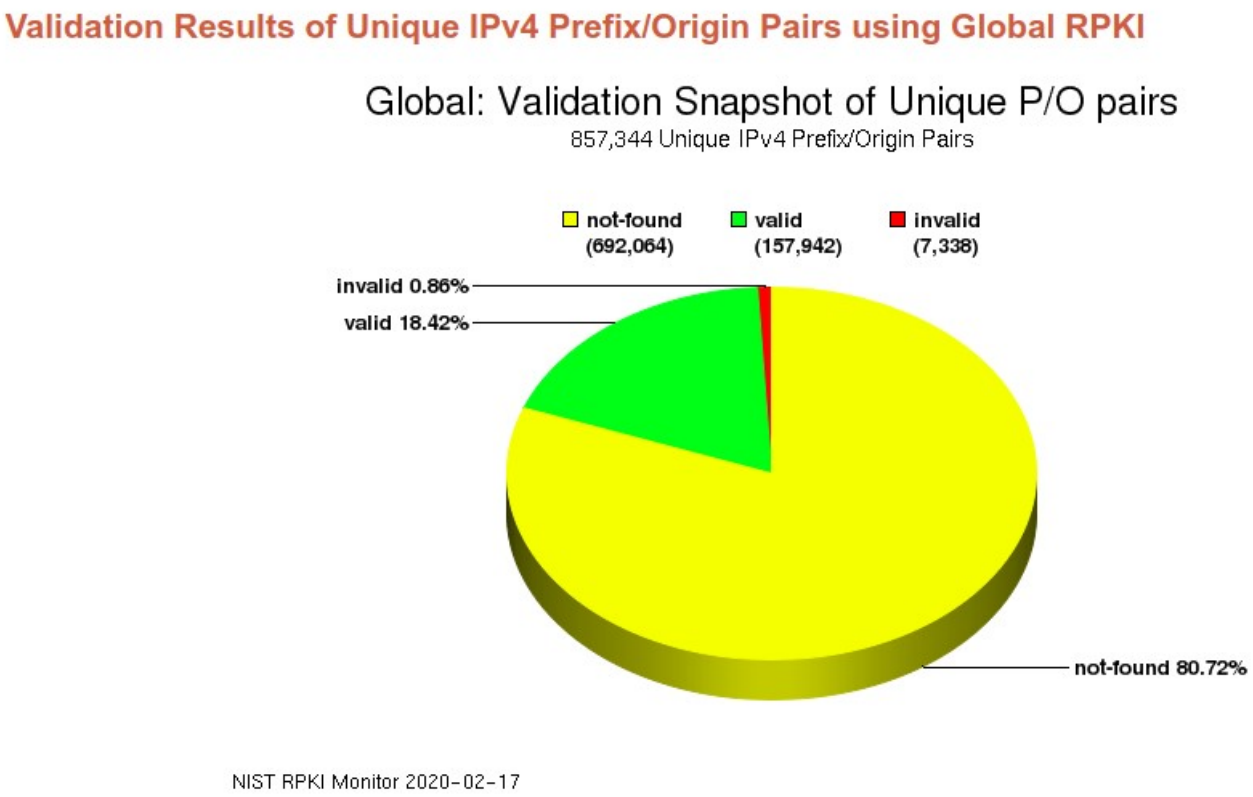

Fig. 2 Statistica sull'adozione di RPKI IPv4 al 17 febbraio 2020 [sorgente NIST https://rpki-monitor.antd.nist.gov/]

Se le recenti statistiche saranno confermate, sembra quindi che RPKI sarà adottato nel prossimo futuro da un numero sufficiente di operatori BGP da poter coprire la grande maggioranza di Prefissi. Questo porterà sicuramente a migliorare l'autenticità degli annunci dei Prefissi, riducendo di molto le possibilità di attacchi di BGP Hijacking.

Note

[1] Anche chiamato “Martian Filtering” ovvero filtri di rotte al più valide su Marte, denominazione valida sinché l'uomo non arriverà su Marte.

[2] Tipicamente un fornitore di traffico Internet, in assenza di specifici accordi contrattuali, invia tutti gli annunci BGP al cliente finale in modo che questi possa bilanciare il proprio traffico tra i vari fornitori.

Riferimenti bibliografici

Rif. 1: RFC-7454 “BGP Operations and Security”

Rif. 2: si veda ad esempio https://www.team-cymru.com/bogon-reference.html

Rif. 3: RFC-2827 “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”

Rif. 4: RFC-5925 “The TCP Authentication Option”

Rif. 5: K.Butler, T.Farley, P.McDaniel, and J.Rexford “A Survey of BGP Security Issues and Solutions”, 2008, https://www.cs.princeton.edu/~jrex/papers/bgp-security08.pdf

Rif. 6: RFC-8205 “BGPsec Protocol Specification”, 2017/09

Rif. 7: RFC-6480 “An Infrastructure to Support Secure Internet Routing” 2012/02

Rif. 8: RFC-920 “NAME/FINGER”

Rif. 9: ICANN "Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)", https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf , 6 June 2014

Rif. 10: Hurricane Electrics “Multi Origin Route Report” https://bgp.he.net/report/multi-origin-routes

Articolo a cura di **Andrea Pasquinucci**