1. Einleitung

Das Internet ist ein globale, dezentralized netzwerk, dessen Komponente viele kleine Netzwerk sind. Deswegen verteilt sich das Internet in vielen kleinen Teilen. Diese Teile heißen AS(Autonomous Systems). Jedes AS hat das eigene Routing-Protokoll, das innerhalb des Ases läuft, sowie OSPF, RIP. Aber wenn Ases miteinander die Route Informationen austauschen möchten, brauchen Sie ein Protokoll, den Ziel zu erreichen.

2.BGP und AS

AS(Autonomous System) ist die Sammlung von der Netze, die von einem Verwalter verwaltet und darin verläuft ein Intra-Routing Protokoll. Jedes AS besitzt ein Teil von den IP Addressen-IP Prefix. IANA(The Internet Assigned Number Authority) liegt auf der obeneste Stufe beim IP-Verteilen im Internet. Drunten stehen 3 RIRs(Regional Internet Registries): the American Registry for Internet Numbers (ARIN), Reseaux IP Europeens (RIPE), Asia Pacific Network Information Centre (APNIC), und Latin American and Caribbean Internet Addresses Registry (LACNIC). Auf den niederigeren Eben liegen viele große ISPs. Diese ISPs leisten die Arbeit, dass sie machen die IP-Prefix, die für sie zur Verfügung stehen, zu einigen kleinen Teilen. Dann verteilen Sie diese kleine IP-Prefixe an untenliegenden kleineren ISPs. Schritt für Schritt würde es endlich eine bestimmte IP-Addresse bei einem bestimmten PC abgeben.

BGP(Border Gateway Protocol) ist jetzt das einzige Inter-Domain Protokoll im Internet. Die BGP-Session basiert auf TCP-Session.Mit BGP können die Routers die Routing-Tabelle beim BGP-Session aktualisieren. Wenn BGP in einem Router läuft, würde dieser Router BGP-Speaker genannt. Es gibt einige BGP-Speakers innerhalb eines Ases. Zwischen diesen BGP-Speakers würde die Inter-domain Route ausgetauscht, und Sie bringen den anderen Routers im AS die Route zur anderen Ases zu Bewusstsein. Einige BGP-Speakers würde als Border-Router ausgewählt. Border Routers bauen BGP-Session zwischen ihnen selbst und die Boder-Routers in den anderen Ases auf, um die Routing-Informationen auszutauschen.

Nach diesem Regel würde es 3 Type der Ases geben: stub, multihomed, and transit. [7] Stub AS ist wie ein Endpunkt in der ISP-Kette. Es kommuniziert nur mit seinem einzigen Anbieter. Multihomed Ases haben nur eine Unterschied zum Stub AS—Sie haben nicht nur ein Anbieter, sondern mehrere verschiedene Anbieter. Transit Ases stehen in der Mitte von vielen Ases. Ein transit As ist zwischen dem Hersteller der Packte und dem Ziel, um die Pakete fortzuschicken.

Es gibt einige Beziehungen zwischen den Ases: Anbieter-zu-Kunde, Kunde-zu-Anbieter, peering-to-peering und sibling-to-sibling.[6].

Bei Anbieter-zu-Kunde Beziehung kommt es zum Ausdruck, dass Anbieter seine Kunden ganze Routing-Tabelle beim BGP-Session schicken würde. Im Gegensatz würde Kunde seinem Anbieter nur die Route in der Routing-Tabelle schicken, die er selbst verwaltet oder von seinen Kunden kenngelernt hat. Wenn zwei Ases für “Peer-to-Peer” Beziehung stehen, stehen Sie auf einer gleichen Stufe.Das heißt,Sie sind gleichberechtigt miteinander. Sie würde ihre Peer-Partner die Route von selbst und ihren Kunden bescheid wissen.

Es gibt vier Sorte von der “BGP-Message”: Open, Keep-alive, Notification, Update. Mit “Open message” würde BGP-Session aufgebaut. Wenn keep-alive Nachrichten ausbleiben, geht BGP von einer Verbindungsstörung aus und unterbricht die entsprechende BGP-Session. Notifikation Message würde nach dem Fehler oder anderen Unfälle geschickt. Dann würde BGP-Session untergebrochen. Diese 3 Messages leisten die Arbeit, den Status des BGP-Session zu kontrollieren. Update Message beinhaltet die Routing-Informationen. BGP ist ein Path-vector Protokoll. Das bedeutet,BGP würde dem Paket zum Ziel auf dem kürzesten Route führen. BGP-Speakers würden von ihren Anbieter, Kunde, Peer, Silbling die Route zum irgendeinen AS wahrnehmen

3.Schwachpunkte des BGPs

Obwohl die große Teile des Angriffs im Internet gegen bestimmte PC ist, welche wie Endpunkte im Internet stehen, können Wir nicht ignorieren, dass es viele Probleme mit BGP gibt. Es gibt fundamentale Schwachpunkte im BGP: “

(1) BGP bietet keinen Mechanismus für den Schutz für die Integrität, die Frische, Authentifizierung für Peer beim Peer-Peer BGP Kommunikation

(2) Kein Mechanismus für die Authentifiziefung für ein AS, wenn es die NLRL Informationen behauptet.

(3) kein Mechanismus für die Authentifizierung für das “Path” Attribut, das von einem AS behauptet würde.”[5]

BGP-Message ist ganz öffentlich. Message würde vielleicht kapput gemacht oder verändert. Wegen der Verzögerung würde älter Message nach der Neue das Ziel erreichen, und im BGP gibt keine eingesetzt Mechanismus, die Order der zu identifizieren. Und BGP bietet keine Authentifikation für Peer.

NLRI steht für “Network Layer Reachability Information ”. Das liegt im BGP-Update-Message, um es zu verbreiten, Welche IP-Prefix von welchem AS verwaltet werden. Beim originalen BGP gibt es keine Mechanismus, es zu beweisen,dass bestimmte IP-Prefix wirklich vom bestimmten AS verwalten würden.

Es gibt auch keinen Mechanismus, mit dem es zu bestätigen, ob ein “Path”, das von einem AS behauptet wird, echt und richtig ist.

4.Die Type des Angriffs auf BGP

Die originale Schwachpunkte im Entwurf des BGPs können die Angreifer nutzen, um die BGP-Session zu unterbrechen oder andere noch schlimmer Schaden zu verursachen. In diesem Kapitel würden wir über die Angriffstype diskutieren.

4.1 Vorstellung

Der Angreifer könnte mit schon bekannten Maßnahmen die TCP-Verbindung angreifen. Zum Beispiel DoS Angriff. Wenn DoS entsteht,würde die BGP-Session unterbrochen und für lange Zeit nicht mehr aufgebaut.

Wenn der Angreifer die BGP-Session zwischen BGP-Speakers eingreifen und die Pakete stehlen, verändern, abfangen und imitieren kann, würde die nomale Verbindung unstabil. Das ist Man-in-the-middle Angriff auf BGP.

A,B sind zwei BGP Route und Sie sind Nachbarn. Die BGP-Session ist Aktiv. C ist ein Angreifer. In diesem Szenarion würde Es ein Beispiel geben.

C entscheidet sich, mit Open-Message anzugreifen:“Der Empfang des OPEN Message würde der BGP Speaker die Verbindung unterbrechen und alle angegliedert BGP Resource auslösen und alle angegliedert Route löschen. Er würde Entscheidung-Prozess verwenden und brachliegend bleiben, wenn der Status der Verbindung “Connect oder Active ” ist. [5]

Man-in-the-middle Angriff ist nicht einfach auszuführen, weil der Angreifer die Sequenz-Nummer der Pakete vermuten soll. Und es gibt auch Mechanismus, wenn ein BGP-Speaker zu oft von anderen BGP-Speakers trennt, würde dieser BGP-Speaker von anderen BGP-Speaker gemäß die Häufigkeit der Unterbrochung ignoriert.

Jetzt konzentrieren wir uns auf die Update-Message und vermuten, dass der Angreifer die Kontrolle auf einem Speaker übernehmen kann. Auf diesem Fall würde der Angriff schrecklicher als die Vorne, weil der Umfang so groß ist, dass er vielleicht viele ISPs beeinträchtigen würde.

Am 24.Februar, Jahr 2008, Pakistan´s Regierung befehlt ISPs in Pakistan,ein Angriff auf Internet

starten. Dann konnten ein großer Teil der Benutzer im Internet nicht mehr Youtube besuchen. Dieser Angriff dauert einige Stunden, bis nur wenn der Filter im BGP bei diesem Unfall diesen Angriff erkannt konnte.
Dieser Fall ist ein typischer Angriff auf BGP. Wir nehmen diesen Fall als ein Beispiel, um es zu bestätigen, dass die Einfluss sehr stark ist, wenn es ein BGP-Angriff gibt, der einen bestimmte Ziel hat, obwohl es diese Erreignisse jetzt noch seltsam gibt.
Sehen Abbildung 1.1
In dieser Topologie der Ases bezeichnet die Beziehungen der Ases. Das Zeichen jeder Verbindung hat die Beziehung zwischen jeden 2 Ases zum Ausdruck gebracht. Wir vermuten jetzt, wenn es keinen Angriff gibt,AS I verwaltet die IP-Prefix 15.0.0.0/8 und hat diese Prefix durch BGP-Session behauptet. E würde als Anbieter für I dieses IP-Prefix empfangen, speichern und noch weiter behaupten. Danach würde andere Ases im Umfang die Route zu 15.0.0.0/8 ausrechnen. Zum Beispiel, in AS-E würde die Route E-I für die Route zu 15.0.0.0/8 gespeichert. Und in AS-F würde F-E-I gespeichert.Schritt für Schritt würde jede AS im Umfang die Route zu 15.0.0.0/8 wissen.

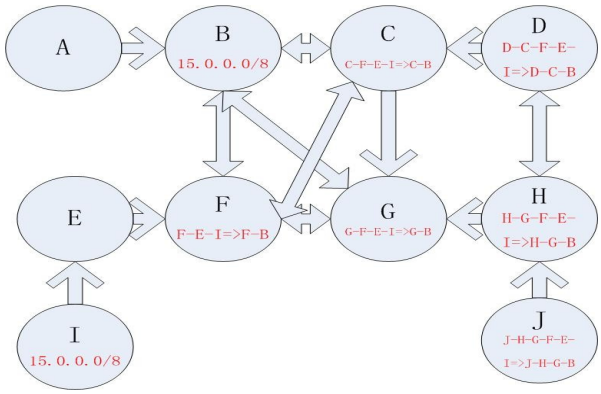
4.2 Angriff

4.2.1 Angriff typ:Prefix hijacking oder Falsch Update-Message

Prefix hijacking bedeutet, ein AS behauptet, dass es ein Prefix verwaltet oder es ein besser, kurzer Route zu einem Prefix führt, obwohl diese Behauptung überhaupt falsch ist.

4.2.1.1 Vorstellung

Ein Angreifer kontrolliert ein BGP-Speaker und dann stellt er eine Behauptung auf, dass er eine besser Route zum IP-Prefix hat oder er dieses Prefix verwaltet. Wenn BGP-Speaker miskonfiguriert würde, kommt dieser Fall auch vor. Wenn die Behauptung geschickt würde, beginnen Ihre Peer-ASes, Anbieter-Ases, Kunden-Ases diese Route gegen in der Datenbank gespeicherte Route zu vergleichen. Wenn Sie finden, dass diese Route besser ist, würde diese Route in den Datenbank gespeichert und in die Routing-Tabelle eingefügt, um die alte Route zu ersetzen. Dann verbreitet Ases diese Route weiter. Und immer mehr Route-Datenbank würde verseucht würden.
In der Abbildung 1.1 vermuten Wir, die Kontrolle über B würde gestohlen und er behauptet, dass er 15.0.0.0/8 verwaltet. Dann würde diese Prefix-Behauptung zu A, C, F, G geschickt. A als Stub-AS nimmt diese Route sofort auf. C vergleichen die Neue gegen die Ältere und findet das Path C-B besser als das Path C-F-E-I. Und Würde C diese Route aufnehmen und in die Datenbank speichern.



<--->: Peer-to-Peer link; --->: Customer-to-Provider link.

Abbildung 1.1 Prefix-Hijacking nach [6]

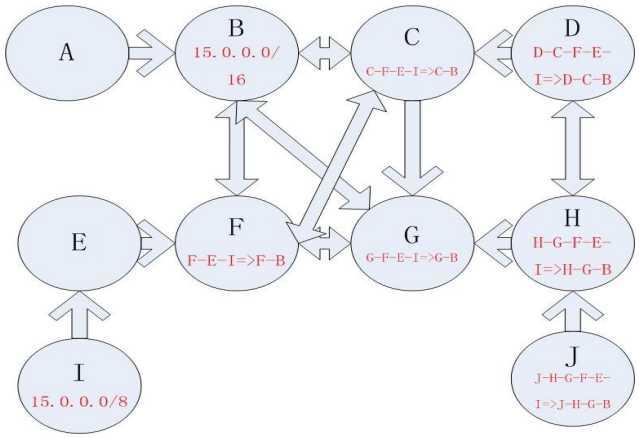


Abbildung 1.2 De-Aggregation nach [6]

Gleicher Fall läuft auch bei F und G. Und die Route-Message würde noch weiter von A, F und G geschickt. Schritt für Schritt verbreitet diese falsche Update-Message. Am Ende würde alle Pakete

aus C, F, G, D, H, J, dessen Ziel 15.0.0.0/8 ist, dem B geschickt.

4.2.1.2 Konsequenz

Prefix-Hijacking oder falsche Update-Message würde Blackholing oder Redirection verursachen.
Blackholing bedeutet, wenn die Pakete, die wegen der falschen Update-Message zum angegriffenen AS geschickt wurden, den falshen Ziel beziehungsweise das angegriffene AS erreichen, würde der Angreifer alle Pakete wegwerfen. Das heißt, diese IP-Prefix ist vielen Ases nicht mehr erreichbar. Der Angriff von Pakistan gehört zum diesen Typ.
Es gibt noch eine Wahl für den Angreifer, eine Rolle wie einige Server im echten AS zu spielen. Zum Beispiel SMTP server[6].
SPF(Sender Policy Framework) ist ein nomaler Einsatz, der in vielen SMTP Servers läuft, um den Sender zu authentifizieren. “SPF fordert auf, dass die Domain, in der SMTP Servers stehen, in DNS die Identität der authentifizierte SMTP Servers legen soll. Ein SMTP Server, der SPF implementiert, kann die Authorität der Addresse des Serders verifizieren, wenn er die Konsistenz der IP Addresse zwischen dem “originating” SMTP Server und dem in Sender Domain schon anthentifizierten SMTP Server.”[6]
Aber dieses Prinzip funktioniert nicht mehr, wenn es Prefix-Hijacking gibt. Der Angreifer soll nur einem SMTP-Server die IP-Addresse wie echter Server verwalten und dann würde die dem Echten SMTP-Server geschickte Emails dem unechten SMTP-Server geschickt. Das Ziel des Angreifers ist, die Informationen in der Emails zu analysieren und stehlen. Diese Maßnahme kann die Spamms bedienen. Wenn der Sender die IP-Addresse der Andere benutzen, kann SPF nicht mehr Spamming entdecken.
Eine andere mögliche Situation würde vorkommen, wenn der Angreifer die Pakete nicht wegwirft, sondern er schickt sie dem richtigen AS. Das heißt “Redirection”. Das Ziel des Angreifers ist vielleicht, die Pakete auf längere Route zu schicken. Und vielleicht würde die Ases, die Pakete erzeugt haben, mehr Geld oder Ressource zu konsumieren.
Es gibt ein Spezielles Typ von “Re-direction“, das “Subvertion“ heißt. Der Angreifer würde diese Pakete zu einigen Links führen. Mit diesen Links kann der Angreifer man-in-the-middle Angriff durchführen, um die Daten zu lauschen.

4.2.2. Angriff Typ 2. : De-Aggregation

Die Unterschied dazwischen ist, bei Prefix-hijacking behauptet der Angreifer, dass er ganz IP-Prefix verwaltet oder dafür besser Route hat. Aber bei De-Aggregation behauptet der Angreifer, dass er ein genaue oder längere IP-Prefix verwaltet oder dafür eine besser Route hat, und er anderen Ases diese Update-Message schicken. Und die Ases, wer diese Update-Message bekommt hat, würde die neue Route ausrechnen. Diese Route würde mit der neue Update-Message sich verbreiten.

4.2.2.1 Vorstellung

In der Abbildung 1.2 würde B vom Angreifer kontrolliert. Er behauptet nicht, dass er das IP-Prefix 15.0.0.0/8 verwaltet, sondern er verwaltet das IP-Prefix 15.0.0.0/16. Dann würde B Update-Message erzeugen und dem AS-A, -F, -G, -C schicken. AS-A nimmt diese Route sorfort auf. C, F, G akzeptieren diese Route und schicken diese Update-Message weiter. Wenn ein AS einem Ziel-PC, dessen IP-Addresse zu disem Prefix gehört, zum Beispiel 15.0.0.1/24, die Pakete schicken will, würde es B als das Ziel auswählen, weil die Netz-Addresse bei 15.0.0.0/16 länger und genauer als bei 15.0.0.0/8 ist.

4.2.2.2 Konsenquenz

Der Konsequenz der De-Aggregation ist sogleich wie IP-hijacking. Blackholing oder Redirection würde vorkommen.

4.2.3 Angriff Typ: Widersprechende Behauptung

Widersprechende Behauptung heißt, der BGP Speaker schickt den verschiedenen Ases verschiedene

Update-Message für ein gleiches Ziel-AS. Es ist dem Angreifer nützlich.

4.2.3.1 Vorstellung

Widersprechende Behauptung ist nicht eine typische Maßnahme für den Angriff. Es ist nomalerweise eine legale Maßnahme, um die Route auszuwählen, wenn es viele Paths gibt, zu einem gleichen Ziel zu führen. Ein AS würde den verschiedenen Ases das nomale Update-Message oder das Update-Message mit der wiederholten AS nummer schicken, um die Pakete auf den lieberen Links zu führen. Sehen Abbildung 2.
AS 3 will B-M als das Hauptlink zum Internet auswählen. Dazu kann AS3 einfach AS-1 und AS2 eine Behauptung schicken, dass das Route zu AS4 sowie {AS-1 AS-3}{AS-2 AS-3} ist und zu AS5 wie {AS-1 AS-3 AS-3 AS-3}{AS-1 AS-3 AS-3 AS-3} ist. Dann ist B-M das Hauptlink zum Internet.

4.2.3.2 Konsequez

Wenn diese Maßnahme vom Angreifer benutzt würde, ist es möglich, dass ein Link der Ases überbeansprucht würde, und die Links würde unterbrochen. Das Netz würde unstabil sein. Das heißt, wenn ein Link unterbrochen ist, würde der Border Router auf diesem Link noch mal alle Route ausrechnen und Update-Message schicken. Andere Ases würden die gleiche Arbeit auch in Angriff nehmen. Aber Wenn das Link nochmal nutzbar würde, würde diese Arbeit wiederholt. Dann geht das Link nochmal kaputt. Obwohl es ein Mechanismus im BGP-Speaker gibt, um diesen Unstabilität zu mildern, würde es auch Schaden geben.

4.2.4 Angriff Typ: virtuelle Link

Angriff mit der vertuellen Links ist ungewöhnlich. Die Voraussetzung für diesen Angriff ist nicht leicht, dass der Angreifer zwei oder mehr BGP-Speaker in den verschiedenen Ases kontrollieren kann. Dann würde der Angreifer ein virtuelle Link zwischen zwei BGP-Speaker erzeugen.

4.2.4.1 Vorstellung

In der Abb.2 würde der Angreifer Router P und R kontrollieren und ein Virtuelles Link dazwischen aufbauen. Dann behauptet P, die Route zum AS-6 ist {AS1 AS6}. Und alle pakete zum AS6 würden dem AS1 geschickt.

4.2.4.2 Konsenquenz

Dieser Angriff verursacht den gleichen Schaden wie Prefix-hijacking.

5. Schutz Maßnahmen

5.1 Ipsec

Um vor dem TCP-Angriff zu schutzen, nutzt man Ipsec. Ipsec ist nicht nur für BGP, sondern auch für anderen Protokoll, weil es die sicherheit auf der Netzwerk-Ebene anbieten.
The IPsec Internet Security Association and Key Management Protocol (ISAKMP) definiziert ein Framework für Schlüssel-Management und “negotiating security services”[Maughan et al. 1998], wenn IKE(Internet Key Exchange) Protokoll die Ausgabe der “dynamic negotiation of session keys”[Harkins and Carrel 1998] behandelt.Das AH(The IPsec Authentication Header) Protokoll[Kent and Atkinson 1998a] und ESP(Encapsulating Security Payload) Protokoll [Kent and Atkinson 1998b]implementieren die Sicherheit auf der Paket-Stufe mit verschiedenen Garantie. Alle solche Services bemühen sich um den Aufbau und Management des Schlüssels, mit dem das “confidentiality” und Authorität der Daten, die auf IP zwischen zwei Endepunkt geführt sind. In BGP ist es eine typische Maßnahme, um die BGP-Messages zu schutzen.[7]
Ipsec ist nicht besonders für BGP entwurf, deshalb kann es nur die Probleme mit Netzwerk-Ebene lösen. Wir brauchen noch mehr Schutz-Maßnahmen für den Schutz des BGPs. Unsere Ziele sind:

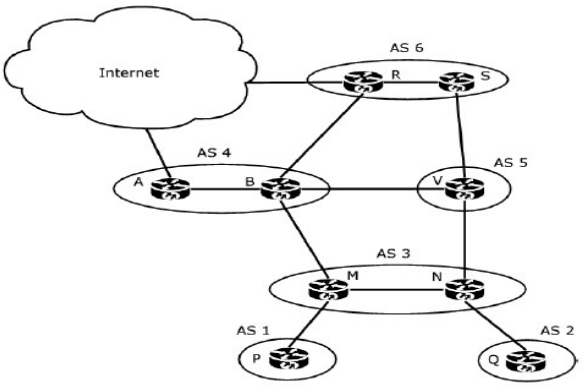


Abb.2 Virtueller Link Angriff aus [1]

“ 1. Jede Update-Message könnte nicht auf der Route verändert und sie soll neuer Routing-Infomationen als die vorne Update-Message beinhalten, den empfangen würde.
2. Die Update-Message ist bestimmt für die BGP-Speakers oder die ASes, die diese Message empfangen sollen.
3. Der Peer, der Update-Message schickt, soll authentifiziert werden, dass er wirklich die Vertretung für sein AS hat, dem Empfänger-AS die Update-Informationen zu schicken.
4. Das AS, das die Route erzeugt und BGP Speaker, die in der Liste über die erreichbare Ziele in Update-Message stehen, soll authentifiziert, um es zu präsentieren, dass diese Ziele von der Organisation verwaltet werden.
5. Die IP-Addresseräume, die in der Update-Message behauptet werden, soll von ICANN an die bestimmte Organisation verteilt werden.
6. Wenn die Update-Message vorzeigt, eine Route ungültig zu sein, Wurde der Peer die Route, die diese ungültige Route beinhaltet hat, abschaffen soll.
7. Am Ende soll der BGP-Speaker, der die Rolle wie entweder Sender oder Empfänger ist, korrekt den Regel des BGP-Prozesses und den Policy des Ases ausführen.”[3]

5.2 S-BGP

S-BGP steht für Secure-BGP. Mit S-BGP kann man die vorne 6 Ziele erreichen. Der 7.Ziel ist nicht erreichbar, weil der Policy in jedem AS das Wirtschaftlicher Geheimnis ist.

5.2.1 Vorstellung

S-BGP basiert auf 3 Mechanismen:PKIs, Attestations, und Ipsec. Ipsec leistet die Arbeit, die Sicherheit auf Netzwerk-Ebene anzubieten.PKIs bietet die Authorität für Eigentumsrecht der IP-Addresse block, Eigentumsrecht der AS Nummer, AS Identität, und die Identiät des BGP-Routers.
Mit PKIs kann man 3 Zertifikate erzeugen. Der Erste ist für die Eingentumsrechte der IP-Addresse. Jedes AS würde ein Zertifikat bekommen, damit es beweisen kann, welche IP-Addresse Block dieses AS verwaltet. Der zweite Typ des Zertifikats verbindet ein Publik-Schlüssel mit einer Organisation und eine Sammlung von der AS-Nummer. Der dritte Zertifikat verbindet ein Publik-Schlüssel mit eine AS-Nummer und ein BGP-Router ID. Mit der Zertifikate kann man beweisen, die echte Beziehungen Zwischen den Organisationen und den Ases. Welche Organisation verwaltet welche Ases würde in den Zertifikate speichert. Die Zertifikate können auch nachweisen, in welchem AS ein bestimmter BGP-Router steht. Die Attestation ist der Kern des S-BGPs. Die Attestation basiert auf PKIs. Es gibt 2 Type von der Attestaion: RA, AA. RA steht für Route Attestation.Der Hersteller ist ein AS oder ein authentifizierter Router, der das AS vertretet. Das Ziel ist ein Transit-AS oder das AS, die Dritte-Rolle-Behauptung für kein BGP darin laufende AS anzubieten.[3]
AA steht für Addresse Attestation. Der Hersteller ist die Organisation, die in der Attestaion liegende

IP-Prefixe verwaltet. Das Ziel ist einige Ases, die authentifiziert ist, diese Prefixe zu behauptung, nämlich der Internet Service Anbieter für diese Organisation.[3]
Die Attestaion würde in einem neuen, optionalen, BGP transitiven Path-Attribut getragen, und Route-Informationen würde von der digitalen Signatur bedeckt. [3] Sehen Abb.3
Privat-Key würde der BGP-Router in der eigenen Datenbank speichern, und Public-Key würde von Hierachishe PKI Infrastruktur gemacht.
In ABB.4 würde es ein Beispiel über die Funktion des SBGPs geben.
1. A erzeugt eine RA für prefix P und zeigt B als Next-Hop für diese Route.
2. A schickt B diese UPDATE-Message inklusiv RA.
3. B validiert mit Publik-Key die Signatur in der RA.
4. B verifiziert die AA für P, um es zu beweisen, dass A wirklich der eigner der Prefix-P ist.
5. B verifiziert, dass B Next-Hop in der RA ist.
6. B erzeugt zwei neue Ras für seine Peers C und D und mit verschiedene Update-Messages zu C und D absenden.[1]

5.2.2 Problem

Mit S-BGP kann man BGP vor fast allen Angriffe schutzen. Aber S-BGP ist keine ideale Schutz-Maßnahme wegen die Probleme für weitere Deployment.
Zuerst braucht man die PKI infrastruktur für S-BGP im Internet gemäß die Hierachie einzusetzen.Wegen des neuen Path-Attributs würde die Update-Message größer und vielleicht braucht BGP-Router RA und AA out-of band auszutauschen. Das würde die Geschwindigkeit der Austausch der Update-Message niedriger gemacht.

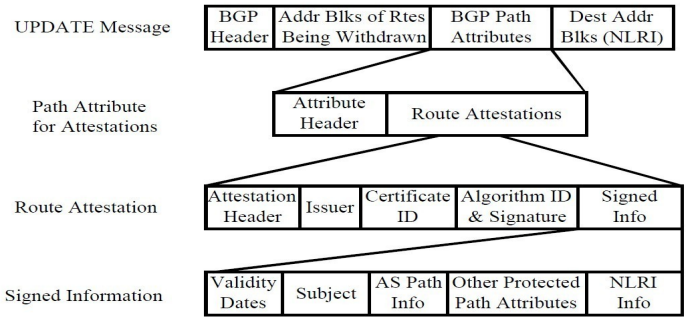


Abb.3 Update message header von S-BGP aus [3]

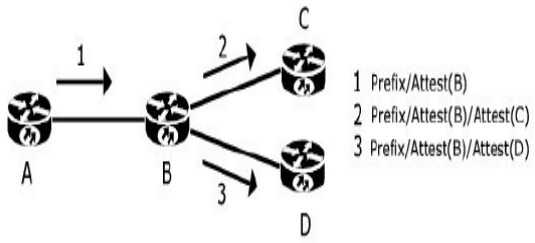


ABB.4 Funktion des S-BGPs aus [1]

Obwohl S-BGP standardisiert würde, würde S-BGP funktionieren, nur wenn die BGP-Router im Internet gleichzeitig updatet und darin S-BGP eingesetzt werden. Es ist unmöglich, weil diese Arbeit zu großen Aufwand treibt.

5.3 Route Filtern

Route Filtering ist jetzt die am weitsten benutzte Schutzmaßnahme für BGP. Es ist einfach und billig einzusetzen. Die Theorie ist sehr einfach, die BGP-Router kontrollieren die Update-Message und filter die ungültige Prefixes, um die BGP-Angriff zu verhindern.

5.3.1 Vortellung

Der Kern des Router Filterings ist die Kontrolle über die IP-Prefix-Behauptung.
Es gibt 2 Type vom Route Filtering: Ingress Filtering und Egress Filtering. Ingress Filtering leistet die Arbeit, die kommende Update-Message zu kontrollieren. Beim Egress-Filtering muss BPG-Router sich entscheidet, welche IP-Prefix er behaupten soll.

5.3.1.1 Kunden Prefix-Filtern

ISP soll die alle IP-Prefixe von Ihren Kunden Filtern. Das ist nicht sehr Schwer aber muss sehr strikt sein. ISP verteilt die IP-Prefixevan ihren Kunden, deshalb weißt er bescheid, welcher Kunde

verwaltet welche Ip-Prefix. Wenn der Kunde ein-homed ist, kann der Anbieter nur die Behauptung über die verteilte IP-Prefixe erlauben. Abb.5 Zeigt ein Beispiel über das Filtern für Kunden.
Aber wenn der Kunde multi-homed ist, ist die Situation kompliziert, weil der Kunde von anderen Anbieter die Ip-Prefixe und Route bekommen kann. In dieser Situation muss Anbieter sich entscheiden, ob er die IP-Prefixe von diesem Kunden filtern soll.
“Wenn es kein Filtern für die Kunden gibt, würde die solche Risiko erscheinen:
1. falsche Prefixe Einfügung. 2. Un-Authorized Route Einfügung 3. Re-advertise andere ISP’s Routes.” [2]Sehen Abb.6.

```
router bgp 100
  neighbor 222.222.10.1 remote-as 101
  neighbor 222.222.10.1 prefix-list customer in
  !
ip prefix-list customer permit 220.50.0.0/2
ip prefix-list customer deny 0.0.0.0/0 le 32
```

Abb.5 Configuration example on upstream aus [2]

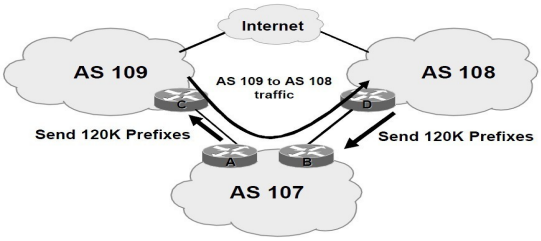


Abb.6 Re-advertise other ISP’s routes (kunde’s T1 becomes the peering link) aus [2]

5.3.1.2 Peer Prefix-Filtern

Jedes ISP soll sich entscheiden, welche IP-Prefix er behaupten und schicken soll. ISP kann seine eigene Ip-Prefixe schicken. Und vielleicht kann er die IP-Prefix,die von seinen Kunden bekommen hat, noch behaupten.
Beim Ingress Filtering gibt es mehrere Regeln:
“1. nicht akzeptieren RFC1918 etc Prefixe. 2. nicht akzeptieren eigene Prefixe. 3. nicht akzeptieren Standardeinstellung(unless you need it). 4. nicht akzeptieren prefixe länger als /24. 5. nicht akzeptieren die Prefixe von ISPs, indem AS Mitgliedschaft hat. 6. Man soll an “Net Policy Filtern” denken.”[2]
In RFC 1918 geht es um “Address Allocation for Private Internets”. Es gibt schon viele IP-Prefixe, die an private Netze verteilt werden, sowie 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
Es gibt noch “Documenting Special Use Addresses”:
“0.0.0.0/8 and 0.0.0.0/32 für Default and broadcast; 127.0.0.0/8 für Host loopback; 192.0.2.0/24 für TEST-NET for documentation; 169.254.0.0/16 für End node auto-config for DHCP.”[2]
Es würde die Fehler oder die Angriffe geben, wenn diese IP-Prefixe in Update-Message erscheint. Deshalb soll diese IP-Prefixe gefiltert werden.

5.3.1.3 Netz Policy Filtern

*“*Net Policy Filtern*”* beschreibt die Policy des Ingress-Filters, mit dem Filter das Minimum der praktischen Verteilung von der RIR(Regional Internet Registry) filtern soll.”
Wenn APNIC´s minimum-praktische Verteilung ist sowie /20, würde “Net Policy Fitern” nur /8 bis / 20 erlauben. Irgendwelche Prefixe, die länger als /20 (Z.B. /21), würde vom Filter weggeworfen.
Net Policy Filtern hat zwei Wirkungen:
1. Reduzieren die Nummer der Prefixe in ein ISP´s RIB.
2. Schutz ISP vor dem “Garbage in Garbage out” Problem im Netz.”[2]
Es gibt 3 Technike für die Net Policy: “
1. Erlaubnis für die Prefixe von RIR´s minimum-praktische Verteilung.
2. Erlaubnis für Prefixe, die von RIRs verteilt und niedriger als die von ISP eingestellte Umgrenzung,(Z.B. /24 vs/20).
3. Negierung gegen die Prefixe, die noch nicht vom IANA verteilt.” [2]
Um diese 3 Technike zu benutzen, muss Filter sofort gemäß der Veränderung im Internet, sowie ein

neues AS erscheint und so weiter, updaten. Das ist nicht einfach, weil ASes zuerst die Registers wissen lassen, dass es die Änderung im Internet gibt. Und dann würde die Liste im Register aktualisiert. Am Ende würde Filter-System aktualisiert. Deshalb gibt Es bestimmtVerspätung für die Aktualisierung.

5.3.2 Problem

Obwohl das IP-Prefix-Filtering schon weltweit benutzt wird, kann dieser Mechanismus BGP aber nicht vor allen Angriffe schutzen. Mit IP-Prefix-Filtern würde die IP-Prefix-Hijacking gelöst. Aber wenn die andere Type von der Angriff enstehen, würde Filtering vielleicht nicht mehr BGP davor schutzen kannSehen Abb.7.

Update der Filter-Datenbank ist auch ein großes Problem. “Das Routing-Update, das auf Filter basiert, steht gengen die Dynamische Eigenschft des Internets. Das völlige Routing-Filtern braucht die globale Kenntnis über die AS´s Topologie und die Beziehungen zwischen den Ases. Die Änderung in der Topologie oder der Policy würde es verurschen, dass das eingesetzte Filter nicht mehr gültig ist. Dann würde der Fehler beim Filtern erscheinen.”[2]

Attack	Filtering	S-BGP
False Updates	Partial	Secure
De-Aggregation	Possible	Secure
Contradictory Advertisements	Possible	Possible
Update Modifications	Possible	Secure
Advertent Link Flapping	Possible	Possible
Instability	Possible	Possible

Abb.7 the effctiveness of fltering and S-BGP aus [1]

6. Zusammenfassung

BGP steht heute auch vor vielen Bedrohungen. Obwohl Angreifer jetzt nicht häufig BGP angreifen, ist der Schaden sehr groß, wenn der Angriff vorkommt. Und das ganze Internet würde lahmlegen. Man arbeitet sehr fleißig dafür, und immer mehr Mechanismus werden erfunden, sowie so-BGP Ps-BGP und so weiter. Das BGP muss sicherer sein, und das Internet auch.

7. Reference

1. Beware of BGP Attacks (Ola Nordström and Constantions Dovrolis College of Computing Georgia Institute of Technology)
2. ISP Security Boot Camp Phase 1-Prepatarion for the Attack BGP Prefix Filtering (Cisco.com)
3. Secure Border Gateway Protocol(S-BGP)---Real World Performance and Deployment Issues (Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo BBN Technologies)
4. Netkit Lab:bgp:prefix-filtering (Università degli Studi Roma Tre Dipartimento di Informatica e Automazione Computer Networks Research Group)
5. RFC 4272
6. Security Issues in the Border Gateway Protocol (BGP) (Evangelos Kranakis P.C. Van Oorschot Tao Wan)
7. A Survey of BGP Security (Kevin Butler (Systems and Internet Infrastructure laboratory Pennsylvania State University) Toni Farley (Arizona State University) Patrick Mcdaniel (Systems and Internet Infrastructure laboratory Pennsylvania State University) Jennifer Rexford (Princeton University))

BGP Sicherheit

KaikaiYang

{ykkowen@hotmail.com}

Seminar “Internet Sicherheit”
Technische Universität Berlin

WS 2009/2010 (15.1.2010)