TUGAS KULIAH MAKALAH
KEAMANAN SISTEM INFORMASI (EC-5010)

-Keamanan routing pada interdomain system-

NAMA : Rizal Ferdiyan

NIM : 132 03 026

Program Studi Teknik Elektro

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

2007

ABSTRAK

Border Gateway Protocol disingkat BGP adalah inti dari protokol *routing* internet. Protocol ini yang menjadi *backbone* dari jaringan internet dunia. BGP adalah protokol routing inti dari internet yg digunakan untuk melakukan pertukaran informasi routing antar jaringan. Ia bekerja dengan cara memetakan sebuah tabel IP network yang menunjuk ke jaringan yg dapat dicapai antar Autonomous System (AS). BGP diciptakan untuk menggantikan protokol routing EGP yang mengijinkan routing secara tersebar sehingga tidak harus mengacu pada satu jaringan backbone saja.

Router router di internet menggunakan sebuah protocol routing antardomain yang disebut Border Gateway Protocol (BGP) untuk berbagi-pakai informasi routing. BGP telah menjadi “produk komersial” yang banyak dipakai dalam dunia internet, dirawat dan dikembangkan oleh insinyur insinyur jaringan yang berpengalaman.

Meskipun begitu, BGP tetap saja belum memberikan garansi sekuritas secara total. Permasalahan permasalahan routing antardomain, seperti routing yang mudah diserang (*vulnerable*) dan lemahnya performansi, telah menjadi penghambat utama dalam banyak kasus.

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet merupakan ‘network of networks’ jaringan dari banyak jaringan. Jaringan jaringan tersebut saling berbagai pakai informasi yang dibundle dalam bentuk paket paket IP, melalui berbagai router. Group router yang berada dibawah pengawasan satu lembaga/korporat dinamakan *autonomous system* (AS). Router router di internet menggunakan sebuah protocol routing antardomain yang disebut Border Gateway Protocol (BGP) untuk berbagi-pakai informasi routing. BGP menjadi suatu standart *de facto* sebagai suatu protocol routing inter-Autonomous System (AS).

Informasi di internet dikirim dalam bentuk paket IP mengikuti alur (path) yang dibentuk oleh router, dari lokasi sumber ke lokasi tujuan. Router, secara kolektif bertanggung jawab atas perawatan semua path agar rute rute ke tujuan dapat dicapai. Dalam hal ini, informasi *reachabilities* network di*share* di antara router router melalui protocol routing. Trafik diterima oleh router, kemudian dikirim berdasarkan informasi *reachabilities* yang tersimpan dalam table forwarding. Informasi yang lain disimpan dalam header paket.

Meskipun BGP secara umum tetap cukup stabil, bukan mustahil pada sesi sesi tertentu sebagai akibat dari teknologi yang telah maju justru membawa masalah masalah bari dibidang securitas. Dan nyatanya, BGP memiliki keterbatasan dalam hal sekuritas dalam routing interdomain.

Mengingat pentingnya peran BGP pada jaringan internet dunia, maka mau tak mau keamanan menjadi issue yang sangat penting dalam penyelenggaraan routing dengan protocol BGP, karena jika BGP terkena *serangan* dari seseorang atau sekelompok orang maka jaringan *backbone* internet akan terganggau.

1.2 Batasan Masalah

Dalam tulisan ini akan dibahas mengenai gambaran routing intenet secara umum, factor keamanan dalam routing, gambaran khusus tentang BGP dan factor keamanan yang berpotensi untuk menggangu proses dari routing BGP serta solusi solusi yang bisa diterapkan untuk mengatasi hal tersebut.

1.3 Tujuan Penulisan

Tulisan ini bertujuan untuk memahami factor factor yang berpotensi menjadi pengganggu dalam proses routing interdomain dan menjelaskan solusi solusi apa saja yang dapat diterapkan untuk mengatasinya.

1.4 Metodologi Penulisan

Metode penelitian yang dilakukan adalah dengan studi literatur-literatur yang terkait dengan tema. Kemudian akan dicoba untuk menerapkan sedikit contoh yang berhubungan dengan topik bahasan.

BAB 2
ROUTING INTERDOMAIN

2.1 Proses Routing

Routing, adalah sebuah proses untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah *internetwork*. Routing juga dapat merujuk kepada sebuah metode penggabungan beberapa jaringan sehingga paket-paket data dapat hinggap dari satu jaringan ke jaringan selanjutnya. Untuk melakukan hal ini, digunakanlah sebuah perangkat jaringan yang disebut sebagai *router*. *Router-router* tersebut akan menerima paket-paket yang ditujukan ke jaringan di luar jaringan yang pertama, dan akan meneruskan paket yang ia terima kepada router lainnya hingga sampai kepada tujuannya.

Routing di Internet diperlukan dalam menentukan jalur untuk mengantarkan paket ke alamat tujuan. Pada kenyataannya di Internet, sangat mungkin terjadi keadaan di mana banyak jalur yang dapat ditempuh untuk menuju suatu alamat tertentu. Agar dapat menentukan jalur mana yang akan dipakai, masing-masing router (alat yang bertugas merutekan paket) saling bertukar informasi tentang topologi jaringan miliknya. Hal ini merupakan salah satu fungsi dari protokol routing. Di Internet, routing ditangani oleh dua protokol routing yang masing-masing memiliki tujuan yang berbeda yaitu routing Interior Gateway Protokol (IGP) dan Exterrior Gateway Protokol (EGP). Protokol routing intradomain bertugas mengatur routing di dalam domain atau dalam satu AS, sedangkan protokol routing interdomain bertugas mengatur routing antar domain atau antar AS. Oleh karena itu router router yang mempunyai nomor AS yang sama dikatakan berada dalam satu domain.

Terdapat dua hal utama yang menjadi alasan pembagian jenis routing di atas. Yang pertama adalah kebutuhan akan skalabilitas. Protokol routing intradomain biasanya memiliki pengetahuan yang detil tentang topologi domain secara keseluruhan. Protokol ini mampu menangani routing menuju ke setiap tujuan dalam domain. Berbeda dengan protokol routing intradomain, protokol routing interdomain tidak memiliki pengetahuan yang detail tentang topologi Internet. Pengetahuan protokol ini hanya sebatas interkoneksi antar domain saja. Selain itu, protokol ini hanya menangani routing hanya kepada kumpulan IP address yang besar saja, akibatnya protokol ini tidak dapat mengantarkan paket ke setiap tujuan di Internet. Hal ini berarti juga mengurangi beban dari router-router di jaringan karena router-router tersebut cukup memiliki tabel routing pada tingkat alamat prefix jaringan yang telah diagregasi.

Alasan kedua dari pembagian routing adalah independensi dari domain. Setiap domain diperbolehkan untuk mengatur routing intradomain mereka secara bebas dan independen dan juga diperbolehkan untuk menerapkan routing policy yang sesuai untuk mereka. Policy ini misalnya suatu domain menolak untuk meneruskan paket transit yang ditujukan ke domain lain. Dengan adanya independensi ini, routing di interdomain lebih kompleks daripada routing intradomain karena policy routing yang diterapkan oleh suatu AS berpengaruh terhadap AS lainnya, khususnya AS tetangga Suatu AS pada umumnya tidak ingin mengungkap topologi intradomain mereka kepada AS lain. Selain itu, suatu AS juga tidak ingin mengungkap hubungan bisnis mereka dengan AS tetangga mereka, sebagai strategi bisnis menghadapi pesaing.

2.2 Routing Interdomain

Pada awalnya, Internet adalah suatu eksperimen jaringan komputer yang digunakan untuk penelitian. Pada perkembangannya, Internet kemudian menjadi jaringan komputer yang terdistribusi dan mendunia. Internet membawa trafik berupa informasi yang dikirim dan diterima oleh orang atau mesin yang berada di dua tempat yang berbeda, selama mereka terkoneksi dengan jaringan. Secara umum, Internet merupakan kumpulan komputer yang terkoneksi secara fisik, baik melalui fiber optic, maupun melalui gelombang elektromagnetik (misalnya dengan satelit atau sistem radio terestrial). Internet merupakan 'networ of networks' jaringan dari banyak jaringan. Jaringan jaringan tersebut saling berbagai pakai informasi yang dibundle dalam bentuk paket paket IP, melalui berbagai router. Seperti yang telah dikatakan diatas group router yang berada dibawah pengawasan satu lembaga/korporat dinamakan *autonomous system* (AS); kita mengenal tga tipe AS yaitu stub, multihome, dan transit.

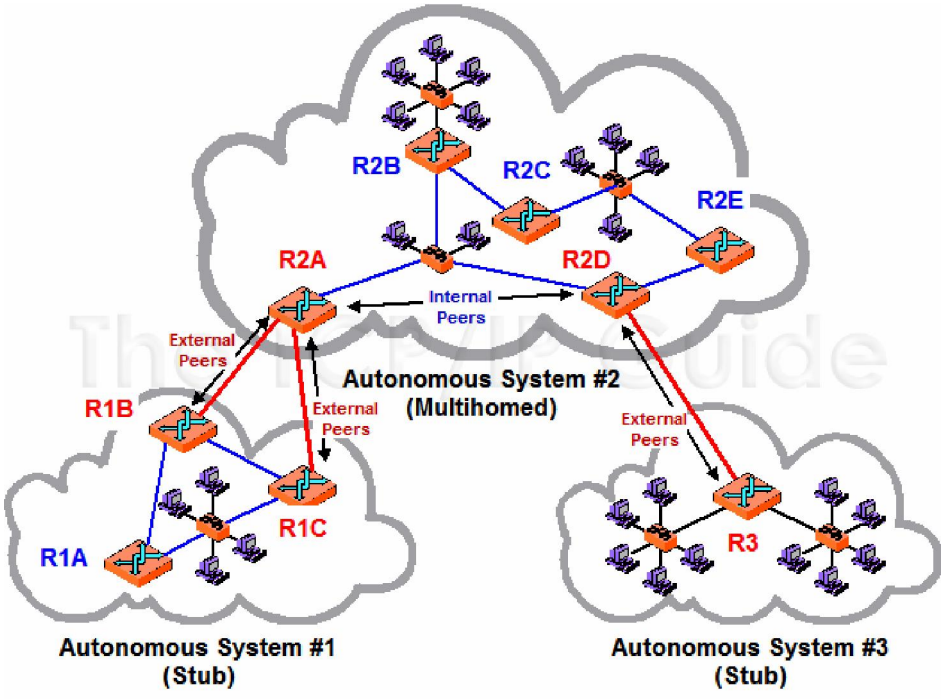
As stub merupakan titik ujung komunikasi (endpoint), sedang AS multihomed adalah AS AS stub dengan multiple link ke internet. AS transit merupakan AS multihomed yang mengizinkan pelepasan traffic melaluinya dan bukan komunikasi endpoint (contohnya provider provider internet).

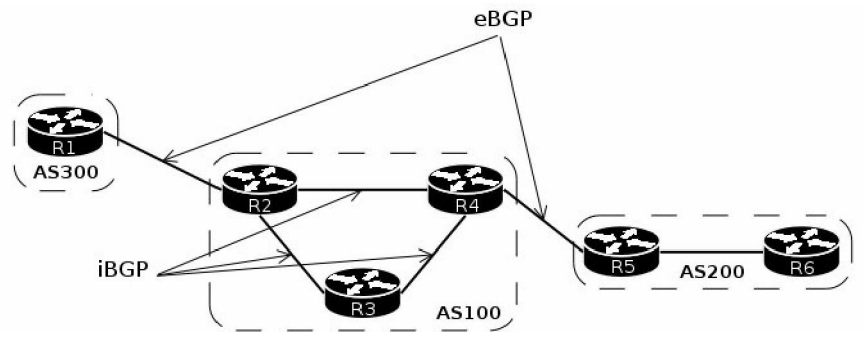
Untuk proses routing interdomain router router menggunakan Exterior Gateway Protocol (EGP). Adapun standar de facto EGP yang dipakai dalam internet adalah Border Gateway Protokol (BGP). Protocol ini yang menjadi *backbone* dari jaringan internet dunia. BGP adalah protokol routing inti dari internet yg digunakan untuk melakukan pertukaran informasi routing antar jaringan. BGP bekerja dengan cara memetakan sebuah tabel IP network yang menunjuk ke jaringan yg dapat dicapai antar Autonomous System (AS). Hal ini digambarkan sebagai sebuah protokol path vector. BGP tidak menggunakan metrik IGP (Interior Gateway Protocol) tradisional, tapi membuat routing decision berdasarkan path, network policies. Dari Januari 2006 hingga saat ini BGP versi 4 masih digunakan.

BAB 3
KEAMANAN ROUTING INTERDOMAIN

3.1 Permasalahan Umum Sekuritas BGP

Sebuah router yang menjalankan protocol BGP dikenal dengan BGP *speaker*. Speaker speaker ini berkomunikasi melintasi TCP dan mereka terbagi menjadi peer peer atau *neighbor neighbor*. TCP adalah protocol yang berorientasi koneksi yang cukup popular dan dapat diandalkan. Dengan mempekerjakan TCP, BGP tidak perlu khawatir memberikan koneksi error pada layer *transport.* Kumpulan beberapa router dinamakan sesi (*session*). Peer peer BGP dalam AS yang sama (internal peer) berkomunikasi via internal BGP (iBGP). Sedang external BGP (eBGP) digunakan diantara speaker speaker berbeda dalam AS AS yang berbeda.





Kedua gambar di atas menunjukkan bagaimana jalinana antarAS dan peer peer BGP. Saat ini di internet terdapat belasan ribu AS. Masing masing AS ini menghasilkan satu atau lebih addres *prefix*. Prefix adalah sebuah representasi untuk satu blok IP IP address.

Pada router router tersebut mereka saling bertukar *message* untuk mengetahui informasi yang terdapat pada tetangganya. Message message BGP tersebut telah menjadi subjek untuk dimodifikasi, dihapus, dipalsukan ataupun direplay secara tidak sah. Eksploitasi eksploitasi ini dapat ditimbulkan oleh beberapa usaha, yang pada intinya membuat router router BGP 'misconfigure'. Miskonfigurasi, skalipun tidak sengaja dapat diartikan sama dengan penyerangan. Miskonfigurasi merupakan factor utama penyebab 'de-aggregasi' spasi addres, terutama dalam table table BGP yang besar. Sebagai contoh jika salah satu AS mengumumkan bahwa ia memiliki address address dalam 24.0.0.0/8, sementara router misconfigures mengklaim memiliki 22.132.0.0/16, maka spasi address terdahulu menjadi di-aggregasi.

Berdasarkan uraian diatas, terlihat bahwa BGP memiliki beberapa kelemahan utama yaitu:

- BGP tidak memproteksi integritas message, keutuhan serta authentikasi sumbernya

- BGP tidak memvalidasi otoritas AS yang mempublikasikan reachabilitas informasi.
- BGP tidak menyakinkan authentikasi path path attribute yang dipublikasikan oleh sebuah AS.

Selama ini arsitektur BGP telah membuka peluang atas beberapa bentuk ancaman, baik karena kesalahan pengelolaan atau aksi aksi serangan yang dilancarkan pihak pihak tertentu. Tiga titik yang sering menjadi target utama pelanggaran dalam konektivitas BGP adalah :

i. Link diantara router router yang saling terhubung
ii. Router itu sendiri yang menangani proses routing
iii. Station menajemen yang mengontrol router router

Bila ditinjau secara umum, serangan serangan BGP yang dilancarkan *attacker* memiliki beberapa tujuan spesifik berikut :

i. Menurunkan kualitas layanan, baik secara local atau global
ii. Merutekan ulang traffic yang disebarkan (melalui sebuah path) ke suatu subjek tertentu. Disini *attacker* dapat melakukan hal hal sbb : mengkopi traffic dan melepaskan ke suatu tujuan, memodifikasi traffic dan melepasnya kembali ke tujuan asli, menghapus salah satu traffic, menyamar sebagai pengirim (subscriber), atau mengkonsumsi traffic yang diarahkan kepadanya dan meresponnya sekehendak hati.

3.2 Bentuk Serangan.

Kelemahan yang ditemukan dalam routing acap kali menjadi celah penyerangan. Saat ini routing antardomain ditengarai memiliki sejumlah kelemahan untuk beberapa bentuk serangan. Secara garis besar ancaman ancaman ini menyerang tiga level komunikas BGP, message control saat menset up sebuah

sesi, message error sepanjang durasi sebuah sesi, dan reachabilitas update update. Dibawah ini sederet bentuk penyerangan yang umum terjadi pada konektivitas BGP.

3.2.1 Eavesdropping

Penyeranga mengintip data dalam kabel. Tipe serangan ini secara potensial memungkinkan penyerang mengakses informasi informasi rehasia yang diforward di antara AS-AS.

Dalam kasus eavesdropping informasi routeing (seperti update update routing), tidaklah begitu dikhawatirkkan. Data data routing BGP dapat bersifat rahasia, tetapi tipe kerahasian ini umumnya tidak begitu kruasial. Namun pada beberapa organisasi besar yang melakukan pertukaran policy policy peer sensitive, perlindungan terhadap data data yang dilepas, jelas menjadi focus perhatian

3.2.2 Replay

Penyerang mencegat (merekam) message, kemudian mengirim ulang ke pengirim original. Pelanggaran ini dapat mengacaukan fungsi dan kemampuan BGP dalam merawat routing, sebab router dapat menjadi overload. Gejala ini sama dengan korban serangan *denial of service* (DOS).

3.2.3 Message insertion

Penyerang memasukkan message gadungan ke sebuah sesi BGP sehingga dapat merusak koneksi peer di antara router router (misal membuat sesi terhenti). Mungkin pula penyerang memasukkan informasi routing data yang tidak benar. BGP tidak dapat secara langsung memproteksi pelanggaran ini.

3.2.4 Message deletion

Penyerang berusaha menangkap message message yang dilepas diantara peer peer BGP dan kemudian menghapusnya. Menghapus update message dapat mengakibatkan table routing tidak akurat. TCP memiliki proteksi yang terbatas untuk serangan semacam ini.

3.2.5 Message modification

Penyerang berusaha menghapus message dari suatu sesi BGP, memodifikasinya lalu memasukkan kembali ke dalam session BGP. Seperti pada penyerangan *message insertion*, pelanggaran semacam ini juga dapat menyebabkan routing tidak akurat, merusak hubungan peer peer dan menggagalkan routing.

3.2.6 Man in the middle

Penyerang berusaha menumbangkan arus komunikasi di antara peer peer dan berperilaku seolah olah sebagai sebagai pengirim (sender) atau sebaliknya sebagai penerima (receiver). Pertahanan BGP atas tipe serangan ini mungkin sama dengan tipe *message insertion, message deletion, message modification.* Dan karena BGP tidak memberikan dukungan authentikasi sumber, maka serangan ini seringkali menjadi bentuk ancaman yang mengkhawatirkan.

3.2.7 Denial of service (DoS)

DoS telah menjadi bentuk ancaman yang paling popular dalam beberapa decade terakhir. Disini para penyerang membanjiri sebuah sesi dengan setumpuk resource yang terus menerus dan melelahkan. Dalam konteks BGP, tipe serangan ini dapat berupa table routing yang kebanjiran banyak rute. Akibatnya ukuran table melampui kapasitas. Kasus ‘self deaggregation’ merupakan bagian dari denial of service manakala sebuah

AS memberitahukan prefik prefik untuk di aggregate. Dengan demikian akan terjadi proses advertising yang tak dibutuhkan. BGP sangat berpeluang untuk mengalami serangan macam ini

Serangan serangan BGP dalam perilakunya bisa berbentuk *pasif* atau *aktif*. Serangan dikategorikan pasif jika penyerang hanya melakukan observasi tanpa melakukan tindakan lebih jauh. Contohnya antara lain berupa: *eavesdropping.*
Bentuk serangan ini biasanya bertujuan mencari aktivitas yang berpeluang diganggu, atau hanya mengintai untuk keperluan penyerangan berikutnya. Sedang bentuk serangan aktif, terjadi manakala seoranga penyerang berusaha secara langsung memanipulasi protocol protocol routing. Serangan serangan yang bersifat merusak biasanya masuk dalam kategori ini.

Serangan BGP pada dasarnya mengganggu infrastruktur dengan cara merusak koneksi diantara peer peer, dengan kata lain penyerang berusaha menutup atau menghentikan sesi sesi BGP dan TCP yang berjalan.
Sekuritas antar domain dapat digambarkan menurut akibat akibat yang terjadi :

- *Disclosure:* eavesdropping, deliberate exposure, sniffing, traffic analysis.
- *Deception :* message insertion, deletion, modification, man in the middle
- *Distruption :* replay, DoS
- *Usurpation :* perolehan kendali atas layanan dan fungsi route

BAB 4
SOLUSI KEAMANAN ROUTING INTERDOMAIN

4.1 Keamanan pada koneksi *peering* antar router BGP.

Ujung dari network, dimana dua autonomous system (AS) bertemu meerupakan factor keamanan yang paling mengkhawatirkan pada protokol BGP. Pada kondisi tersebut kedua AS tersebut diatur dan dijaga oleh dua organisasi yang berbeda dengan tujuan dan prinsip yang berbeda pula.

Jika terjadi koneksi *peering* antar router BGP maka BGP speaker yang mengadakan koneksi tersebut akan sangat rawan untuk diserang. Jika seseorang ataupun organisasi telah dapat menyerang dan menguasai BGP speaker maka dia akan mendapat kontrol atas network tempat BGP speaker tersebut bernaung.

Terdapat beberapa cara untuk melindungi BGP speaker, diantaranya sbb : traffic filter, MD5 authentication, *Generalized TTL*.

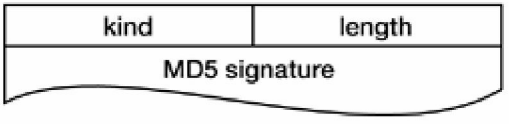
4.1.1 Traffic Filter

Langkah pertama untuk melindungi BGP speaker adalah packet filter. Pada umumnya melakukan *filtering* terhadap semua paket yang keluar masuk network merupakan langkah yang bagus. Sebagai contohnya *filtering* dapat dilakukan dengan melakukan blocking terhadap paket paket yang akan masuk kecuali yang paket yang kita inginkan. Namun dalam melakukan *filtering* ini kita harus secara explicit menyatakan paket apa saja yang kita perbolehkan untuk mengakses network kita dan setelah itu kita mendefinisikan paket yang akan diblocking selain dari paket yang kita perbolehkan.

4.1.2 MD5 authentication

BGP juga dapat menggunakan mekanisme authentication MD5 untuk melakukan authentikasi dengan peer tertentu dalam melakukan transmisi paket. MD5 tidak digunakan dalan melindungi paket (melindungi paket agar tidak berubah) juga tidak digunakan untuk menghilangkan informasi yang ditransmisikan pada paket, namun MD5 digunakan untuk melakukan *verifikasi* peer yang aktif.

Authentikasi MD5 berdasarkan pada mekanisme *key*, yang dikenal juga dengan mekanisme *shared secret*, yang dapat dirubah setiap waktu dan dibagi oleh kedua BGP peer. Setiap router menggunakan kunci ini, dan dengan proses matematika (MD5 algoritma) untuk membuat suatu nomor. Nomor ini disebut *diggest signature*, disertakan dalam paket ketika dikirimkan. Penerima menggunakan local dan membuat suatu nomor yang sama dengan paket yang diterima. Namun jika penerima tidak dapat membuat suatu nomor yang sama maka paket akan terbuang. *Key* ini tidak ditransmisikan dalam suatu koneksi, jadi network administrator harus melakukan konfigurasi *key* secara manual. Jika ingin melakukan perubahan terhadap *key* maka harus dilakukan secara manual. Pada paket yang ditransmisikan MD5 disisipkan dengan menambah suatu header baru pada TCP header :

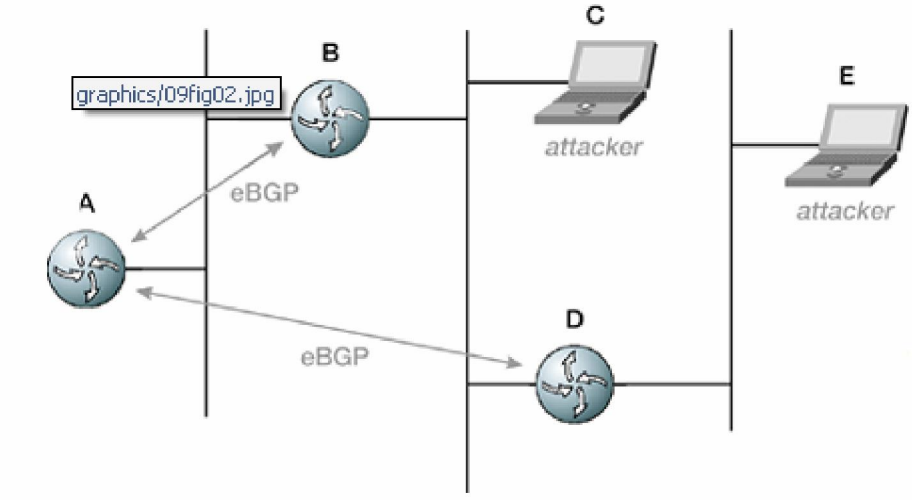


- Kind : mengindikasikan type dari TCP option header. Pada kasus ini, hal ini menandakan TCP software dan MD5 *message digest* yang diikutsertakan dalam TCP header.

- Length: Parameter ini selalu berisi 18 untuk TCP MD5 diggest authentication header.
- MD5 Signature: Parameter ini berisi MD5 authentication digest, yang selalu diconfigurasi dengan 16 octets.

4.1.3 *Generalized TTL*

Salah satu kelemahan dari BGP adalah BGP menggunakan TCP sebagai mekanisme transport. Hal ini berarti pada *unicast* paket, yang dapat berasa dari *host* manapun di internet, dapat melakukan serangan kepada BGP router. Untuk mengatasi hal ini, beberapa methode dapat digunakan, Mekanisme keamanan *Generalized TTL*, yang dijelaskan dalam RFC 3682 merupakan methode untuk memastikan tidak ada paket yang dikirimkan oleh *host* yang berada di luar jangkauan dari peer yang telah dikenal dan diterima oleh BGP speaker.



Misalkan suatu penyerang ingin masuk router A, maka penyerang dapat menggunakan host C dan mengirimkan *unicast* paket kepada ip address router A. Jika ia dapat menemukan kombinasi yang tepat dari nomor TCP sequence dan informasi lainnya, maka penyerang dapat

mengganggu *session* antara router A dan router B atau ia dapat menyisipkan informasi yang salah terhadap system routing dengan malakukan *hijacking* session antara router A dan router B.

Namun bayangkan jikan router A memutuskan bahwa router B terkoneksi secara langsung dan jika router B melakukan konfigurasi TTL pada tiap paket yang ditransmisikan pada 255, maka A menerima paket tersebut dengan paket TTL yang sama atau mungkin 254. Jika hal ini dikonfigurasi pada kedua router maka C tidak termasuk dalam daerah dimana serangan dapat dilancarkan. Satu satunya cara agar C dapat melakukan penyerangan kepada A adalah melakukan konfigurasi TTL terhadap paket yang dikirim dengan nilai lebih besar dari 255, yang tidak mungkin dilakukan.

Tipe pertahanan ini dapat juga diaplikasikan pada multihop BGP session. Sebagai contoh jika router A mengetahui bahwa jarak router D adalah dua hops, maka filtering dapat dilakukan dengan cara hanya menerima paket dengan nilai 253 ataupun lebih besar.

4.2 Protokol protokol tambahan dalam routing interdomain.

Selain methode keamanan diatas terdapat juga protokol protokol khusus yang telah diciptakan untuk meningkatkan keamanan dari routing interdomain. Protokol protokol tersebut diantaranya adalah : Secure BGP (s-BGP), Interdomain Route Validation (IRV) service, dan Secure Origin BGP (soBGP)

4.2.1 Secure BGP (s-BGP)

Secure BGP adalah salah satu alternative untuk menjalankan BGP secara lebih *secure* atau aman. Melalui fitur fiturnya, secure BGP berusaha menangani isu isu sekuritas mayor yang ditemukan dalam BGP.

S-BGP mempresentasikan ekstensi untuk BGP

- s-BGP menggunakan fasilitas BGP standart untuk membawa data tambahan tentang path path dalam update message
- s-BGP menambahkan set tambahan untuk mengecek algoritmas seleksi rute BGP

S-BGP mencegah perangkap perangkap yang umumnya terjadi dalam infrastruktur routing saat ini. Mekanisme s-BGP menawarkan dinamika yang sama dengan BGP origin, dan dapat dikatakan setaraf.

Arsitektur sekuritas yang ditawarkan s-BGP tersusun dalam tiga mekanisme, yang ketiganya bersama sama membangun system autorisasi dan authentikasi yang handal:

1. Public Key Infrastructure (PKI)
2. Path attribute BGP baru, dan
3. Masukan untuk IP security

PKI bekerja menggunakan sertifikat sertifkat virtual untuk menyimpan kunci kunci public (public keys). Pengesahan 'ditandatangani' oleh BGP speaker memakai 'tanda tangan' private key yang diasosiasikan dengan public key dalam sertifikat PKI. Path attribute BGP-baru, diperkenalkan untuk membawa pengesahan pengesahan dalam update message. Dengan demikian, path attribute memberikan metode untuk memvalidasi message message update BGP.

Solusi yang ditawarkan ketiga mekanisme di atas sebetulnya mengacu pada *hop integrity, origin authentication,* dan *path validation.*

- Hop integrity

Hop integrity diberikan oleh s-BGP melalui *per-hop data integrity* dan *per-hop source authentication.* s-BGP menggunakan protocol Encapsulating Security Payload (ESP) dari IPSec untuk memberikan tipe sekuritas ini.

- Origin authentication

  Diberikan s-BGP menggunakan PKI dan pengesahan pengesahan address. Infrastruktur PKI menggunakan dua sertifikat untuk memungkinkan router router mengaunthetikasi identitas dan autorisasi sebuah speaker BGP. Satu PKI disajikan untuk alokasi address; yakni menetapkan organisasi kepemilikan dari IP IP address. PKI kedua memanage penugasan AS dan asosiasi asosiasi router melalui kombinasi dari tiga sertifikat: AS number dan public key organisasi; AS number dan public key-nya; serta AS number dan juga nama informasi router (Domain name system (DNS), ID, juga public key). Pengesahan pengesahan address digunakan oleh AS AS pembuka dan menetapkan bahwa sebuah AS memiliki otoritas untuk mengadvertise sebuah path ke spasi address tertentu, dan ia ditandatangani oleh pemilik owner spasi address tersebut. Tanda tangan dalam sebuah pengesahan adalah berupa private key yang dibubuhkan oleh owner, yang sesuai dengan public key dalam sertifikasi PKI untuk alokasi address.

- Path validation

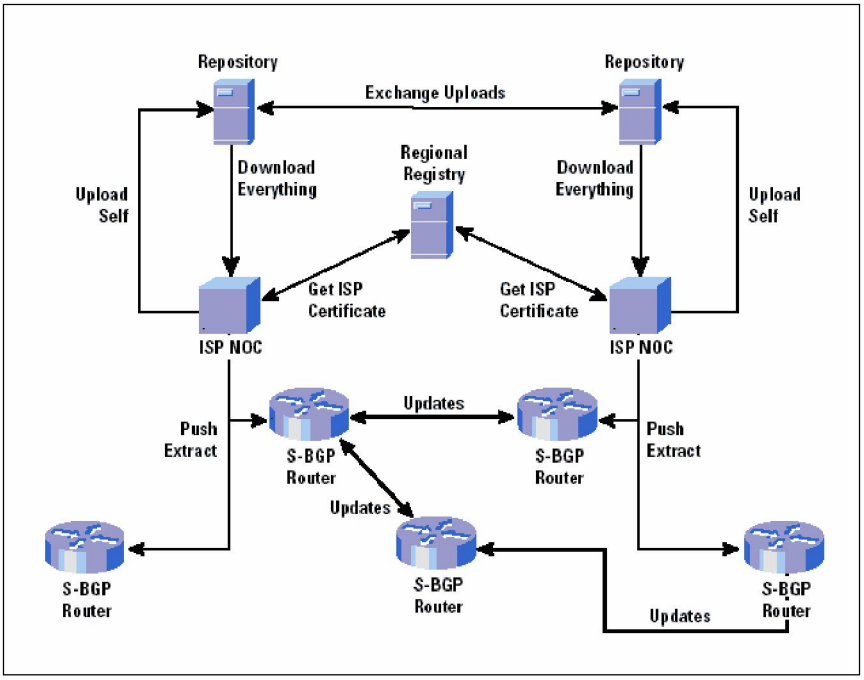
  Diberikan dengan bantuan pengesahan pengesahan rute. Pengesahan pengesahan ini digunakan ini digunakan oleh AS transit untuk mengijinkan verifikasi informasi path.

Saat dikombinasikan dengan sertifikat sertifikat PKI yang diperkenalkan s-BGP, suatu speaker dapat memvalidasi otentitas dan integritas setiap AS

dalam suatu path dari sumber ke neighbor terdekat dengan cara membandingkan pengesahan pengesahan dan database sertifikat.

Design s-BGP

- S-BGP menggunakan teknologi
    - IPsec untuk melindungi komunikasi point to point trafik BGP
    - Public Key Infrastructure untuk memberikan layanan autorisasi
    - Framework yang mempresentasikan spasi address dan AS 'ownership'
    - Attestations (pengesahan/data tanda tangan digital) untuk mengikat informasi authorisasi ke update message.



- S-BGP menuntut router router untuk :
    - Mengantarkan sebuah pengesahan saat menggenerasikan sebuah update untuk router s-BGP yang lain.

- Memvalidasi pengesahan pengesahan yang diasosiasikan dengan update yang diterima dari router s-BGP yang lain.

IPsec dalam s-BGP

- s-BGP memakai IPsec untuk memproteksi semua traffic BGP di antara router router neighbor
- IPsec menerapkan kriptogafi untuk authentikasi data, integritas data, dan fitur fitur anti replay.
- IPsec dapat juga digunakan untuk memfilter semua traffic managemen yang dialamatkan ke sebuah router, dengan demikian dapat meningkatkan keamanan protocol protocol managemen yang lain.
- IPsec memperhatikan opsi MD5 TCP yang banyak digunakan dalam teknologi sekuritas saat ini.

PKI dalam s-BGP.

- Sertifikat sertifikat public key (X.509) dikeluarkan untuk ISP ISP dan atau subscriber untuk mengidentifikasi pemilik (owner) sebuah prefix AS dan prefix prefix.
- Prefix prefix dan public key dalam sertifikat sertifikat digunakan untuk memeriksa autorisasi pengesahan pengesahan address.
- Pengesahan pengesahan address, AS dan public keys dari sertifikat sertifikat digunakan sebagai input untuk memverifikasi update message.
- PKI tidak sepenuhnya memberi jaminan bagi organisasi-organisasi, melainkan hanya menegaskan dan mengmodifikasi hubungan-hubungan antara registri-registri regional, ISP ISP, dan subscriber subscriber.

4.2.2 Interdomain Route Validation (IRV) service

Layanan Interdomain Route Validation service adalah protocol penerima (receiver) yang diasosiasikan dengan arsitektur yang bekerja dalam lingkungan BGP. Ini berbeda dengan s-BGP yang berusaha menggantikan BGP. Dalam protocol ini, setiap AS memiliki validator yang dirancang IRV, yang berguna untuk mengauthentikasi informasi yang diterima saat routing update message. Penerima message selanjutnya dapat memilih untuk menyakinkan sebuah update dengan mengeceknya pada IRV neighbor melalui sebuah query.

Dalam model ini, masing masing AS memiliki tanggung jawab untuk memilih algoritma yang menetapkan kapan sebuat update message harus dipertanayakan. Bergantung keputusan, sebuah message dapat dicurigai. AS dapat melakukan query atas semua AS di sepanjang path (via komunikasi IRV) untuk memeriksa autentitas dan akurasi message tersebu. Solusi IRV dapat dikatakan unik sebab ia tidak perlu menggunakan public/private key atau teknologi signature seperti yang terjadi dalam s-BGP.

Tiga komponen utama dalam system IRV:

- Hop integrity

  Diberikan oleh system IRV oleh karena validator validator dapat berbicara ke semua elemen dalam network. DI sini data integrity

disiapkan sebanyak yang dibutuhkan. Meski begitu, ini tidak diberikan dalam basis per message.

- Origin authentication

  Authentikasi origin ini diberikan melalui cara yang sama dengan saat mengauntetikasi sumber (source). Dengan cara mengkorborasi data IRV IRV pengirim dan neighbor, metode ini memiliki kemampuan

- Path validation

  Disiapkan dalam IRV untuk meng query setiap AS dalam path yang diberikan dalam sebuah update message.

4.2.3 Secure Origin BGP (soBGP)

Secure origin BGP (soBGP) bekerja memproses sebuah ekstensi untuk BGP. Tidak seperti s-BGP dan IRV, solusi ini tidak menyelenggarakan protocol atau arsitektur baru. Melainkan hanya menambahkan perbaikan perbaikan atas protocol BGP standar. Ektensi ini menyajikan sebuah metode authentikasi yang memanfaatkan tipe message BGP baru, SECURITY.

Message security memungkinkan speaker BGP melakukan share sertifikat sertifikat yang memuat kunci kunci public (public key). Sertifikat sertifikat ini ditanda tangani oleh pengirim (sender) menggunakan sebuah private key, mengizinkan penerima (receiver) memvalidasi pasangan public/private key tersebut. Solusi soBGP nyatanya cukup handal untuk memvalidasi semua advertisement BGP.

Fokus utama system soBGP melingkupi:

§ Origin authentication

Diberikan dalam soBGP melalui tiga tipe sertifikat yang ditransportasikan oleh message security:

- Entity
- Policy dan
- Authorization

Sesuai dengan namanya, sertifikat entity digunakan untuk memverifikasi eksistensi sebuah entity (misalnya sumber/source) dalam sebuah system routing. Sertifikasi policy memberikan informasi tentang AS yang dapat digunakan untuk memvalidasi authentisitasnya. Adapun sertifikasi Authorization memberikan informasi tentang otoritas AS untuk memperkenalkan sebuah addres.

§ Path validation

Diberikan melalui verifikasi path dan validasi validasi AS. Verifikasi path disupport melalui pembuatan databases path. Untuk membangun databases ini setiap speaker mengumumkan pada AS yang lain bahwa ia dikoneksikan via sebuah file ‘attached AS’ dalam sertifikat poliy. Dari informasi ini, speaker speaker dapat mulai membentuk sebuah database path untuk semua path yang mungkin bagi sebuah prefix.

§ Integritas Hop

Perhatian integritas data sebenarnya menyakinkan bahwa data yang mendarat pada router penerima tidak termodifikasi sedikit pun selama transmisi berlangsung. Adapun modifikasi modifikasi data disini bisa beragam bentuk. Contoh sederhananya, adalah perubahan nilai AS Path ke sebuah prefix sehingga data dirutekan melintasi link yang salah. Contoh lainnya adalah permasalahan authentikasi sumber (source authentication). Authentikasi sumber berkaitan dengan permasalahan tentang penetapan bahwa sebuah peer benar benar berasal dari si pengirim asli. Jadi dalam hal ini, tidak ada manipulasi.

BAB 5
KESIMPULAN

BGP adalah protocol yang menyuguhkan routing interdomain di internet. Meskipun BGP secara umum cukup stabil, bukan mustahil pada sesi-sesi tertentu, akibat teknologi yang makin maju, justru membawa masalah masalah baru di bidang sekuritas (security). Dan nyatanya, BGP memiliki keterbatasan dalam hal sekuritas routing antardomain.

Mengingat pentingnya peran BGP pada jaringan internet dunia, maka mau tak mau keamanan menjadi issue yang sangat penting dalam penyelenggaraan routing dengan protocol BGP, karena jika BGP terkena *serangan* dari seseorang atau sekelompok orang maka jaringan *backbone* internet akan terganggau.

Untuk mengatasi issue keamanan pada protocol BGP dapat dilakukan dengan berbagai cara, diantaranya sbb : Secure BGP (s-BGP), Interdomain Route Validation (IRV) Service, Secure Origin BGP (soBGP) ataupun solusi keamanan pada waktu terjadi koneksi *peering* antar router BGP.

DAFTAR PUSTAKA

1. RFC (Request For Comment) 4271, *Border Gateway Protocol*
2. RFC 4272, *BGP Security Vulnerabilities Analisys*
3. Kevin Butler, *A survey for BGP security,* Computer Communication.
4. Aiello,W., Ioannidis, J., andMcDaniel, P. 2003. Origin authentication in interdomain routing ACM CCS'03, Washington, DC, USA
5. Alaettinoglu, C. and Shankar, A. U. 1995. The viewserver hierarchy for interdomain routing: Protocols and evaluation. IEEE Journal on Selected Areas in Communications 13, 8 (Oct.),1396–1410.
6. Avramopoulos, I., Kobayashi, H., Wang, R., and Krishnamurthy, A. 2004. Highly secure and e cient routing. IEEE INFOCOM 2004, Hong Kong, PRC.
7. Baltatu, M., Lioy, A., Maino, F., and Mazzocchi, D. 2000. Security issues in control, man-agement and routing protocols. Computer Networks (Amsterdam, Netherlands: 1999) 34, 6,881–894. Elsevier Editions, Amsterdam.