	عنوان مقاله: مزایا و چالشهای امنیتی پروتکل BGPSec تهیه کننده/گان مدرک و رشته تحصیلی رشته شغلی اکرم گل پرور مهندسی کامپیوتر-سخت افزار کارشناس زیرساخت‌های فناوری اطلاعات و ارتباطات اداره کل/دفتر: معاونت فنی(اداره کل طرح و توسعه شبکه)

مزایا و چالشهای امنیتی پروتکل BGPSec

چکیده

پروتکل BGP از آسیب‌پذیری‌های امنیتی متعددی رنج می‌برد، به‌عنوان مثال، routing update های جعلی منجر به ربودن و یا ممانعت ارسال ترافیک می‌شود. اگرچه پروتکل BGPsec ادعا دارد که این آسیب‌پذیری‌ها را با بررسی و ارزیابی routing update می‌تواند برطرف کند اما با توجه به آسیب پذیری های امنیتی ذاتی BGP، برخی آنان با وجود پیاده سازی BGPsec، به عنوان مثال قابلیت ربودن ترافیک، همچنان وجود دارد. در این مقاله به بررسی سیستماتیک آسیب‌پذیری‌های BGP با BGPsec می‌پردازیم و اینکه تضمین امنیتی مورد نظر در inter-domain routing بدست نمی‌آید وتأثیر آسیب‌پذیری‌ها را با استفاده از یک ردیابی داده واقعی اندازه‌گیری می‌کنیم.

کلیدواژه: inter-domain routing، routing path، routing update، routing path

مقدمه

BGP یک پروتکل مسیریابی بین دامنه‌ای است که امکان اتصال اینترنت را به سیستمهای مستقل(ASهای متفاوت) فراهم می‌کند. AS یعنی شبکه‌هایی که توسط سازمانهای مختلف اداره می‌شوند. این پروتکل بین ASها اطلاعات دسترسی به همسایگان رو مبادله کرده و یکی از بهترین مسیرها را که از همسایگان یاد گرفته برای انتقال بسته‌ها انتخاب می‌کند. از آنجاییکه BGP مکانیزم امنیت داخلی ندارد تا از routing update ارسالی توسط ASاطمینان حاصل کند، موجب بروز آسیب پذیریهای جدی شده است. بنابراین هر AS (یا هر روتر BGP) هر مسیری یا هر routing path را با BGP میتواند اعلام کند. برای مثال در سال ۲۰۰۸ در شرکت Telecomپاکستان (AS17557) یک routing path غیر مجاز برای prefix 208.65.153.0/24 اعلام کرد و PCCW هنگ کنگ(AS3491) این آدرس جعلی را به بقیه اعلام کرد که منجر به ربودن ترافیک YouTube برای بیش از دوساعت شد. بسیاری از ترافیک های جعلی و سرقت های ترافیکی توسط حملات BGP و اشتباه در پیکربندی گزارش شده است. لذا چنین آسیب پذیریهایی بطور جدی روی امنیت مسیریابی بین دامنه ای تأثیر گذار است.

جهت جلوگیری از اعلام مسیرهای جعلی یا نادرست انواع روش‌های امن سازی BGP پیشنهاد شده است. با این حال بیشتر این طرحها به‌دلیل پیچیدگی پیاده‌سازی، در عمل قابل اجرا نیست. بعنوان مثال Prefix filtering چنانچه توسط ISP ها بصورت صحیح پیاده‌سازی شود، می‌تواند از حملاتی مانند traffic hijacking جلوگیری کند ولی در عمل به علت پیچیدگی پیاده‌سازی، این فیلترینگ توسط ISPها اجرا نمی‌شود. در این میان BGPSec بهترین روش امن سازی است که اخیراً توسط IETF پیشنهاد شده است که بوسیله آنAS ها تأیید صحت و اعتبار BGP route را انجام می‌دهند.

در این مقاله ابتدا آسیب‌پذیری‌های موجود پروتکل مسیریابی بین دامنه‌ای یعنی BGP با فعال سازی BGPsec را به منظور دستیابی به مسیریابی بین‌دامنه‌ای امن یعنی تحویل صحیح بسته میان AS ها بررسی می‌کنیم. این مطالعات نشان می‌دهد با وجود تلاش جهت رفع

آسیب‌پذیریها، ولی همچنان آسیب‌پذیری‌های جدی در طرح‌های امن‌سازی BGP مثلاً با استفاده از BGPSec وجود دارد. چندین حمله BGP جهت نشان دادن اینکه امن سازی BGP همچنان با ضعفهای اساسی مواجه هست، ساخته میشود. تأثیر این آسیب پذیریها را با استفاده از real trace ارزیابی میکنیم و متوجه میشویم که آسیب پذیریها جهت حملات براحتی قابل استفاده هستند. به منظور رفع این آسیب‌پذیریها و کاهش تأثیر آنها روش امن‌سازی با استفاده از طراحی و پیاده سازی BGPSec را بررسی می‌کنیم.

۱ - ویژگی‌های مطلوب جهت امن سازی BGP

هدف از inter-domain routing اطمینان ازصحت ارسال بسته‌ها میان ASها بامحاسبه و تعیین مسیرهای صحیح به سمت مقصد صحیح است.

- **مسیریابی Blackhole-Resistant** :

هر AS نمی‌تواند ترافیک شبکه را هک کند. معمولاً از Blackhole جهت جذب ترافیک به یک AS خاصی که در حالت عادی از آن AS عبور نمی‌کند، استفاده می‌شود. این ویژگی امنیتی از دونوع prefix hijacking جلوگیری می‌کند:

۱-Traffic Hijacking : ترافیک‌هایی که prefix hijacking شده‌اند، بطور کامل Drop شده و نمی‌تواند به مقصد اصلی باز گردانده شود.

۲- Traffic Interception : ترافیک‌هایی که prefix hijacking شده‌اند، می توانند به مقصد اصلی بازگردانده شوند. توجه داشته باشید که این حمله تأثیری روی دسترسی شبکه ندارد.

- **مسیریابی Loop-Free Routing:**

هیچ ترافیکی جز در اثر routing update نادرست وارد یک forwarding loop نمی‌شود. forwarding loop مکانیزم تقویت حمله را فراهم کرده، می‌تواند بر اتصالات شبکه، overload لینک‌ها و یاحتی قطعی شبکه تأثیرگذار باشد. به‌ویژه تاثیر این حلقه ها شامل از دست رفتن قابل توجه بسته‌های داخل حلقه و افزایش بار لینک و Delay , Jitter برای بسته های خارج از حلقه می باشد. بنابراین، این ویژگی دسترسی شبکه را بطور قابل ملاحظه ای کاهش می‌دهد.

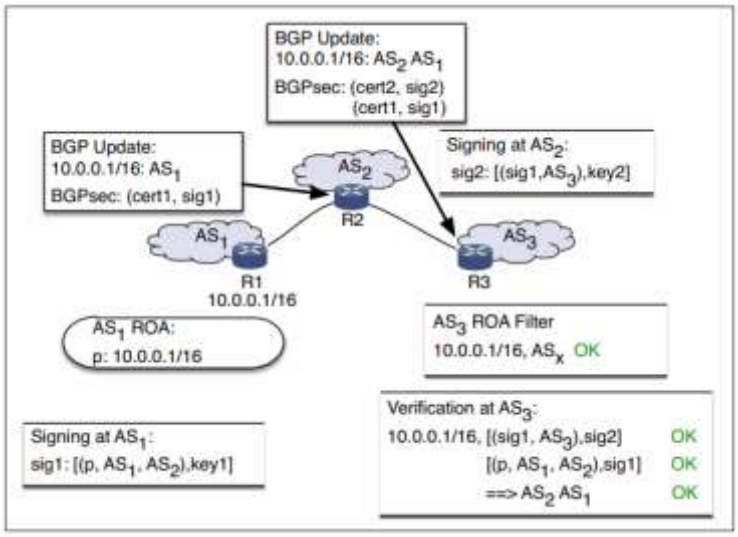
۲ - امنیت BGP با استفاده از BGPSec:

طرح های قبلی امن سازی BGP مانند S-BGP ، SOBGP و SPV بر تأیید صحت routing updates و مجوز ASها تمرکز دارد. برای مثال S_BGP هم اعتبار Prefix مبدأ و هم routing path را جهت امنیت BGP بررسی میکند ولی S_BGP سربار محاسباتی و ارتباطی قابل ملاحظه‌ای دارد. اخیراً IETF جهت استاندارد سازی یک پروتکل امن BGP، پروتکل BGPSecرا معرفی کرده است که هدف آن کاهش سربار و در عین حال تضمینهای امنیتی مشابه S-BGP که اعتبارسنجی Prefix مبدأ و routing path می باشد.

BGPSec از RPKI (Resource Public Key Infrastructure) جهت احراز هویت Prefix مبدأ استفاده می‌کند. سرویس RPKI توسط رجیسترهای اینترنت منطقه ای مختلف مانند RIPE، APNIC، ARIN وبنام ROA (route origination authorization) برای همان AS که مجوز انتشار Prefixرا دارد، ارائه می‌شود. ROA مشخصاتی مانند Prefix ، حداکثر طول Prefix که مجوز انتشار

دارد و AS هایی که مجوز انتشار prefix دارند را شامل می‌شود. هر AS که routing update دریافت می‌کند، ROA را بررسی می‌کند و Prefixهای غیرمجاز را rejectمی‌کند.

شکل ۱ یک ROA را نشان می‌دهد که مشخص می‌کند که AS x مجاز به انتشار Prefix(10.0.0.0/16) می‌باشد. با بررسی ROA، ASها، برای مثال AS z با موفقیت، اعتبار AS x و prefix اعلام شده از طرف آن را تأیید می‌کند.

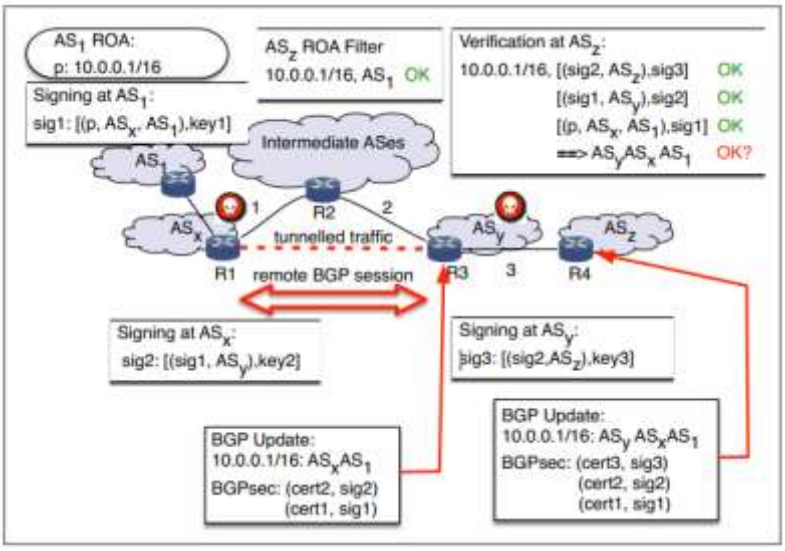


شکل ۱ امنیت BGP با استفاده از BGPSec

مشابه دیگر روشهای امن سازی مانند S-BGP ، BGPsec نیز تلاش می‌کند تا AS Number صحیح را در جدول مسیریابی به گونه‌ای اعلام کند که مسیرهای اعلام شده به درستی AS Path واقعی مورد استفاده جهت ارسال بسته ها را نمایش دهند. در این راستا، BGPSec با استفاده از RPKI رجیسترهای مختلف جهت انتشار گواهی‌های تخصیص داده شده به AS Number را در جدول Routing Table اعتبارسنجی می‌کند. برای سادگی از AS بعنوان موجودیتی جهت امضا و تأیید جدول مسیریابی در این مقاله استفاده می‌شود. هر AS ، مسیر مشخص شده در routing update را قبل از ارسال آن به همسایه تأیید می‌کند . تفاوت BGPSec و S-BGP تنها بررسی تطابق امضای تأیید شده رمزگذاری شده در routing update دریافتی و AS Number که routing update را ارسال کرده است، می‌باشد. شکل ۱ نمونه‌ای از اعتبارسنجی در BGPSec را نشان میدهد. AS1 در این شکل prefix p را امضاکرده، شماره ASخودش یعنی AS1، و همچنین شماره ASکه بروزرسانی به آن ارسال می‌شود که در اینجا AS2 هست، امضا را در routing update جاسازی کرده و به AS2 ارسال می‌کند. AS2 ابتدا امضا را قبل از انجام بروز رسانی جهت تأیید هویت ارسال کننده routing update بررسی میکند اگر نتیجه بررسی مورد تأیید بود، امضای تأیید شده قبلی و شماره AS همسایه که Update به ان ارسال می‌شود و در اینجا AS3 هست را به routing update اضافه کرده و به AS3 ارسال می‌کند.

۳ - آسیب‌پذیری‌های BGPSec

با وجود ادعای BGPsec به‌رفع آسیب‌پذیریهای BGP اما همچنان BGPSec نمی‌تواند خصوصیات امنیتی لیست شده در بالا را فراهم کند. بطور خاص BGPSec آسیب‌پذیری‌های زیر را دارد:



شکل ۲ - حمله Wormhole به AS z باقرارگرفتن بین AS x و AS y

۱-۳- آسیب پذیری Control Plane

با وجود اینکه هدف BGPSec امنیت Control Plane با جلوگیری از حملات Blackhole ناشی از Route Hijacking و انتشار مسیرهای جعلی است، با این حال حملات Route hijacking با استفاده از حمله wormhole در اینترنت هنوز حتی با پیاده‌سازی کامل BGPsec امکان‌پذیر است.

۱-۱-۳- Wormhole Attack:

این حمله می‌تواند توسط هر AS با هدف ایجاد لینکهای جعلی جهت hijack ترافیک و بدون نیاز به تغییر در پروتکل BGP و یا پیاده‌سازی آن تولید شود. این حمله اگرچه توسط توسط BGPSec مورد توجه قرار نمی‌گیرد اما برای رفع این مشکل اطمینان از مسیریابی مقاوم در برابر blackhole ضروری است. شکل ۲یک حمله اولیه wormhole را نشان می‌دهد. فرض کردیم ASx و ASY ترافیک ارسالی از ASZ را جذب و hijack کنند. برای این منظور این دو AS با همکاری هم و تولید یک routing path، ASهای واسط (مثلاً Ask و ASi) را در اعلام routing path مخفی کرده و لذا طول routing path از دیدگاه ASz از routing path واقعی کوتاهتر بوده و به راحتی تانل بین آنها ایجاد می‌شود. همانگونه که در شکل ۲ نشان داده شده است فرض کنید ASx و ASy دو AS همکار هستند. AS1 مواردی شامل prefix 10.0.0.1/16، شماره As1 و شماره AS دریافت کننده که در اینجا ASx هست را امضا کرده و همه را با هم در گواهینامه ROA در Update مسیریابی جاسازی کرده و به ASx ارسال می‌کند. پس از بررسی امضا، ASx امضای تولید شده توسط As1 را به همراه AS جعلی مثلاً ASy را امضا و route update به ASYمی‌فرستد، جایی‌که wormhole میان ASX و ASy ساخته شده است. بنابراین ASY امضای معتبردر route update جعلی تولید شده توسط ASx را دریافت کرده است، اگرچه session ایجاد شده بین ASx و ASy براساس لینک جعلی بوده است. برای انتشار بیشتر route update جعلی، ASy تنها بایستی امضای ASx را به همراه AS قربانی که در اینجا ASz هست را جهت دریافت ترافیک‌های سمت ASz امضا کند. با دریافت route update ، ASz ، prefix مبدا 10.0.0.1/16 ارسالی از مبدا را با استفاده از گواهینامه ROA بصورت موفقیت آمیزی بررسی کرده و مسیر جعلی را تأیید میکند. (ASy,ASx,AS1). در این تنظیمات ASZ مسیر جعلی را بعنوان مسیر اولویت‌دار بجای مسیر واقعی چنانچه کوتاهترین مسیر در بین تمام مسیرهای Learnشده باشد، را انتخاب می‌کند.

پس بطور خلاصه تبانی میان ASها می‌تواند منجر به تولید لینک جعلی و تولید حمله wormhole شود به گونه‌ای که routing updateها شامل مسیرهای جعلی با امضای معتبر از منظر ASقربانی باشد که حتی با پیاده‌سازی BGPSec نیزقابل تشخیص نیست.

متاسفانه امکان جلوگیری از ربوده شدن Prefix مبدأ وجود ندارد ، لذا حمله wormhole هنوز هم می‌تواند مسیریابی blackholes را در اینترنت افزایش دهد حتی اگر همه روتر های BGP به BGPSec مجهز باشند.

۲-۱-۳- Protocol Manipulation Attack :

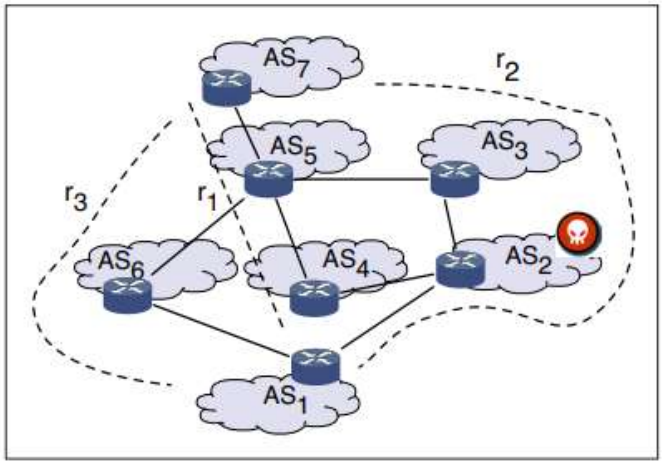
در این حمله رهگیری ترافیک با نفوذ در شاخصهای(MRAI) و (RFD) رخ می‌دهد. مهاجم می‌تواند اولویت مسیرها را به گونه‌ای تغییر دهد که AS قربانی بصورت اشتباهی مسیر با اولویت کمتر را به عنوان مسیر ارسال ترافیک انتخاب کند.

برای مثال همانطور که در شکل ۳ نشان داده شده است یک AS مخرب که در اینجا AS2 هست دو مسیر با الویت:

r1: {AS1, AS2, AS4, AS5} و r2: {AS1, AS2, AS3 ,AS5} را کنترل می‌کند و این در حالی است که مسیر خوب دیگر r3: {AS1 ,AS6, AS5, AS8}, توسط AS مخرب کنترل نمی‌شود و ترتیب اولویتهای AS1 بدین صورت است: r1 > r2> r3.

حال فرض می‌کنیم RFD فعال نباشد. AS2 مسیر AS1 به AS4 را اطلاع رسانی کرده و آن را بلافاصله پس می‌گیرد. بعد از بازه زمانی MRAI، AS2 مسیر AS1 به AS3 را اعلام کرده و سپس آن را پس می‌گیرد. As2 مسیر فوق را بصورت دوره‌ای اعلام کرده و پس از هر بازه زمانی MRAI پس می‌گیرد.AS2 بصورت پیوسته و در بازه های زمانی مرتب مسیر فوق را اطلاع رسانی کرده و پس از هر بازه زمانی MRAI آن را باطل میکند. تا زمانیکه مسیر صرفنظر شده با توجه به MRAI به اندازه تأخیر باشد، مسیر r1 و r2 همچنان وجود دارند حتی اگر پس گرفته شده باشند. در نتیجه از دید AS7، AS1 غیر قابل دسترس هست اگرچه مسیر r3 وجود دارد. اگر مسیر بهینه r4 از AS1 به AS7 با اولویت پایین تر از r3 وجود داشته باشد، As7 مسیرr4 را ترجیح می‌دهد به دلیل اینکه مسیر r3 بطور دائم میرا می‌شود. بطور مشابه حملات مشابه با استفاده از تایمر RFD ایجاد می‌شود.

بطور خلاصه دراین حمله با هدف لایه control Plane، دستکاری مسیرهای دارای اولویت بالاتر رخ می‌دهد. این حمله با فعال سازی BGPSec روی پروتکل BGP قابل شناسایی نمی‌باشد به این علت که کلیه مسیرها قابل تأیید هستند.



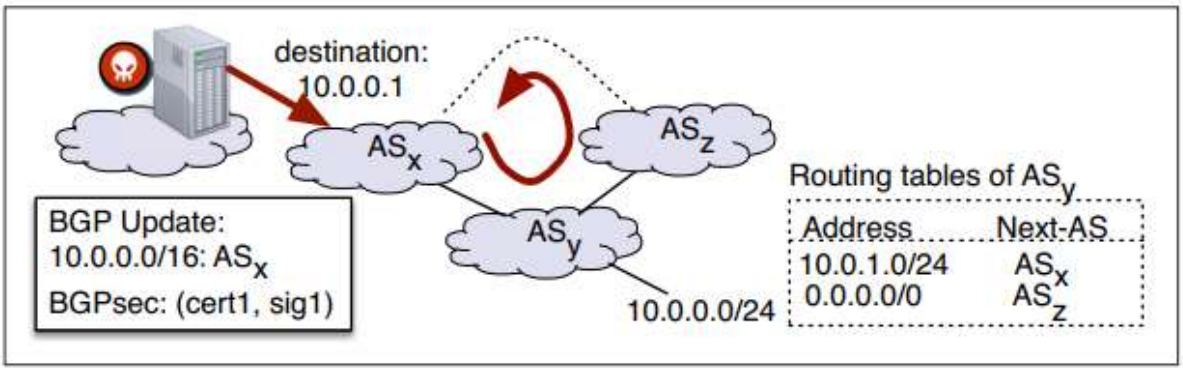
شکل ۳- حمله Protocol Manipulation

۲-۳-آسیب پذیری Data Plane

: Mole Attack

مسیریابی بدون Loop یکی از مهمترین خصوصیات برای هر پروتکل مسیریابی است. هکرها میتوانند با ایجاد Loop و Overload لینکهای شبکهT موجب حمله Mole Attack شوند. این حمله ویژگی مسیریابی بدون loop را نقض می‌کند.

این حمله با ایجاد Loop وقتی رخ می‌دهد که ROA برای یک Prefix براساس کاربرد Prefixعمل نکند. به این معنی که یک Prefix اختصاص داده شده به یک As نبایستی بصورت کامل مصرف شود. این حمله می‌تواند به راحتی از چنین Prefix های استفاده نشده‌ای برای نقض ویژگی مسیریابی بدون loop استفاده کند. در اینترنت در حال حاضر As های بزرگتر توسط (RIRS)معمولاًبلوک بزرگی از Prefix ها به آنها اختصاص می یابد ، اما آنها تنها بخشی از آنرا استفاده می‌کنند(یعنی بلوکهای کوچکتری از Prefixها). در این حملات این Prefix های استفاده نشده و یا تخصیص داده نشده اگر به درستی در BGP اعلام نشوند، میتوانند با ایجاد ترافیک با prefix های استفاده نشده، مورد توجه هکرها قرار گیرد. شکل ۴ نمونه ای از این حمله را نشان میدهد:



شکل ۴ - حمله Mole Attack با ایجاد Forwarding Loop دائمی و OverLoad شدن لینکهای AS

ASy به دو xAS و z متصل هست و default Route روی ASz تعریف شده است. فرض می‌کنیم ASy مجاز به اعلام Prefix 10.0.0.0/16 باشد. همچنین فرض میکنیم ASy کلیه Prefix ها را بصورت کامل استفاده نکرده و sub-prefix 10.0.0.0/24 به هیچ مشتری اختصاص داده نشده است. بنابراین ترافیک با مقصد 10.0.0.0/24 مطابق با default Route و سیاستهای مسیریابی اتخاذ شده بطور مداوم میان ASx,y,z در گردش است.

خاطر نشان می‌شود که اگرچه prefixهای IPV4 بطور کامل تخصیص داده شده است ولی تعداد قابل توجهی از Ip Address ها هنوز استفاده نشده اند. لذا Mole Attack همچنان به آسانی قابل اتفاق افتادن است. این شرایط برای IPV6 به مراتب خطرناکتر است. همانگونه که قبلا هم گفته شد علت اصلی رخ دادن Mole Attack در اینترنت درحالیکه BGPSec پیاده سازی شده است، عدم انتشارگواهی RPKI مطابق با Prefix های استفاده شده است. به هرحال، فرآیند اعلام Prefix در شکل فوق نشان داده شده است. اگرچه Mole Attack تنها با انتخاب مسیر اتفاق نمی افتد، اما با مسیریابی بین دامنه‌ای امن چنین حملاتی در سطح شبکه کاهش می‌یابد.

بنابراین mole attack به هکر اجازه می‌دهد تا به راحتی loop ایجاد کرده و از آن سوء استفاده کند. حتی می‌تواند منجر به congestion در لینکهای میان As ها و Overload لینکها با تولید ترافیک توسط prefix های استفاده نشده، شود. توجه به این نکته ضروری است

که حتی مهاجم ممکن هست این روش را انتخاب نکرده بلکه تولید botnet برای تولید ترافیک پس از بررسی prefix های استفاده نشده کند.

توجه به این نکته ضروری است که اگرچه هدف از BGPSec رفع آسیب پذیریهای Data Plane نیست اما جهت رفع مشکلات BGP صحت ارسال بسته اهمیت دارد و این آسیب پذیری احتمالا با عملکرد صحیح پروتکل برطرف می‌شود.

۳-۳-آسیب پذیری های ناشی از ناسازگاری بین Data Plane و Control Plane

Protocol Manipulation Attack:

Protocol Manipulation Attack این امکان را به هکر میدهد که حتی با پیاده سازی BGPSecکه بتواند Route update ارسالی برای AS قربانی را طوری تغییر دهد که hijack ترافیک رخ دهد. این حمله با ناسازگاری میان Control Palne و plane data اتفاق می‌افتد. مشابه حمله رخ داده به control Plane این حمله پیامهای مسیریابی را دستکاری می‌کند با این تفاوت که در مورد اول پیامهای با تغییر در پیاده سازی BGP دستکاری می‌شود ولی در این مورد پیامها بصورت مستقیم با تغییر در پیامهای اعلام مسیر اتفاق می افتد.

در طراحی فعلی BGPSec فرض می‌شود که مسیرهای محاسبه شده توسط control Plane بصورت کامل در Data Plane اجرا می شود یعنی مسیریابی در control Plane و Data Plane با هم هماهنگ و سازگار بوده و مکانیزمی جهت بررسی این سازگاری وجود ندارد.

شکل ۵ مثالی از این حمله را نشان می‌دهد.

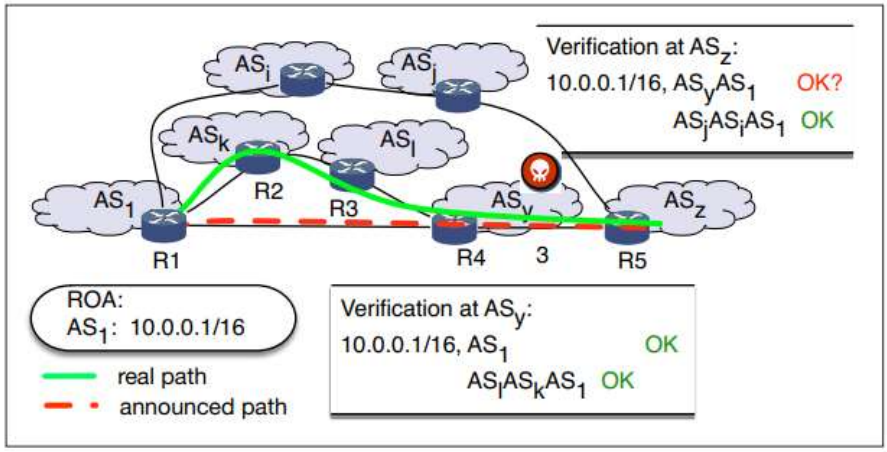


Figure ۱ حمله Protocol Manipulation با فراهم کردن امکان اطلاع رسانی مسیر کوتاهتر جعلی توسط هکر

فرض می‌کنیم ASy قصد دارد ترافیک سمت ASz را جذب کند. برای دستیابی به این هدف، Asy یک قرارداد سرویس انتقال با AS1 جهت دریافت بروزرسانی‌های صحیح به همراه امضای صحیح AS1، مبادله می‌کند.AS1 شماره AS مربوط به AS1 و ASy و همچنین Prefix را امضا کرده سپس این امضا و گواهی ROA را در route update تعبیه کرده و به سمت ASy از طریق BGP Session ارسال می‌کند. در همین حال ASy یک route update از AS1 مجاز دریافت می‌کند که شامل مسیر {ASl, ASk, AS1} می‌باشد. Asy مبدأ prefix و همچنین مسیر را با توجه به گواهی ROA که شامل AS1 و مسیر {ASl, ASk, AS1} هست

را با موفقیت تأیید می‌کند. ASy اولین مسیر را بعنوان بهترین مسیر که در اینجا ASl هست را اتخاذ کرده و به آن اولویت بالا اختصاص می‌دهد و این درحالی است که هنوز این مسیر به ASz اطلاع رسانی نشده است.

در این تنظیمات ASz دو مسیر مورد تأیید را با گواهی ROA مورد تأیید از Asy و AsJ دریافت خواهد کرد. برای مثال {AS y, AS1} و {ASj, ASi, AS1}. از آنجایی‌که طول مسیر اول دریافتی از ASy از مسیر دوم دریافتی از ASj کوتاهتر است، لذا ASz مسیر {AS y, AS1} دریافتی از ASy را انتخاب میکند. لذا ترافیک از ASZ به سمت ASy ربوده شده در حالیکه مسیر اصلی ترافیک {AS y, ASl, ASk, AS1} بجای {AS y, AS1} می‌باشد. این پروتکل اجازه می‌دهد که AS مخرب مسیری را که می‌تواند گواهی BGPSec را بگیرد ولی در واقع وجود ندارد، ایجاد کند. لذا چنانچه route update از مسیرهای اعلام شده استفاده کند AS قربانی نمی‌تواند آن را اعتبارسنجی کند.

BGPSec جهت هماهنگی بین Data Plane و Control Plane که آسیب‌پذیری منجر به حملات manipulation می‌شود را هیچ ضمانتی نمی‌دهد. با بهره‌برداری از این آسیب‌پذیری، حتی در صورتی که Data Plane و Control Plane به درستی تأیید شده هستند، ترافیک به راحتی hijack می‌شود.

۴ - ارزیابی و اقدامات متقابل

در این بخش به ارزیابی اثربخشی و تاثیر حملات بالا و سپس ارائه اقدامات متقابل برای مهار حملات می پردازیم.

۴-۱- ارزیابی آسیب پذیری

تأثیر حملات بالا را با آثار واقعی آنها بررسی می‌کنیم. ابتدا توپولوژیAS را جهت بررسی تأثیر wormhole attacks از CAIDA (http://as-rank.caida.org/data/) ارزیابی میکنیم. توجه داشته باشید که protocol manipulation attacks اثرات مشابهی بر ارسال بسته دارند، لذا برای سادگی نتایج اینجا ارائه نمی‌شود. فرض می‌کنیم همه AS ها می‌توانند مخرب باشند. بصورت تصادفی تعداد ۱۰ جفت AS برای تولید حمله و بررسی تعداد مسیرهای hijack شده توسط حمله انتخاب می‌کنیم. توپولوژی شامل ۳۴ AS همراه با As های همسایه آنهاست. ما مستقیماً از گزارشات CAIDA جهت تنظیم ارتباطات بینAS ها استفاده می‌کنیم. درنتیجه توپولوژی شامل AS۱۴۲۵ و ۱۴۰۵ لینک تعداد مسیرها حدود ۵۵۱۰ می‌باشد. بصورت تصادفی AS هایی را که بیشتر از سه همسایه دارند، برای تولید حمله و ارزیابی تعداد مسیرهایAS که تحت تأثیر حمله قرارمی‌گیرند را انتخاب می‌کنیم. شکل ۶-a تعداد مسیرهایhijack شده توسط wormhole attacks را نشان می‌دهد. مشاهده می‌شود که درحدود ۷۲ درصد AS ها حداقل یک مسیر متأثر از حمله دارند. توجه داشته باشید که حمله می‌تواند توسط ISP مخرب یا مهاجمینی که از BGP سوء استفاده می‌کنند، تولید شود. بویژه، مهاجمین می‌توانند به راحتی از آسیب‌پذیری روترهای در معرض خطر به راحتی با تغییر پیکربندی روتر برای این منظور استفاده کنند. بنابراین می‌توان نتیجه گرفت که پروتکل BGP پیشرفته(BGPSec) چنانچه AS مخرب وجود داشته باشد، نمی‌تواند در خصوص مسیریابی بین دامنه‌ای کاملاً امن باشد.

دوم، تأثیر mole attacks را بررسی می‌کنیم. مجموعه اطلاعات IP های استفاده نشده را جمع آوری کرده و تعداد لینکهای تحت تأثیر ترافیک تحویل شده به این IP ها را بررسی می‌کنیم. با استفاده از ابزارهای traceroute کلیه مسیرها با کلیه پیشوندهای /24 بررسی می‌شود. همچنین از اطلاعات router-view ها برای نگاشت Prefix ها به AS های مربوطه استفاده میکنیم به‌گونه‌ای که لینکهای AS مسیر ارسال Packet درtraceroute هستند. آسیب‌پذیریهای مختلف لینکهای AS که برای mole attacks قابلیت سوء

استفاده دارند را شناسایی می‌کنیم. شکل ۶-b توزیع لینک‌های آسیب‌پذیری که قابلیت ایجاد ترافیک روی پیشوندهای 24/ استفاده نشده را دارند، نشان می‌دهد. متوجه شدیم که بیشتر لینک‌های آسیب‌پذیر را با استفاده از بیش از ۵ بلاک پیشوند 24/ را میتوان مورد سوء استفاده قرار داد.

بطور خاص از این حمله برای حمله DDOS توسط مهاجمین استفاده می شود.دقت کنید که mole attack توسط کاربران معمولی در اینترنت میتواند ایجاد شود. بنابراین این حمله میتواند خیلی مخفیانه در شبکه قربانی اختلال ایجاد کند.

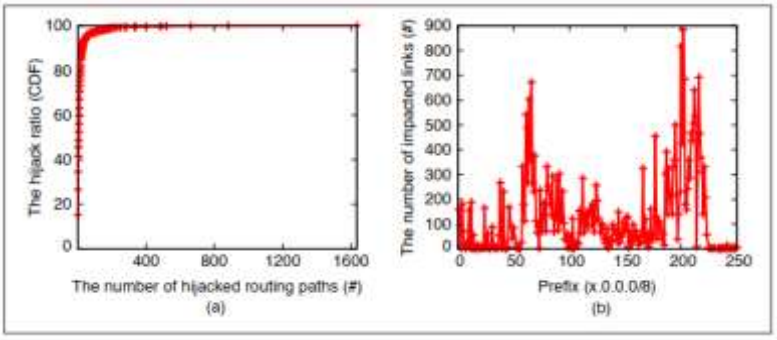


Figure ۲ - تأثر آسیب پذیری ها در مسیریابی بین ASها

۲-۴-اقدامات متقابل احتمالی

در این بخش درخصوص اقدامات احتمالی در برابر حملات بالا که شامل تقویت پروتکل BGPSec و امکان طراحی یک روتر تلفیقی است بحث می‌کنیم.

۱-۲-۴- Enhanced BGPsec Protocol:

علت اصلی mole attacks این هست که AS ها نمیتوانند لینکهای موجود AS در مسیریابی را تأیید کنند.برای حل این موضوع میتوان BGPSec را جهت تولید گواهینامه ROA فقط برای پیشوندهای استفاده شده و تولید گواهینامه لینکها (به جای شماره AS) توسعه داد. بدین ترتیب یک BGP روتر میتواند صحت لینکهای واقعی روی مسیر اعلام شده با پیشوندهای استفاده شده تأیید کند. بنابراین تنها مسیرهای دارای لینک‌های فیزیکی انتخاب و اعلام می‌شوند تا مانع وقوع این حمله شود و تنها ترافیکی که از prefix های مجاز باشد ارسال و Prefix های استفاده نشده بلاک میشود و درنتیجه از mole attacks جلوگیری میکند.بطور خاص میتوان یک مکانیزمی برای BGPSec ایجاد کنیم که بصورت اتوماتیک سازگاری میان Prefix های اعلام شده و استفاده شده را تشخیص داده و سپس Prefix های استفاده نشده را بلاک کند. با استفاده از مکانیزم نفوذ، AS میتواند بصورت اتوماتیک Prefixهای اختصاص داده شده و Prefixهای جدول مسیریابی را تجزیه و تحلیل کند. برای مهار حمله protocol manipulation که ترفیک را هک میکندعلت اصلی تغییرات مسیریابی در routing update بررسی شده تا از میرایی مسیرهای خوب جلوگیری کند.

۴-۲-۲- Consolidated BGPsec Router Design:

می‌توان از پردازنده‌های با کیفیت مثل Intel SGX و ARM TrustZone در روترها جهت پیاده‌سازی روتر بگونه‌ای که هر روتر BGP مسیر و بسته دریافتی از همسایگان را بررسی و مانع ارسال در مسیرهای مخرب میشود. روترهای BGPSec که از پردازنده-های با کیفیت استفاده کنند برای مثال Intel SGX که معماری مبتنی بر دستورالعمل هست، می‌تواند مانع دسترسی و تغییر حافظه اجزای سیستم شود. هدف از طراحی روتر قابل اعتماد با پردازنده با کیفیت، تأیید و تصدیق مسیر صحیح به سمت همسایگان می باشد. همچنین بجز طراحی، BGP روتر میتواند برای تصدیق مسیریابی همسایگان از اجرای صحیح BGP و آنچه که انتظار می‌رود استفاده کند. بنابراین حمله protocol manipulation قابل تشخیص و پیشگیری است.

۵ - نتیجه گیری:

در این مقاله به بررسی آسیب‌پذیری‌های موجود در BGPSec پرداخته و مشاهده کردیم که BGP با فعال سازی قابلیت BGPSec به دلیل اشکالات اساسی آن نمی‌تواند به ویژگیهای مطلوب امنیتی در خصوص مسیریابی بین‌دامنه ای دست یابد. در همین راستا به برخی طرح ها برای ایمن سازی مسیریابی بین دامنه ای جهت تضمین ویژگیهای امنیتی اشاره کردیم.

۶ - مراجع

[1] “BGP with BGPsec: Attacks and Countermeasures.” [Online]. Available: https://ieeexplore.ieee.org/document/8594708

[2] K. Butler et al., "A Survey of BGP Security Issues and Solutions", *Proc. IEEE*, vol. 98, no. 1, pp. 100-22, 2010.

[3] " J. Durand, I. Pepelnjak and G. Doering, BGP Operations and Security, 2015.