**مدل کاهشِ مسیر یابی سیلابی( TCP SYN با جعل IP )**

اینترنت بصورت یک برنامه کاربردی و بدون هیچ امنیتی طراحی شده بود.

مجموعه پروتکل های IP/TCP بصورت بسیار گسترده برای انتقال داده ها استفاده می شود و تمام میزبان های شرکت کننده در انتقال و ارتباط هیچگونه سوء قصدی ندارند. هیچ فضای امنیتی و مراقبتی در سایر پروتکل های میزبان قرار داده نشده است. از این رو هکرها می توانند آدرس IP راجعل کنند و بصورت مخفیانه آن رانزد خود نگه دارند و همچنین آنها می توانند مسیر هک خود را پنهان کنند.

زمانی که هکر ها بسته ها را با منبع جعلی به آدرس های اینترنتی می فرستند روتر ها آنها را بدون کنترل اعتبار همانند بسته های دیگر به مقصدهایشان می فرستند. این بسته های جعلی پهنای باند را مصرف می کنند و اغلب کارهای مخربی همچون حمله به DDOS را انجام می دهند. این حمله باعث عدم دسترسی کاربران به شبکه اینترنت می شود. این تخریب بوسیله خروجی منبع شخص قربانی انجام می شود.

یکی از تاییده های اصلی اینترنت نسل امروز احراز هویت آدرس منبع است. شبکه اصلی با مقصد در ارتباط است و دسترسی به بسته ها را دارد و با استفاده از این آسیب پذیری هکر سعی می کند آدرس منبع را جعل کند و آن را بعنوان یک سرور اصلی نشان دهد. ما با پیروی از این روش سعی در کاهش جعل IP داریم و با استفاده از شبکه ناظر بربسته ها نظارت میکنیم.

مدل کاهش مسیر یابی سیلابی برای TCP SYN بوسیله جعل IP ،برای بررسی TCP و تشخیص کاراکتر مورد قبول بسته و توسعه پیشگیری از حمله به DDOS طراحی شده است. تشخیص حمله بوسیله جعل IP به DDOS با استفاده از نظارت بر بسته ها و میزان فضای اشغال آنها، ساده است و بسته هایی با چنین آدرس IP پذیرفته نمی شوند.

هکر می تواند با استفاده از جعل IP به سرور قربانی آسیب برساند. عمدتا فرستنده IP جعلی نمی تواند پاسخ به IP را دریافت کند. ما با استفاده از کاوشگر TCP و عیب یابی می توانیم به IP جعلی پاسخ داده و لایه های دیگر را از حمله هکر نجات دهیم. در این مرحله سرور میزبان کدی را که باید TCP تغییر کند یا پنجره بسته شود را می فرستد تا بسته برگشت پیدا کند.

باید ملاحضه شود تا منبع پاسخ درستی به IP جعلی دهد. اگر بر فرض منبع نتواند TCP راتغییر دهد یا پنجره را ببند سرور میزبان متوجه می شود که بسته ها از منبع جعلی فرستاده شده است.

1. **تکنیک های جعل IP**

برای ساخت یک IP جعلی نیاز به یک TCP آسیب پذیر داریم. 3 راه برای تبادل وجود دارد.باید توجه داشت که سرور دارای یک ساختار بزرگ باشد و بسته های SYN را بدون در نظر گرفتن صحت آنها قبول کند.

در طول حمله SYN، هکر بسته های SYN را با آدرس IP که اصلا وجود ندارد یا استفاده نمیشود، میفرستد. در خلال 3 راه تبادل، زمانی که سرور اطلاعات درخواست را به حافظه پشتیبانی میدهد، بسته های SYN منتظر اجرای درخواست توسط فرد قربانی هستند.زمانی که درخواست منتظر اجرا شدن است بسته ها در حافظه پشتیبانی باقی می مانند. از آنجایی که منبع IP جعلی وجود ندارد، سرور درخواست ایجاد شده توسط بسته جعلی SYN هکر را اجرا نمی کند.

هر اتصال نیم باز بر روی حافظه پشتیبانی تا زمانی که مهلت آن تمام شود، باقی می ماند.SYN-ACK 5بار ارسال مجدد میگردد. در این صورت مهلت زمان آنها بعد از هر بار ارسال 2برابر افزایش پیدا می کند. مهلت زمان اولیه 3 ثایه است. بنابراین در تلاش های بعدی این زمان 6/12/24/48 ثانیه می رسد. در خواست های پی درپی باعث پر شدن حافظه پشتیبانی می شود.

بنابراین درخواست جدید و مشروعی برای پردازش وجود ندارد و اینگونه سرورهای شبکه از کار می افتند.بطور کلی فضایی که سیستم عامل به حافظه پشتیبانی اختصاص داده است کم است و حتی یک حمله در مقیاس کوچک هم می تواند مخل کارکرد سیستم شود. از سوی دیگر یک کامپیوتر که SYN جعلی که با یک IPجعلی مخل کارایی آن شده است بوسیله یک پیکر بندی SYNحذف می شود.

1. **جعل IPدر دنیای امروزه**

با توجه به نتایج بدست آمده از تحقیق در مورد IPهای جعلی می توان به این نتیجه رسید که IP های جعلی یکی از بزرگ ترین مشکلات موجود در دنیای امروز اینترنت هستند. در این راستا پیش بینی هایی انجام شده است. با وجود فیلتر های ورودی و خروجی کاربران مخرب نمی توانند بسیاری از آدرس های IP را مورد حمله قرار دهند.

1. **بات نت ها Botnets**

بات نت مجموعه ای از نرم افزار های اطلاعاتی یا ربات ها است. این نرم افزار مخرب با استفاده از IRC ربات ها به شبکه آسیب می زند. افزایش میزان محبوبیت استفاده از بات نت ها ما را به این باور می رساند که هکرها دیگر نیازی به استفاده از جعل IP ندارند. اما در حقیقت جعل IP همچنان یک مشکل باقی مانده است و بعنوان یک دارایی برای هکر ها است.

پایه برخی بات نت ها بر اساس نوع حمله است برای مثال در یک حمله گسترشی DNS DDOS جعل IP یک امر حیاتی برای موفقیت هکر است. حتی اگر بات نت از IP جعلی استفاده نکند، خطر جعل IP هنوز وجود دارد.

1. **اندازه گیری های نسبی**

روش استفاده شده برای جلوگیری از TCP SNY به اینگونه است که با بکارگیری و استفاده از سرور بعنوان یک آشکار ساز حمله، و روتر محلی جلوگیری از حمله هکر صورت میگیرد.

برای ایجاد اتصال TCP با سرور، هر فرد باید یک سیگنال SYN بفرستد و مجبور است که یک SYN/ACK با سیگنال AC دریافت کند. برای شناسایی حمله هکر، درخواست SYN که بوسیله فرد فرستاده می شود به جدول داده سرور می رود و تا زمانی که کد SYN/ACK به کاربر برسد، اطلاعات فرستاده شده توسط فرد در جدول داده ها بعنوان آدرس IP ذخیره می شود و SYNشمارش می شود.

اگر شمارش SYN در جدول داده بیشتر از حد مجاز بود، سرور بصورت محرمانه جزئیات حمله را به روتر محلی می فرستد و احتمالا روتر محلی به هکر می فرستد و کلیه بسته ها را به گره مربوطه باز ارسال می کند. اگر روتر محلی خطر را تشخیص دهد از فرستادن آن به گره ها جلوگیری میکند.(مقصود از گره همان node) می باشد.

سیستم عامل انگشت نگاری نیز می تواند بسته های جعلی را تشخیص دهد. اگر منبع جعلی باشد انگشت نگاری می شود و نتیجه انگشت نگاری با انگشت نگاری که قبلا انجام شده مقایسه می شود و در صورت عدم تطابق بسته جعلی شناسایی می شود. حتی پس از آن نتیجه انگشت نگاری میتواند با یک دیوار آتش یا همان فایر وال مختل شود. اگر فیلتر فایر وال وجود داشته باشد و پاسخ را تغییر بدهد سیستم انگشت نگاری قابل اعتماد نخواهد بود.

**فیلترینگ هاپ کانت(HCF)**

مسیر رسیدن بسته ها به یک سرور و دادن آنها به سرور دیگر را در خلال یک زمان مشخص جایی است که یک هاپ کانت ساخته می شود. هاپ کانت نقشه آدرس IP را برای HC می فرستد و سپس هکر یک بسته جعلی به سرور میزبان می فرستد. بسته هاپ کانت اصلی شبیه یک هاپ کانت جعلی نیست اما به دلیل اینکه ممکن است یک هاپ کانت مسیرش را برای رسیدن به روت های مختلف تغییر دهد نمی توان همه ی هاپ کانت ها را فیلتر کرد زیرا این عمل منجر به اشتباهات کاذب شود. برای کاهش این اشتباه از HCF فقط برای برطرف کردن ترافیک بین بسته ها استفاده می شود.

استفاده ازکوکی های SYN روشی است برای جلوگیری از باز شدن اتصالات به منبع با آدرس جعلی.

در ابتدا فرد یک بسته SYN+ACK با کد های مخصوص به همراه یک رشته اعداد یا کوکی به سرور می فرستد این بسته دارای برچسب زمانی و سایز است.وقتی که بسته به سرور می رسد، سرور آن را بررسی می کند و در صورتی که توالی اعداد فرستنده یک مقدار مشخص کوکی+1 باشد، برای آن یک جایگاه اختصاص می دهد. به دلیل اینکه یک کوکی شامل یک کلید امنیتی سرور است هکر ها نمی توانند مقادیر کوکی را حدس بزنند.

با این حال، به دلیل برخی از ناسازگاری های سیستم عامل با پسوند TCP ، تا زمانی که SYN میزبان پر نشود، کوکی SYN کار نمی کند. یک هکر ممکن است یک ترافیک جعلی ایجاد کند و در عملکرد مکانیسمSYN اختلال ایجاد کند. مدیران ممکن است برای اتصالات از کوکی استفاده کنند اما باید نسبت به اثرات جانبی آن نیز آگاه باشند.

مکانیسم دیگری که برای جلوگیری از جعل IP استفاده می شود، مکانیسم استفاده از پازل IP است. سرور یک پازل(جدول)IP به کاربر می فرستد و سپس کاربر با استفاده از برخی محاسبات آن را حل می کند و بعد از اینکه سرور پازل حل شده از کاربر را گرفت به او اجازه اتصال می دهد. این روش بعنوان یک بازدارنده قوی از حمله هکر و فرستادن بسته های جعلی جلوگیری میکند. از آن جا که IP یک معما شده است و هکر قادر به حل آن نیست هکر نمی تواند سرور را حک کند.

1. **کاوش TCP برای پاسخ به بسته های آرگیومنت(Argument)**

این روش برای، کاهش مسیر یابی سیلابی آدرس IP جعلی استفاده می شود.

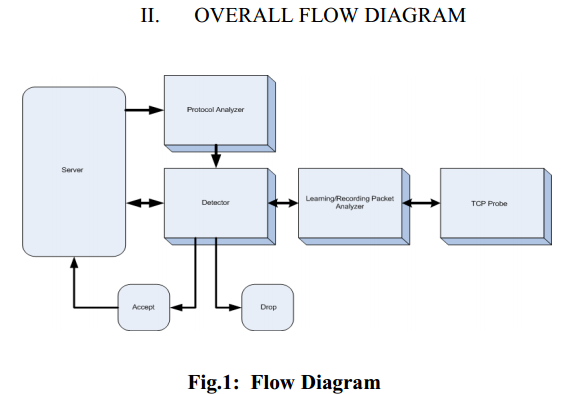
یک TCP ساده نمی تواند از حمله هکر ها در امان باشد و ممکن است شماره و رمزهای متوالی آنها برای هکر ها قابل حدس زدن باشد.

معمولا فرستنده بسته جعلی هیچ پاسخی دریافت نمیکند. ما با استفاده از کاوش TCP برای پاسخ دادن به صحت بسته، یک پیام هوشمند به سایر لایه ها می فرستیم تا از حمله هکر در امان بمانند.

در این جا میزبان گیرنده یا فرستنده، پیامی مبنی بر اینکه باید TCP تغییر کند یا بسته مجدا ارسال شود، می فرستد.

با توجه به پیغام باید برسی شود که آیا منبع به درستی پاسخ میدهد یا خیر. اگر به هر دلیلی از منبع پاسخی دریافت نشد این نشان می دهد که بسته جعلی است در غیر اینصورت بسته جعلی نیست.

ثبت ارتباطTCP کلید این روش است. در نمودار جریان کلی در شکل 1 می توان این پروسه را دید.

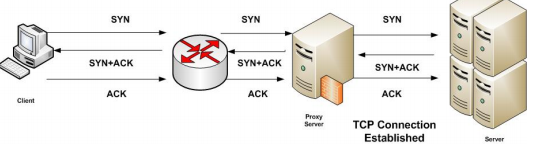


این یک ساختار بر پایه سرور میزبان است که با توجه تصمیم کاربر ارتباط برقرار می شود. آنالیزور پروتکل بسته را بررسی می کند که آیا این بسته از پروتکل TCP پیروی میکند و آیا مشخصات داده شده توسط کاوشگر TCP است یا خیر.

آنالیز بسته ها ثبت می شود و در زمان کاوش TCP مشخصات آن تایید می گردد.

زمانی که کاربر تلاش برای اتصال به سرور داردTCP بررسی میکند که آیا بسته دریافتی از سمت کاربر را پس بفرستد یا قبول کند. در همین مورد اگر هکر بخواد به سرور متصل شود، نمی تواند، زیرا که قادر به ارسال پاسخ به TCP نیست.

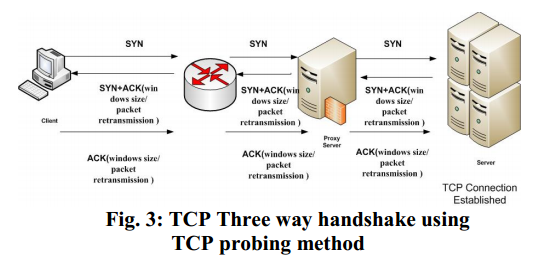
در شکل 2 ، 3راه ارتباط با سناریو طبیعی را می بینیم.



در این شکل میتوان 3راه اتصال به بسته SYN را که توسط کاربر برای ایجاد یک اتصال فرستاده می شود و توسط بسته SYN+ACK پاسخ داده می شود را مشاهده کرد.

اگر فقط پاسخ SYN به کاربر داده شود اتصال نیمه امن برقرار می شود و این امر منجر به حمله SYN جعلی می شود. اگر بسته با SYN+ACK پاسخ داده شود میتوان یک اتصال امن با سرور در یک سناریو نرمال داشته باشیم.

در شکل 3، 3راه اتصال با استفاده از کاوشگر TCP برای پاسخ به بسته های آرگیومنت، نشان داده شده است.

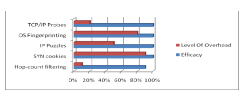


در این روش یک سری مشخصات به ACK اضافه می شود که این اندازه پنجره TCP را تغیر میدهد یا منجر به ارسال مجدد آن می شود. بر اساس این مشخصات ارسال بسته به همراه یک ACK از طرف کاربر برای ایجاد یک ارتباط امن به سرور فرستاده می شود. بسته پاسخ داده شده توسط سرور باید با مشخصات مطابق باشد.TCP با استفاده از آنالیز ثبت شده بسته، تشخیص می دهد که بسته پذیرش یا رد شود.

آنالیزور بسته با توجه به پاسخ بسته TCP ACK که توسط سرور داده شده است تشخیص می دهد که آیا باید سرور با استفاده از TCP اندازه پنجره را تغییر دهد یا بسته را دوباره ارسال کند.

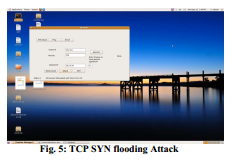
بخش چهارم:

مقایسه نتایج و مباحث

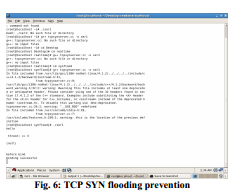


به نظر می رسد که TCP/IP اثربخشی بهتربا سر بار کمتر نسبت به روش های دیگر پیشگیری از جعلIP به منظور جلوگیری از حمله به DDOS ، دارد.

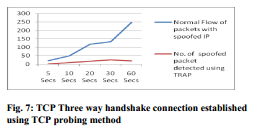
این عملکرد در پهنای سرور جایی که کاوش TCP برای پاسخ به بسته آرگیومنت بدنبال تشخیص و نشان دادن IP جعلی است، صورت میگیرد.



ما با استفاده از یک تایمر خودکار و یک IP جعلی یک حمله سیلی TCP SYN با هدف حمله سیلی و با افزایش و کاهش تعداد بسته های TCP SYN انجام دادیم( مراجعه به شکل 5و6). روش پیشگیری سیلی TCP SYN شناسایی می شود و مانع حمله از یک آدرس IP جعلی میشود و از پاسخ بسته TCP/ACK جلوگیری می شود.



شکل 7 در زیر برقراری 3راه اتصال را نشان می دهد.



با استفاده از روش کاوش TCP، TCP بسته های آرگیومنت را پاسخ می دهد و بسته های جعلی را پیدا میکند و به بیرون از مدار پرتاب می کند. البته این کار با توجه به اطلاعات و مشخصه های ACK انجام می شود.

و همچنین در این شکل مقایسه بین یک جریان طبیعی یک بسته با IP جعلی و تعداد بسته های جعلی شناسایی شده و پاسخ به بسته های آرگیومنت توسط TCP را می توان مشاهده کرد.

بخش پنجم:

نتیجه گیری و برنامه های آینده

کاوشگر TCP برای جواب دادن به بسته های آرگیومنت یک روش بسیار مفید است. زیرا IP و بسته های جعلی را به خوبی شناسایی میکند. این روش تعدا بسته های جعلی را کاهش می دهد ولی بسته های UPP را پشتیبانی نمیکند. همچنین این روش بسیار مناسبی برای جلوگیری از مسیر یابی سیلابی TCP SYN است. این روش می تواند مادامی که IP های جعلی را شناسایی می کند مسیر یابی سیلی TCP SYN را کاهش دهد.

این شیوه فقط از مسیر یابی سیلابی TCP SYN پشتیبانی می کند و نمی تواند به مبازه با مسیر یابی سیلابی UDP برود. همچنین کاوشگر TCP دارای هزینه سربار و محاسبه، برای دریافت پاسخ و آنالیز سربار از کاربر است.

در آینده ما سعی در آنالیز و ارائه راه حل برای IP های جعلی که در سایر محیط ها کار می کنند، داریم.