راه حل های آسیب پذیری و تهدیدات در شبکه تعریف شده نرم افزاری (SDN)

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 2581–2589

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)

Aayush Pradhan[a], Rejo Mathew[b]*

[a]IT Department, Mukesh Patel School of Technology Management and Engineering, Mumbai 400056, India

ترجمه

حامد عبدالراق

https://github.com/hamed-abd

شماره دانشجویی: ۹۴۹۷۲۸۳۲۸

چکیده: در جهان در حال پیشرفت امروز، اندازه و الزامات شبکه ها افزایش می یابد که می تواند سنگین باشد زیرا حرکت با سوئیچ ها کاملاً بی نظم است. SDN به برنامه ریزی و اجرای مستقل سوئیچ ها کمک می کند. SDN روشی برای ایجاد قابلیت برنامه ریزی برای توسعه برنامه های شبکه با جدا کردن سطح کنترل از سطح داده است. امنیت شبکه تعریف شده نرم افزاری (SDN) یک موضوع آزاد است. جدا کردن سطح کنترل از سطح داده ، تعدادی از چالش های امنیتی مانند حمله مرد در وسط (MITM) ، انکار سرویس (DoS) ، حملات اشباع بیش از حد و غیره را باز می کند. در این مقاله ، ما به بررسی اجمالی شبکه تعریف شده نرم افزاری (SDN) ، چالش ها ، مشکلات و راه حل های آنها پرداخته ایم. ابتدا ، ما در مورد معماری SDN ، به دنبال آن توضیحات تهدیدات و در آخر ، پیشنهاد برخی راه حل ها برای تعبیه کردن امنیت بحث کردیم.

کلمات کلیدی: شبکه تعریف شده نرم افزاری(SDN) ، DDoS ، خراب کردن بسته ، حقه ARP ، نیروی وحشیانه ، بهره برداری از API

۱ - معرفی

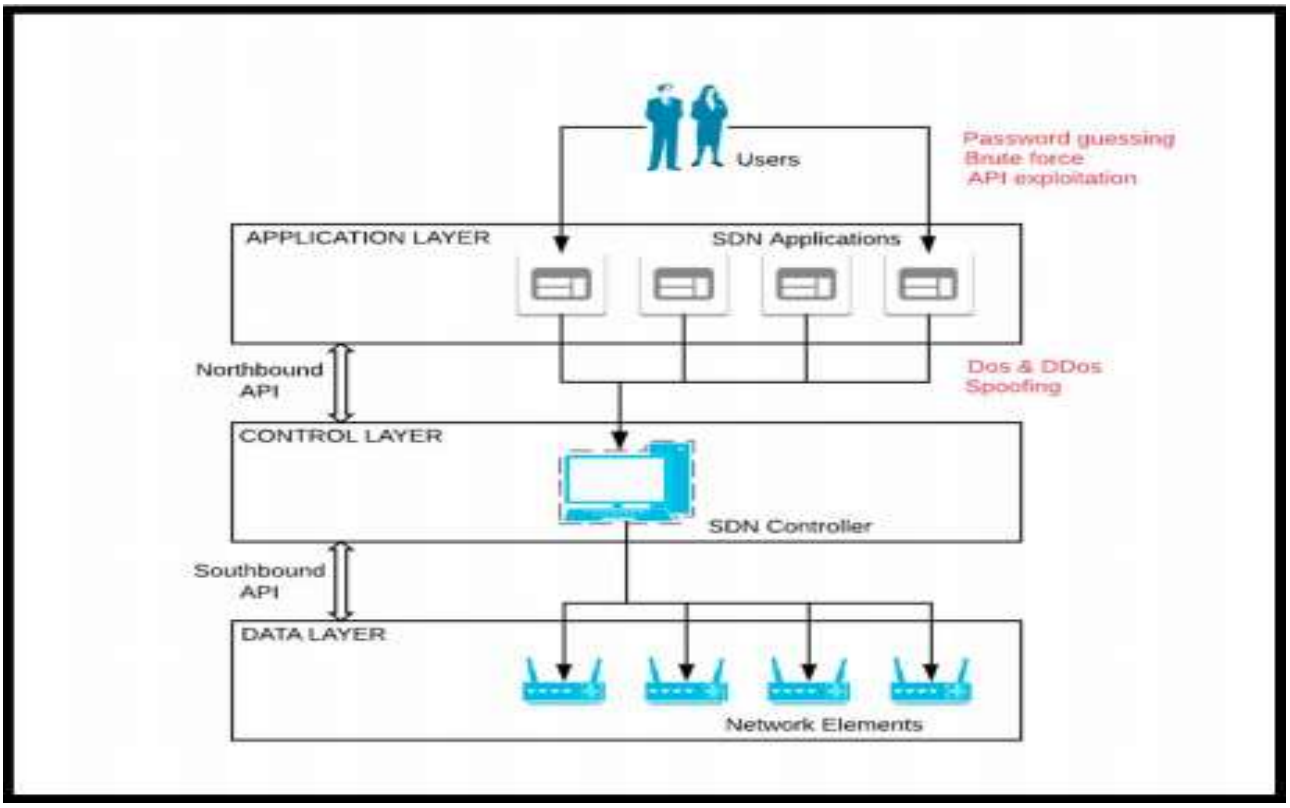
SDN یک فناوری شبکه است که هواپیماهای کنترلی قابل برنامه ریزی و انتزاع طرح داده را فراهم می کند و شبکه های مجازی سازی شده خود را بدون درک فناوری های جامع سخت افزاری به طور صریح مدیریت می کند. SDN از جداسازی سطح کنترل از سطح داده و همچنین جداسازی کنترل کننده سلسله مراتبی منطقی از تعامل سطح داده و برنامه های کنترلی جاری در بالای شبکه پشتیبانی می کند.[1]

SDN از ۳ لایه تشکیل شده است :[1]

- لایه زیرساخت: به عنوان شالوده برای یک معماری SDN عمل می کند. این لایه از دستگاه های شبکه فیزیکی و مجازی مانند سوئیچ ها و روترها و لوازم مختلف دیگر شبکه تشکیل شده است که به یک شبکه اساسی برای به جلو بردن ترافیک شبکه، تبدیل می شود.
- لایه کنترل: این لایه شامل یک سطح کنترل متمرکز است که در آن منطق تجارت برای آوردن و نگه داشتن انواع مختلف اطلاعات شبکه مانند جزئیات وضعیت ، جزئیات توپولوژی ، جزئیات آماری و غیره در کنترل کننده نوشته می شود.
- لایه کاربرد: از دستگاه های مختلف شبکه ، ابزارهای شبکه و برنامه های تجاری که از طریق کنترل کننده با لایه کنترل تعامل می کنند، تشکیل شده است.

معماری های SDN به طور کلی سه جز دارند:[2]

- برنامه های کاربردی SDN : این برنامه ها برنامه هایی هستند که منابع مورد نیاز را با کمک برخی از رابط های برنامه نویسی کاربردی (API) با کنترل کننده مرتبط می کنند.
- کنترل کننده ی SDN: کنترلر یک وجود منطقی است که دستورات یا الزامات را از لایه کاربرد دریافت می کند و سپس بسته به نوع عملکرد مورد نیاز ، آنها را به اجزای شبکه در آن شبکه خاص منتقل می کند.
- دستگاه های شبکه SDN : این دستگاه ها قابلیت حمل و نقل و پردازش داده های شبکه را کنترل می کنند همانطور که در شکل ۱ نشان داده شده است.



شکل ۱. معماری SDN همراه با بردارهای احتمالی حمله

۲- آسیب پذیری در SDN

آسیب پذیری هایی که ممکن است در کنترل کننده مستقر باشند می تواند به شرح زیر باشد:

- احراز هویت ضعیف:

احراز هویت کم هر شرایطی را تعریف می کند که ظرفیت فرآیند احراز هویت در مقایسه با ارزش دارایی ایمن شده نسبتاً ضعیف باشد.

- رمزگذاری ناقص:

رمزگذاری از معادلات پیچیده ریاضی برای پنهان کردن اطلاعات از خارجی ها ، تبدیل اسناد ، پیام ها و پرونده ها به چرت و پرت نامفهوم استفاده می کند. به طور معمول ، اسناد رمزگذاری شده برای رمزگشایی به یک کلید نیاز دارند ، اما در برخی شرایط ، هکرها ممکن است مکانیسم های احراز هویت را دور بزنند و به اطلاعات ممتاز دسترسی پیدا کنند. ممکن است منجر به دسترسی غیر مجاز به متجاوزان شود.

- افشای اطلاعات:

افشای اطلاعات زمانی است که یک برنامه کاربردی از اطلاعات حساس و محرمانه از موجودیت ها که در شرایط عادی انتظار نمی رود به موضوع موردنظر دسترسی داشته باشد، به اندازه کافی محافظت نمی کند. که این می تواند بیشتر منجر به کنترل ترافیک شبکه شود.

کنترل کننده جزء هسته در SDN است، از این رو اگر کسی کنترلر موجود در سطح کنترل را درست مدیریت نکند ، ممکن است یک پتانسیل نقطه حمله و خرابی باشد. کنترل کننده جریان داده ای را که در سطح داده صورت می گیرد ، تعریف می کند. از این رو، وقتی کنترل کننده مورد حمله قرار گیرد و به خطر بیفتد ، قطعاً روی شبکه تأثیر بدی خواهد گذاشت. کارهای زیادی برای مقایسه کنترل کننده های SDN با کمترین تعداد آسیب پذیری ها انجام شده است که در این میان Floodlight و OpenDaylight دو کنترل کننده با نتایج تقریباً مشابه بودند.[16]

۳- تهدیدهای SDN

لیست تهدیدات احتمالی در SDN را می توان به طور گسترده ای بر اساس منطقه هدفمند دسته بندی کرد :

- کنترل کننده SDN
- دستگاه های شبکه
- ارتباط داده ها بین کنترل کننده و دستگاه های مختلف شبکه

- ارتباطات بین چندین کنترل کننده در دامنه های مختلف یا شبکه های مختلف

بردارهای تهدید امنیتی SDN فهرست شده در پایین توسط [۴] عبارتند از:

- جریانات ترافیکی جعلی
- حمله به ضعف های موجود در سوییچ ها
- حملات به ارتباطات درگیر در سطح کنترل (بین کنترل کننده و سایر دستگاه های شبکه، همچنین بین کنترل کننده و API ها)
- کمبود مکانیسم های امنیتی قوی برای اطمینان از اعتماد بین کنترل کننده و سایر برنامه های کاربردی

انواع حملات احتمالی که در حین اجرای SDN امکان پذیر است را می توان به عنوان تهدید بر روی هر یک از لایه ها طبقه بندی کرد که در جدول ۱ به تصویر کشیده شده است.

۳-۱ سطح کنترل

سطح کنترل توپولوژی شبکه را تعریف می کند[3] . این یک مفهوم اصلی در فناوری مسیریابی شبکه است. آن مسئول مرتبط کردن روترها و تبادل اطلاعات در مورد پروتکل است. طیفی از پروتکل های مسیریابی برای تعریف و مدیریت اتصالات استفاده می شود .انواع زیر حملات احتمالی به این لایه است:

۳-۱-۱ دستکاری شبکه

در این نوع حمله، متجاوز با ساختن داده های نادرست در شبکه، کنترل کننده را به خطر می اندازد و سپس به طور همزمان حملات دیگری را به شبکه آغاز می کند.

۳-۲ سطح داده

این سطح به عنوان سطح حمل و نقل نیز شناخته می شود. [3] این ترافیک را مطابق با منطق سطح کنترل به پرش بعدی در طول مسیر به سمت شبکه هدف منتخب منتقل می کند. روتر از طریق بسته های سطح داده می رود. روترها / سوئیچ ها از سطح کنترل پیکربندی شده برای ورود و خروج فریم ها و بسته ها استفاده می کنند. انواع زیر حملات احتمالی به این لایه است:

۳-۲-۱ انحراف ترافیک

چنین نوع حملاتی برای عناصر مختلف در شبکه اتفاق می افتد، به ویژه در سطح داده ای که در آن مهاجم عنصر شبکه را برای هدایت دوباره جریان ترافیک به خطر می اندازد و به دنبال آن آسیب پذیری های بیشتر را با روش هایی مانند استراق سمع کاوش می کند.

۳-۲-۲ حمله کانال جانبی

حمله دیگری که عناصر شبکه را در سطح داده هدف قرار می دهد حمله کانال جانبی است. برای انجام موفقیت آمیز این حمله ، مهاجم از اطلاعات خاص شبکه مانند اطلاعات زمان بندی (از جمله جزئیات مدت زمان ایجاد اتصال جدید) کمک می گیرد تا تجزیه و تحلیل کند که آیا یک قانون جریان وجود دارد یا خیر.

۳-۳ سطح کاربرد

سطح برنامه در شبکه، ردیف برنامه ها و خدمات شامل سطح کنترل و توابع شبکه سطح داده است. در این لایه دستگاههای متداول شبکه قرار دارند. [3] عملکرد این دستگاه ها در شبکه تعریف شده نرم افزاری تا حد زیادی یکسان است، اما تحویل آنها انتزاعی، متمرکز و اغلب مجازی است. انواع زیر حملات احتمالی به این لایه است:

۳-۳-۱ دستکاری برنامه

در چنین حملاتی، مهاجم می تواند به هر برنامه SDN دسترسی پیدا کند (گاهی اوقات با امتیاز بالا) و می تواند در انجام اقدامات غیرقانونی روی شبکه موفق باشد. بهره برداری از آسیب پذیری برنامه می تواند باعث اثرات نامطلوبی مانند سوء عملکرد شبکه، قطع سرویس یا استراق سمع اطلاعات شود.

حملات امنیتی	لایه کاربردی	لایه کنترل	لایه داده
دسترسی غیرمجاز • هواپیماربایی کنترل کننده • برنامه غیر مجاز	✓	✓ ✓	✓

نشت داده • مدیریت اعتبارنامه • کشف سیاست حمل و نقل		✓ ✓	
اصلاح داده ها • اصلاح جریان داده		✓	✓
خود داری از خدمات • غرق شدن کنترل کننده • غرق شدن سوییچ		✓	✓ ✓
مشکلات پیکربندی • عدم تصویبTLS • اجرای سیاست	✓ ✓	✓ ✓	✓ ✓

جدول ۱. حملات به لایه های مختلف درSDN

۳-۴ حملاتی که می توانند تمام قسمتهای SDN را تحت تأثیر قرار دهند

۳-۴-۱ انکار خدمات توزیع شده (DDoS)

مراحل مربوط به DDoS عبارتند از:

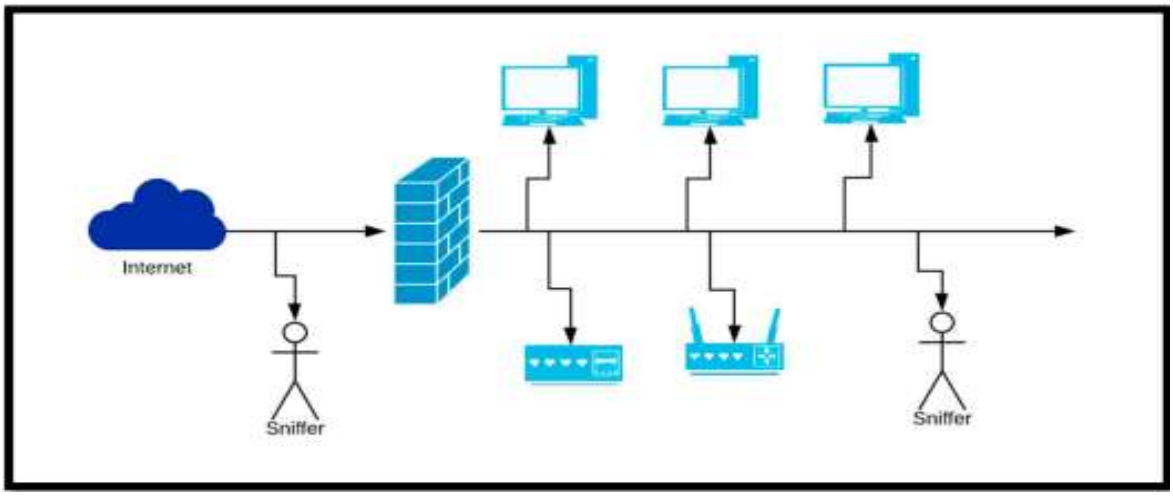
- در ابتدا، مهاجم یک سری بسته تقلبی ایجاد می کند که آدرس منبع آنها طوری جعل می شود که به نظر می رسد یک بسته معتبر است.
- بسته ها پس از معرفی به شبکه از طریق سوئیچ ها عبور می کنند. سوئیچ ها فرض خواهند کرد که بسته ها مشروع هستند.
- سپس سوئیچ ها این بسته ها را به کنترل کننده ی خواستار برای یک قاعده جریان جدید، میفرستند. اینجاست که مشکل پیش می آید. کنترل کننده اکنون بسته ها را شناسایی می کند و بلافاصله یک ورودی جریان برای بسته های جعلی ایجاد می کند. این فرایند زمان بر است.

- سپس مهاجم به طور مداوم بسته های جعلی را که منابع کنترل کننده را برای پردازش بسته های جعلی اشغال می کند، ادامه می دهد. بسته های قانونی هیچ شانسی برای هدایت توسط کنترل کننده نخواهند داشت، بنابراین کار انجام شده توسط کنترل کننده کاملاً بی فایده است.
- این روند طولانی منابع کنترل کننده را از پای در می آورد. این بسته های جعلی کنترل کننده را برای مدت زمانی خاص غیرقابل دسترسی می کند. فقدان کنترل کننده کل سرویس های شبکه را در SDN به خطر می اندازد.[5]

۲-۴-۳ بسته خراب کن

بسته خراب کن ها روشی برای جمع آوری ترافیک شبکه به منظور ارزیابی ترافیک برای استفاده بالقوه هستند. این روش برای یک دستگاه، کامپیوتر یا سخت افزار بسته خراب کن فراخوانی می شود. علاوه بر این که دستیابی به ابزار چقدر ساده است، عملکرد نرم افزاری که می تواند ترافیک داخل و خارج را ضبط کند، مهاجمان را ترغیب می کند تا از این روش برای منافع خود استفاده کنند. به دلیل عدم فعالیت ابزارها ، آنها می توانند بدون تغییر شبکه همانطور که در شکل ۲ نشان داده شده است ، به راحتی اطلاعات را جمع آوری کنند.

هنگامی که ما در مورد محیط شبکه غیر سوئیچ صحبت می کنیم، ترافیک شبکه برای هر دستگاه متصل در آن شبکه خاص منتشر می شود. بنابراین ، هر دستگاهی می تواند بسته ها را خراب کند. از طرف دیگر، در مورد محیط شبکه سوئیچ شده، بسته ها مستقیماا فقط به آدرس مقصد ارسال می شوند. در چنین شرایطی، به جز دستگاه میزبان مقصد، سایر دستگاه ها قادر به دیدن ترافیک نخواهند بود.[6]



شکل ۲. حمله بسته خراب کن

۳-۴-۳ حمله حقه یARP

مثال متداول حمله حقه ی ARP حمله Man-in-the-Middle (MITM) است. در حمله مرد در وسط، مهاجم مخفیانه ارتباطات بین دو طرف را باز پخش می کند و شاید تغییر می دهد.

استراق سمع نوعی حمله مرد در میانه است که در آن فرد متجاوز ارتباط مستقلی با قربانیان برقرار می کند و برای آنها پیام می فرستد تا آنها باور کنند که مستقیماً با یکدیگر به صورت خصوصی صحبت می کنند. این نوع حمله اطلاعات توپولوژی شبکه و برنامه های کاربردی مبتنی بر توپولوژی را خراب می کند.

۳-۴-۴ بهره برداری API

یک برنامه نویس با کمک API ها از سیستم عامل درخواست می کند. در هر عنصر رایانه ای، رابط برنامه برنامه (APIs) ممکن است در برابر توانایی هکر در انجام انتشار اطلاعات غیرمجاز آسیب پذیر باشد.

۳-۴-۵ حدس رمز عبور یا Brute Force

این حمله می تواند بر روی هر مولفه SDN یا عنصر غیر SDN رخ دهد. یک کاربر غیرمجاز می تواند با حدس گذرواژه یا نیروی بی رحمانه به SDN دسترسی پیدا کند. یک حمله بی رحمانه اساساً روش خطای اصابت و امتحان توسط نرم افزار برای رمزگشایی داده های رمزگذاری شده مانند رمزهای عبور یا کلیدهای رمزگذاری که با تلاش همه جانبه استفاده می شود، است.

٤- راه حل ها

۴-۱ راه حل برای DDos - تجزیه و تحلیل رفتار کاربر از طریق شناسایی از طریق انتروپی

یکی از راه های شناسایی مشخصه ی حمله DDoS استفاده از روش آنتروپی است[5] . انتروپی تصادفی بودن DDoS را تست می کند. هر چه نسبت تصادفی بودن بیشتر باشد، مقدار آنتروپی نیز بیشتر است. آنتروپی پس از دریافت مجموعه ای از بسته ها تعیین می شود. نسبت به آستانه ، نتیجه اندازه گیری آنتروپی محاسبه می شود .اگر آنتروپی بالاتر یا کمتر از آستانه باشد ، DDoS مشاهده می شود .با تشخیص زودهنگام ، مدیر شبکه می تواند بیشتر از آن استفاده کند.

۴-۲ راه حل برای بسته خراب کن - رمزگذاری با استفاده از گواهینامه های SSL

امنیت SDN را می توان با استفاده از رمزگذاری SSL به همان روشی که شبکه های سنتی انجام می دهند، انجام داد. به منظور ایمن سازی ارتباط بین دستگاه های شبکه و کنترل کننده، گواهینامه های SSL در سطح داده پیاده سازی می شوند. دو مرحله در SSLگنجانده شده است: فرآیندهای دست دادن و انتقال داده ها. [7] نیاز اولیه فاز دست دادن بررسی این است که آیا سوئیچ و کنترل کننده هر دو برای انتقال داده آماده هستند یا خیر.

مراحل مربوط به این فاز دست دادن عبارتند از:

- در مرحله اول، سوئیچ از کنترل کننده دزخواست کلید عمومی می کند.
- سپس کنترل کننده یک گواهی ارسال می کند که حاوی کلید عمومی است. این گواهی کنترل کننده را تأیید می کند و اعتبار سوئیچ ها را مشخص می کند. برای به دست آوردن گواهینامه ، کنترل کننده باید کلید عمومی خود را برای صدور گواهی (CA) ارسال کند. CA به ترتیب گواهی تولید می کند و به ترتیب اثر انگشت ایجاد می کند.
- سپس CA این اثر انگشت را با کلید خصوصی خود رمزگذاری می کند تا امضای گواهی ایجاد کند.
- برای دریافت اثر انگشت ، سوئیچ باید امضای تازه ایجاد شده را با کلید عمومی CA رمزگشایی کند. همچنین سوئیچ باید به طور خودکار اثر انگشت گواهی را تعیین کند.
- گواهی با مقایسه هر دو اثر انگشت تأیید می شود. اگر با هم مطابقت نداشته باشند، گواهینامه دستکاری شده است.
- با استفاده از یک الگوریتم کلید عمومی، کنترل کننده و سوئیچ اطلاعات کلید مخفی را پس از اتمام احراز هویت در هر دو طرف ارزیابی می کنند.
- فاز دست دادن سرانجام زمانی تمام می شود که کنترل کننده و سوئیچ آماده استفاده از کلید مخفی باشند.

در مورد مرحله انتقال داده، اطلاعات خروجی به قطعه هایی تقسیم شده و به کد تأیید پیام (MAC) پیوست می شوند. MAC اثر انگشت محاسبه شده از داده ها با کلید خاص خود است .این کلید کلید مخفی تولید شده در طی فرآیند دست دادن نیست.

۴-۳ راه حل حمله ی حقه ARP - استفاده از روش های مختلف مانند وصله گذاری، ابزار، نقشه برداری و غیره

برای حل حملات حقه ARP ، راه حل های پیشگیرانه که می توانند انتخاب شوند به شرح زیر است[8] :

۴-۳-۱ احراز هویت ARP

پروتکل ARP به گونه ای اصلاح خواهد شد که بسته های ARP را پردازش نکند مگر اینکه و تا زمانی که آنها یک کد رمزنگاری از پیش تعریف شده را نگه دارند. برخی از نمونه های متداول [9] S-ARP (Secure-ARP) و TARP هستند. این روش معایب خاص خود را دارد. این رویکرد باعث ایجاد تعارض با دستگاههایی می شود که هنوز از پروتکل عمومی اولیه ARP استفاده می کنند.

۴-۳-۲ وصله سیستم عامل

هدف از این روش وصله گذاری سیستم عامل برای جلوگیری از حقه در ARP است. اما برای هسته های مختلف سیستم عامل، این استراتژی نیاز به وصله دیگری دارد. یک سیستم عامل وصله ممکن است به درستی با سایر عملیات وصله نشده تعامل نداشته باشد. مکانیسم های Anticap و Antidote چند راه حل برای مشکلات حقه ARP هستند که هسته سیستم عامل را ترمیم می کنند.

۴-۳-۳ بازرسی پویا ARP (DAI)

برخی از سوئیچ ها دارای ویژگی امنیتی بازرسی پویا ARP (DAI) هستند[10] . سوئیچ ها برای جلوگیری از حملات حقه ARP با قطع کردن درخواست ها و پاسخ های ARP و انداختن بسته های نامعتبر آدرس IP-to-MAC ، از DAI استفاده می کنند. مسئله اصلی این رویکرد این است که عملکرد DAI در همه سوئیچ ها وجود ندارد.

۴-۳-۴ ابزارهای تخفیف ARP

چندین ابزار نرم افزاری برای سبک کردن(تخفیف) حملات حقه توسعه یافته است. مکانیسم های تشخیص خوبی برای سیستم های تشخیص رایگان مانند ARPWatch و XArp وجود دارد، اما آنها نمی توانند حفاظت کامل را ایجاد کنند. AntiNetcut [11]، NoCut [11] و AntiARP [11] ابزار نرم افزاری دیگری هستند. با این حال، این ابزارها دارای مشکلات بسیاری از جمله میزان بالای مثبت کاذب و منفی کاذب و میزان بالای بی اثر بودن هستند.

۴-۳-۵ نگاشت های ARP استاتیک

با پیکربندی دستی ورودی های ARP می توان حملات جعل ARP را بهتر مدیریت کرد. در انجام این کار، مهاجم هیچ شانسی برای جعل حافظه نهان ARP از طرف میزبان دیگر ندارد. با این وجود، برای شبکه های بزرگ این روش عملی نیست. اما این راه حل برای شبکه های مقیاس بزرگ قابل دوام نیست. در شبکه هایی که از آدرس دهی DHCP استفاده می کنند قابل استفاده

نیست. علاوه بر این ، مستعد خطا خواهد بود و به سرپرست شبکه زیادی نیاز دارد .چندین راه حل برای غلبه بر این اشکالات مانند DAPS [12]و NIDPS [13] ارائه شده است.

۴-۴ راه حل برای بهره برداری - API استفاده از ربات ها برای امنیت قوی

یک راه حل مدیریت ربات که از API ها در برابر حملات خودکار محافظت می کند و تضمین این که فقط کاربران واقعی می توانند به API دسترسی داشته باشند مهم است. ضمن در نظر گرفتن راه حلی مانند این، پوشش گسترده و شناسایی تهدیدات، گزارش دقیق، بررسی و گزینه های همه کاره را برای پیاده سازی در نظر بگیرید.

برای جلوگیری از سوء استفاده از API می توان اقدامات پیشگیرانه را انجام داد:

- نظارت و مدیریت در مدیریت تماسهای API از اسکریپتهای خودکار (رباتها)
- حذف احراز هویت ابتدایی
- اقدامات در حال اجرا برای جلوگیری از استفاده از ربات های شبه انسان پیچیده برای جلوگیری از دسترسیAPI
- استفاده از محدودیت های نرخ مبتنی بر رمز برای محدود کردن تعداد IP ها، جلسات و نشانه ها بر اساس کل استفاده از API
- رمزگذاری قوی باید داشته باشد

۴-۵ راه حلی برای حدس رمز عبور یا Brute Force

با استفاده از الگوریتم هایی مانند سوئیچ فروشنده، رمزهای عبور قوی و به روزرسانی مکرر و غیره، می توان از چنین نوع حملاتی جلوگیری کرد.

سایر راه حل های ممکن برای جلوگیری از زورگویی شامل [14] :

- قفل کردن حساب ها
- ورود به سیستم با زمان محدود - امکان دسترسی به کاربران انتخابی در یک زمان خاص به شبکه
- احراز هویت مبتنی بر پرس و جو
- تأیید اعتبار گذرواژه یکبار مصرف- این رمز عبوری است که فقط برای یک جلسه ورود به سیستم در دستگاه معتبر است

- استفاده از Captcha- کپچا نوعی آزمون چالش پاسخ ریاضی است که برای تصمیم گیری در مورد انسان بودن کاربر استفاده می شود.
- ورود به سیستم آدرس IP منحصر به فرد - استفاده از برخی از آدرس های IP ممتاز را که توانایی بازنویسی هر دستور دیگری در شبکه را دارند فعال کنید.

۵- تحلیل و بررسی

استفاده از گذرواژه یکبار مصرف (OTP)	محدود کردن دسترسیAPI	استفاده از رباتها	رمزگذاری با استفاده ازSSL	تجزیه و تحلیل آنتروپی	
بدون تکنیک رمزگذاری	بدون رمزگذاری داده ها	آنها رمزگذاری قوی ارائه می دهند	کاربر فقط با کلید دقیق می تواند دسترسی داشته باشد	بدون رمزگذاری داده ها در حین انتقال	رمزگذاری
کاربر فقط می تواند با استفاده از OTP صحیح وارد شود	احراز هویت کاربر	احراز هویت اولیه را فراهم می کند	فقط ارائه دهنده گواهی SSL قابل اعتماد است	آنتروپی برنامه های توپولوژی را تأیید نمی کند	احراز هویت
قابل استفاده نیست	بله ، با محدود کردن تعداد کاربران	بسته به رباتهایی که استفاده می شود ممکن است باشد یا نه	متجاوزان می توانند برای دریافت گواهی SSL معتبر مشکل داشته باشند	بدون محافظت در برابر فیشینگ ، فقط تجزیه و تحلیل رفتار کاربر	محافظین در برابر فیشینگ
فقط به کاربران مجاز اجازه دسترسی به شبکه را می دهد	فقط تعداد کاربران بر اساس تعداد IP محدود است	بستگی به نوع ربات استفاده شده دارد	قابل استفاده نیست	از این ویژگی پشتیبانی نمی کند	دسترسی به داده

جدول ۲. جدول مقایسه راه حل های مختلف

۶- نتیجه

ما می توانیم این مقاله را با بیان اینکه کنترل کننده مرکزی آسیب پذیرترین قسمت از ساختار SDN است، نتیجه بگیریم. از جدول ۲، یک بررسی مختصر در مورد تهدیدها و راه حل ها می توان درک کرد. اگرچه یک سیستم کنترل شبکه متمرکز و قابلیت

برنامه ریزی شبکه می تواند منجر به پیاده سازی قوی و مناسب امنیت شود، اما همچنین چالش های جدیدی را برای امنیت ایجاد می کند. بنابراین، ما بیشتر نقاط ضعف امنیتی در SDN و راه حل های پیشنهادی آنها را در این مقاله ارائه داده ایم.

با توسعه تدریجی فناوری SDN ، احتمالش بسیار بالاست که تهدیدات امنیتی جدیدی رخ بدهد. ما تصور می کنیم که SDN می تواند یکی از مهمترین فن آوری ها باشد که با گذشت زمان منجر به پیشرفتهای امنیتی شبکه می شود .نوآوری های SDN همچنین رایانه سازی ابر را آسان تر می کند.[15]

ویژگی های برجسته پشتیبانی شده توسط SDN قابلیت انعطاف پذیری، قابلیت اطمینان بسیار بالا، تأخیر کم سطح کنترل توزیع شده و غیره هستند که به SDN کمک می کند تا به سمت شبکه های گسترده و شبکه های هسته ای ۵G تجسم یابد. برای دستیابی به قابلیت اطمینان بالا و تأخیر کم در میزان ترافیک متنوع، سطح کنترل توزیع شده باید به صورت پویا مدیریت شود[17] .

مراجع

[1] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, (2015) "Security in Software Defined Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2317-2346, Fourthquarter

[2] T. D. Nadeau, K. Gray, (2013) “SDN: software defined networks.” O’Reilly Media, Inc

[3] S. Hogg, (2014) “SDN Security Attack Vectors and SDN Hardening”

[4] D. Kreutz, V. Ramos, E. R. Christian, (2015) “Software Defined Networking: A Comprehensive Survey”, Proceedings of the IEEE, Vol. 103, No.1

[5] S. M. Mousavi, M. St-Hilaire, (2015) “Early detection of DDoS attacks against SDN controllers.”, IEEE International Conference on In Computing, Networking and Communications (ICNC)

[6] R. Spangler, (2003) “Packet sniffing on layer 2 switched local area networks.”, Packetwatch Research

[7] W. Chou, (2002) “Inside SSL: the secure sockets layer protocol.”

[8] M. Jammala1, T. Singha, A. Shamia, R. Asalb, and Y. Lic, (2014) “Software-Defined Networking. State of the Art and Research Challenges” Computer Networks, vol. 72, pp. 74–98

[9] D. Bruschi, A. Ornaghi, E. Rosti, (2003) “S-ARP: a secure address resolution protocol”, 19th Annual Computer Security Applications Conference

[10] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html#wp1039201

[11] A. M. Abdelsalam, A. El-Sisi, V. Reddy, (2015) “Mitigating ARP Spoofing Attacks in Software-Defined Networks”, ICCTA

[12] X. Hou, Z. Jiang and X. Tian, (2010) "The detection and prevention for ARP Spoofing based on Snort,", International Conference on Computer Application and System Modeling

[13] S. G. Bhirud, V. Katkar, (2011) "Light weight approach for IP-ARP spoofing detection and prevention,", Second Asian Himalayas International Conference on Internet (AH-ICI)

[14] G. Sowmya, D. Jamuna, M. Venkata Krishna Reddy, (2012) “Blocking of Brute Force Attack”, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 6

[15] S. Mishra, M. A. R. AlShehri, (2017) “Software Defined Networking: Research Issues, Challenges and Opportunities”, Indian Journal of Science and Technology, Vol 10

[16] S. Rowshanrad, V. Abdi, M. Keshtgar (2016) “Performance evaluation of SDN controllers: Floodlight and OpenDaylight”, IIUM Engineering Journal, Vol. 17, No. 2

[17] B. Görkemli, S. Tatlıcıoğlu, A. M. Tekalp, S. Civanlar and E. Lokman (2018) "Dynamic Control Plane for SDN at Scale", IEEE Journal on Selected Areas in Communications, vol. 36, no. 12, pp. 2688-2701