**بهبود امنیت شبکه از طریق شبکه سازی تعریف شده توسط نرم افزار (SDN)**

شبکه سازی تعريف شده از طريق نرم افزار (SDN) تکنولوژی در حال ظهوری است که اخيرا توجه بسیاری را در صنعت و دانشگاه به خود جلب کرده است. با جدا کردن منطق کنترلی از پیاده سازی بسته و اختصاصی دستگاه های شبکه رایج، محققان و نوآوران قادر به طراحی توابع / پروتکل های شبکه نوین به روشی بسیار انعطاف پذیرتر، قدرتمند تر و ساده تر شدند. ما اعتقاد داریم SDN فرصت های تحقیق جدیدی را برای امنیت فراهم می کند و می تواند تا حد زیادی به تحقیقات امنیتی شبکه تاثیر گذار باشد. با این حال، تا به امروز SDN به درستی توسط جامعه امنیت شناخته نشده است. در این بررسی سیستماتیک در مورد امنیت SDN، بررسی می کنیم که چگونه ویژگی های جدید ارائه شده توسط SDN می تواند به افزایش امنیت شبکه و فرآیند امنیت اطلاعات کمک کند. به کمک استدلال سیستماتیک، فرصت هایی توسط SDN برای امنیت شبکه ارائه شده، از این رو امیدواریم بینش جدیدی را برای تحقیقات آینده در این حوزه مهم فراهم کنیم.

کلمات کلیدی: شبکه سازی تعريف شده از طريق نرم افزار، امنیت شبکه

**1- مقدمه**

شبکه سازی تعريف شده از طريق نرم افزار (SDN) به سرعت به عنوان یک تکنولوژی نوید دهنده برای شبکه های آینده ظهور کرده است. با جدا کردن صفحه کنترل از صفحه داده، امکان افزودن آسان توابع و یا پروتکل های شبکه جدید، خلاق و قدرتمند، SDN توجه زیادی را از سوی دانشگاه ها و صنعت به خود جلب کرده است. در دانشگاه ها، از زمان انتشار OpenFlow که یک مولفه کلیدی برای تحقق مفهوم SDN است، بسیاری از ایده های تحقیق مبتنی بر SDN / OpenFlow پیشنهاد شده است (و همچنان ادامه دارد). در صنعت، SDN به عنوان نمونه جدیدی برای شبکه های آینده به طور گسترده ای در نظر گرفته می شود و بسیاری از شرکت ها به منظور تقویت معماری شبکه خود، یا برای کاهش هزینه های عملیاتی و فعال سازی برنامه های کاربردی شبکه های جدید / توابع، در حال گسترش SDN هستند و یا آن را گسترش داده اند..

به طور کلی اهداف و مشارکت های اصلی این مقاله دو مورد زیر هستند:

اول، ما به طور سیستماتیک فناوری SDN را به محدوده گسترده تر از محققان امنیتی معرفی می کنیم. ما معتقدیم دلیل اینکه جامعه امنیت با SDN آشنایی کمی دارد، عمدتا به این خاطر است که در حال حاضر به اندازه کافی در معرض آن قرار نگرفته است. درک عمیق تر از تکنولوژی SDN به محققان امنیتی کمک خواهد کرد تا خدمات جدید، جالب و بهتر و یا سیستم های دفاعی هوشمند شبکه را تولید کنند.

دوم، ما بررسی عمیقی در مورد اینکه چگونه ویژگی های SDN می تواند به امنیت منافع کمک کند انجام دادیم، نشان داده شده این مورد با تحقیقات پیشرفته در زمینه های دیگر مرتبط است. با نشان دادن این فرصت های جدید که توسط SDN به ارمغان آورده می شوند، امیدواریم که در آینده ایده های خلاق جدید بیشتری در این زمینه ایجاد کنیم.

**2- بیان مسئله**

ما معتقدیم که SDN می تواند مزایا قابل توجهی برای تحقیقات امنیتی داشته باشد و همچنین می تواند با تحقیقات امنیتی موجود ترکیب شود. یادآوری می کنیم که مطالعه و یا مسائل افزایش تهدیدات امنیتی و آسیب پذیری مربوط به خود SDN (مثلا مراجع [49، 41، 28، 31، 61، 21، 59، 44]) مورد نظر این مقاله نیست. در عوض، می خواهیم به طور سیستماتیک از فرصت ها و چالش های موجود در مورد چگونگی استفاده از SDN برای امنیت شبکه بهره ببریم. برای این منظور، ما با بررسی ویژگی های جدید ارائه شده توسط SDN شروع می کنیم، سپس بررسی می کنیم که چگونه این ویژگی ها می توانند توابع امنیتی خاص را ارتقا دهند. در نهایت، ما بیشتر در مورد چالش های اجرای برنامه های امنیتی با SDN در دنیای واقعی بحث می کنیم.

**3- چگونه امنیت شبکه از ویژگی های SDN بهره می برد؟**

در این بخش، بررسی خواهیم کرد چگونه ویژگی های جدید SDN، که در بخش قبلی بحث شده اند، می توانند مزایایی برای امنیت شبکه داشته باشد. علاوه بر این، برخی نمونه های امنیتی برنامه های کاربردی که قبلا پیشنهاد شده اند و می توان در آینده به آن دست یافت، به منظور کمک به مردم در درک مزایای آنها ارائه می شود.

***A. کنترل جریان دینامیک***

مزایای استفاده از امنیت شبکه: کنترل جریان شبکه به صورت دینامیکی امکانات بسیاری در توابع امنیتی شبکه فراهم می کند. ابتدا، می توانیم تابع کنترل دسترسی دینامیک را اجرا کنیم، که معمولا برای محافظت از شبکه استفاده می شود. از قبل، ما باید یک میدل باکس مستقل (مانند فایروال) را برای دستیابی به کنترل درون خطی نصب کنیم. با این حال، با کمک SDN، ما نیازی به نصب میدل باکس های کوچک اضافی نداریم، بلکه فقط از یک دستگاه شبکه استفاده کنیم (مثلا یک سوئیچ / روتر OpenFlow) که از توابع SDN برای کنترل دسترسی پشتیبانی می کنند. علاوه بر این، می توانیم جریان های شبکه را با جزئیات دقیق (از 1 تا 12 تایی) کنترل کنیم، این همچنین ما را قادر می سازد تا جریان های شبکه را به طور موثرتری کنترل نماییم.

***B. قابلیت مشاهده شبکه­ای با کنترل جریان مرکزی***

مزایای امنیت شبکه: نظارت شبکه فعالیت مهم و ضروری در امنیت شبکه است. به طور رایج، برای نظارت بر کلیه زیر شبکه ها (از جمله ترافیک کلی و ترافیک داخلی)، نیاز به نصب یا راه اندازی سنسورهای نظارت و جمع آوری اطلاعات شبکه در هر دستگاه شبکه یا لینک داریم، که به نظر می رسد درک اینها در شبکه های بزرگ در دنیای واقعی آسان نیست.

***C. برنامه پذیر بودن شبکه***

مزایای امنیت شبکه: توابع امنیت شبکه عموما با استقرار برخی از واسطه های سخت افزاری یا نصب برخی از برنامه های نرم افزاری ساخته می شوند. آنها توابع از پیش تعریف شده برای امنیت شبکه دارند، و معمولا این تغییر و یا اصلاح این توابع آسان نیست. با این حال، گاهی اوقات پیش بینی عملکرد امنیتی لازم برای یک شبکه سخت است. پس، در این مورد، چه می شود اگر معلوم گردد باکس های امنیتی مستقر برای تامین امنیت شبکه ضروری نیستند، اما نیاز به نصب یک تابع امنیتی متفاوت دارند؟ ما می توانیم باکس های قدیمی را از بین ببریم و باکس جدید خریداری کنیم که سبب هزینه اضافی می شود.

***D. صفحه داده ساده شده***

مزایای امنیت شبکه: در مقایسه با دستگاه های نسل قبلی، سخت افزار (مثلا صفحه نمایش داده) برای SDN میتواند به راحتی تغییر کند، زیرا از مدول های سخت افزاری نسبتا ساده­ای تشکیل شده و مدول های صفحه کنترل پیچیده را به حرکت وا می دارد. این کار برای گسترش سرویس های جدید شبکه فرصتی فراهم می کند (به عنوان مثال [9]). این مفهوم همچنین می تواند به امنیت اعمال شود. ما می توانیم سطح داده SDN را گسترش دهیم تا آن را برای اهداف امنیتی مناسب تر کنیم.

***E. اظهار نهایی***

با وجود این که ما هر یک از ویژگی ها را به صورت جداگانه بحث می کنیم، اما اذعان داریم که در واقع سخت است که آنها را برای برنامه های امنیتی خاص جدا سازیم. به عنوان مثال، فایروال توزیع شده [22] به طور طبیعی می تواند ویژگی های چندگانه، مانند کنترل جریان دینامیکی و دید شبکه را با کنترل متمرکز ترکیب کند. تصور می کنیم برنامه های امنیتی آینده SDN می توانند هر مجموعه ای از ویژگی های SDN را برای دستیابی به قابلیت های مورد نظر خود ترکیب کنند.

**4- چگونه ویژگی های SDN موجب افزایش امنیت اطلاعات می شود؟**

پیش از این، ما در مورد چگونگی استفاده از ویژگی های SDN در امنیت شبکه بحث کرده ایم و اکنون خواهیم دید که چگونه این ویژگی ها سه گانه امنیت اطلاعات را بهبود می دهند. این سه ویژگی عبارتند از: (i) پیشگیری، (ii) شناسایی و (iii) پاسخ، که یک چارچوب اساسی، شناخته شده برای فعال سازی قابلیت دفاعی قوی هستند.

*A. پیشگیری*

پیشگیری فرایند متوقف کردن مهاجمان از تماس با اهداف به منظور حفاظت است، و معمولا با تنظیم برخی سیاست های امنیتی تعیین می کنند که چه کسی (یا چه چیزی) می تواند (یا نمی تواند) به آنها دسترسی داشته باشد. این فرآیند نیاز به برنامه ریزی دقیق و تحقیق برای به حداقل رساندن اشتباهات دارد، زیرا ممکن است سیاست های امنیتی کاربران را مسدود کنند و یا حالات مخرب را بپذیرد. بنابراین، تعیین سیاست های امنیتی مهم ترین کار است، سیاست های امنیتی معمولا پس از تصمیم گیری تغییر نمی کنند. با این حال، بسیاری از معماری های موجود در شبکه کاملا پیچیده و متغیر هستند، و در نتیجه کنترل دسترسی بر اساس سیاست های استاتیک ممکن است برای حفاظت و مدیریت یک شبکه بزرگ و دینامیک کافی نباشد. در این مورد، ما نیاز به یک روش کنترل دسترسی دینامیکی داریم که برخی از دستگاه های شبکه جدید پشتیبانی می کند، اینکار معمولا نیاز به نصب میدل باکس های اضافی در شبکه دارد.

*B. تشخیص*

تشخیص یک فرایند امنیتی مهم به منظور کشف شبکه های نفوذی است و معمولا از دو روش تشخیص استفاده می شود: (i) تشخیص سوء استفاده و (ii) تشخیص غیر متعارف. تشخیص سوء استفاده، حملات مبتنی بر الگوهای شناخته شده (a.k.a.,signature) را تشخیص می دهد و تشخیص غیر متعارف با شناسایی الگوهای مخرب در ترافیک شبکه که با رفتارهای معمول طبیعی مطابقت ندارند، حملات را پیدا می کند.

*C. پاسخ*

پاسخ به حملات (به عبارتی دیگر، مقابله با حمله) بخش مهمی در چارچوب امنیت دفاعی قوی است. با این حال، با توجه به مطالعات انجام شده سخت ترین بخش امنیت شبکه این قسمت می باشد. به طور رایج، برای پاسخ دادن به حملات، ممکن است میدل باکس هایی را نصب کنیم تا آزمایشات حمله یا انزوا یا قربانی کردن میزبان را برای محافظت از میزبان های دیگر در شبکه انجام دهند. ویژگی کنترل جریان دینامیک SDN می تواند به طور قابل توجهی برای افزایش این فرایند مورد استفاده قرار گیرد. این آزمایشات می تواند به راحتی توسط این ویژگی کاهش یابد و همچنین انزوای شبکه یا قرنطینه را می توان به راحتی با SDN اجرا کرد.

**5. بحث و گفتگو**

هدف اصلی این مقاله این است که پاسخ های معقولی را برای پرسش اصلی در تحقیق بدست آورد - آیا می توانیم ویژگی های جدید ارائه شده توسط SDN را برای افزایش امنیت شبکه افزایش دهیم؟(چگونه؟). بر اساس نظرسنجی های جدی و تجزیه و تحلیل عمیق ویژگی های SDN و برنامه های کاربردی مورد بحث در این مقاله، ادعا می کنیم که SDN می تواند به وضوح عملکرد توابع امنیت شبکه را بهبود بخشد. اولا، توانایی آن در کنترل جریان شبکه به صورت دینامیک می تواند قابلیت انعطاف پذیری عملکرد توابع امنیتی را در یک شبکه فراهم کند، زیرا به ما اجازه می دهد تا توابع امنیتی را در دستگاه های شبکه فعال SDN بدون نصب دستگاه های اضافی (مانند میدل باکس) فعال کنیم. دوما، قابلیت مشاهده شبکه آن می تواند کنترل شبکه را با توجه به امنیت به درستی انجام دهد. این قابلیت دید کلی برای ما فراهم می کند و بنابراین می توانیم حملات شبکه ای را که به طور گسترده ای در اینترنت (مانند اسکن شبکه گسترده یا DDoS) توزیع شده اند، بسیار موثر تر از سیستم های مانیتورینگ شبکه، درک کنیم و متوجه شویم. سوما، قابلیت برنامه ریزی آن به ما کمک می کند تا توابع امنیت پیشرفته تر شبکه را توسعه دهیم. می توانیم (نسبتا) به راحتی یک سیستم امنیتی نمونه اولیه را بدون نیاز به تلاش زیاد پیاده سازی و اجرا کنیم. به همین ترتیب، ویژگی های SDN را می توان در تسریع توسعه تابع امنیتی جدید و شبکه پیشرفته استفاده کرد.

**6. نتیجه گیری**

در این مقاله، فناوری SDN را معرفی می کنیم و به طور سیستماتیک آن را برای امنیت استفاده می نماییم. اگر چه بسیاری از افراد تا به حال به این تکنولوژی علاقه مند شده اند، اما تاکنون محققان امنیتی هنوز به خوبی از آن استفاده نکرده اند. ما بر این باوریم که SDN می تواند در عین حال یکی از تاثیر گذارترین فن آوری ها برای ایجاد نوآوری های مختلف در امنیت شبکه باشد. امیدواریم که این مطالعه نه تنها بتواند مقدمه سریع و مرورکلی منظمی ارائه دهد بلکه بتواند بینش قابل توجهی نیز برای استفاده از SDN به منظور برنامه های امنیتی بهتر و تحریک تحقیقات آینده در این منطقه مهم فراهم کند.