

سنة الفجر

سمینار

عنوان

امنیت کنترلر در شبکه‌های نرم افزار محور

نگارنده:

۶	چکیده
۷	فصل اول: مقدمه
۸	۱-۱- مقدمه
۱۰	فصل دوم: مطالعه شبکه های نرم افزار محور
۱۱	۱-۲- مقدمه
۱۱	۲-۲- شبکه های نرم افزاری
۱۳	۳-۲- چگونگی پیدایش SDN
۱۷	۴-۲- ایده SDN
۱۸	۵-۲- معماری SDN
۱۹	۲-۵-۱- اجزای تشکیل دهنده SDN
۱۹	۲-۵-۱-۱- کنترلرها
۲۰	۲-۵-۱-۲- سوئیچ های مجازی
۲۰	۲-۵-۱-۳- شبکه های هم پوشان (Overlay)
۲۰	۲-۵-۲- ساخت اجزای SDN هوشمند و سریع
۲۲	۶-۲- پروتکل OpenFlow
۲۳	۷-۲- رابطه شبکه واقعی با SDN
۲۴	۸-۲- بررسی ویژگی های SDN
۲۶	۲-۸-۱- نیازمندی های در حال رشد شبکه
۲۷	۲-۹- اهداف SDN
۲۸	۲-۱۰- جمع بندی
۳۰	فصل سوم: بررسی و ارزیابی امنیت در کنترلرها
۳۱	۳-۱- مقدمه
۳۱	۳-۲- ارتباط بین کنترلرگرا
۳۲	۳-۳- تحقیقات مرتبط با کنترلرگرا

۳-۴-	توان عملیاتی کنترلر.....	۳۴
۳-۵-	امنیت SDN.....	۳۵
۳-۵-۱-	ملاحظات امنیت SDN و کنترلرها.....	۳۶
۳-۵-۲-	تهدیدهای شناسایی شده در کنترلرها.....	۳۷
۳-۵-۲-۱-	نقشه تهدیدات اصلی در SDN و بخش کنترلر.....	۳۸
۳-۶-	مسائل امنیتی کنترلر.....	۴۰
۳-۴-۶-	جمع بندی.....	۴۲

فصل چهارم: نتیجه گیری و پیشنهادات

۴-۱-	نتیجه گیری و پیشنهادات.....	۴۳
۴-۱-	نتیجه گیری و پیشنهادات.....	۴۴
	مراجع	۴۶

فهرست اشکال

- شکل ۱-۲- سیستم شبکه های نرم افزار محور..... ۱۷
- شکل ۲-۲- معماری SDN..... ۱۸
- شکل ۳-۲- کنترلر ها در SDN..... ۱۹
- شکل ۴-۲- ساختار شبکه هم پوشان..... ۲۰
- شکل ۵-۲- شبکه با کنترلر مرکزی..... ۲۳
- شکل ۶-۲- مقایسه شبکه های سنتی (سمت چپ) و SDN (سمت راست)..... ۲۴
- شکل ۷-۲- مفهوم شبکه نرم افزار محور و پروتکل Open Flow..... ۲۵
- شکل ۸-۳- توان عملیاتی کنترلر..... ۳۵
- شکل ۹-۳- نقشه تهدیدات اصلی در SDN و بخش کنترلر..... ۳۷

فهرست جداول

- شکل ۲-۱- مقایسه برنامه های کاربردی SDN مختلف ۲۸
- شکل ۳-۲- پیاده سازی کنترلر جاری مطابق با استاندارد OpenFlow ۳۴
- شکل ۳-۳- تهدیدات اختصاصی در مقابل غیر اختصاصی ۳۹
- شکل ۳-۴- مقایسه مساله امنیت SDN و کنترلر و راه حل آنها ۴۱

چکیده:

شبکه نرم افزار محور (SDN) یک تکنولوژی جدید است که می تواند در طراحی و مدیریت ما بر شبکه، نوآوری داشته باشد. اگرچه به نظر می آید که این تکنولوژی سریعاً نمایان شده اما، SDN بخشی از تاریخچه طولانی مدت زحمت ها برای ایجاد شبکه های کامپیوتری با قابلیت برنامه ریزی بیشتر می باشد. بزرگ ترین چالش امنیت SDN، این واقعیت است که SDN از کنترل متمرکز استفاده می کند. اگر سرور SDN مورد حمله قرار بگیرد یا دسترسی دستاوردهای یک هکر به کنترلر SDN ترافیک شبکه، می تواند در اطراف فایروال نرم افزارهای مخرب قرار داده و می تواند گره های شبکه را الوده سازد. در این سمینار علاوه بر بررسی شبکه های تعریف شده نرم افزار به مطالعه و ارزیابی امنیت SDN و کنترلر پرداخته می شود.

کلمات کلیدی: SDN، امنیت، کنترلر، ترافیک شبکه.

فصل اول

مقدمه

سال ۲۰۰۵ آزمایشگاه‌های شبکه دو دانشگاه برکلی و استنفورد برعلیه وضع موجود قیام کردند و برآن شدند که شبکه‌ها را از وابستگی صرف به سخت افزار رها سازند. استادان این دانشگاه‌ها در پی افزودن قابلیت‌های نرم افزاری اختصاصی به شبکه بدون دخالت و وابستگی به سخت افزار بودند. تلاش‌هایی شد و استانداردهایی به مرحله پیش نویس درآمد و نظریه‌هایی رد و بدل گردید تا اینکه در سال ۲۰۰۸ یکنام برسرزبان‌ها افتاد Open Flow. پروتکلی آزمایشی برای ارتباط با سخت افزارهای مختلف بود. سازمان‌ها و شرکت‌هایی که دارای چندین سرور یا مرکز داده بودند می‌توانستند از طریق Open Flow با سخت افزار و بسترهای فیزیکی این سرورها ارتباط داشته باشند و کنترل و مدیریت حداقلی روی دیتای عبوری اعمال کنند. از سویی دیگر شرکت‌های ارائه دهنده سرویس‌های بیسیم و وایفای یک کنترلر مرکزی نرم افزاری برای ارتباط با ده‌ها و صدها اکسسپوینت در یک شبکه طراحی کردند و مورد استفاده قرار دادند. به علت ماهیت شبکه‌های بیسیم و نحوه عملکرد و مدیریت اکسسپوینت‌ها این تئوری شدنی بود که بتوان با یک کنترلر چندین شبکه و سخت افزار را پیکربندی کرد اما در شبکه‌های اترنت کابلی این امر ناممکن به نظر می‌رسید. سال‌های ۲۰۱۰ و ۲۰۱۱ دوران به سر آمدن صبر شرکت‌هایی مانند مایکروسافت، یاهو، فیسبوک، گوگل و وریزون بود. این شرکت‌ها با انبوهی از دیتا عبوری از سرورها و سخت افزار شبکه خود روبرو بودند اما توانایی اعمال هیچ گونه الگوریتم هوشمندی برای بهره برداری از این دیتاها را نداشتند؛ تمایل داشتند قابلیت‌های خاص خود را و ایده‌های خلق شده در آزمایشگاه‌هایشان را روی شبکه پیاده‌سازی کنند اما با سد بزرگی به نام سخت افزار و شرکت‌های توسعه دهنده سخت افزار مواجه می‌شدند. در سال ۲۰۱۱ این پنج شرکت در کنار شرکت ششمی به نام Deutsche Telekom بنیاد (Open Networking Foundation) را راه‌اندازی و وظیفه آن را استانداردسازی و انتشار پروتکل Open Flow به عنوان اصلی‌ترین جزء شبکه‌های نسل آینده موسوم به SDN سرآیند Software Defined Networking تعریف کردند. به فاصله یکسال نسخه‌های جدیدی از این پروتکل منتشر شد و بیش از ۸۰ شرکت بزرگ صنعت شبکه و مجازی سازی از جمله سیسکو، جونیپر، VMware، ایتتل، آیبی ام، اوراکل و غیره به عضویت ONF درآمدند و SDN را به پیشرانند و ده‌ها شرکت نوپای وارد این صنعت شدند. و اینگونه سروصدای SDN به هوا برخاست و بزرگترین تحول چند دهه اخیر شبکه‌ها رخ داد: شبکه‌های نرم افزارمحور.

اگر بخواهیم شبکه‌های نرم افزارمحور SDN (Software Defined Networking) را خیلی ساده تعریف کنیم باید بگوییم: نسل جدیدی از شبکه‌ها که با استفاده از لایه‌های مجازی، سویچ‌های مجازی، کنترلر مرکزی، استانداردهای ارتباطی و API های سطح بالا سعی می‌کنند برخی از کارهای کنترلی و مدیریتی سویچ‌ها و روترهای شبکه را در لایه‌های بالاتر به صورت نرم افزاری انجام دهند. به زبان دیگر SDN وابستگی به سخت افزار را کاهش داده و قابلیت های نرم افزاری و هوشمندی شبکه را افزایش می‌دهد. از این رهگذر سازمان ها و شرکت‌های گسترده می‌توانند خودشان اقدام به برنامه‌ریزی و برنامه نویسی برای شبکه خودشان کرده و قابلیت های سفارشی و اختصاصی را به وجود بیاورند که نتیجه آن سرویس‌های جدیدی برای مشتریان است. شکل زیر شمایی از SDN را نشان می‌دهد. لایه کنترل که می‌تواند یک سویچ مجازی یا یک محصول کنترلر مرکزی باشد دستورات لایه برنامه‌های کاربردی را با زبان Open Flow به سخت افزار منتقل و سخت افزار داده‌ها را براساس نیازها و سیاست های اعمال شده جابه جا و هدایت می‌کند. شبکه‌های نرم افزار محور یک تکنیک سازماندهی شبکه است که اخیراً بسیار مهم و برجسته شده است. در اساس SDN ، داده‌ها و اطلاعات کنترلی تجهیزات شبکه مانند سویچ‌ها و روترها، switch packet ها Switch LAN ها توسط یک Application Programming Interface (API) یا رابط برنامه نویسی کاربردی، جدا می‌شود. در ساختارهای فعلی، در شبکه های بزرگ روترها و سایر تجهیزات شبکه، هم داده و هم اطلاعات کنترلی را در بر دارند که کار بهینه‌سازی ساختار شبکه را بسیار مشکل می‌سازد. افزایش چشمگیری که این گونه شبکه‌ها در سطح جوامع دیده می‌شود ؛ از جمله چالش‌هایی که با آن روبرو هستند امنیت می‌باشد، با راه کارهای ارائه شده در سطح مختلف این گونه از شبکه‌ها از جمله بخش امنیت کنترلرها می‌توان از دستیابی به اطلاعات شبکه جلوگیری کرد. در این سمینار به صورت جامع به بررسی و مطالعه امنیت SDN و کنترلرها پرداخته می‌شود.