
بسم الله الرحمن الرحيم

سمینار

عنوان
امنیت کنترلر در شبکه‌های نرم افزار محور

نگارنده:

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

فهرست جداول

چکیده:

شبکه نرم افزار محور (SDN) یک تکنولوژی جدید است که می‌تواند در طراحی و مدیریت ما بر شبکه، نوآوری داشته باشد. اگرچه به نظر می‌آید که این تکنولوژی سریعاً نمایان شده اما، SDN بخشی از تاریخچه طولانی مدت زحمت‌ها برای ایجاد شبکه‌های کامپیوتری با قابلیت برنامه ریزی بیشتر می‌باشد. بزرگ‌ترین چالش امنیت SDN، این واقعیت است که SDN از کنترل متمرکز استفاده می‌کند. اگر سرور SDN مورد حمله قرار بگیرد یا دسترسی دستاوردهای یک هکر به کنترلر SDN ترافیک شبکه، می‌تواند در اطراف فایروال نرم افزارهای مخرب قرار داده و می‌تواند گره‌های شبکه را الوده سازد. در این سمینار علاوه بر بررسی شبکه های تعریف شده‌ی نرم افزار به مطالعه و ارزیابی امنیت SDN و کنترلر پرداخته می‌شود.

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

فصل اول

مقدمه

۱-۱- مقدمه

سال ۲۰۰۵ آزمایشگاه‌های شبکه دو دانشگاه برکلی و استندفورد 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 برسرزبان ها افتاد Open Flow. پروتکلی آزمایشی برای ارتباط با سخت افزارهای مختلف بود. سازمان‌ها و شرکت‌هایی که دارای چندین سرور یا مرکزداده 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 شبکه های اترنت کابلی این امر ناممکن به نظر می‌رسید. سال های ۲۰۱۰ و ۲۰۱۱ دوران به سر آمدن صبر شرکت‌هایی مانند مایکروسافت، یاهو، فیسبوک، گوگل و ورایزون 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 اصلی ترین جزء شبکه های نسل آینده موسوم به SDN سرآیند Software Defined Networking تعریف کردند. به فاصله یکسال نسخه‌های جدیدی از این پروتکل منتشر شد و بیشاز ۸۰ شرکت بزرگ صنعت شبکه و مجازی سازی از جمله سیسکو، ، جونیپر، ،VMware اینتل، آیبی ام، اوراکل و غیره به عضویت ONF درآمدند و SDN را به پیشراندند و ده ها شرکت نوپای وارد این صنعت شدند. و اینگونه سروصدای SDN به هوا برخاست و بزرگترین تحول چند دهه اخیر شبکه ها رخ داد: شبکه های 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، سوییچ‌های مجازی، کنترلر مرکزی، استانداردهای ارتباطی و API های سطح بالا سعی می‌کنند برخی از کارهای کنترلی و مدیریتی سوییچ‌ها 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 سوییچ 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 اخیرا بًسیار مهم و برجسته شده است. در اساس SDN ، داده‌ها و اطلاعات کنترلی تجهیزات شبکه مانند سوئیچ‌ها و روترها، switch packetها Switch LANها توسط یک Application Programming Interface (API) یا رابط برنامه نویسی کاربردی، جدا می شود. 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.