بسمه تعالی

IPV6 و چالشهای روبرو

همانطوریکه می دانیم در IPV4 فضای پیش بینی شده برای اختصاص یک آدرس منحصر به فرد برای هر رایانه در شبکه و اینترنت ۳۲ بیت بود که در سال ۱۹۹۵، حدود ۱/۳ آن اشغال شد و به سیستمهای رایانه ای تخصیص یافت . با توجه به محدودیت ظرفیت آدرس دهی آن ، این فضا دارد به انتها می رسد. لذا روالهای NAT بکار گرفته شد تا بر این اشکال فائق آیند.

به هر حال ۲ بتوان ۳۲ برای کلیه سیستمهای آدرس پذیر کم بود . جمعیت دنیا ۶ تا ۷ میلیارد است و بنا به گفته شرکت مایکروسافت به تعداد میز کار باید PC وجود داشته باشد که این تعداد رایانه برای IPv4 کفایت می کند ولی فقط رایانه که نیست که IP می خواهد بلکه بسیاری از دستگاهها نیز دیگر IP خور شده اند و این موضوع حرکت به سمت IPV6 را سرعت داده است.

ابتدا در سال ۱۹۹۴، IPV6 را تعریف کردند و از دسامبر ۱۹۹۵ تدوین شده ودر سال ۱۹۹۸ با استاندارد RFC2480 معرفی گردید. طبق پیش بینی های انجام شده قرار بود در سال ۲۰۰۸، سیستم آدرس دهی IPV4 به IPV6 تبدیل شود که به لحاظ عدم پشتیبانی کامل همه سخت افزارهای ارتباطی شبکه، میسر نشد. اکنون برای سال ۲۰۱۲ برنامه ریزی شده است و در صورتی که OS های ویندوز و سخت افزارهای مسیر یاب IPV6 را پشتیبانی کنند، این موضوع تحقق می یابد. هم اکنون بسیاری از کمپانی های تولید تجهیزات شبکه، پشتیبانی از IPV6 را انجام می دهند و OS های ویندوز , Linux و Mac osx هم پشتیبانی از IPV6 را در دستور کار خود قرار داده اند.

اکنون ما جزایر IPV6 را در دریای IPV4 داریم ولی بعدها معکوس می شود و این موضوع مترجم های این دو پروتکل را نیز در بر می گیرد. به هر حال با تبدیل IPV4 32 bit به IPV6 128 bit حالا حالاها مشکل آدرس دهی در اینترنت و شبکه را نخواهیم داشت. ولی مثل هر پروژه ای باید برای مدتی IPV6 , IPV4 با هم و همزمان استفاده شود، یعنی مدتی به

طور موازی کار شود تا اینکه پس از یک دوره زمانی یکی جایگزین دیگری شود. الان از Dual Stack استفاده می شود و یا Tunneling از IPV6 به ۴ IPv داریم.

ولی داستان تبدیل سیستم آدرس دهی به همین خوبی و خوشی هم تمام نمی شود چون شروع بکارگیری IPV6 هم با چالشهایی همراه است . مثلا اینکه موبایل بودن IPV6 امکان برخی حملات را بیشتر می کند و یا اینکه در IPV6 روشهای پویش تغییر می کند. علاوه بر اینها در ابتدای راه اندازی IPV6 چون اطلاعات و دانش آن بین متخصصین شبکه کم است ، تهدید ها نیز بیشتر است.

آنچه مهم است این است که در IPV6 نسبت به IPV4 به امنیت شبکه توجه بیشتری شده است به طوریکه باید گفت طراحی IPV4 بر اساس عدم وجود مهاجم در شبکه شکل گرفت و صرفا با هدف رسیدن بسته ها در کمترین زمان به مقصد انجام شده بود. یعنی در زمان طراحی IPV4 به لحاظ رشد کمتر تکنولوزی ICT، هنوز هکرها و نفوذ کنندگان مثل امروز فعال وپرکار نبودند و لذا موضوع C-I-A در نظر گرفته نشد.

سیستم آدرس دهی IPV4 با این فرض تهیه شد که در شبکه تهاجم وجود ندارد.(عملا مشکل امنیتی هم نداشتیم) ولی به تدریج این مشکل بوجود آمد و چون منافع مادی وجود داشت، انگیزه هم وجود داشت که هکر به طور عمدی وقت و انرژی بگذارد و به شبکه ها نفوذ کند. لذا با توجه به تهدید های رو به رشد، امروزه دیگر C-I-A + هم مطرح شده است .

در ابتدا امنیت را در بالاترین لایه دیدند یعنی هر کسی برای خودش در برنامه کاربردی Application Layer امنیت بگذارد و مسئول آن نیز خود فرد بود. این یعنی بوجود آمدن ایمنی توسط خود شخص. ولی اگر بخواهیم شبکه ایمن داشته باشیم باید این ایمنی از دید کاربر مخفی باشد یعنی امنیت را درلایه های پایین تر بوجود آوریم ، حتی در لایه فیزیکی که دیگر معلوم نیست این اطلاعات مال کی است. هر چه به لایه پایین تر برویم اینکه تشخیص دهیم این اطلاعات مال چه کسی است ، معلوم نیست. یعنی ما ایمنی اعمال می کنیم ولی برنامه های کاربر تغییر نمی کند.

در IPV4 امنیت و C-I-A دیده نشده است ولی در IPsec از طریق AH , ESP امکان C-I-A فراهم شده است که در IPsec این جزئی از پروتکل است . یعنی می توان فهمید که بسته IP از کجا می آید.

یکی از تفاوتهای عمده در IPv6، تاثیر اندازه شبکه است، یعنی وقتی شبکه بزرگ شود زمان مهاجم نیز برای نفوذ کردن زیادتر می شود. پس اگر در IPV4 Port Scanning در ۱۰ ساعت کل شبکه را می توانست اسکن کند در IPV6 این زمان بزرگتر می شود و حوصله هکر سر رفته و احتمال نفوذ هم کاهش می یابد.

متاسفانه در لایه IP در IPV4 Authentication رعایت نشده بود. مثلا این پاکت مال کی است و از کجا می آید و هر کسی می توانست ادعا کند که این بسته مال او است یعنی شما می توانستید ادرس IP را تغییر دهید چرا که هدف و طراحی IP عموما بر این بود این بسته کجا می خواهد برود نه اینکه از کجا می آید یعنی به Source Address کاری نداشت. ولی در IPV6 به آدرس مبدا IP هم کار دارد.

در IPv6 حملات نظیر Smurfing محقق نمی شود. یعنی نمی توان ماشین قربانی را دچار حمله DOS کرد. در روش DOS هکر از یک IP مشخص(رایانه آسیب پذیر قربانی) Broadcast می کند. یعنی آدرس قربانی را بجای خودش می گذارد و همه کاسه و کوزه ها سر رایانه قربانی خراب شده و خود هکر مصون می ماند. ولی در IPV6 ، Broadcasting وجود ندارد. حملاتی نظیر Treadrop , Joltz هم محقق نمی شود. پروتکل ICMP برای broadcasting یک پروتکل گزارش خطا است لذا نظارت امنیتی روی آن نمی شود و این یعنی مشکل و هکرها می توانند روی آن حملات را طراحی کنند.

در IPV4 ، Fragmentation انجام می شود یعنی بسته های تکه تکه شده را می فرستادیم و این باعث می شود که قربانی منتظر می ماند تا این بسته ها بیاید و اگر تکه ای به عمد نیامد، این انتظار طولانی است. در حالیکه IPV6 ، Fragmentation به این شکل را کنسل می کند.

علی ثاقب موفق
فوق لیسانس مهندسی فناوری اطلاعات