بسم الله الرحمن الرحيم

سوال:من شنيده ام كه SSL بين Application Layer و Network Layer "مي نشيند".اين به چه معنا است؟

سوال بسيار خوبي است.براي پاسخ به اين سوال ابتدا بايد هدف يک پروتکل را مشخص کنيم.وظيفه و هدف اصلي يک پروتکل اجراي قواعد چگونگي تبادل اطلاعات بين دو نقطه است.اين قواعد Syntax ، semantics و synchronization مروبوط به ارتباط ، تبادل ها و انتقالات را در برمي گيرند.بيشتر ارتباطات شبکه به صورت isolation کار نمي کنند.به همين خاطر ، به صورت لايه اي با هم کار مي کنند که به اين روش protocol stack گويند. در اين روش ، ترکيبي از پروتکل هاي مشخص با هم کار مي کنند ، و هر پروتکل در Stack وظايف ويژه اي را انجام مي دهند.

پروتکل Secure Sockets Layer يا SSL پروتکل استانداردي است که کار رمزنگاري و تصديق هويت را انجام مي دهد و به عنوان مرسوم ترين پروتکل براي امن کردن ارتباطات اينترنتي استفاده مي شود.قبلا از SSL بيشتر در مرورگرهاي اينترنت به صورت دوگانه Application-Protocol استفاده مي شد که به عنوان HTTPS نيز شناخته مي شود.به هر حال اين پروتکل به صورت نامريي است و براي کاربر قابل مشاهده نيست ، و در تمام برنامه هايي که از TCP/IP استفاده کنند در درسترس خواهد بود.

همانگونه که تصورمي کنيد ، براي مطمئن شدن از اين که يک پروتکل وظايفش را خود و يا با پروتکل هاي ديگر که با يکديگر کار مي کنند ، درست انجام مي دهد ، کار بسيار پيچيده اى است.به هيمن دليل مدل هاي زيادي براي کمک مهندسين که بتوانند protocol stack را تصور کنند ، توسعه داده شده اند. هر مدل توضيح خلاصه اي از نحوه کار پروتکل ها به آن شکلي که بايد کار کنند ، را ارايه داده است.بهترين مدل OSI (Open System Interconnection) که از هفت لايه براي گروه بندي سرويس هايي که بايد پروتکل ها آن ها را انجام دهند استفاده مي کند.پروتکل مشابه TCP/IP نيز از چهار يا پنج لايه استفاده مي کند.دو لايه اول هر مدل به صورت منطقي به کاربر نزديکتر مي باشند.لايه هايي که پايين تر هستند ، به صورت فيزيکي به تبادل داده می پردازند.

در مدل OSI در لايه هفتم ، سرويس هاي مخصوص Process ها اجرا مي شوند.لايه سوم يعني لايه شبکه ، مشکلات ناشي از دريافت پاکت ها در شبکه را حل مي کند.پروتکل SSL در نه واقع جزو پروتکل هاي لايه شبکه است و نه لايه برنامه.به همين دليل مي گويند که SSL بين لايه شبکه و لايه برنامه مي نشيند.

به دليل موقعيت SSL ، اين امكان به Client داده مي شود كه حفاظت امنيتي انتخاب شده را براي برنامه هاي منحصر به فرد اجرا كند.به همين دليل امنيت بيشتري را نسبت به دسته اي از روش هاي رمزنگاري كه در برنامه ها وجود دارد ، فراهم مي آورد.رمزنگاري داده ها گاهي ممكن است بدون استفاده از لايه شبكه هم انجام شود.بنابراين ، هنگامي كه از SSL براي رمزنگاري ترافيک شبكه استفاده مي شود ، فقط داده هاي لايه شبكه رمزنگاري مي شوند.

Copyright© by Siahacker
2007 All Rights Reserved