

سید نامی مدرسی

۹۷۳۳۰۶۹

بهار ۱۴۰۱

تمرین عملی HTTP

مهندسی اینترنت

سوال ۱)

ما می توانیم روی اینترفیس های مختلف دستگاه پورت هایی را باز کنیم. حال فرض کنید مثلاً برای wifi ما یک پورت را باز کنیم به این معنی می شود که برای همه باز است اما اگر صرفاً برای اینترفیسی که قرار است با سرور داخلی کار کنیم باشد صرفاً برای شبکه داخلی می شود برای همین ما می توانیم روی اینترفیس مناسب پورتی را باز کنیم تا رد و بدل پیام به سرور داخلی انجام بشود.

راه دیگر هم این است که این سرویس روی اینترنت باشد اما فقط کلاینت های خاص امکان استفاده از آن را داشته باشند که برای این کار باید یک پراکسی سرور داشته باشیم که درخواست ها را دریافت کند و اگر معتبر بود یعنی از کاربران سرویس بود درخواست را به سرور مورد نظر ارسال کند و پاسخ به برگرداند اما اگر کلاینت مورد نظر نبود درخواست به سرور داده نمی شود.

سوال ۲)

در پروتکل TLS دو کلید عمومی و خصوصی داریم. کلاینت به کمک کلید عمومی و سرور به کمک کلید خصوصی و عملیات رمزکردن می توانند کلید سشن را تولید و بازیابی کنند. به کمک این کلید می توان ارتباط بین کلاینت و سرور را داشت. اگر کلاینتی بدون این کلید ها درخواستی ارسال کند به این معنا است که این کلاینت در بین کلاینت های سرویس ما نیست پس نباید به سروی دسترسی داشته باشد.

فلسفه پشت این روش به این شکل است که فقط کلاینت هایی که مورد تایید باشند یعنی همان کلاینت های مجاز کلیدی دارند و به کمک این کلید می توانند ارتباط برقرار کنند و مابقی کلاینت ها امکان این کار را ندارند انگار که هر کلاینت یک کلید دارد و برای استفاده از سرویس باید این کلید را وارد کند. پس به کمک این روش می توانیم همانند jwt authentication، به کلاینت هایی پاسخ بدهیم و به بقیه که معتبر نیستند پاسخی ندهیم.