چرا Sequence Number آغازین در پروتکل TCP از عدد 0 یا 1 تنظیم نمی‌شود، بلکه شروع از یک عدد تصادفی می‌باشد؟ جهت توضیح بهتر، ترجیحا از یک مثال استفاده کنید.

دلیل اول و مهم تر امنیت است. در صورتی که سرور sequence number را از یک عدد رندوم شروع کند میتواند از بسیاری از حملات spoofing جلوگیری کند. این حملات به این صورت انجام میشوند که هکر با ارسال تعداد زیادی پکت syn سعی میکند که کانکشن های زیادی با سرور برقرار کند.

نوع دیگر حمله session hijacking است که در آن، هکر سعی میکند که به کمک پیشبینی sequence number، کنترل session بین دو هاست دیگر را در اختیار بگیرده و داده های خود را در بین پیام های این دو وارد کند.

مثلا هکر تعداد زیادی پکت SYN تولید میکند، و با سورس آیپی های مختلف این بسته های را به سمت سرور ارسال میکند.

سرور این بسته ها را دریافت کرده و پکت SYN/ACK را در پاسخ ارسال میکند. در این قسمت مهم، در صورتی که sequence number ها برای هکر قابل پیشبینی باشد، میتواند به سرور پکت ACK را در پاسخ ارسال کند و کانکشن را برقرار کند.

اگر سرور sequence number ها را به صورت رندوم انتخاب کند هکر نمیتواند پکت ACK را برای سرور ارسال کند و کانکشن برقرار نمیشود.

یا مثلا فرض کنیم که یک یوزر میخواهد به حساب کاربری خود در بانک متصل شود و برای این کار یک session تشکیل میشود. در صورتی که sequence number این session قابل پیشبینی باشد، هکر میتواند حمله session hijacking را انجام دهد و با در اختیار گرفتن session، تمام اطلاعات حساس این کاربر را بدزدد. اگر عدد به صورت رندوم باشد، این کار برای هکر بسیار سخت تر میشود.

دلیل دیگر این امر برای جلوگیری از تداخل multi session بین دو هاست است. اگر sequence number ها از یک عدد یکسان شروع شوند امکان تداخل دو session بیشتر میشود. البته روش های دیگری هم برای جلوگیری از تداخل دو session درادامه وجود دارند اما رندوم بودن sequence number اول میتواند احتمال تداخل را بسیار کم تر کند.