به نام خدا

سه سوال اول از سوالات میان ترم می آید

تمامی جواب های فوق از جزوه برادر عالی زاده می باشد

۴–احراز هویت کربروس را توضیح دهید؟از صفحه ۳۰ تا ۴۱ می باشد

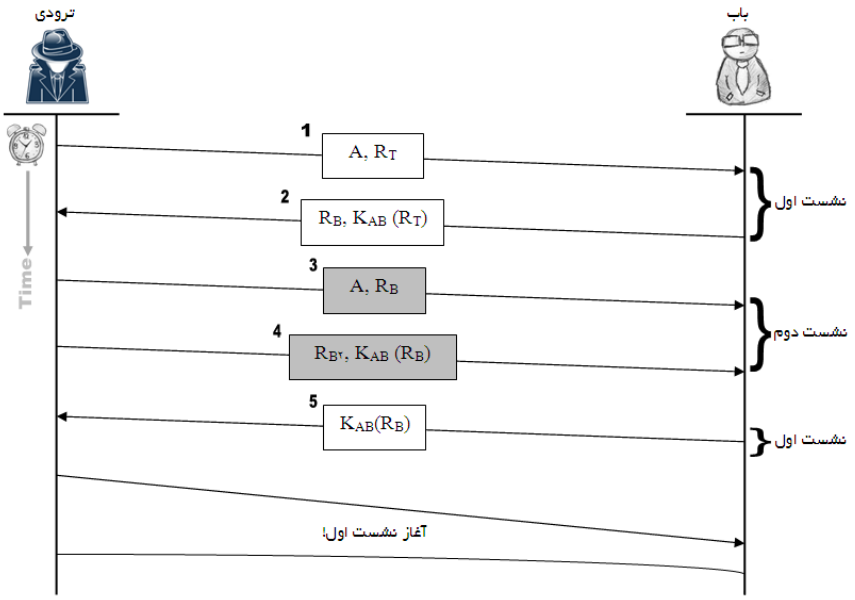
۵–در مورد IP Sec **توضیحات کامل بدهید ؟ از صفحه ۴۸ تا صفحه ۵۸می باشد**

۶–معماری امنیت در مدل چند لایه شبکه را توضیح دهید؟از صفحه ۴۲ تا صفحه ۴۸

۷–حمله بازتاب را به صورت کامل شرح دهید؟

الف) ترودی با ارسال شناسه کاربری آلیس و رشته چالش خود، نشستی را با باب آغاز می کند و باب نیز بلافاصله با رمز کردن رشته چالش ترودی ، رشته چالش خودش یعنی RB را برای ترودی می فرستد.

ب) ترودی در این لحظه باید رشته چالش باب را رمزنگاری کرده و پس بفرستد ولی از آنجا که کلید KAB را دز اختیار ندارد لذا نشست اول را نیمه تمام نگه داشته و بار دیگر تقاضای ایجاد یک نشست دوم با باب می کند ولی این بار رشته چالش باب یعنی RB را به عنوان رشته چالش خودش به باب تحویل می دهد . حال طبق روال معمول ، باب باید با رمزنگاری RB و ارسال نتیجه (به همراه رشته چالش جدید) نشست دوم را پیش ببرد.



شکل (۳) حمله بازتاب (Reflection Attack)

ج) با دریافت KAB(RB) از نشست دوم، ترودی بلافاصله به سراغ نشست ناتمام اول رفته و نتیجه KAB(RB) را به باب تحویل می دهد تا نشست اول تکمیل شود. بدین ترتیب ترودی فریب کار یک نشست کامل با باب ایجاد کرده است.

در شکل (۴) پیام های نشست دوم برای تمایز از نشست اول به رنگ تیره نشان داده شده اند. به نحوی که مشاهده می کنید در «حمله بازتاب» ترودی هر آنچه را که باب در نشست اول سوال می کند، در نشست دوم از خود باب می پرسد و جواب خودش را به خودش تحویل می دهد!

اشکالاتی که در این پروتکل وجود دارد عبارتند از:

+ مشتری توانسته سرویس دهنده را واردار کند قبل از خودش هویت خود را اثبات کند . بدین ترتیب یک فریبکار قادر خواهد بود قبل از آنکه مدرکی در خصوص هویت خود ارائه بدهد اطلاعات با ارزشی از طرف مقابل کسب کند

+ گاهی سرویس دهنده ها قادر خواهند مجبورند از نشستهای موازی و همزمان پشتیبانی کنند لذا باید مکان یزم احراز هویت به گونه ای طراحی شده باشد که نتوان اطلاعات بدست آمده از یک نشست را در نشست موازی دیگر به کار گرفت.

+ ترجیحاً باید طرفین ، رشته های چالش خود را از مجموعه های متفاوتی انتخاب کنند. به عنوان مثال اگر در مکانیزم قبل ، شروع کننده مجبور به استفاده از اعداد زوج و پاسخ دهنده مجبور به استفاده از اعداد فرد برای رشته چالش خود بود، این مشکل پدید نمی آمد.

به هرحال در هر مکانیزم احراز هویت باید اشکالات بالا مورد مطالعه قرار بگیرد و استحکام آن در مواجهه با حمله بازتاب اثبات شود.

قبل از آنکه روش جدیدی را معرفی کنیم اجازه بدهید استحکام مکانیزم شکل (۱) را بررسی کنیم.

فرض کنید باب و آلیس هر دو بتوانند آغازگر یک نشست باشند . در چنین وضعیتی ترودی خواهد توانست علیه آلیس، «حمله بازتاب» ترتیب بدهد. (اگرچه در بسیاری از سرویس دهنده ها فقط مشتری شروع کننده یک نشست است و سرویس دهنده هیچگاه آغازگر نشست نخواهد بود ولی در برخی از سرویس دهنده های یک نشست است و سرویس دهنده هیچگاه آغازگر نشست نخواهد بود ولی در برخی از سرویس دهنده های توزیع شده بانک اطلاعاتی هر دو ماشین در شبکه می توانند آغازگر نشست باشند.) به شکل (۴) دقت کنید؛ روال حمله بازتاب به شرح زیر است:

۱. در اولین مرحله آلیس شناسه کاربری خود را برای ایجاد نشست با باب بر روی شبکه ارسال می کند غافل از آنکه ترودی در میانه راه این پیام را دریافت کرده و مانع از رسیدن آن به باب می شود.

۲. در دومین مرحله، ترودی پاسخ آلیس را ناتمام گذاشته و خودش نشست دومی را با آلیس آغاز می کند . یعنی با ارسال شناسه باب خودش را به دروغ باب معرفی می کند.

۳. طبق مکانیزم شکل (۱) ، آلیس باید پاسخ آغازگر نشست را با تولید یک رشته چالش و ارسال آن بدهد. این رشته چالش را RA بنماید.

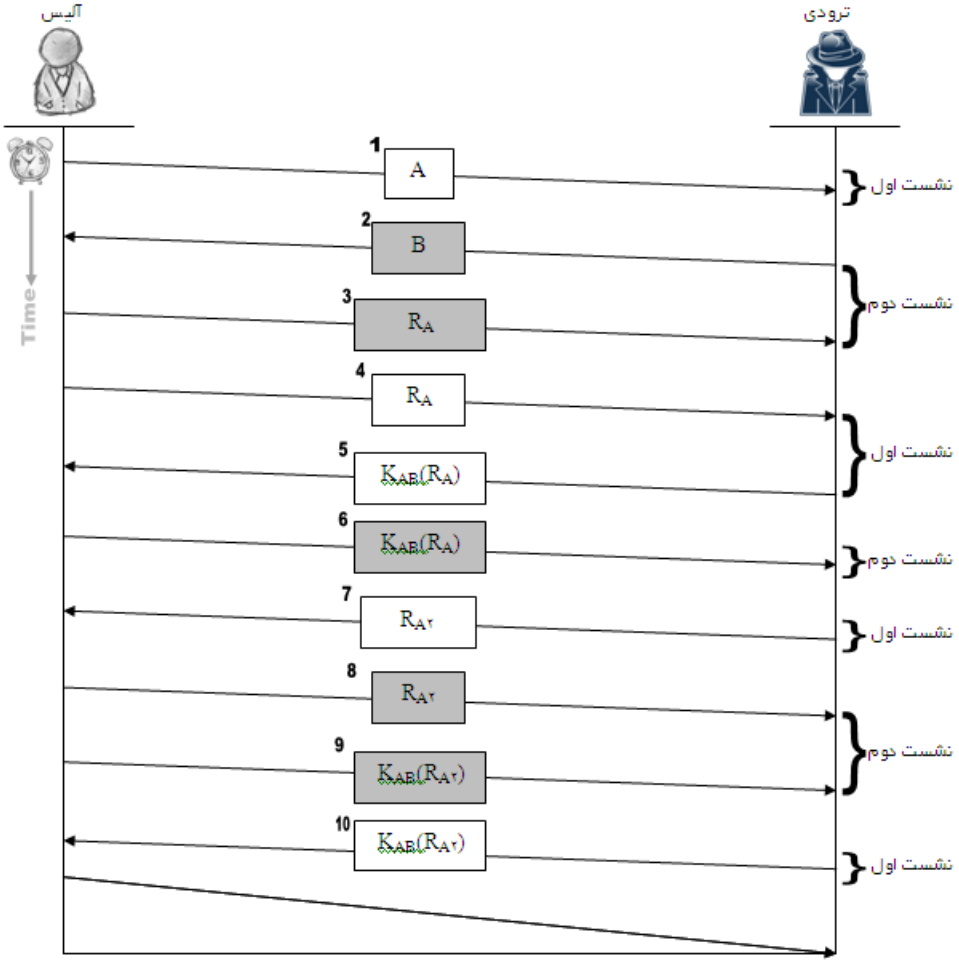
۴. در اینجا ترودی RA دریافتی از نشست دوم را در قالب رشته چالش نشست اول به خود آلیس بر میگرداند.

۵. آلیس به عنوان آغازگر نشست اول موظف بوده RA را با کلید مشترکان رمز کرده و نتیجه KAB(RA) را برگرداند و بدیهی است که این کار را انجام می دهد.

۶. ترودی با دریافت KAB(RA) از نشست اول همان را به عنوان پاسخ نشست دوم به آلیس برمیگرداند.

۷. حال آلیس در ادامه نشست اول رشته چالش دیگری (مثلاً RA2) را برای باب دروغین می فرستد.

۸. بار دیگر ترودی با دریافت RA2 آن را به عنوان رشته چالش خودش در ادامه نشست دوم به آلیس برمیگرداند.



شکل(۴) حمله بازتاب علیه مکانیزم «چالش و پاسخ»

۹. آلیس به تبعیت از مکانیزم RA2 را رمزنگاری کرده و نتیجه KAB(RA2) را برای ترودی برمیگرداند.

۱۰. ترودی با دریافت KAB(RA2) آن را برای تکمیل نشست اول به سوی خود آلیس برمیگرداند . بدین ترتیب هردو نشست تکمیل می شود.

کوتاه سخن آنکه ترودی ضمن فریب آلیس توانسته دونشست کامل را با او برقرار کند و آلیس هم متوجه چنین موضوعی نیست.

آنچه که مسلم است پیاده سازی یک روش احراز هویت که در مقابل چنین حملاتی مقاوم باشد به ظرافتهای خاص و

مطالعات دقیق نیاز دارد.

۸–اصول شش گانه کرکهف را را نام ببرید؟

اصول شش گانه کرکهف

۱) سیستم رمزنگاری اگر نه به لحاظ تئوری که در عمل غیرقابل شکست می باشد.

(2سیستم رمزنگار نباید هیچ نکته پنهان و محرمانه ای داشته باشد بلکه تنها چیزی که باید سری نگاه داشته شود کلید رمز است. طراح سیستم رمزنگار نباید جزئیات سیستم خود را حتی از دشمنان مخفی نگه دارد.

(3کلید رمز باید بگونه ای قابل انتخاب باشد که اولا بتوان براحتی آن را عوض کرد و ثانیا بتوان آن را بخاطر سپرد. و نیازی به یادداشت کردن کلید رمز نباشد.

(4متون رمزنگاری شده باید از طریق خطوط تلگراف قابل مخابره باشند.

(5دستگاه رمزنگاری یا اسناد رمز شده باید توسط یک نفر قابل حمل ونقل باشد.

(6سیستم رمزنگاری باید به سهولت قابل راه اندازی و کاربری باشد. چنین سیستمی نباید به آموزشهای مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل ها نیاز داشته باشد.

۹–جملات زیر را تعریف کنید

دیواره آتش:ص ۵۸و ص۵۹

VPN:ص ۵۶ و ص۵۷

:IPs

۹–جمع بندی کلی نسبت درمورد درس امنیت شبکه از دیدگاه خود به صورت کامل بیان کنید؟