مبانی رایانش امن

تمرین سوم

فایل‌های پاسخ خود را با الگوی HW3-۹۴۳۱XXX-StudentName.pdf نامگذاری نمایید.
در صورت مشاهده تقلب برای طرفین نمره صفر درنظر گرفته خواهد شد.
در صورت وجود هرگونه اشکال یا سوالی از طریق ایمیل alireza97hi@gmail.com موارد را بیان کنید.

تمرینات فصل چهارم

۱.نحوه استفاده مجدد از ticket توسط یک فرد غیرمجاز در Kerberos را توضیح دهید.

۲.هدف استفاده از session key در Kerberos چیست؟ نحوه توزیع آن توسط AS چگونه است؟

۳.در هر یک از موارد زیر یک پروتکل احراز هویت یک طرفه بیان شده است. در هر مورد روش کار پروتکل را توضیح دهید و حمله‌ای که نسبت به آن آسیب‌پذیر است مثال بزنید.(U و O دو کاربر متفاوت هستند و منظور از تابع E رمزکردن تحت کلیدی که همان متغیر اول است می‌باشد)

الف)

$O \rightarrow U : ID_O$
$U \rightarrow O : E(PR_O, R_۲)$
$O \rightarrow U : R_۲$

ب)

$O \rightarrow U : ID_O$
$U \rightarrow O : R_۱$
$O \rightarrow U : E(PR_O, R_۱)$

۴.یک کاربر نیاز به اتصال به یک سرور دارد و برای تبادل اطلاعات به صورت رمزنگاری متقارن نیز یک کلید امن بین کاربر و سرور نیاز است. یک راهکار امنیتی برای دریافت کلید امن بیان کنید و مشخص کنید که در این راهکار چگونه امکان حمله replay و سوء استفاده از ارسال مجدد پیام‌های کاربر به سرور جلوگیری شده است.

۵.پروتکل زیر جهت به اشتراک‌گذاری یک session key بین دو کاربر A و B است(منظور از N_A نانس که یک عدد تصادفی است می‌باشد و همچنین کلید K_{AB} بین دوکاربر از قبل به اشتراک گذاشته شده است):

$A \rightarrow B : A, N_A$
$B \rightarrow A : E(K_{AB}, [N_A, K'_{AB}])$
$A \rightarrow B : E(K'_{AB}, N_A)$

الف) بیان کنید که هر دو کاربر چگونه به صحت ارسال این کلید که از فرد قابل اعتمادی آمده، اطمینان دارند؟
ب) چگونه میتوانند به این اعتماد برسند که این session key یک کلید fresh و جدید است؟