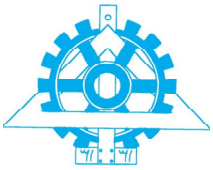


به نام خدا

امنیت شبکه- پاییز ۹۵

تمرین کامپیوتری اول

در پوشه پروژه کدهای سه سرور و یک کلاینت به زبان C و MATLAB پیاده‌سازی شده‌اند. سرور با شناسه ۰ تاریخ و زمان فعلی را در اختیار کلاینت قرار می‌دهد. سرور با شناسه ۱ قیمت دلار و سرور با شناسه ۲ عدد پی را ارسال می‌کنند. در حال حاضر سرورها اصالت کاربران را احراز نمی‌کنند و کاربران نیز نمی‌توانند اصالت هویت سرورها را احراز کند. هدف از این پروژه ایجاد سامانه‌ای است که در آن اصالت کاربران و سرورها قابل احراز باشد. برای پیاده‌سازی سامانه می‌توانید از زبان سی در محیط Linux یا از MATLAB استفاده کنید. توجه نمایید دانشجویانی که به زبان MATLAB پیاده سازی انجام می دهند، حداکثر نصف نمره تمرین و دانشجویانی که به زبان C شبیه سازی می کنند حداکثر یک و نیم برابر نمره تمرین را خواهند گرفت.

به زبان c

در هریک از پوشه ها با وارد کردن دستور زیر کدها کامپایل و ساخته می‌شوند.

```
$make
```

برای پاک کردن فایل‌های کامپایل شده می‌توانید از دستور زیر استفاده کنید.

```
$make clean
```

برای بالا آوردن هرکدام از سرورها کافیست درگاهی که قرار است به آن گوش دهند را به عنوان ورودی وارد کنید.

بنابراین برای اجرای هر کدام از سرور ها باید دستور زیر را اجرا کنید :

$./Server_name portnum

برای اجرای برنامه کلاینت کافیست درگاه و آدرس سرور مورد نظر خود را وارد کنید.

$./Client address portnum

برای مثال اگر می‌خواهید سرور با شناسه شماره ۰ را بالا بیاورید می‌توانید پس از کامپایل کردن کد مربوط به سرور شماره ۰ ، دستور زیر را اجرا کنید تا سرور اجرا شده و بر روی درگاه ۸۰۰۰ به درخواست‌ها پاسخ دهد.

$./server0 8000

در ادامه می‌توانید برنامه کلاینت را با آدرس(IP) و درگاه مربوط به سرور شماره ۰ اجرا کنید. اگر سرور بر روی کامپیوتر کلاینت اجرا شده است باید از آدرس localhost (یا 127.0.0.1) استفاده کنید.

$./client localhost 8000

در این صورت خروجی برنامه به صورت زیر خواهد بود :

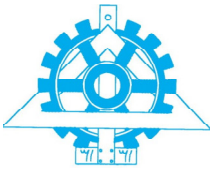
server reply: Current server time and date is Thu Oct 27 12:49:14 2016

برای یادگیری نحوه کار با کامپایلر gcc می‌توانید از آدرس اینترنتی زیر استفاده کنید:

https://www3.ntu.edu.sg/home/ehchua/programming/cpp/gcc_make.html

کدهای کلاینت و سرورها را مطالعه کنید و نحوه عملکرد آن‌ها را متوجه شوید. برای اطلاع بیشتر از socket programming می‌توانید از آدرس اینترنتی زیر استفاده کنید:

http://www.linuxhowtos.org/C_C++/socket.htm



اسکریپت MATLAB

ساختار پوشه‌ها مانند قسمت قبل است. برای اجرای هر کدام از سرورها کافیست تابع مربوط به آن سرور را با شماره درگاه مورد نظر به عنوان ورودی اجرا کنید. برای مثال برای اجرای سرور شماره ۰ می‌توانید تابع زیر را فراخوانی کنید تا سرور اجرا شده و بر روی درگاه ۴۰۱۳ منتظر بماند :

Server0(4013)

برای اجرای کلاینت باید یک برنامه جدید MATLAB باز کنید و در آن تابع client با آدرس و درگاه سرور مورد نظر خود به عنوان ورودی را اجرا کنید. اگر سرور نیز بر روی همین کامپیوتر اجرا شده‌است باید از آدرس 127.0.0.1 استفاده کنید. برای مثال برای ارتباط با سرور قسمت بالا باید تابع زیر را فراخوانی کنید:

client('127.0.0.1', 4013)

برای اجرای همزمان سرورها باید چند برنامه MATLAB را همزمان باز کنید.

بخش اول

برنامه‌ای بنویسید که امکان ذخیره نام کاربری و رمز عبور کاربران و کلید K_C مربوط به هر کاربر را داشته باشد. این برنامه باید اطلاعات را داخل یک ساختمان داده مناسب (یک فایل ساده نیز می‌تواند مورد استفاده قرار بگیرد) ذخیره کند. همچنین این برنامه باید امکان اضافه کردن کاربر جدید، پاک کردن کاربران پیشین یا تغییر رمز عبور را داشته باشد.

این برنامه باید به ازای هر کاربر جدید فایلی به نام آن کاربر در یک پوشه مشخص ایجاد کند و رمز عبور را در خط اول و کلید K_C مربوط به کاربر را در خط دوم آن ذخیره کند. کلید K_C از ۱۲۸ بیت اول چکیده (با الگوریتم SHA256) رمز عبور کاربر به‌دست می‌آید. نام کاربری و رمز عبور یک رشته (string) با بیشینه طول مشخص‌اند.

این فایل در ادامه برای احراز اصالت کابران مورد استفاده سرور KDC قرار می‌گیرد

بخش دوم

یک برنامه سرور جدید به نام KDC (key distribution center) بنویسید که وظایف سرورهای AS و TGS را در پروتکل شرح داده شده در ادامه را انجام دهد.

هنگام شروع به کار این سرور کاربر باید امکان تعیین مدت اعتبار بلیط‌های مخصوص سرور و TGS را داشته باشد. به عبارت دیگر این سرور به صورت زیر اجرا می‌شود.:

$./KDC port database_folder tgs_lifetime v_lifetime

ورودی اول شماره درگاهیست که سرور باید به آن گوش دهد، ورودی دوم آدرس پوشه فایل‌های مربوط به کاربران است که در بخش قبل ایجاد شده است. ورودی اول مدت زمان اعتبار بلیط‌های tgs به ثانیه و ورودی چهارم مدت زمان اعتبار بلیط‌های سرور به ثانیه است.

۱. C > KDC : $ID_C||ID_{server}$

کلاینت پس از اتصال به سرور KDC ، نام کاربری و شناسه سرور مورد نظر خود را ارسال می‌کند. شناسه‌های معتبر به شرح زیرند:

- شناسه ۰ : برای گرفتن بلیط برای ارتباط با سرور شماره ۰
- شناسه ۱ : برای گرفتن بلیط برای ارتباط با سرور شماره ۱

- شناسه ۲ : برای گرفتن بلیط برای ارتباط با سرور شماره ۲
- شناسه ۳ : برای گرفتن بلیط برای ارتباط با سرور TGS

۲. C > KDC : $ticket_{tgs}$ (if in previous step $ID_{server} == 0\ or\ 1\ or\ 2$)

اگر کلاینت قصد گرفتن بلیط ارتباط با سرورهای عادی را داشته باشد، در پیام بعدی بلیط tgs خود را نیز ارسال می‌کند. اگر مدت زمان اعتبار بلیط $ticket_{tgs}$ ای که کاربر ارائه می‌دهد، سرور باید با خطای مناسب به کلاینت گزارش دهد. همچنین سرور KDC باید فیلد TS (time stamp) داخل بلیط را چک کند تا از به روز بودن آن مطمئن شود.

۳. KDC > C: $E(K_C\ .\ ticket_{tgs})$ or $ticket_v$

اگر کلاینت قصد گرفتن بلیط tgs داشته باشد در مرحله بعد سرور KDC در پوشه فایل‌های کاربران جست‌وجو می‌کند تا فایل مربوط به نام کاربری ارسال شده را پیدا کند و سپس بلیط tgs را می‌سازد(K_{tgs} به صورت ثابت و از پیش تعیین شده‌است) و آن را با کلید K_C رمز می‌کند و برای کلاینت ارسال می‌کند.

اگر کلاینت قصد گرفتن بلیط $ticket_v$ سرور KDC تنها بلیط tgs ارسالی را با کلید K_{tgs} رمزگشایی می‌کند و بررسی می‌کند که مقادیر آن درست و منطبق با آدرس و نام کاربری ارائه شده باشند، سپس بلیط مورد نظر کلاینت را ارسال می‌کند.

$$Ticket_{tgs} = \mathrm{E}(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$$
$$Ticket_v = \mathrm{E}(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$$

برنامه کلاینت را به گونه‌ای تغییر دهید که پس از اجرا بررسی کند که آیا بلیط مربوط به سرور مورد نظر یا tgs را در اختیار دارد یا نه. اگر بلیط tgs را نداشت باید از کاربر رمز عبور و نام کابری را درخواست کند و به سرور KDC متصل شده و بلیط tgs را دریافت و آن را ذخیره کند(در یک فایل به فرمت دلخواه). در ادامه برنامه، کلاینت باید بدون درخواستی از کاربر به سرور KDC متصل شده و بلیط مربوط به سرور را دریافت کند و به سرور متصل شود.

اگر بلیط tgs پیش از این ذخیره شده باشد برنامه کلاینت باید بدون درخواستی از کاربر به KDC متصل شده و بلیط مربوط به سرور را درخواست کند. هرگاه مدت اعتبار هر یک از بلیط ها تمام شده باشد سرور(KDC یا سرورهای خدمات دهنده دیگر) باید به کلاینت اطلاع دهد تا مجدداً برای دریافت بلیط اقدام کند. در صورتی که مدت اعتبار بلیط tgs تمام شده باشد کلاینت باید از کاربر درخواست نام کاربری و رمز عبور بکند.

برنامه سرورها را به گونه‌ای تغییر دهید که تنها در صورت دریافت بلیط مناسب، خدمت خود را به کلاینت ارائه دهند. فرض شده است که یک کلید مشترک ثابت از پیش تعیین شده (داخل کد) در اختیار هر سرور عادی و سرور KDC وجود دارد.

نکات

- کدها باید به زبان C/C++ در محیط Linux یا MATLAB (در لینوکس یا ویندوز) نوشته شوند.
- برنامه های شما باید به خوبی نشان‌دهنده وقایع باشند. برای مثال اگر داده‌ای ارسال یا دریافت می‌شود باید نمایش داده می‌شود. اگر داده رمزشده است باید متن‌اصلی، متن رمز و کلید رمزنگاری نمایش داده شود. نحوه استفاده از سامانه نهایی و آرگومان‌های ورودی هر برنامه و کامنت‌های مناسب باید در کد نوشته شده باشد.
- برای انجام خدمات رمزنگاری در زبان C می‌توانید از کتابخانه gnu libssl-dev استفاده کنید. برای پیاده-سازی توابع رمزنگاری در زبان متلب می‌توانید از پیاده‌سازی‌های متن‌باز موجود در اینترنت استفاده کنید.
- کدهای فعلی برای ارتباط ساده کلاینت/سروری نوشته شده‌اند و تنها متغیر string ارسال و دریافت می‌شود. توجه شود که امکان ارسال و دریافت هر متغیری با هر ساختاری وجود دارد.