به نام خدا

شبکه های کامپیوتری – بهار ۹۴

تمرین کامپیوتری اول

تاریخ تحویل :سه شنبه ۱۲ / ۱۲ / ۹۳

هدف :

آشنایی با socket programming

دورنما :

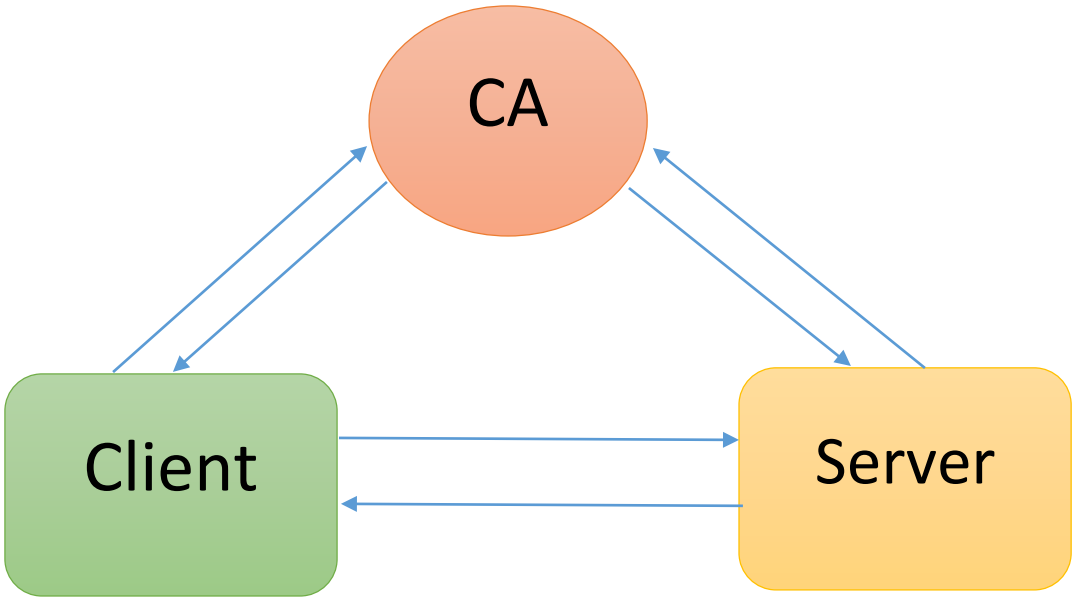
کانال شبکه یا سوکت شبکه، نقطه پایانی جریان ترافیک ارتباطات بین پردازشی در تمام طول یک شبکه رایانه‌ای است. امروزه، بیشترین ارتباطات بین رایانه‌ها بر پایه پروتکل اینترنت می‌باشند، بنابراین بیشترین سوکت‌های شبکه، سوکت‌های اینترنت هستند .کیستون نیز یک نوع خروجی برای اتصال رایانه با شبکه است.

یک سوکت رابط برنامه‌نویسی نرم‌افزار (Socket Application Programming interface یا Socket API)، که اجازه می‌دهد یک برنامه کاربردی سوکت‌های شبکه را استفاده و مدیریت نماید، معمولاً توسط سیستم عامل ارایه می‌گردد. سوکت‌های اینترنت رابط برنامه‌نویسی نرم‌افزار معمولاً براساس استاندارد سوکت برکلی هستند.

یک نشانی سوکت، ترکیبی از نشانی پروتکل اینترنت (IP) و شماره درگاه (Port Numebr) و بسیار شبیه به یک شماره تماس تلفنی است که ترکیبی از پیش شماره تماس و یک شماره داخلی که به پیش شماره افزوده گردیده است. بر پایه این نشانی، سوکت‌های اینترنت، بسته‌های اطلاعات دریافتی را به برنامه‌های کاربردی مرتبط و یا پردازش و ریسه مناسب تحویل می‌دهند.

مسأله :

در این تمرین شما باید یک سیستم رأی‌گیری الکترونیکی را پیاده سازی کنید. در این فاز شما کافی است به صورت ساده این سیستم متشکل از یک رأی‌دهنده و یک مرکز پرداز شی و یک مرکز احراز اصالت در نظر بگیرید. به طور خلاصه هر رأی دهنده ابتدا باید با مرکز احراز اصالت ارتباط برقرار کرده و با دادن مشخصات خود به او نام کاربری و رمز عبور و گواهی معتبر کسب کند. سپس به سرور اصلی وصل شده و با ارائه‌ی گواهی خود به او کاندیدای مورد نظر را انتخاب می کند. در طرف دیگر سرور با مرکز احراز اصالت ارتباط برقرار می‌کند و از او تأییدیه‌ی گواهی ارائه شده را درخواست می‌کند. در صورتی که گواهی از اعتبار لازم برخوردار بود رأی او ثبت می شود. بدیهی است که هرکس فقط یک بار مجاز به رأی دادن می‌باشد.



رأی دهنده:

برنامه رأی دهنده یک برنامه‌ی کارفرما (client) ساده است که می‌تواند به مرکز پردازش و شمارش آرا متصل شده و افراد مختلف با نام کاربری، رمز عبور و گواهی خود از طریق این سیستم رأی خود را اعلام

می‌کنند. همچنین این برنامه باید بتواند یک زوج کلید عمومی و خصوصی تولید کند و مشخصات خود را به صورت رمز شده برای مرکز تولید گواهی ارسال کند و گواهی دریافتی را که به صورت یک فایل خواهد بود را برای مرکز آرا ارسال نماید.

دستورات :

- Register E(PR_{hasan}, [#SSN, #Username, #Password, #re_Password]) : Register 123456789 Hasan ***** *****

کاربر مشخصات خود را برای مرکز تولید گواهی ارسال کرده و نام کاربری و رمز عبور او در سیستم ثبت می شود و گواهی او صادر می گردد. لازم به ذکر است با وارد شدن این دستور توسط کاربر شما باید ابتدا گواهی مورد نیاز برای او را از مرکز تولید گواهی دریافت کنید. در این دستور کاربر فقط مشخصات SSN,Username,Password را وارد می‌کند و شما باید این مشخصات را به صورت رمز شده در اختیار CA قراردهید. (PR_{hasan} کلید خصوصی کاربر است که در سمت کلاینت ساخته می‌شود)

- Connect Server [#Server Port Number, #Username, #Certificate] : Connect Server 2000 hassan

وصل شدن به پورت 2000 سرور توسط مدیر. (چگونگی تبادل گواهی به اختیار شماست می‌توانید آدرس آن را از کاربر بخواهید یا اینکه برای هر کاربر گواهی‌اش را با نام خودش ذخیره کرده و با اجرای این دستور توسط هر کاربر گواهی مربوط به وی را ارسال کنید)

- Show Candidates [] : Show Candidates

دریافت لیست نامزدها از سرور

- Vote [#Username, #Candidate Code] : Vote Hasan 15

کاربر Hasan به کاندید شماره ۱۵ رأی می دهد.

- Show Log[#Username, #Password] : Show Log Admin *****

این دستور توسط مدیر سیستم وارد می شود و می تواند لیست تمام رأی دهندگان از این سیستم را نشان دهد. (فقط نام کاربری آنها !)

- Disconnect [#Username, #Password] : Disconnect Admin *****

قطع ارتباط با مرکز از طرف مدیر سیستم

سرور :

در سرور قرار است لیستی از نامزدها وارد سیستم شود و این لیست در اختیار رأی دهندگان گذاشته می‌شود و سپس آرا آنان جمع آوری شده و بعد از هر تغیر بروزرسانی، در فایل ذخیره و نمایش داده می شود. هم چنین در این برنامه باید زمان آغاز و خاتمه ی رأی گیری به مراکز اعلام شود و این امکان نیز وجود داشته باشد که در صورت نیاز پیغامی به همه یا به یک مرکز خاص ارسال شود در این برنامه باید دستورات زیر پیاده سازی شود:

دستورات :

- Add Candidate [#Candidate Name, #Candidate Code] : Add Dr. Rahimi 12

افزودن کاندید جدید

- Show All Results [] : Show All Results

نشان دادن همه‌ی آرا همه ی صندوق ها

- Set Voting Time[#Start Time, #End Time]: Set Voting Time 8:00 20:00
  تعیین زمان مجاز برای رأی گیری
- Extend Voting Time[#New End Time]: Extend Voting Time 23:00
  تمدید بازه ی ثبت نام

مرکز تولید گواهی:

این مرکز به طور مستقیم دستوری را دریافت نمی کند و فقط به پیغام های رسیده از جانب کاربر یا مرکز پردازش پاسخ مناسب می‌دهد.

نکات تکمیلی:

- **ارتباط سرور و کلاینت با مرکز گواهی به اختیار شماست.**
- **چگونگی رمز کردن و رمزگشایی پیام ها نیز در اختیار شما ست اما در زمان تحویل باید به مکانیزم های آن مسلط باشید.**
- **برای تولید گواهی و چگونگی کار با آن می توانید از منابع اینترنتی کمک بگیرید**
- **برای درک بهتر مسئله و همچنین پیاده سازی مکانیزم های خواسته شده می توانید از لینک های زیر استفاده کنید :**
- http://www.codepool.biz/tech-frontier/how-to-use-openssl-generate-rsa-keys-cc.html
- https://www.safaribooksonline.com/library/view/secure-programming-cookbook/0596003943/ch07s06.html
- /https://pki-tutorial.readthedocs.org/en/latest
- http://en.wikipedia.org/wiki/X.509
-

بخش امتیازی:

برنامه را طوری تغییر دهید که امکان داشتن چندین مرکز تولید گواهی وجود داشته باشد.

نکات مهم :

- تمرین را در گروه‌های دو نفری انجام دهید
- زبان برنامه نویسی مجاز C و C++ است که تحت لینوکس تحویل گرفته می‌شود.
- نوشتن Makefile الزامی است.
- در برنامه‌ی خود باید Error Handling را رعایت کنید و در صورت بروز خطا پیغام منا سب را چاپ کنید.
- فایل‌های خود را به صورت CN-CA1-[SID1]-[SID2] ارسال کنید.

و به کوتاهی آن لحظه شادی که گذشت

غصه هم خواهد رفت

آنچنانی که فقط خاطره ای خواهد ماند

لحظه ها عریانند

به تن لحظه خود جامه اندوه میپوشان هرگز

در پناه حق سربلند و سلامت باشید