به نام خدا

مبانی رایانش امن

دکتر موزرانی

پروژه پایان ترم

مهلت تحویل: ۲۵ تیر ساعت ۲۳:۵۹

در این پروژه هدف طراحی و پیاده سازی یک سیستم بانکداری به صورت امن می باشد.

شما بایستی دو برنامه بنویسید یک برنامه به عنوان سرور که بر روی یک سیستم که قرار است سرور شما باشد قرار خواهد گرفت و یک برنامه کلاینت که هر شخصی که بخواهد از سیستم شما استفاده کند بایستی آن را در اختیار داشته باشد و ضمن اجرا دستورات را در آن وارد کرده تا بتواند با آن کار کند سپس با توجه به فرضیات مسئله بصورت خلاصه؛ فرآیند ثبت نام و ورود، کنترل دسترسی، رمزنگاری و تبادل کلید و نیز logging را طراحی کنید که در ادامه به تفصیل به آن ها پرداخته می شود.

نیازمندی های کارکردی و عملیاتی

زمانی که کاربری برنامه کلاینت را اجرا می کند چنانچه پیش تر ثبت نام نکرده باشد تنها مجوز ثبت نام دارد و در صورتی که قبلا ثبت نام کرده باشد اکنون مجوز ورود نیز دارد.

ثبت نام در سیستم

دستور ثبت نام بدین شکل می باشد:

Signup [username] [password]

[username] : نام کاربری

[password] : رمزعبور

در این دستور دو امر می بایست مورد توجه قرار گیرد:

- کاربر با نام کاربری تکراری نباید بتواند در سیستم ثبت نام کند.
- رمز عبور کاربر می بایست به میزان کافی امن باشد در غیر اینصورت نباید بتواند در سیستم ثبت نام کند. (از دانشی که در درس آموخته اید برای پیاده سازی مکانیزم تشخیص رمز عبور مناسب و نامناسب استفاده کنید.)

چنانچه کاربر با موفقیت ثبت نام شود و یا عمل ثبت نام موفقت آمیز نباشد (خطا یا عدم امکان)، در هرمورد پیام مناسب را برای وی ارسال نمایید.

ورود به سیستم

دستور ورود بدین شکل می باشد:

Login [username] [password]

چنانچه نام کاربری و رمز عبور صحیح باشد کاربر با موفقیت وارد شده و مجوز درخواست ساخت حساب یا عضویت در یک حساب بانکی را میتواند بدهد و در غیر اینصورت پیام مناسب مبنی بر نادرستی هر یک از اطلاعات و خطای ورود به وی نشان داده شود.

استفاده از مکانیزم های امنیتی بیشتر در این قسمت اختیاری است و نمره اضافه را شامل می شود برای مثال شما می توانید مکانیزم های امنیتی زیر را به دلخواه خودتان پیاده سازی نمایید:

- اگر کاربر به تعداد n مرتبه رمز عبور خود را نادرست وارد کند به مدت m دقیقه ban شده و اجازه ورود نداشته باشد.
- پیاده سازی یک honeypot به طوری که در صورت تشخیص کاربر به عنوان مهاجم وی به یک سامانه غیرواقعی هدایت شده و رفتار او زیر نظر گرفته شود.

عملیات بانکی

در سیستم بانکداری مورد نظر، هر فرد پس از ثبت نام و ورود به حساب کاربری خود، عملیات زیر را میتواند انجام دهد:

۱- ایجاد حساب بانکی

Create [account_type] [amount] [conf_label] [integrity_label]

[account_type] : نوع حساب بانکی که میتواند شامل حساب سپرده پس انداز کوتاه مدت، سپرده پس انداز بلند مدت، حساب جاری و حساب قرض الحسنه باشد.

[amount] : موجودی اولیه حساب

[conf_label] : برچسب محرمانگی حساب

[integrity_label] : برچسب صحت حساب

در صورتی که افتتاح حساب موفقیت آمیز بود یک شماره حساب (account_no) ۱۰ رقمی برای کاربر از جانب سرور ارسال شود. (شماره حساب های ایجاد شده می بایست یکتا باشند.)

۲- درخواست اشتراک در حساب بانکی فرد دیگر

Join [account_no]

هر حساب بانکی در ابتدا یک صاحب حساب دارد (فردی که حساب را افتتاح کرده است.) و زمانی با این درخواست موافقت میشود که صاحب حساب آن را تایید نماید و پس از آن امکان دسترسی مناسب به حساب مذکور بنابر برچسب های اعطایی برای این کاربر می بایست فراهم شود.

۳- قبول اشتراک حساب با یک کاربر

Accept [username] [conf_label] [integrity_label]

صاحب حساب بوسیله این دستور به کاربران منتخبی که برای اشتراک در حساب مربوطه درخواست عضویت داده اند اجازه داده و همچنین به آن کاربر یک برچسب محرمانگی و یک برچسب صحت نیز نسبت داده میشود. این برچسب در کنترل دسترسی به این حساب مورد استفاده قرار خواهد گرفت.

۴- مشاهده تمام حساب های کاربر

Show_MyAccount

کاربر با وارد کردن این دستور کلیه شماره حساب هایی که در آن ها عضو است را میتواند مشاهده کند.

۵- مشاهده اطلاعات حساب

Show_Account [account_no]

کاربر ضمن ارسال این دستور می تواند حساب بانکی موجود که به نام وی ثبت شده است و اطلاعات آن را مشاهده نماید. (اطلاعاتی مربوط به ۵ واریز اخیر، ۵ برداشت اخیر، نوع حساب، تاریخ افتتاح حساب، میزان موجودی و نام صاحب یا صاحبان حساب) این امر علاوه بر صاحب حساب برای کسانی که سطح دسترسی خواندن بر روی حساب ها داشته باشند نیز فراهم است.

انتقال وجه

۱- واریز وجه

Deposit [from_account_no] [to_account_no] [amount]

همه کاربران میتوانند به حساب های مختلف واریز وجه داشته باشند.

۲- برداشت وجه

Withdraw [from_account_no] [to_account_no] [amount]

تنها کسانی میتوانند از حساب برداشت کنند که دسترسی نوشتن بر روی حساب داشته باشند.

رمزنگاری

سرور یک زوج کلید دارد. کلید خصوصی درون سرور نگهداری میشود و کلید عمومی آن در برنامه کلاینت hardcode میشود. سپس با هم یک پروتکل تبادل کلید اجرا کرده و یک کلید نشست با هم تبادل میکنند. بدین صورت که کلاینت کلید نشست را با کلید عمومی سرور رمز کرده و در سمت سرور این کلید رمزگشایی میشود. با این کلید و یک الگوریتم رمز متقارن تمامی ارتباطات میان کلاینت و سرور را رمز کنید

حتما می بایست از الگوریتم های امن و همچنین طول کلید مناسب استفاده کنید.

کنترل دسترسی

مدل کنترل دسترسی در این سیستم ترکیبی از کنترل دسترسی اجباری (MAC) مبتنی بر مدل ها BLP و BIBA و کنترل دسترسی تفویضی (DAC) می باشد. هر کاربر و همچنین هر حساب

یک برچسب محرمانگی و یک برچسب صحت دارند که توسط صاحب حساب تنظیم شده و به همین منظور استفاده میشوند. با استفاده از برچسبها و همچنین قواعد S-property, *-property در این دو مدل عملیات های برداشت، واریز پول و نمایش حساب های بانکی را کنترل کنید.

صاحب اولیه هر حساب نیز دسترسی کامل بر روی حساب های خود دارد.

برچسب های محرمانگی به ترتیب از محرمانه ترین به غیرمحرمانه ترین عبارت اند از :

TopSecret | Secret | Confidential | Unclassified

برچسبهای صحت به ترتیب از قابل اعتماد ترین به غیر قابل اعتمادترین عبارت اند از :

VeryTrusted | Trusted | SlightlyTrusted | Untrusted

تصدیق اصالت

در این سیستم مشخصات محرمانه کاربران (مانند پسورد) در سمت سرور بایستی به صورت امن (درهم ریزی شده با الگوریتم مناسب و با salt تصادفی) نگهداری شود.

رویدادنگاری

تمامی رویدادهای مهم در قالب لاگ بایستی ثبت شوند.

همچنین به عنوان بخش اختیاری می توانید یک سیستم تحلیل رویداد بنویسید که موارد زیر را به اطلاع شما برساند:

تخطی از قوانین کنترل دسترسی

تلاش زیاد یک کاربر برای ورود

لطفًا به نکات زیر توجه نمایید:

- در صورت وجود سوال و یا ابهام، می‌توانید به ایمیل های زیر پیام دهید:

Sara.br1378@gmail.com (سارا برادران)

ae.naderi@gmail.com (عاطفه نادری)

- پروژه در قالب گروه های حداکثر ۳ نفره قابل تحویل است.
- فایل پروژه را در سامانه تحویل دهید و به فرم name_stdnumber.zip باشد.
- زمان ارائه آنلاین پروژه متعاقبا اعلام می گردد.

سلامت و موفق باشید.