دانشگاه فردوسی مشهد

مبانی امنیت اطلاعات

تاریخ تحویل: ۱۴۰۳/۰۳/۲۲

Mini Project

دانشجویان محترم لطفا به نکته های زیر توجه کرده و آنها را رعایت کنید:

تحویل پروژه فقط از طریق سامانه آموزش مجازی دانشگاه(Vu) امکان پذیر است.

از سورس کد های سایر گروه ها استفاده نکنید، در صورت اثبات کپی برداری -به هر دلیلی-، نمره تکلیف طرفین از ۱۰۰ نمره، صفر(-۰-) خواهد شد.

تحویل پروژه بعد از مهلت مشخص شده نمره ای نخواهد داشت.

فایل ارسالی حتما به صورت Zip بوده و نام گذاری فایل به صورت Fullname_Student.number_HWnumber.zip باشد.

"Secure Chat"

هدف:

امروزه ارتباطات نقش اساسی در جامعه، زندگی و حتی حکومت‌ها ایفا می‌کند که بخش گسترده‌ای از این امر را ارتباطات از راه دور در بستر اینترنت شکل داده است. همین امر موجب شد تا ما سامانه‌ها و شبکه های اجتماعی متعددی را به منظور برقراری انواع ارتباطات ساخته و استفاده کنیم، اما همواره یکی از بزرگترین چالش های ارتباط از راه دور تامین امنیت برای آن بوده است.

برای رفع این چالش ما از ویژگی های نظیر ارتباطات محرمانه (Confidential Communication)، کنترل دسترسی (Access Control)، احراز هویت (Authentication)، یکپارچگی(Integrity) و عدم انکار(Non-repudiation) بهره می‌بریم تا تدابیر امنیتی لازمه را اجرا کنیم.

هدف کلی پروژه ایجاد یک محیط امن برای ارتباطات است که در آن محرمانه بودن، اصالت، یکپارچگی و عدم انکار تضمین، حفاظت از اطلاعات حساس تبادل شده بین کاربران برقرار می‌شود و به طور کلی خطرات امنیتی کاهش می‌یابد.

صورت پروژه:

در این پروژه قصد داریم که یک سامانه چت امن برای ارتباط کاربران طراحی کنیم که چندین موجودیت و ویژگی را داشته باشد. ویژگی های این سامانه به شرح زیر است:

ثبت نام:

در ابتدا کاربران باید توانایی ساخت یک حساب کاربری را داشته باشد که شامل فیلد های پست الکترونیک(Email)، نام کاربری(user name)، رمز عبور(password) و تایید رمز عبور (confirm the password) می‌باشد. پس از ثبت نام حساب کاربری ساخته شده و کمترین میزان سطح دسترسی لازم به کاربر اعطا شود.

پس از ثبت نام یک کاربر یک کلید متقارن برای وی توسط سامانه ساخته شده و تنها در اختیار کاربر قرار خواهد گرفت، همچنین فیلد های مد نظر قسمت پیشین به همراه کلید عمومی متناظر آن کاربر در یک ساختار ذخیره سازی داده ذخیره خواهد شد.

*نکته ای که باید به آن توجه داشته باشید رمز عبور کاربر به صورت فاش ذخیره نمی‌شود و می‌بایست حتما از Salt استفاده کنید.

برای این امر می‌توانید از دو رویکرد متفاوت استفاده کنید که به شرح زیر است:

رویکرد اول:

در یک منبع ذخیره سازی به صورت key-value شناسه کاربری و Salt ذخیره شود و متناظر با آن نام کاربری سایر اطلاعات وی در یک منبع ذخیره سازی دیگر ذخیره شود.

رویکرد دوم:

در یک منبع ذخیره سازی، تمامی فیلد های اطلاعاتی هنگام ثبت نام به همراه salt ذخیره شود.

- توجه داشته باشید که ایمیل پیش از این نباید ثبت شده باشد و همچنین تایید رمز عبور می‌بایست مطابق با رمز عبور باشد.
- همچنین برای ذخیره سازی داده های خود از هر نوع پایگاه ذخیره سازی(آرایه، استراکت و یا پایگاه داده) استفاده کنید.

ورود:

پس از ثبت نام، کاربر به واسطه نام کاربری و رمز عبور خود وارد سامانه شود و متناسب با سطح دسترسی از خدمات استفاده کند. در این بخش می‌بایست نام کاربری و رمز عبور به درستی معتبر شناخته شود.

هنگام ورود کاربر در رویکرد اول، فیلد اطلاعاتی نام کاربری دریافت و شناسه متناظر یافت شده و نهایتا salt مد نظر را برداشت کرده و به رمز عبور ورودی چسبانده(concat) و با فیلد ذخیره شده هنگام ثبت نام مقایسه کند.

هنگام ورود کاربر در رویکرد دوم، فیلد اطلاعاتی نام کاربری در منبع یافت می‌شود و سطر نظیر آن که حاوی سایر اطلاعات کاربر می‌باشد برای احراز هویت مورد استفاده قرار می‌گیرد.

سامانه:

در این سامانه ما می‌خواهیم بستر تبادل اطلاعات کاربران را فراهم سازیم که می‌تواند فردی یا گروهی باشد.

سامانه وظیفه ارسال کلید، بررسی و اعطای مجوز های لازم را دارد.

چت خصوصی همتا به همتا(فردی):

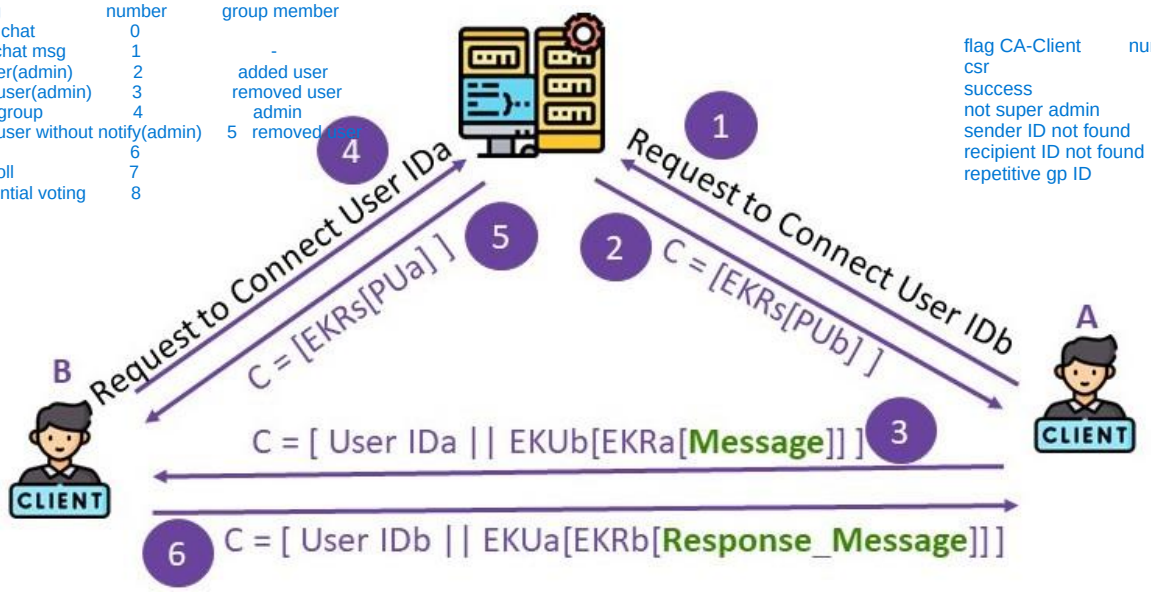
در این قسمت کاربر از سامانه، درخواستی به منظور ارتباط با یک نام کاربری را ارسال میکند، پس از این، سامانه راه ارتباطی وی(برای مثال آدرس آی پی) و کلید عمومی وی را برای کاربر ارسال میکند. کاربر به واسطه کلید عمومی کاربر مد نظر و همچنین کلید خصوصی یک پیام رمز شده برای مقصد ارسال می‌کند. احراز اصالت این پیام به واسطه کلید خصوصی (امضای پیام) تامین شود.

کاربر با ارسال پیام باید نام کاربری خود را به صورت فاش برای وی ارسال کند و باقی پیام خود را با کلید خصوصی خود و کلید عمومی کاربر رمز کند.

در بخش زیرین نمونه یک پیام لازم برای ارتباط امن قرار گرفته که شامل یک نام کاربری است که به یک پیام امضا شده با کلید خصوصی فرستنده (کاربر a)و رمز شده با کلید عمومی کاربر مقصد (کاربر b) می‌باشد.

flag	number	group member
private chat	0	
group chat msg	1	-
add user(admin)	2	added user
delete user(admin)	3	removed user
create group	4	admin
delete user without notify(admin)	5	removed user
voting	6	
send poll	7	
confidential voting	8	

flag CA-Client	number
csr	0
success	1
not super admin	2
sender ID not found	3
recipient ID not found	4
repetitive gp ID	5



تصویر ۱ : سناریو مد نظر به منظور ایجاد چت شخصی

سناریوی چت خصوصی:

- کاربر A به منظور پیام به کاربر B یک درخواست به سامانه ارسال می‌کند.
- سامانه کلیک عمومی کاربرB را که امضا کرده است برای وی ارسال می‌کند(نحوه ارتباط این دو کاربر وابسته به سناریو شماست و می‌تواند آی پی نیز ارسال کند).
- سپس کاربر A یک پیام رمز شده با کلید عمومی کاربرB و امضا شده با کلید خصوصی خودش را برای B ارسال میکند.(ID کاربر A باید فاش برای کاربر B ارسال شود).
- پس از دریافت پیام کاربر B اصالت پیام را بررسی و به منظور پاسخ مانند بخش قبل کلید عمومی A را از سامانه دریافت کرده.
- نهایتا یک پیام در پاسخ وی ارسال می‌کند که توسط کلید عمومی A رمز و توسط کلید خصوصی خودش امضا شده.

چت گروهی:

هر کاربری که سطح دسترسی ایجاد چت گروهی را دارا باشد می‌تواند یک بستر ارتباطی عمومی ایجاد کرده و کاربران مد نظر خود را به آن افزوده یا حذف کند.

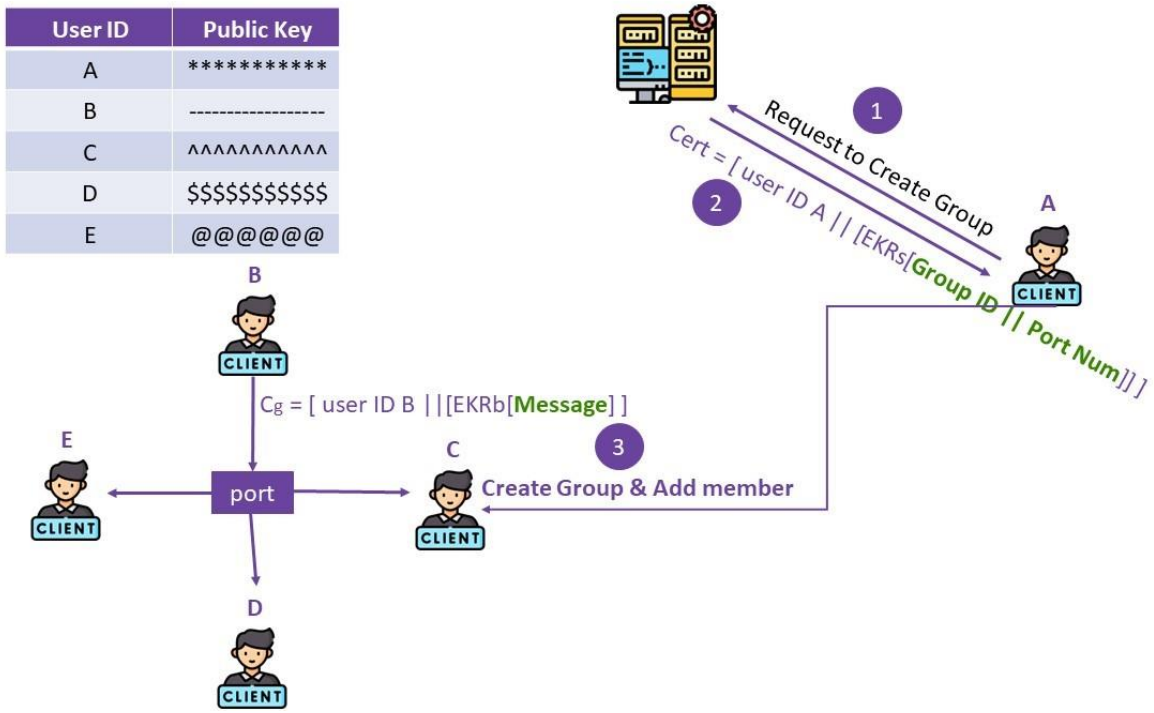
به منظور افزودن اعضا، تنها می‌بایست User ID و Public Key کاربر را به جدول ذخیره اطلاعات گروه که برای همگان در دسترس است افزوده و گواهی (cert) صادر شده برای وی را از طریق چت خصوصی برای کاربر مد نظر ارسال کند.

همچنین توجه داشته باشید که کاربر ایجاد کننده سطح دسترسی افزودن یا حذف کردن کاربر را تنها برای چت ایجاد شده توسط وی را دارد و به سایر چت های گروهی دسترسی مد نظر را ندارد.

به منظور سهولت پروژه انتظار توافق بر روی کلید نشست نمی‌باشد و تنها فرستنده پیام داخل چت گروهی باید پیام را امضا کند تا سایر کاربران امکان تغییر آن را نداشته باشند و همچنین امکان انکار توسط وی نباشد، همچنین نام کاربری فرستنده برای همگان باید نمایش داده شود تا بتوانند پیام دریافتی را رمزگشایی کنند.

برای این رمز گشایی همانند چت خصوصی(فردی) از سامانه درخواستی به منظور ارسال کلید عمومی این کاربر ارسال می‌گردد.

پس از دریافت کلید عمومی فرستنده، همه کاربران توانایی خواندن پیام وی و احراز اصالت را دارا هستند.



تصویر ۲ :سناریو مد نظر به منظور ایجاد چت گروهی

سناریوی چت گروهی:

- کاربری که سطح دسترسی ساخت گروه را دارد یک درخواست برای ایجاد یک گروه را به سامانه ارسال می‌کند.(درخواست شامل ID کاربر هست که می‌بایست امضا شده باشد توسط وی و یک ID برای گروه تعیین کند).
- پس از بررسی سطح دسترسی کاربر و عدم تکراری بودن ID گروه، این چت گروهی ایجاد و یک گواهی برای آن صادر می‌شود.
- سپس کاربر دارای گواهی می‌تواند چت گروهی را ایجاد کند و کاربران مد نظر خود را به این چت اضافه کند و در یک پایگاه داده دخیره کند و همچنین گواهی چت گروهی را برای کاربر مد نظر از طریق چت خصوصی ارسال کند.
- سپس هر یک از کاربران که بخواهند در چت پیامی ارسال کنند باید پیام خود را با کلید خصوصی خود امضا کنند و پیام را روی پورت مشخص شده ارسال کنند.
- سایر کاربران به واسطه دسترسی به جدول کلید عمومی احراز اصالت پیام را انجام می‌دهند.

مدیریت کاربران:

یک کاربر از پیش ساخته شده با سطح دسترسی کامل(super admin) باید بتواند سطح دسترسی کاربران را مدیریت کند و متناسب با نوع کنترل دسترسی مد نظر نقش، ویژگی یا دسترسی اعطا کند.

- برای کنترل دسترسی با انتخاب خود از الگو های سطح دسترسی RBAC یا ABAC می‌توانید استفاده کنید.

به طور کلی ما پنج ویژگی مهم برای سامانه در نظر گرفته ایم:

- چت خصوصی همتا به همتا (کمترین سطح دسترسی را لازم دارد)
- ایجاد چت گروهی
- افزودن کاربر به چت گروهی
- حذف کاربر از چت گروهی
- امکان اعطای ویژگی ها

نکات قابل توجه

- مهلت تحویل تکلیف، ساعت ۲۳:۵۹ روز سه شنبه مورخ ۱۴۰۳/۰۳/۲۲ می‌باشد.
- دانشجویان گرامی تا تاریخ مشخص شده فرصت دارند تا فایل‌های زیر را در سامانه مجازی درس در بخش **mini project** آپلود نمایند.
- تهیه گزارش کتبی(مستندات) از فرآیند پیاده سازی و اجرا الزامی است.
- فایل های ارسالی شامل مستندات و کد های اجرایی می‌باشد.
- این تکلیف به‌صورت گروهی در قالب گروه های دو نفره تعریف شده و قابل انجام است و مشخصات اعضای گروه باید در مستندات ذکر شود.

چه عواملی باعث می شود از این فعالیت نمره کسب نکنید:

- عدم تحویل فایل ها در سامانه vu
- مشاهده شباهت بیش از حد معقول
- عدم تسلط به موضوع در جلسه ارائه