

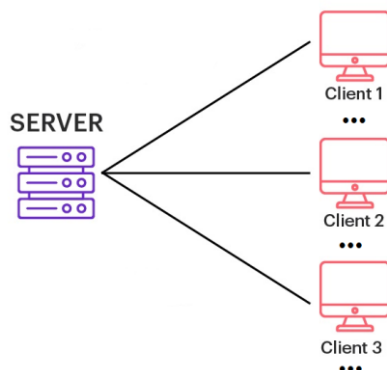


مقدمه

در این پروژه قرار است یک **پیام‌رسان امن** ایجاد کنید که از رمزنگاری انتها به انتها^۱ برای تبادل پیام استفاده می‌کند. انجام پروژه عملی درس در قالب گروه‌های ۳ نفره امکان‌پذیر است. لذا تا تاریخ ۱ خردادماه فرصت دارید تا از طریق این [جدول](#) نسبت به اعلام اسامی نفرات گروه خود اقدام نمایید.

معماری سامانه

دو موجودیت اصلی این پیام‌رسان امن عبارت‌اند از: کارخواه و کارگزار. شمای معماری این پیام‌رسان را در شکل ۱ مشاهده کنید. در ادامه هرکدام از بخش‌های معماری را موردبررسی قرار خواهیم داد.



شکل ۱- معماری سامانه

¹ End-to-end encryption



کارخواه^۲


کارخواه به عنوان رابط میان کاربر و کارگزار نقش ایفا می‌کند. این رابط از نوع خط فرمان^۳ است و نیازی به پیاده‌سازی واسط کاربری گرافیکی^۴ یا واسط کاربری متنی^۵ نیست.


زمانی که یک کارخواه می‌خواهد پیامی را به کارخواه دیگر بفرستد، آن پیام را به کارگزار ارسال می‌کند و کارگزار آن پیام را به صورت انتها به انتها به کارخواه دیگر ارسال می‌کند.


فرضیات:


۱. کارخواه کلید عمومی کارگزار را دارد یا می‌تواند از آن دریافت نماید.
۲. برای ایجاد یک ارتباط ایمن، تمام مراحل ایجاد یک نشست ایمن و انتها به انتها رمزنگاری شده باید از طریق یک کارگزار انجام گردد و هیچ موجودیت مورد اعتماد دیگری وجود ندارد.

قابلیت‌ها:

۱.  ایجاد حساب کاربری
مانند هر برنامه دیگری کاربران در وهله اول باید ثبت‌نام نمایند و حساب کاربری خود را ایجاد کنند، سپس از طریق نام کاربری و گذرواژه خود وارد سیستم شوند.

۲.  نمایش کاربران آنلاین
کاربران باید بتوانند لیستی از سایر کاربران متصل به کارگزار (کاربران آنلاین) را مشاهده کنند.

۳.  ارسال و دریافت پیام
هر کارخواه از طریق رمزنگاری انتها به انتها پیام‌هایی را به سایر کاربران ارسال و از آن‌ها دریافت می‌کند. درواقع زمانی که یک کارخواه می‌خواهد پیامی را به کارخواه دیگر ارسال کند، آن پیام را با کلید جلسه رمز کرده و برای کارگزار ارسال می‌کند، سپس کارگزار آن را به کارخواه دیگر فوروارد کرده و کارخواه دیگر با استفاده از کلید جلسه آن پیام را رمزگشایی می‌کند.

۴.  نگهداری پیام‌ها به صورت امن
پیام‌ها باید به صورت امن در سمت کارخواه ذخیره شوند. بدین معنا که اگر مهاجم توانست به سیستم کاربر نفوذ کند، نتواند پیام‌ها را مشاهده کند.

^۲ Client

^۳ Command line

^۴ GUI (Graphic User Interface)

^۵ TUI (Text User Interface)



۵. نگهداری کلید به صورت امن



هر کارخواه باید کلیدهای مورد استفاده‌اش را به صورت امن در سمت خودش ذخیره کند. بدین معنا که اگر مهاجم توانست به سیستم کاربر نفوذ کند، نتواند آن کلیدها را به دست آورد.

۶. ایجاد و مدیریت گروه

هر کاربر باید بتواند یک گروه ایجاد نماید و در آن پیام ارسال کند و همچنین سایر پیام‌های گروه را مشاهده کند. همچنین هر کاربر باید بتواند به گروهی که ادمین آن است، کاربران آنلاین دیگر را اضافه کند.

۷. تأیید صحت نشت از طریق کانال امن



فرض کنید کارگزار از روی کنجکاوی با دستکاری پارامترهای ارتباط قصد شنود ارتباط دو طرف را داشته باشد. راه‌حلی ارائه دهید و پیاده‌سازی کنید تا دو طرف یک ارتباط بتوانند به راحتی از امن بودن و انتها به انتها رمزنگاری بودن ارتباط از طریق یک کانال امن ثانویه اطمینان حاصل کنند. (مانند نمایش شکل‌های^۶ یکسان در تماس تلگرام)

۸. تازه‌سازی کلیدهای نشت



در صورتی که اطلاعات محرمانه یک نشست (کلید نشست، کلید خصوصی و ...) به هر دلیلی (مانند حمله موفق یک مهاجم به یک کارخواه) به دست مهاجم برسد، هر کاربر باید این امکان را داشته باشد تا تمامی اطلاعات محرمانه را از نو بسازد و تمام موجودیت‌های نشست با استفاده از متغیرهای جدید به مکاتبه ادامه دهند.



کارگزار^۷

کارگزار یک موجودیت صادق ولی کنجکاو به حساب می‌آید که روند ارسال پیام به صورت انتها به انتها و تبادل کلید بین کارخواه‌ها را مدیریت می‌کند. کارگزار همچنین مسئول احراز هویت و ثبت نام کاربران پیام‌رسان می‌باشد.

فرضیات:

۱. کارگزار مورد اعتماد است و همچنین مورد حمله قرار نگرفته است.

قابلیت‌ها:

۱. ثبت نام و احراز هویت کاربران و نگهداری اطلاعات مربوطه به صورت امن



کاربران قبل از استفاده پیام‌رسان، می‌بایست اقدام به ایجاد حساب کاربری نمایند و سپس با نام کاربری و کلمه عبور خود وارد پیام‌رسان شوند. رمز عبور کاربران باید به صورت امن در سمت کارگزار ذخیره شود به شکلی که در صورت دسترسی یک مهاجم به مخزن اطلاعات احراز هویت کاربران، مهاجم نتواند رمز عبور کاربران را به دست آورد.

۲. ارسال پیام‌ها به مقصد



کارگزار، پیامی که یک کارخواه می‌خواهد به کارخواه دیگر ارسال کند را به صورت رمز شده دریافت می‌کند و آن را به کارخواه دیگر ارسال می‌کند و پس از ارسال آن پیام، آن را از سمت خودش حذف می‌کند.

۳. ارائه لیست کاربران آنلاین به کارخواه



کارگزار باید بتواند لیستی از کاربران آنلاین را به هر یک از کارخواه‌ها ارائه کند.

۴. ارسال و دریافت پیام‌های مربوط به ساخت کلید نشست



در صورتی که دو کارخواه قصد مکالمه داشته باشند، کارگزار باید پیام‌های لازم برای ایجاد کلید نشست بین طرفین را بین آن‌ها ردوبدل کند.

۵. نگهداری اطلاعات گروه‌ها

نام گروه‌های ایجاد شده، لیست اعضای گروه و نقش هر عضو باید در سمت کارگزار ذخیره شود.



نیازمندی‌های امنیتی:

پیام‌رسانی که طراحی می‌کنید به‌عنوان یک پیام‌رسان امن باید نیازمندی‌های زیر را برآورده کند.

۱.  رمزنگاری انتها به انتها^۸
تمامی پیام‌های بین دو کارخواه باید به‌صورت انتها به انتها رمزنگاری شوند. در رمزنگاری انتها به انتها دو کارخواه از طریق یک کارگزار با یکدیگر پیام تبادل می‌کنند ولی کارگزار نمی‌تواند محتوای پیام را مشاهده کند.
۹.  تازگی کلید^۹
در زمان توافق کلید بین دو کارخواه، هر دو باید از تازگی بودن کلید اطمینان حاصل کنند.
۱۰.  محرمانگی
محرمانگی پیام‌های ردوبدل شده بین کارخواه‌ها باید حفظ شود و جلوی افشای غیرمجاز آن‌ها گرفته شود.
۲.  صحت و یکپارچگی^{۱۰}
حمله‌کننده نباید بتواند پیام‌های ردوبدل شده بین کارخواه‌ها را تغییر دهد.
۳.  حفظ سازگاری^{۱۱}
ترتیب پیام‌های ارسال‌شده توسط فرستنده و دریافت‌شده توسط گیرنده باید سازگار باشد. به این معنا که دریافت‌کننده باید بتواند متوجه شود که ارسال‌کننده با چه ترتیبی آن پیام‌ها را ارسال کرده است.
۴.  احراز اصالت^{۱۱}
اصالت ارسال‌کننده پیام باید حفظ شود و حمله‌کننده نباید بتواند از طرف یک کارخواه پیامی را ارسال کند.
۵.  عدم انکار^{۱۲}
فرستنده یک پیام نباید بتواند انکار کند که یک پیام را ارسال کرده است.
۶.  کنترل دسترسی
فقط ادمین هر گروه می‌تواند عضو جدیدی را به گروه اضافه کند و سایر اعضای گروه چنین دسترسی‌ای ندارند ولی همه اعضای گروه می‌توانند در گروه پیام ارسال کنند و همچنین همه پیام‌های ردوبدل شده در گروه را مشاهده کنند.
۷.  حمله مردی در میان^{۱۳}
حمله مردی در میان در هیچ‌کدام از مراحل ارتباط دو موجودیت نباید امکان‌پذیر باشد.

^۸ End-to-End Encryption

^۹ Key freshness

^{۱۰} Integrity

^{۱۱} Authentication

^{۱۲} Non-repudiation

^{۱۳} Man-in-the middle



۸. حمله تکرار^{۱۴}



حمله تکرار در هیچ کدام از مراحل ارتباط دو موجودیت نباید امکان پذیر باشد.

۹. استفاده از الگوریتم‌های رمزنگاری امن



از الگوریتم‌های رمزنگاری امن استفاده کنید.

۱۰. محرمانگی پیشرو^{۱۵}

محرمانگی پیشرو تضمین می‌کند که اگر مهاجم کلید بلندمدت را به دست آورد، نمی‌تواند کلید جلسه‌های^{۱۶} گذشته را به دست بیاورد و در نتیجه محرمانگی پیام‌هایی که در گذشته تبادل شده‌اند حفظ می‌شود.

۱۱. محرمانگی آینده^{۱۷}

محرمانگی آینده تضمین می‌کند که اگر مهاجم کلید بلندمدت^{۱۸} را به دست آورد، نمی‌تواند کلید جلسه‌های آینده را به دست بیاورد و در نتیجه محرمانگی پیام‌هایی که در آینده تبادل می‌شوند، حفظ خواهد شد.

فعالیت‌های امتیازی:

۱. امکان ارسال پیام به کاربران آفلاین که قبلاً با آن‌ها کلیدی تبادل نشده است (تبادل کلید غیرتعاملی)(/۱۰).
۲. حذف اعضا از گروه توسط ادمین امکان پذیر باشد. توجه داشته باشید عضو حذف شده از گروه نباید امکان رمزگشایی پیام‌های جدید گروه را داشته باشد (/۱۰).

¹⁴ Replay attack

¹⁵ Forward secrecy

¹⁶ Session key

¹⁷ Future Secrecy

¹⁸ Long-term key



ارزیابی پروژه:

در زمان تحویل پروژه شما باید یک سناریو حاوی سه کارخواه و یک کارگزار ایجاد کرده باشید و در این سناریو با استفاده از نمایش جزئیات پارامترهای استفاده‌شده در پروتکل نشان دهید که پروژه شما عملکردهای گفته‌شده را دارد و نیازمندی‌های امنیتی خواسته‌شده را برآورده می‌کند.

تحویل دادنی‌ها:

تحویل دادنی‌های پروژه عبارت‌اند از:

۱. فایل PDF مستندات پروژه که حاوی اطلاعاتی در مورد نحوه طراحی و پیاده‌سازی هرکدام از نیازمندی‌های پروژه و همچنین نحوه راه‌اندازی و اجرای پروژه باشد. در این فایل باید تمامی نیازمندی‌های امنیتی برای پیام‌رسان خود را بررسی نمایید و توضیح کاملی درباره دلیل برآورده شدن و یا نشدن آن‌ها بیان کنید.
۲. کد منبع پروژه به همراه فایل requirements.txt که حاوی لیست کتابخانه‌های لازم برای اجرای کدها است.

نکات مهم

- پیاده‌سازی پروژه می‌بایست با زبان پایتون انجام شود.
 - خروجی پروژه شما باید مطابق با استاندارد عنوان‌شده در زیر باشد:
- DNS-Project-GID.zip..... (GID شماره گروه شماست)
- DNS- Project-GID.pdf (فایل مستندات)
- Source Codes..... (پوشه حاوی کدهای منبع)
- requirements.txt
- پیاده‌سازی امکانات، زیرساخت‌ها و ارتباطات مابین اجزای پروژه تماماً برعهده شماست، اگرچه می‌توانید از کتابخانه‌های رایج (به‌عنوان مثال برای انجام رمزنگاری و ...) استفاده کنید ولی مجاز به استفاده از کتابخانه‌هایی که بخشی از پروژه را پیاده‌سازی کرده‌اند نیستید.
 - در صورتی که تقلبی محرز شود، نمره کل پروژه گروه خاطی برابر با <<منفی ۱۰۰>> ثبت خواهد شد.