دانشگاه صنعتی امیرکبیر

دانشکده‌ی مهندسی کامپیوتر

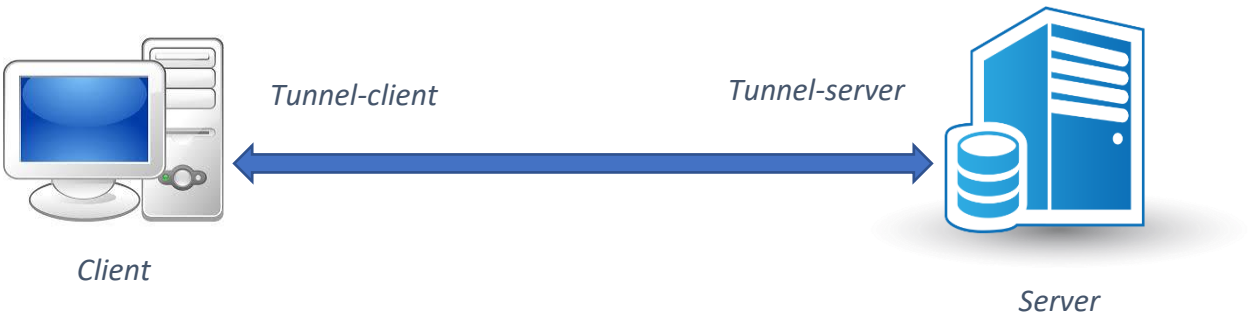
امنیت اطلاعات و ارتباطات

Department of Computer Engineering and Information Technology

پروژه‌ی اول (فاز اول)

تونل امن

در این پروژه قصد داریم یک تونل امن که بتوان توسط اپلیکیشن‌های مختلف مانند سرویس ایمیل POP۳، FTP و ... از آن استفاده کرد را بسازیم. این تونل امن از دو جزء اصلی تشکیل شده است: تونل کلاینت و تونل سرور. تونل کلاینت روی دستگاه کلاینت اجرا می‌شود و منتظر یک اتصال از سوی اپلیکیشن دیگری مانند یک mail reader می‌ماند. هنگامی که یک اتصال از پورت محلی دریافت شد، تونل کلاینت، شماره‌ی پورت را داخل یک جدول داخلی بررسی می‌کند تا نام و شماره‌ی پورت سرویس از راه دور را برای اتصال پیدا کند. برای مثال، جدول ممکن است اعلام کند که پورت محلی POP۳ مربوط به پورت POP۳ روی میزبان mypop.com است. سپس تونل کلاینت به تونل سرور روی میزبان متصل می‌شود (در اینجا mypop.com)، یک اتصال امن با تونل سرور برقرار می‌کند و مانند یک تقویت کننده میان اپلیکیشن و سرویس از راه دور عمل می‌کند (در اینجا سرورPOP۳). در میزبان، تونل سرور، اتصالی که از سوی کلاینت آمده را تایید می‌کند، یک اتصال امن با کلاینت برقرار می‌کند و به پورت محلی مربوط به سرویس متصل می‌شود (در اینجا پورت محلی POP۳). در این لحظه، تونل سرور به عنوان یک تقویت کننده میان اپلیکیشن و سرور محلی عمل می‌کند. مانند شکل زیر:



زبان پیاده سازی پروژه دلخواه است.

نکات پیاده‌سازی

- برای مبادله‌ی کلید جلسه، ابتدا فرض کنید که به صورت فیزیکی، دو سیستم مبدا و مقصد، دارای یک فایل که بصورت رمز شده روی هریک از سیستمها قرار دارد، می‌باشند. داخل این فایل رمز شده، کلید مشترکی برای دو سیستم مبدا و مقصد قرار داده شده است. این کلید دارای یک برچسب زمانی[1] می‌باشد که پس از اتمام انقضا، معتبر نیست(هر کلید، دارای یک فیلد انقضا است). سپس با استفاده از این کلید، کلید جلسه را مبادله می‌کنیم. کلید جلسه هم باید توسط یکی از طرفین ایجاد شده، با کلیدی که بصورت فیزیکی مبادله شده، رمز شود و برای طرف دیگر ارسال شود. توجه کنید که کلید جلسه هم باید یک برچسب زمانی داشته باشد. دقت کنید که باید هر لحظه چک کنید و قبل از گذشتن انقضای کلیدها، کلیدهای جدید مبادله کنید.
- انقضای کلیدی که بصورت فیزیکی مبادله شده، برابر همان مدت زمانی است که مبدا با مقصد ارتباط برقرار می‌کند. یعنی قبل از اتمام جلسه، باید کلیدهای فیزیکی جدید مبادله و در سیستم‌های مبدا و مقصد به صورت رمز شده ذخیره شود.
- برای انقضای کلید جلسه، می‌توانید مثلا هر یک دقیقه کلید جدید را مبادله کنید(با کلید جلسه‌ی قبلی رمز و مبادله کنید). این پارامتر باید قابل تنظیم باشد.
- برای ارتباط امن، با استفاده از رمزنگاری متقارن، همه‌ی پیغام‌ها را با استفاده از کلید جلسه مبادله کنید. (در مبدا رمزنگاری و در مقصد رمزگشایی کنید.)
- توجه کنید که از Secure Socket های آماده نمی‌توانید استفاده کنید و باید یک ارتباط TCP برقرار کرده و امکانات امنیتی آن را با استفاده از موارد ذکر شده پیاده سازی کنید.
- توجه کنید که برای ارسال داده‌ها، بصورت Byte Stream عمل کنید تا اینکه بتوان انواع فایل‌ها را هم رمزنگاری کرد.
- برای تست برنامه، باید روی سیستم‌های جداگانه صورت گیرد و یا اینکه از Virtual Machine استفاده شود.

[1] Time Stamp

نکات دیگر

- پروژه را باید هر نفر به تنهایی پیاده سازی کند و تحویل حضوری دارد که زمان آن متعاقبا اعلام خواهد شد.
- کدها بررسی و در صورت وجود تطابق تقلب گرفته می‌شود.
- مهلت ارسال پروژه تا تاریخ جمعه ۱۰ آبان ماه ۱۳۹۸ می‌باشد.