

## پروژه دوم درس شبکه - Telnet الهام رازی - 9731019

1. تلنت، پروتکلی است که در سال 1969 معرفی شد و اینترنتی مبتنی بر متن را برای ارتباط دو طرفه با یک دستگاه یا سرور را فراهم می آورد. داده‌ی کاربران در این پروتکل (که مربوط به لایه‌ی اپلیکیشن است) با استفاده از پروتکل TCP که در لایه‌ی انتقال است، منتقل می‌شود. معمولاً، از تلنت بر روی یک ترمینال برای اجرای توابع از راه دور مورد استفاده قرار می‌گیرد.

از کاربردهای تلنت، می‌توان به تست کردن میل سرور ها و وب سرورها از راه دور اشاره کرد.

2. این پروتکل پیش از همه گیری اینترنت معرفی شده است، به خودی خود هیچ گونه رمزگذاری ای بر روی داده‌ی منتقل شده انجام نمی دهد و درواقع هیچگونه مسایل امنیتی در آن رعایت نمی‌شود. به همین دلیل، از آن در شبکه های اینترنتی چندان استفاده نمیشود.

3. پروتکل TLS، پروتکلی است که با استفاده از رمزگذاری، امنیت end-to-end داده هایی که بین برنامه ها در شبکه رد و بدل می شوند را تامین می‌کند. لازم به ذکر است که این پروتکل، داده ها را در سیستمی که آن را دریافت یا ارسال کرده تضمین نمی‌کند؛ فقط امنیت آن در زمان انتقالش در شبکه توسط پروتکل فراهم می‌شود. TLS در بالای TCP قرار گرفته و برای رمزگذاری اپلیکیشن هایی مانند HTTP، FTP، SMTP و غیره مورد استفاده قرار می گیرد.

در این پروتکل، از دو روش رمزگذاری متقارن و غیر متقارن استفاده می شود که در روش متقارن، داده با استفاده از یک کلید خصوصی که برای فرستنده و گیرنده شناخته شده است، رمزگذاری و رمزگشایی می‌شود. البته این اشتراک گذاری کلید هم باید به صورت امنی انجام شود.

در روش غیر متقارن، برای رمزگذاری از زوج کلیدهای خصوصی و عمومی استفاده می‌شود. کلید عمومی به صورت ریاضی واری با کلید خصوصی رابطه دارد. به دست آوردن کلید خصوصی از کلید عمومی، چندان راحت نیست. این موضوع به ارسال کننده امکان این را می‌دهد که با استفاده از کلید عمومی دریافت کننده، داده را رمزگذاری کنند. اما این داده، تنها با استفاده از کلید خصوصی دریافت کننده قابل رمزگشایی است. این روش به نسبت از روش متقارن امنیت بالاتری دارد.

## • TLS HANDSHAKE

- Client hello message: کلاینت ابتدا با استفاده از ارسال این پیام به سرور، handshake را آغاز می‌کند.
- Server hello message: در جواب پیام قبلی کلاینت، سرور یک پیام حاوی ssl certificate و اطلاعات دیگری را هم می‌فرستد.
- Authentication: کلاینت سرتیفیکت ارسالی سرور را بررسی می‌کند تا مطمئن باشد که سرور هویت اصلی را دارد.
- Premaster secret: کلاینت رشته رندوم دیگری از بایت را برای سرور ارسال میکند. این رشته با استفاده از کلید عمومی رمزگذاری شده و تنها با استفاده از کلید عمومی توسط سرور رمزگشایی می‌شود. سرور هم این پیام را رمزگشایی می‌کند.
- Session keys: کلاینت و سرور هر دو session key هایی را از client random، server random و Premaster secret تولید می‌کنند. هر دو باید به نتیجه مشابهی برسند.
- Client & server are ready: حال کلاینت و سرور یک پیام finished به همراه session key ها برای هم ارسال می‌کنند.
- Secure Symmetric encryptin achieved: مرحله tls handshake تکمیل شده و حال انتقال داده ها با استفاده از session key ها ادامه می‌یابد.

در تصویر زیر، میتوان محتوای پیام رمزگذاری شده را مشاهده کرد که قابل خواندن نیست:

```
Wireshark · Packet 456 · Adapter for loopback traffic capture

> Frame 456: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{...}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1
> Transmission Control Protocol, Src Port: 1031, Dst Port: 6412, Seq: 598, Ack: 2394, Len: 46
▼ Transport Layer Security
  ▼ TLSv1.3 Record Layer: Application Data Protocol: Application Data
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 41
    Encrypted Application Data: fd8849b8cf025fd8c9b75e063093db4c75b8c5033ffde56086a8ac82f3276dff80ec8fd4...
```

```
0000  02 00 00 00 45 00 00 56 00 d1 40 00 80 06 00 00  ....E..V..@....
0010  c0 a8 38 01 c0 a8 38 01 04 07 19 0c c0 f0 b8 f1  ..8...8.....
0020  82 08 6d 74 50 18 27 f0 39 a3 00 00 17 03 03 00  ..mtP...9.....
0030  29 fd 88 49 b8 cf 02 5f d8 c9 b7 5e 06 30 93 db  )..I...^..0..
0040  4c 75 b8 c5 03 3f fd e5 60 86 a8 ac 82 f3 27 6d  Lu...?...^...m
0050  ff 80 ec 8f d4 7d b9 70 f0 a5  ....}.p..
```

در تصویر زیر هم می توان محتوای یک پیام با استفاده از پروتکل تلنت را مشاهده کرد که به صورت متنی ساده و بدون هیچگونه تمهیدات امنیتی قابل خواندن است.

