Topic

Transport Layer Security (TLS) Secure Socket Layer (SSL)

Group Members: ***Roll No.***

Ali Akber ***1406***

Rana Assad Ali ***1407***

Qasim Ali ***1425***

Toseef Khadim ***1427***

BS(cs 4rth smester)

SSL
(Secure Socket Layer)

SSL History

- Netscape developed The Secure Sockets Layer Protocol (SSL) in 1994, as a response to the growing concern over security on the Internet.

- SSL was originally developed for securing web browser and server communications.
- SSL v3.0 was specified in an Internet Draft (1996)

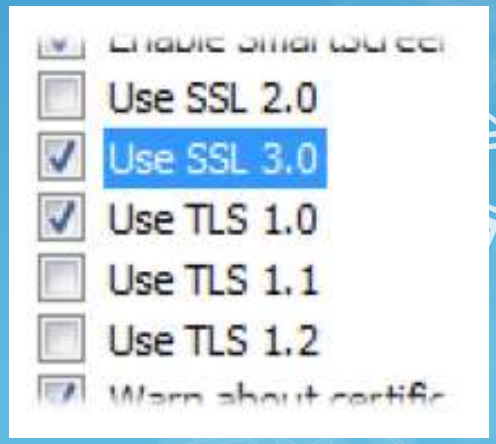
SSL (Secure Socket Layer)

- SSL is a Secure Sockets Layer
- SSL is the standard security technology for establishing an encrypted link between a web server and a browser.
- This link ensures that all data passed between the web server and browsers remain private and integral
- There are several versions of the SSL protocol defined. The latest version, the Transport Layer Security Protocol (TLS), is based on SSL 3.0

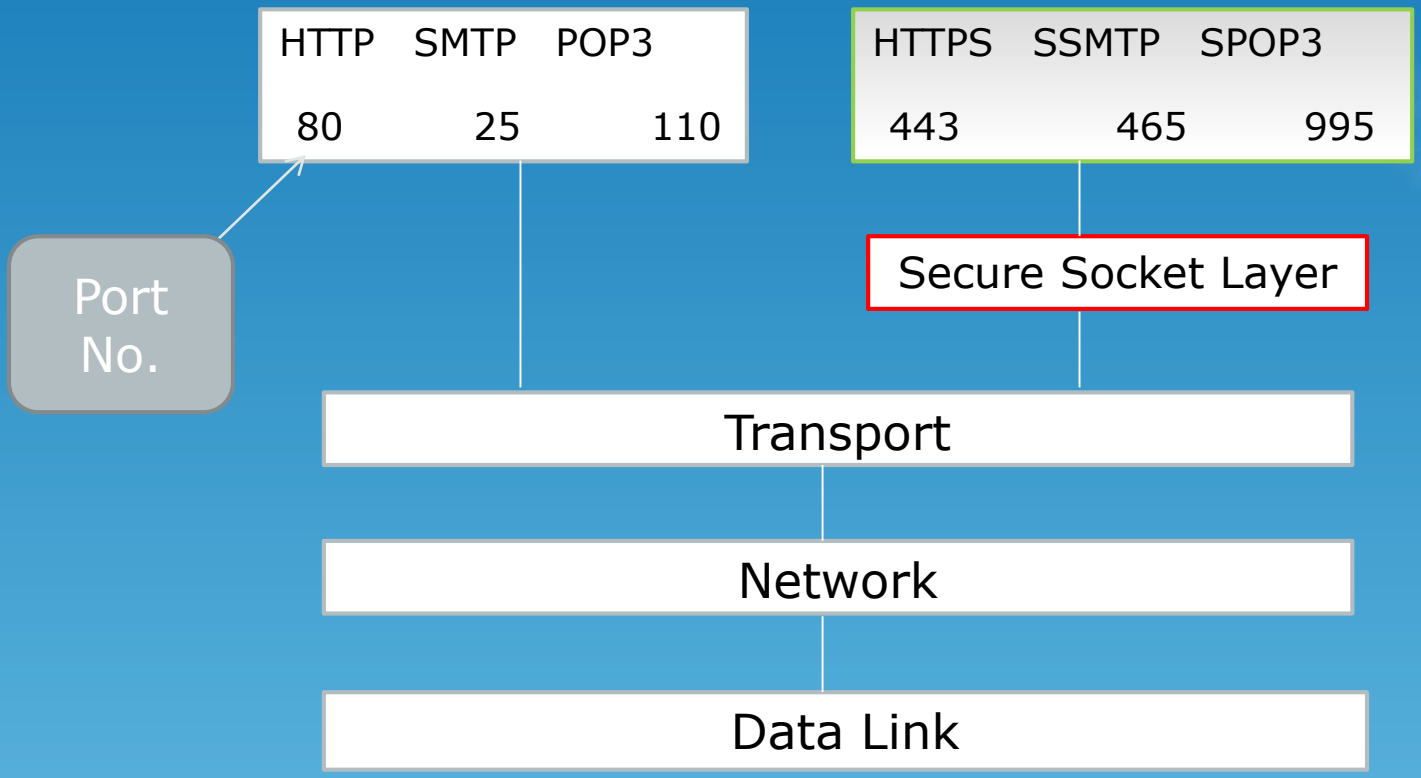
SSL Version 1.0

SSL Version 2.0

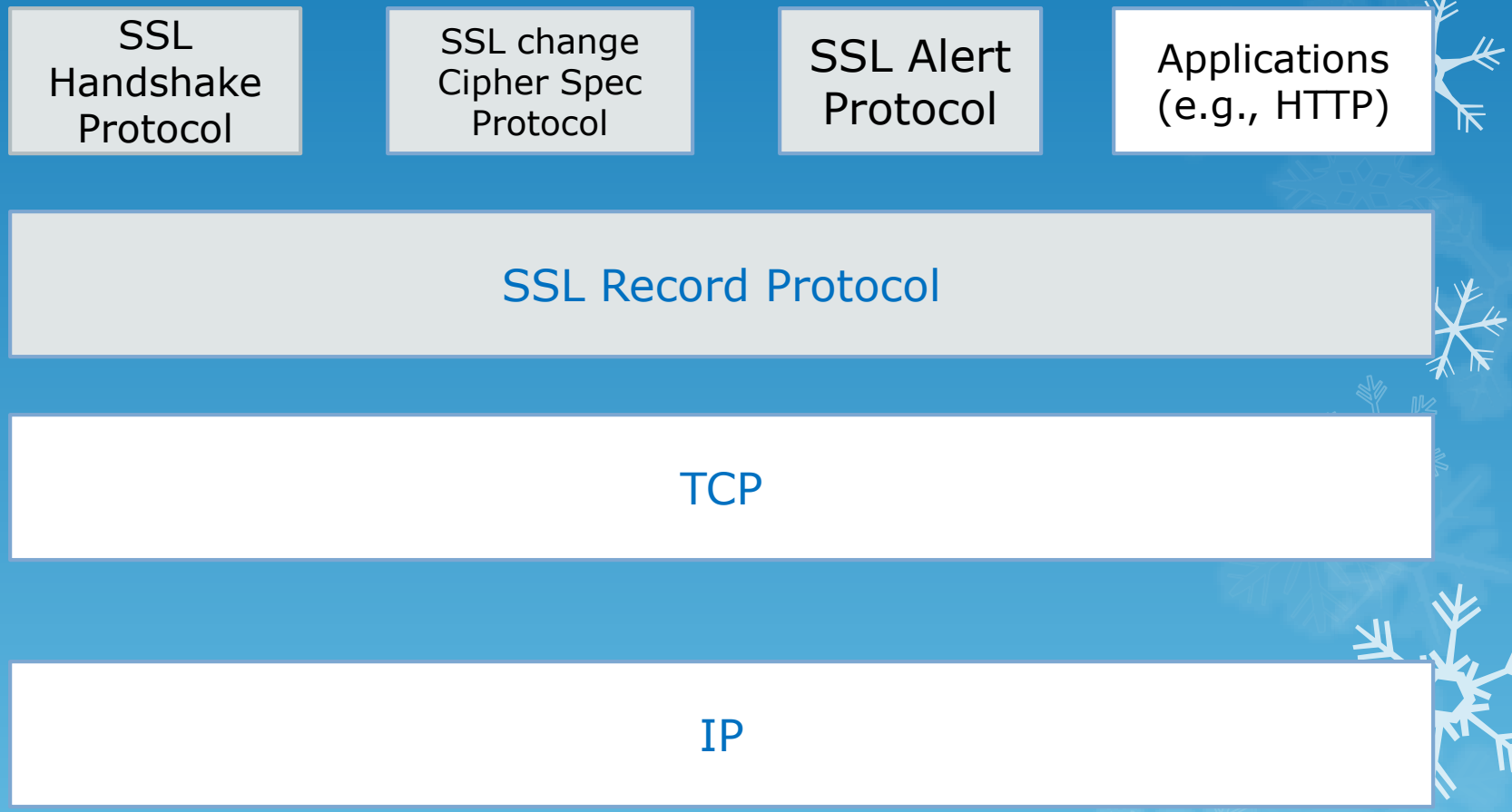
SSL Version 3.0



Where SSL fits?

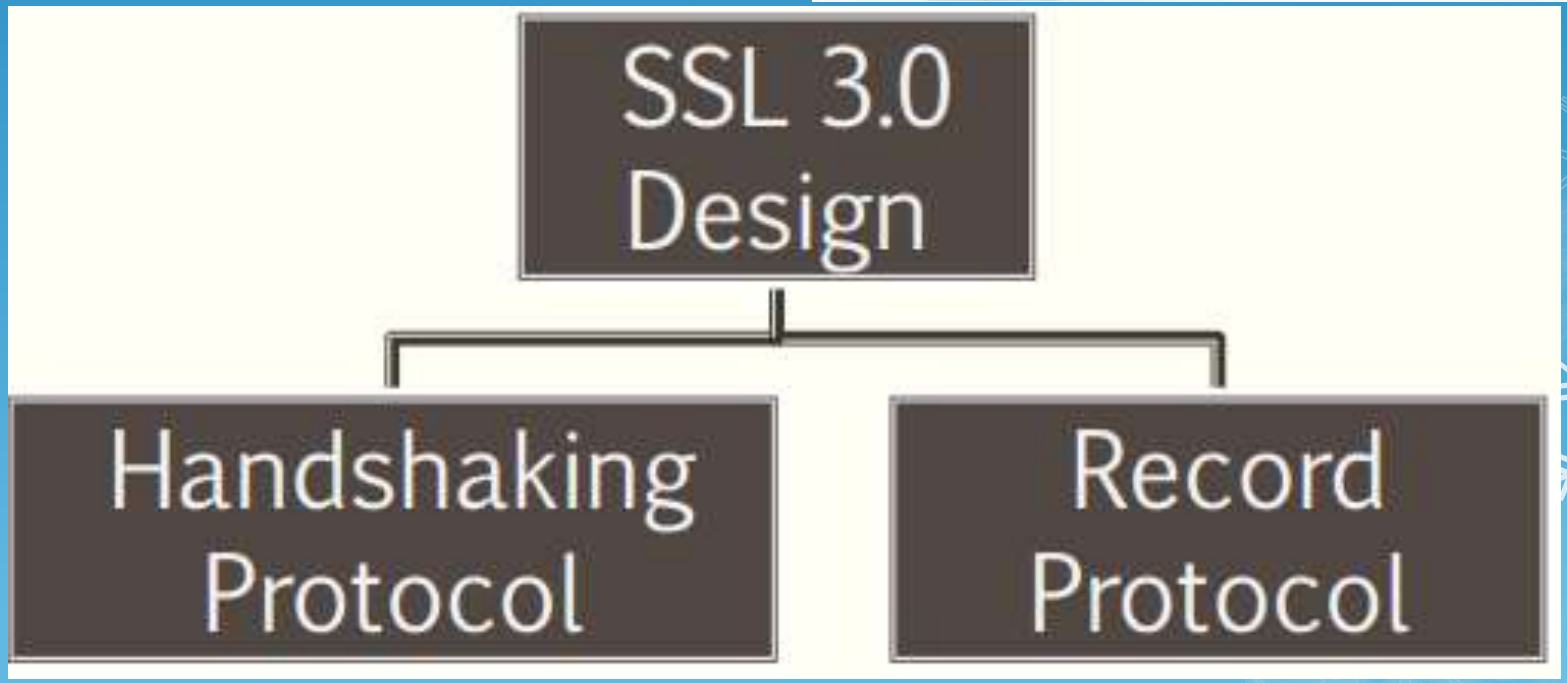


SSL architecture



SSL

- It is the most widely known as the protocol that, coupled with HTTP, secures the Web and uses the “https” URI scheme



SSL components

- **SSL Handshake Protocol**
  - Negotiation of security algorithms and parameters
  - Key exchange
  - Server authentication and optionally client authentication
- **SSL Record Protocol**
  - Fragmentation
  - Compression
  - Message authentication and integrity protection
  - Encryption
- **SSL Alert Protocol**
  - Error messages (fatal alerts and warnings)
- **SSL Change Cipher Spec Protocol**
  - A single message that indicates the end of the SSL handshake

SSL Goals

Confidentiality

The data being transmitted over the Internet or network needs confidentiality. In other words, people do not want their credit card number, account login, passwords or personal information to be exposed over the Internet.

Integrity Protection

The data needs to remain integral, which means that once credit card details and the amount to be charged to the credit card have been sent, a hacker sitting in the middle cannot change the amount to be cha rged and where the funds should go.

Authentication

Your organization needs identity assurance to authenticate itself to customers / extranet users and ensure them they are dealing with the right organization.

Your organization needs to comply with regional, national or international regulations on data privacy, security and integrity

Reality!!!


SPYWARE
UPDATE
VIRUS
SECURITY
SPAM
HACKER
IDENTITY
PHISHING
FIREWALL
INTERNET
PASSWORD

Transport Layer Security (TLS)

Two protocols are dominant today for providing security at the transport layer

- Secure Sockets Layer (SSL) protocol
- **Transport Layer Security (TLS) protocol**

Definition:

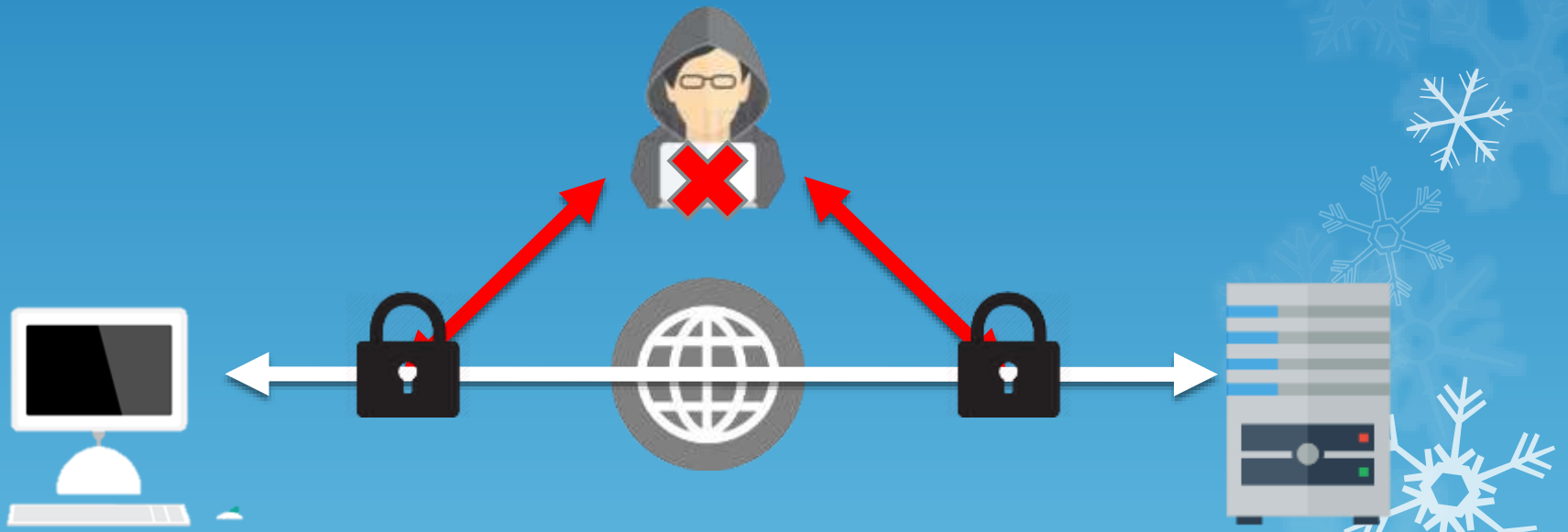
- Transport Layer Security (TLS) was designed to provide security at the transport layer.
- TLS was derived from a security protocol called Secure Sockets Layer (SSL).

Transport Layer Security (TLS)

- TLS is the successor to the Secure Sockets Layer (SSL).
- Transport Layer Security (**TLS**) is a protocol that ensures privacy between communicating applications and their users on the Internet.
- Is a widely deployed protocol for securing client-server communications over the internet.
- TLS is designed to prevent eavesdropping, tampering, and message forgery

Why do we need it?

- TLS ensures that no third party may eavesdrop or tamper with any message.

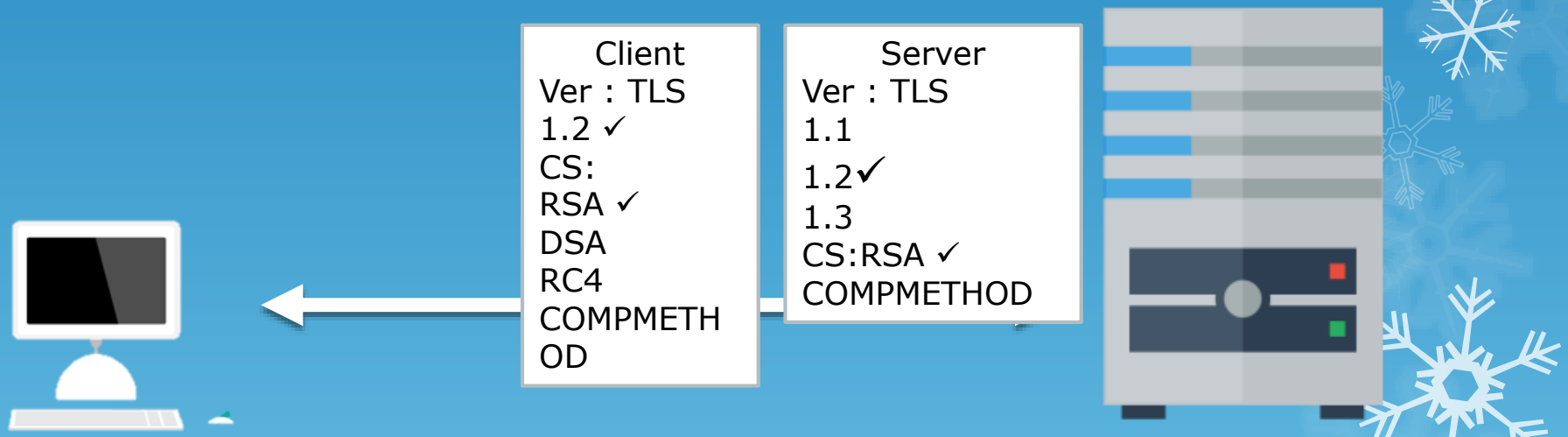


Working of Transport Layer Security

- The Client connect to server (using TCP). The client can be anything.
- The Client sends a number of specifications :
  - Version of SSL/TLS
  - Which cipher suites, compression method it wants to use.

Working of Transport Layer Security

- The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the client's options (if it supports one), and optionally picks a compression method.



Working of Transport Layer Security

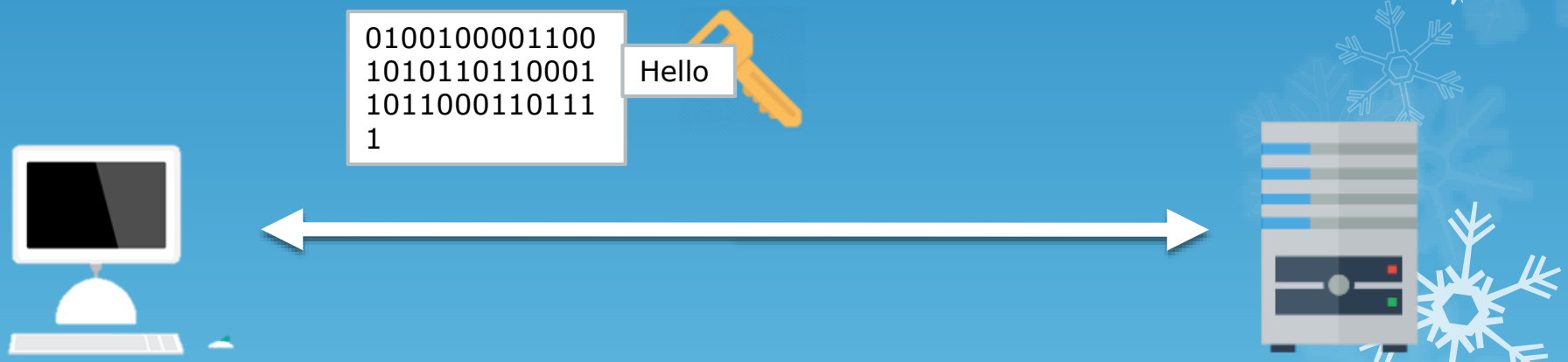
- After this the basic setup is done, the server sends its certificate.
- This certificate must be trusted by either the client itself or a party that the client trusts.
- For example if the client trusts GeoTrust, then the client can trust the certificate from Google.com, because GeoTrust cryptographically signed Google's certificate.

Working of Transport Layer Security

- Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged.
- This can be a public key, a "PreMasterSecret" or simply nothing, depending on the chosen ciphersuite.

Working of Transport Layer Security

- Both the server and the client can now compute the key for the symmetric encryption.



Working of Transport Layer Security

- The handshake is now finished, and the two hosts can communicate securely.

Working of Transport Layer Security

- To close the connection, a close notify 'alert' is used. If an attacker tries to terminate the connection by finishing the TCP connection (injecting a FIN packet), both sides will know the connection was improperly terminated. The connection cannot be compromised by this though, merely interrupted

Benefits of TLS\SSL

- Encryption
  - TLS can help to secure transmitted data using encryption.
- Interoperability
  - TLS works with most Web browsers, including Microsoft Internet Explorer and Netscape Navigator, and on most operating systems and Web servers.
- Algorithm flexibility
  - TLS provides options for the authentication mechanisms, encryption algorithms, and hashing algorithms that are used during the secure session.
- Ease of deployment
  - Many applications use TLS transparently on a Windows Server 2003 operating systems.
- Ease of use
  - Because you implement TLS beneath the application layer, most of its operations are completely invisible to the client.

Govt municipal degree college Faisalabad