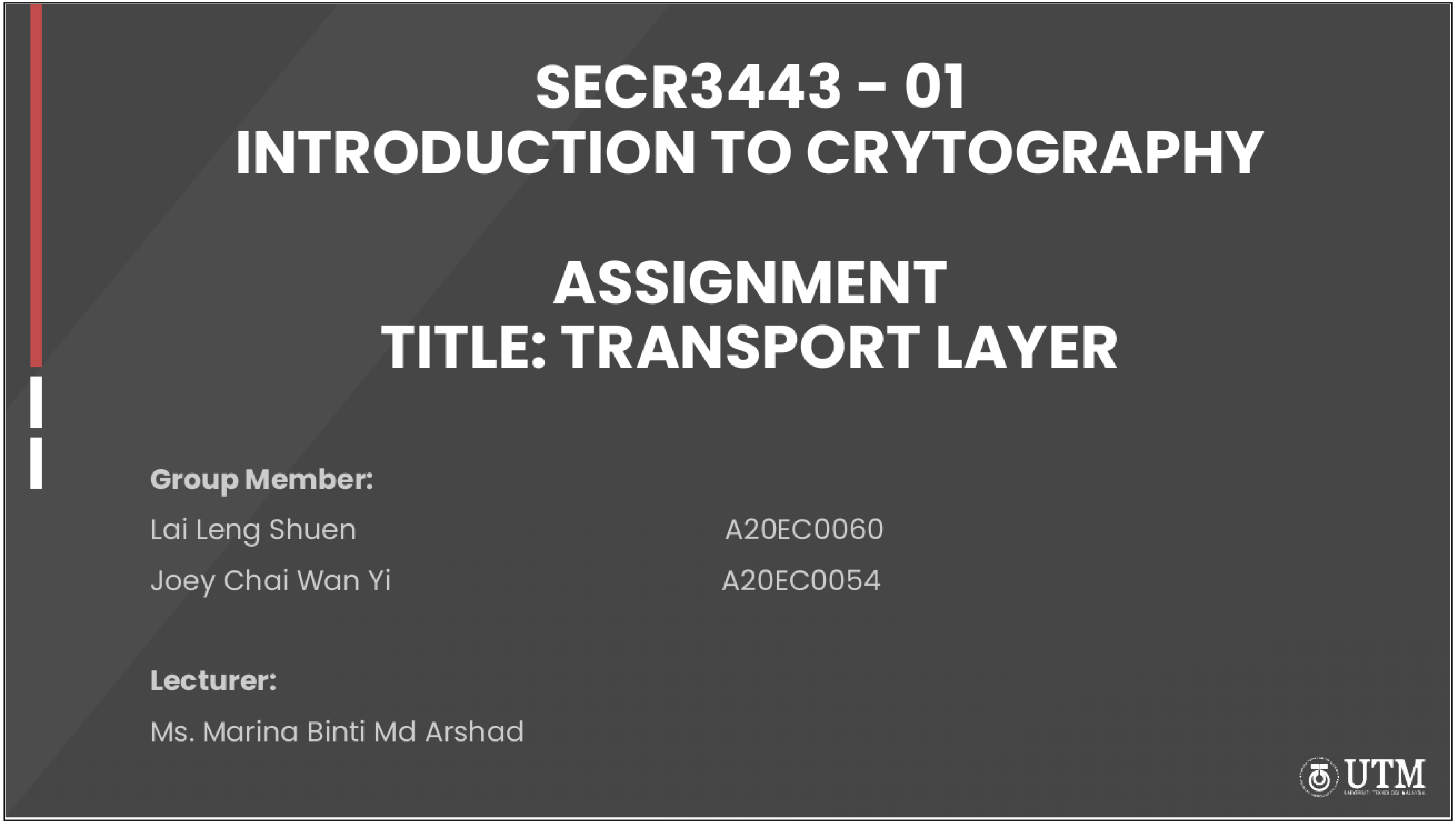
# a

*by* Chai Wan Yi Joey

**Submission date:** 28-Dec-2022 05:07PM (UTC+0800)
**Submission ID:** 1986801487
**File name:** CryptoAssignment.pdf (532.96K)
**Word count:** 1658
**Character count:** 9241



# SECR3443 – 01
# INTRODUCTION TO CRYTOGRAPHY

# ASSIGNMENT
# TITLE: TRANSPORT LAYER

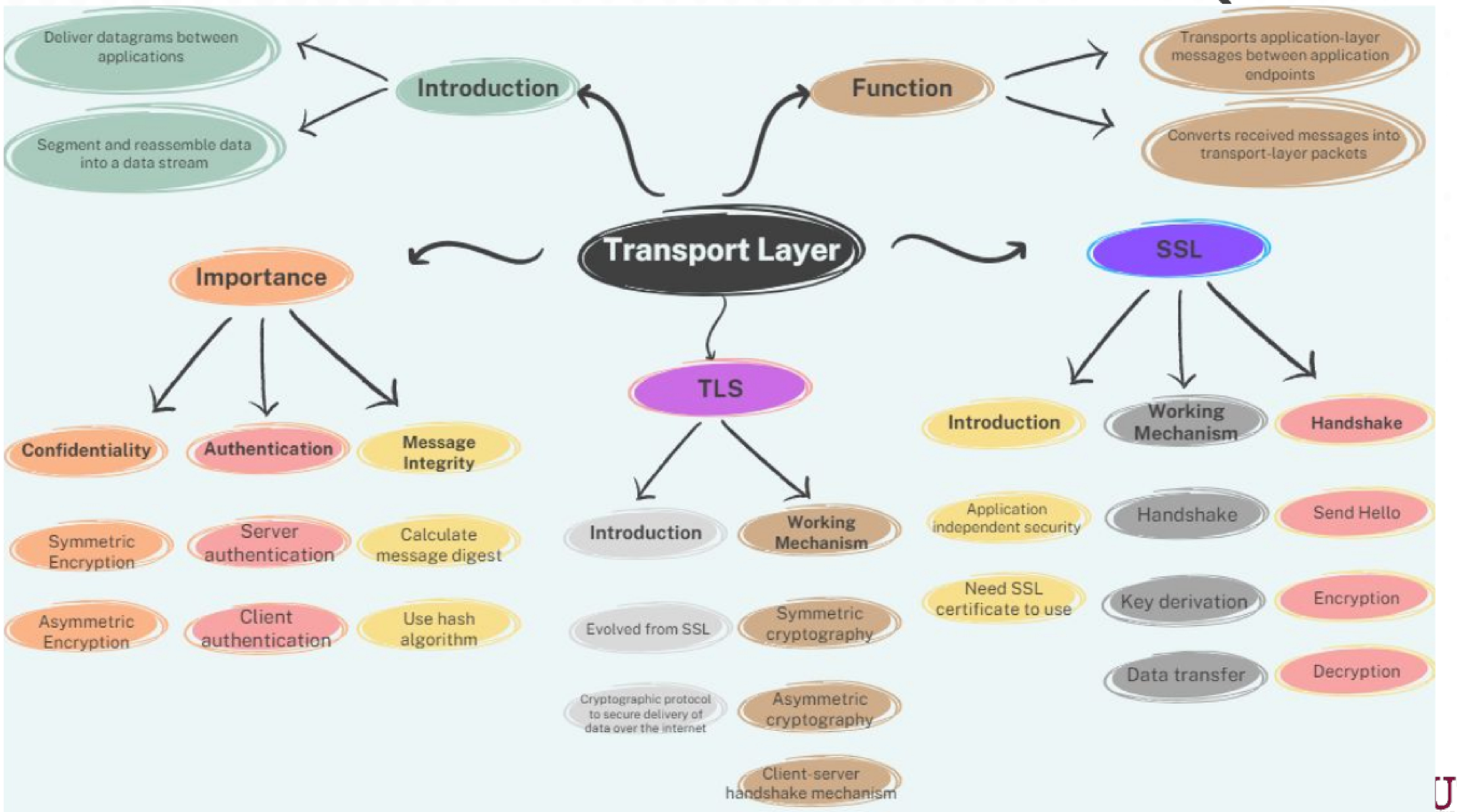
**Group Member:**

| | |
|---|---|
| Lai Leng Shuen | A20EC0060 |
| Joey Chai Wan Yi | A20EC0054 |

**Lecturer:**

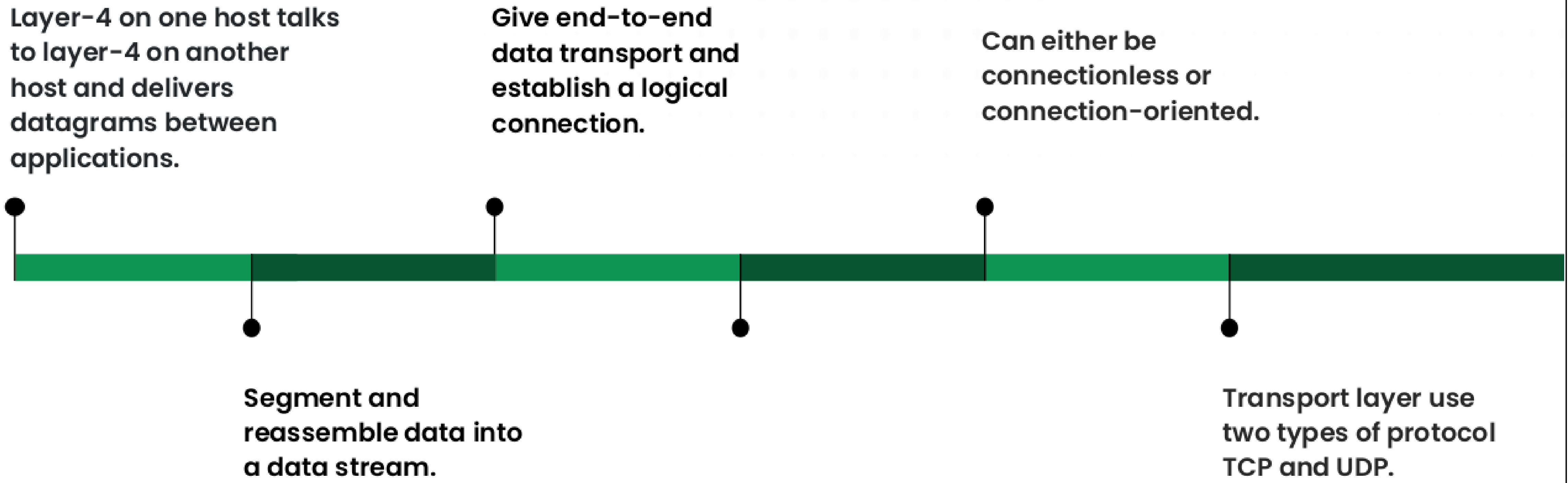
Ms. Marina Binti Md Arshad

# Overview (MindMap)



- Transport Layer
  - Introduction
    - Deliver datagrams between applications
    - Segment and reassemble data into a data stream
  - Function
    - Transports application-layer messages between application endpoints
    - Converts received messages into transport-layer packets
  - Importance
    - Confidentiality
      - Symmetric Encryption
      - Asymmetric Encryption
    - Authentication
      - Server authentication
      - Client authentication
    - Message Integrity
      - Calculate message digest
      - Use hash algorithm
  - TLS
    - Introduction
      - Evolved from SSL
      - Cryptographic protocol to secure delivery of data over the internet
    - Working Mechanism
      - Symmetric cryptography
      - Asymmetric cryptography
      - Client-server handshake mechanism
  - SSL
    - Introduction
      - Application independent security
      - Need SSL certificate to use
    - Working Mechanism
      - Handshake
      - Key derivation
      - Data transfer
    - Handshake
      - Send Hello
      - Encryption
      - Decryption

# Introduction to Transport Layer



Layer-4 on one host talks to layer-4 on another host and delivers datagrams between applications.

Segment and reassemble data into a data stream.

Give end-to-end data transport and establish a logical connection.

Can either be connectionless or connection-oriented.

Transport layer use two types of protocol TCP and UDP.

# Function of Transport Layer

1. **Transports application-layer messages between application endpoints**

2. **Converts received messages into transport-layer packets**

3. **Provide reliable or unreliable transport of application-layer messages**

- Reliable transport, TCP
  - *Segmentation, Flow control, Congestion control, Multiplexing, Demultiplexing*
- Unreliable transport, UDP
  - *Multiplexing, Demultiplexing, Checksum*

UTM

# Importance of SSL and TLS

## 01 Encryption

- Hide and transfer data of a web client and a web server.
- Data is secure during transport before it reaches the final destination.

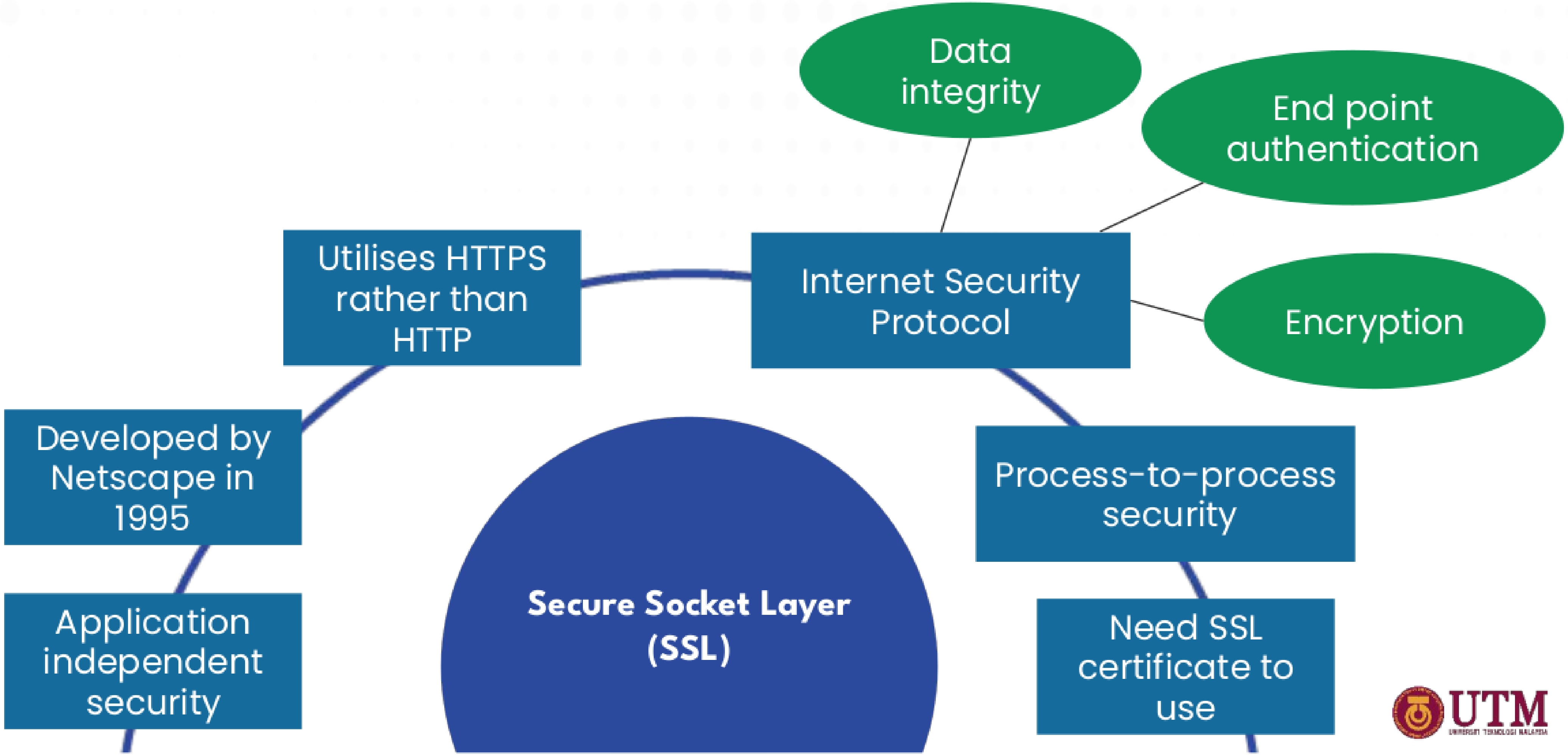
## 02 Authentication

- Data that is sent to and received from who they claim to be.
- Avoid malicious “man in the middle” imitating a site.

## 03 Integrity

- No alteration of data during transport before reaching the recipient.
- Data that is received without any loss and changes.

# What is Secure Socket Layer (SSL)?



Secure Socket Layer (SSL)

Utilises HTTPS rather than HTTP

Internet Security Protocol

Data integrity

End point authentication

Encryption

Developed by Netscape in 1995

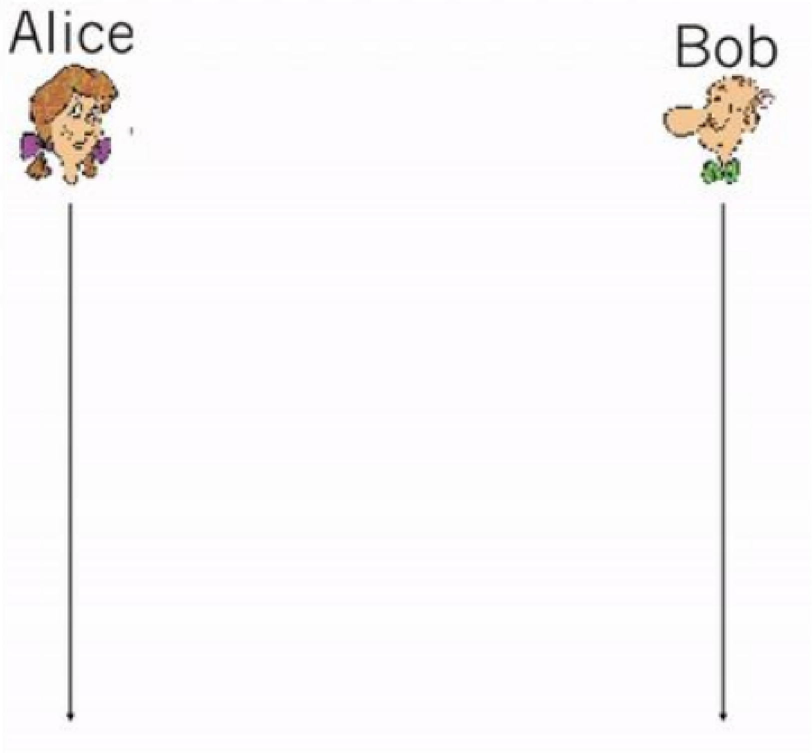
Process-to-process security

Application independent security

Need SSL certificate to use

# How SSL works?

- Based on digital certificates that have been digitally signed with public keys.
- Work in three stages: handshake, key derivation, and data transfer.
- SSL has its own socket API, which is similar to the standard TCP socket API.



# How SSL works? (Handshake)

**TCP Connection**

Alice needs to establish a TCP connection with Bob, verify that the receiver is really Bob, and send Bob a master secret key

**Send Hello**

Alice sends Bob a hello message. Bob then replies with his certificate, which contains his public key.

**Encryption**

Alice then generates a Master Secret (MS), encrypts the MS with Alice’s public key to create the Encrypted Master Secret (EMS), and sends the EMS to Bob.

**Decryption**

Bob decrypts the EMS with his private key to get the MS. After this phase, except for Alice and Bob, no one will know the master secret for this SSL session.

# How SSL works? (Key Derivation)

01 **Using separate key instead of master key**

- More safe

02 **Generate 2 keys types**

- Encryption key and MAC keys
- Alice generates E_A, M_A
- Bob generates E_B, M_B

03 **Uses of keys**

- E_A & E_B use to encrypt data
- M_A & M_B use to verify data integrity

# How SSL works? (Data Transfer)

To transfer data, huge messages are broken down into smaller records

The M_B key will be used to append the record, and the E_B key will be used to encrypt the record + MAC.

To ensure data integrity, a Message Authentication Code (MAC) is appended to each record, and the record appended with the MAC is encrypted.

# What is Transfer Layer Security (TLS)?

01 · Evolved from Secure Socket Layer (SSL).

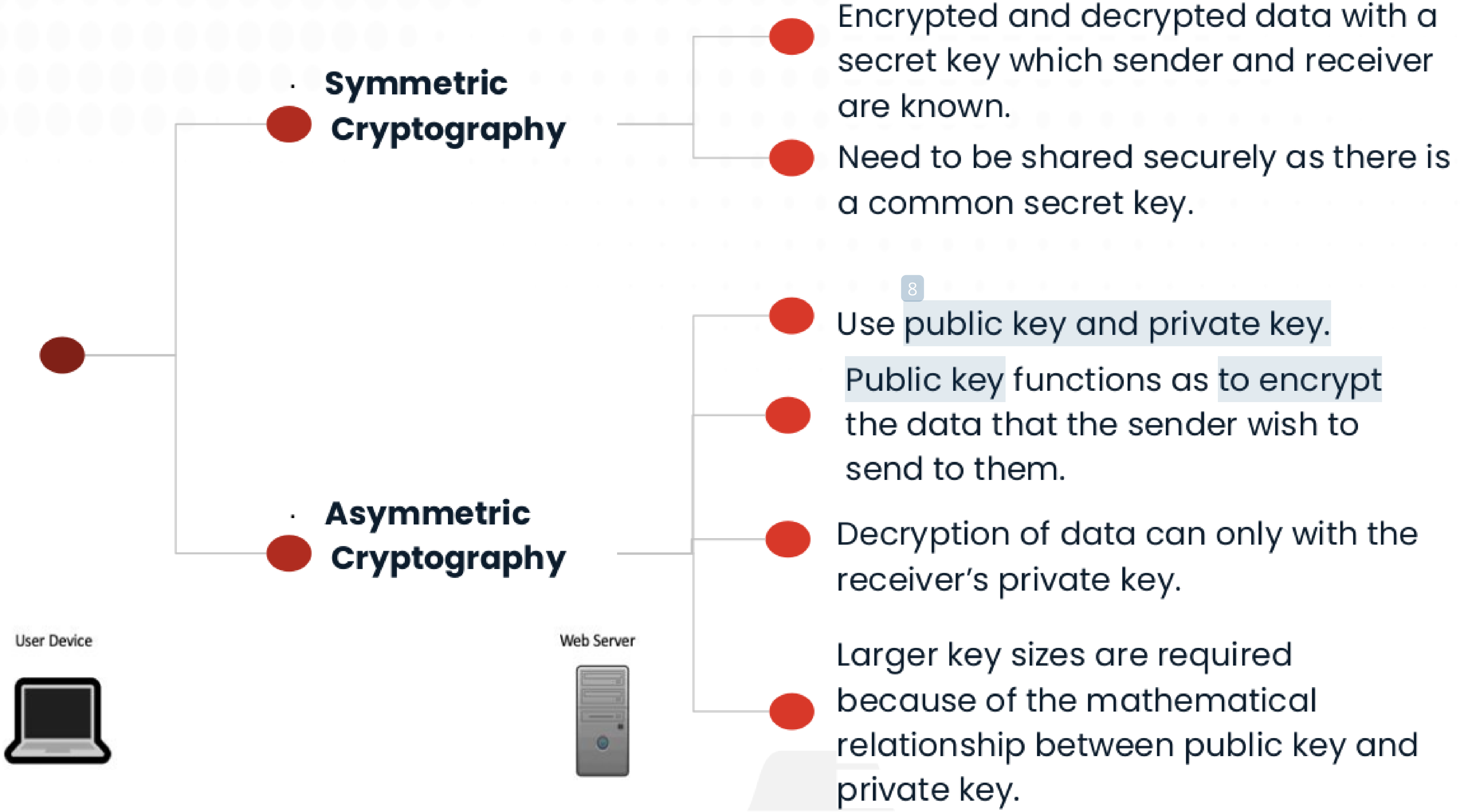
02 · Cryptographic protocol to secure delivery of data over the Internet.

03 · Protect users' data from security threats.

04 · Give confidentiality, message integrity and authentication between applications.

05 · Use in online transactions, files transfer, securing emails, a virtual private network (VPN) connections and instant messages.

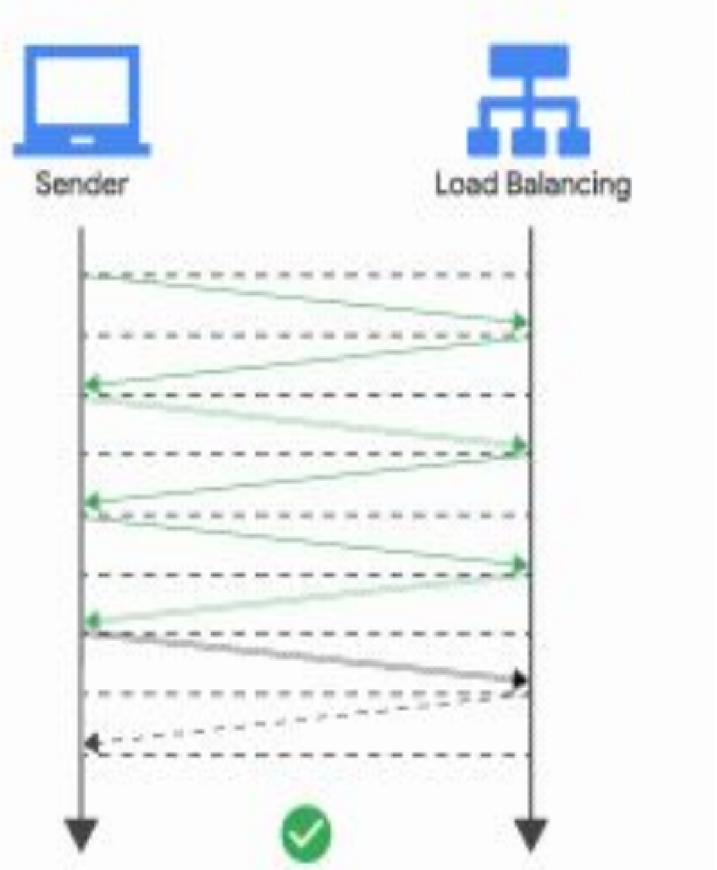
# How TLS works?



- Symmetric Cryptography
  - Encrypted and decrypted data with a secret key which sender and receiver are known.
  - Need to be shared securely as there is a common secret key.
- Asymmetric Cryptography
  - Use public key and private key.
  - Public key functions as to encrypt the data that the sender wish to send to them.
  - Decryption of data can only with the receiver's private key.
  - Larger key sizes are required because of the mathematical relationship between public key and private key.

## Client-server handshake mechanism:

- The client forwards a “hello” message to the server which include a list of available TLS versions. Then, it selects an appropriate cipher suite that generates a random number.
- The server forwards a message consists of TLS certificate and cipher suite that generated by itself.
- The client confirms the SSL certificate with the certificate authority.
- The client sends a pre-master key which encrypted by the public key while decryption can only done by the private key of the server.
- The server decrypts the pre-master key.
- The client and server produce session keys from pre-master keys and random numbers.
- The client and server forward a message together with the session key.
- The client and server create secure symmetric encryption.



## Confidentiality in SSL & TLS

### Symmetric Encryption

- Used for data encryption with the same algorithm and key.
- Need appropriate cipher suite for encryption.

### Asymmetric Encryption

- Used for transporting shared secret keys.
- No key distribution problem.

### Example

- The adversary can guess the messages although they do not know the content of messages.

# Message Integrity in SSL & TLS

01 **Calculate message digest**

- An irreversible cryptographic hash of the message.
- The sender computes the message digest, then sends them to the receiver.
- The receiver calculates the message hash and contrasts it with the one from the sender.
- If matches, the message is intact.

02 **Use hash algorithm for MAC computations**

- Need a secret encryption key during computing and verifying the hash.
- Give a guarantee to the receiver that the message originated from the sender.
- MD5, SHA-1 and SHA-256.

03 **Example**

- When Alice is talking to someone, only she and that someone can modify the data.

# Entity Authentication in SSL & TLS

| | | Description |
|---|---|---|
| 1 | Server Authentication | • Certificates (SSL certificates / TLS certificate) that confirm the identity of the server for server authentication<br>• SSL certificate certified by a publicly trusted certificate authority (CA) is trustworthy. |
| 2 | Client Authentication | • Server requests that the client produce a key pair for authentication<br>• SSL certificate's core private key is held by the client, not the server<br>• Before beginning encrypted communication, the server checks the private key.<br>• The server decrypts the data given by the client in the client authentication handshake using the public key of the client certificate.<br>• The exchange of completely encrypted communications using a private key is used to verify authentication. |

# Conclusion

In a nutshell, we covered the details of the transport layer, what SSL and TLS are, their role in confidentiality, message integrity, and entity authentication. SSL and TLS are essential to web security as they give integrity and security yo network devices. For example, e-commerce business is closely related to our daily life.

# Acknowledgement

We would like to thank you Ms. Marina Binti Md Arshad, who
provided us with appropriate guiding principles for this group project and frequent consultations throughout the project.

# Reference

Alnatheer, M. A. (2014). Secure Socket Layer (SSL) Impact on Web Server Performance. *Journal of Advances in Computer Networks*, *2*(3), 211–217. https://doi.org/10.7763/jacn.2014.v2.114

Bhiogade, M. S. (2002). *Secure Socket Layer*.

Boyd, C., Hale, B., Mjølsnes, S. F., & Stebila, D. (2016, February). From stateless to stateful: Generic authentication and authenticated encryption constructions with application to TLS. In Cryptographers' Track at the RSA Conference (pp. 55-71). Springer, Cham.

Chou, W. (2002). Inside SSL: The secure sockets layer protocol. *IT Professional*, *4*(4), 47–52. https://doi.org/10.1109/MITP.2002.1046644

Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. Applied Computing and informatics, 10(1-2), 68-81.

Dastres, R., & Soori, M. (2020). Secure Socket Layer (SSL) in the Network and Web Security. In *Interna-tional Journal of Computer and Information Engineering*. https://hal.archives-ouvertes.fr/hal-03024764

Dierks, T., & Allen, C. (1999). The TLS protocol version 1.0 (No. rfc2246).

D. V. Bhatt, S. Schulze and G. P. Hancke, "Secure Internet access to gateway using secure socket layer," in IEEE Transactions on Instrumentation and Measurement, vol. 55, no. 3, pp. 793-800, June 2006, doi: 10.1109/TIM.2005.862009.

# Reference

G. Apostolopoulos, V. Peris and D. Saha, "Transport layer security: how much does it really cost?," IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320), 1999, pp. 717-725 vol.2, doi: 10.1109/INFCOM.1999.751458.

International Business Machines Corporation (IBM). (2022). *Securing IBM WebSphere MQ*.

Ivanov, O., Ruzhentsev, V., & Oliynykov, R. (2018, October). Comparison of modern network attacks on TLS protocol. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 565-570). IEEE.

Jager, T., Kohlar, F., Schäge, S., & Schwenk, J. (2017). Authenticated confidential channel establishment and the security of TLS-DHE. Journal of Cryptology, 30(4), 1276-1324.

Kwon, E. K., Cho, Y. G., & Chae, K. J. (2001, January). Integrated transport layer security: end-to-end security model between WTLS and TLS. In Proceedings 15th International Conference on Information Networking (pp. 65-71). IEEE.

Meyer, C., & Schwenk, J. (2013). Lessons learned from previous SSL/TLS attacks-a brief chronology of attacks and weaknesses. Cryptology ePrint Archive.

M. K. Ferst, H. F. M. de Figueiredo, G. Denardin and J. Lopes, "Implementation of Secure Communication With Modbus and Transport Layer Security protocols," 2018 13th IEEE International Conference on Industry Applications (INDUSCON), 2018, pp. 155-162, doi: 10.1109/INDUSCON.2018.8627306.

# Reference

Rescorla, E. (2018). The transport layer security (TLS) protocol version 1.3 (No. rfc8446).

Robinson, P. (2001). *Understanding Digital Certificates and Secure Sockets Layer (SSL)*. http://www.entrust.com/

SCharjan MsPriyanka Bochare Yogesh RBhuyar, M. S. (2013). An Overview of Secure Sockets Layer. *International Journal Of Computer Science And Applications*, *6*(2). www.researchpublications.org

Sirohi, P., Agarwal, A., & Tyagi, S. (2016, October). A comprehensive study on security attacks on SSL/TLS protocol. In 2016 2nd international conference on next generation computing technologies (NGCT) (pp. 893-898). IEEE.

S. Turner, "Transport Layer Security," in IEEE Internet Computing, vol. 18, no. 6, pp. 60-63, Nov.-Dec. 2014, doi: 10.1109/MIC.2014.126.

Weaver, A. C. (2006). Secure Sockets Layer. *Computer*, *39*(4), 88–90. https://doi.org/10.1109/mc.2006.138

a

ORIGINALITY REPORT

| 16% | 13% | 3% | 12% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | archive.org<br>Internet Source | 8% |
| 2 | Submitted to Edith Cowan University<br>Student Paper | 2% |
| 3 | Submitted to University of Leicester<br>Student Paper | 1% |
| 4 | Submitted to Kingston University<br>Student Paper | 1% |
| 5 | www.ieee-security.org<br>Internet Source | 1% |
| 6 | cps-vo.org<br>Internet Source | 1% |

| | | |
|---|---|---|
| 7 | ebin.pub<br>Internet Source | 1 % |
| 8 | www.ee.ucla.edu<br>Internet Source | 1 % |
| 9 | "M817 Block 2 week 10 asymmetric encryption WEB097768", Open University<br>Publication | 1 % |
| 10 | Submitted to University of York<br>Student Paper | 1 % |

| | | | |
|---|---|---|---|
| Exclude quotes | On | Exclude matches | < 7 words |
| Exclude bibliography | On | | |