SC3030 TERM PAPER

NETWORK SECURITY PROTOCOLS

LIM DONG WAN

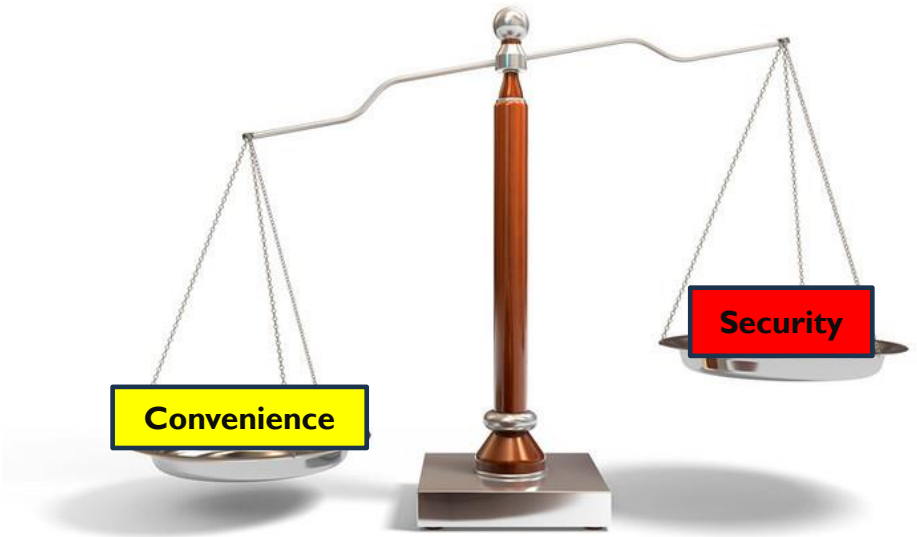
U2122455D

OVERVIEW

- Introduction
- Significance of Network Security
- Network Security Vulnerability Issues
- Network Security Protocols:
  - Internet Protocol Security (IPSec)
  - Transport Layer Security (TLS)
- IPSec VS TLS
- Future of Network Security

INTRODUCTION

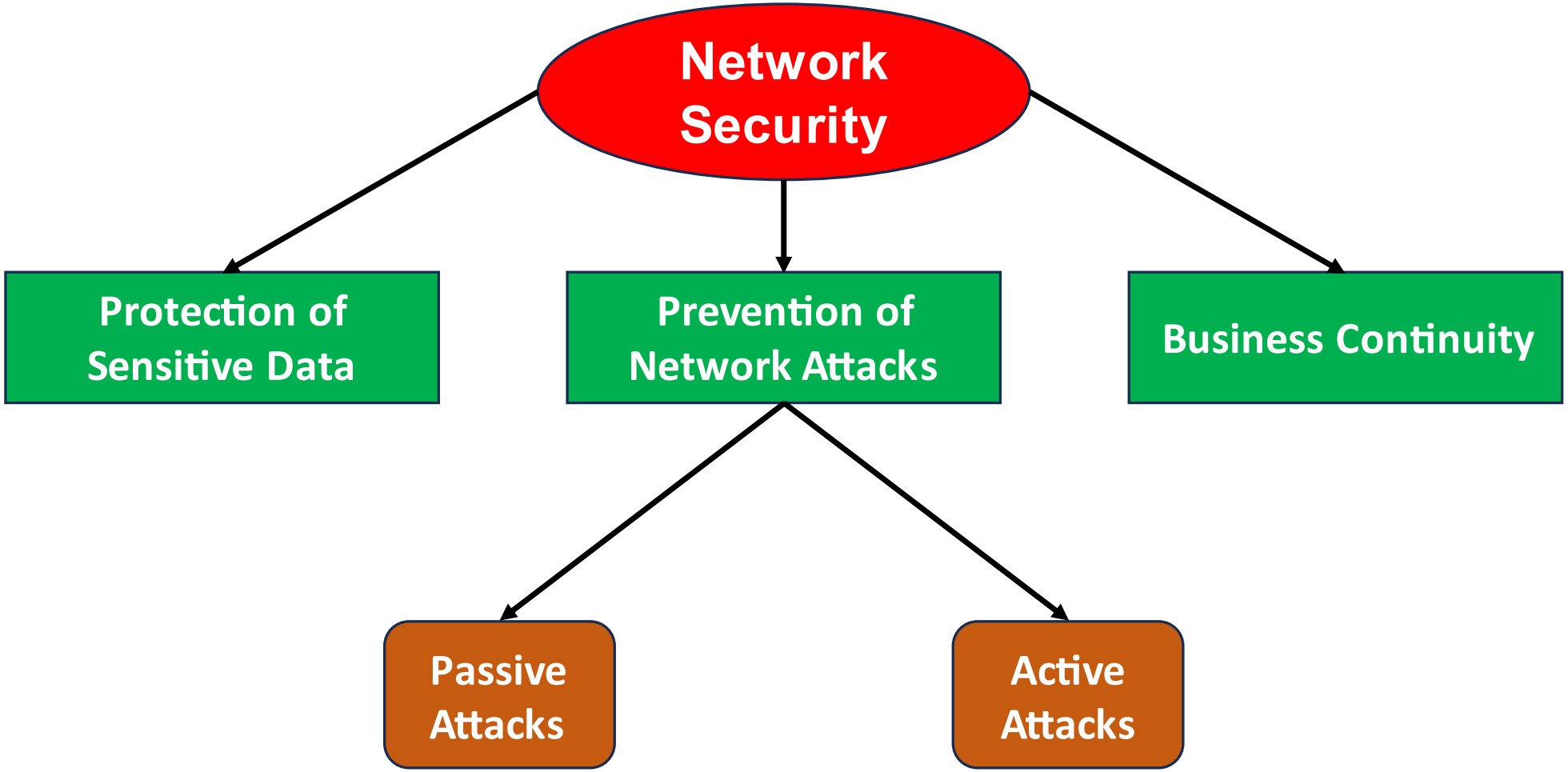
- Internet has become part and parcel of people's lives:
  - COVID-19 has made the Internet ubiquitous
- Network environment has become more complex
- Emerging security threats make computer networks more vulnerable



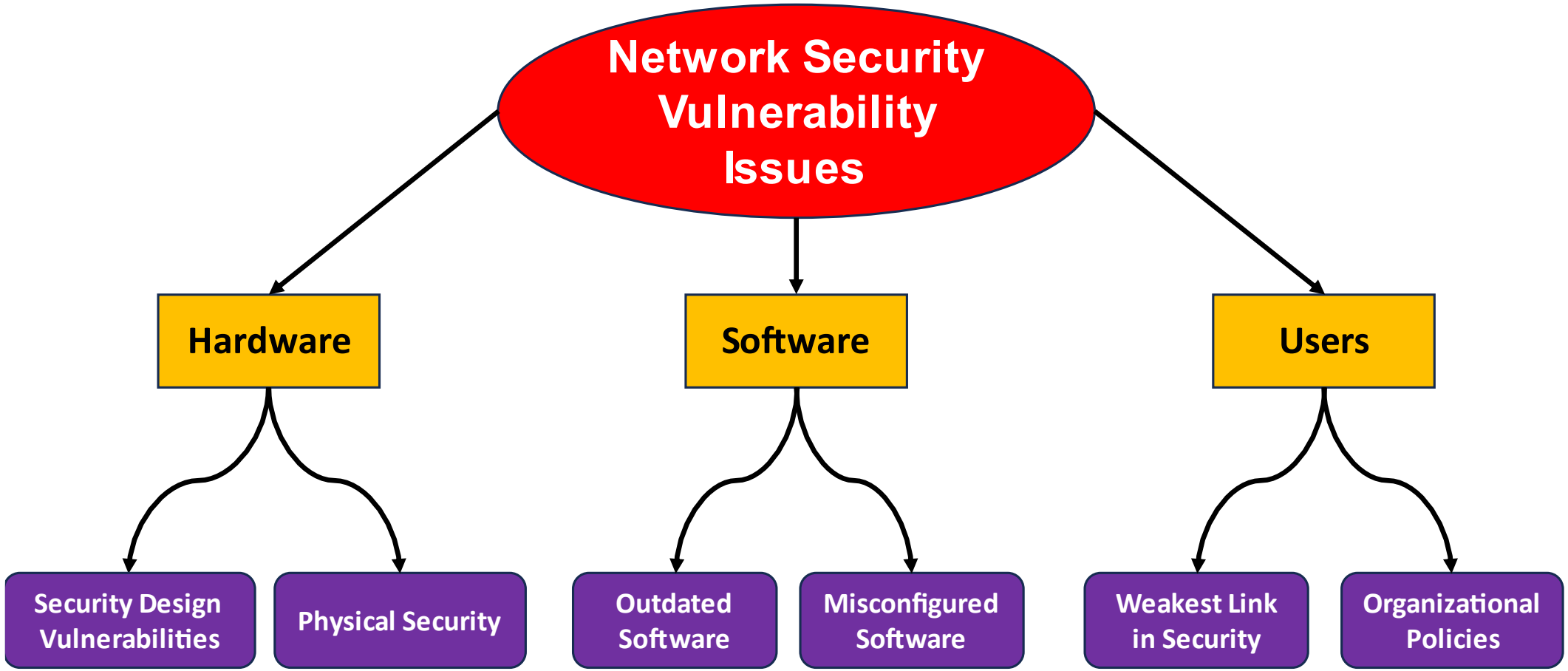
NETWORK SECURITY

- Essential subset of computer security
- Establishes a robust communication network and implements mitigatory measures:
  - Confer the **CIA triad - Confidentiality, Integrity, Availability** – of data
  - Prevent unauthorized access and malicious actions by external parties
  - Safeguard network connection, resources and assets
- Must continuously evolve to tackle present cybersecurity challenges

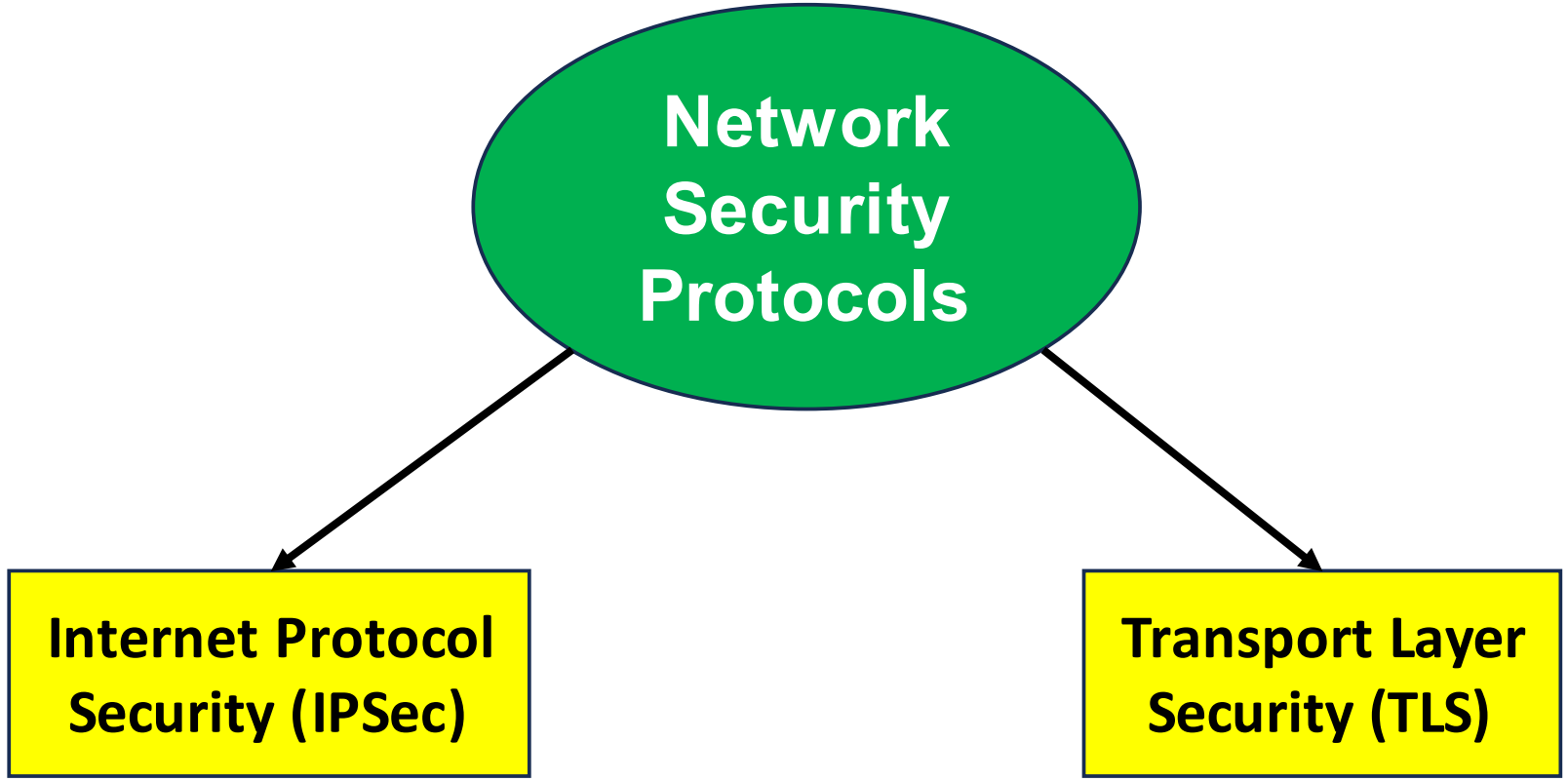
SIGNIFICANCE OF NETWORK SECURITY



NETWORK SECURITY VULNERABILITY ISSUES

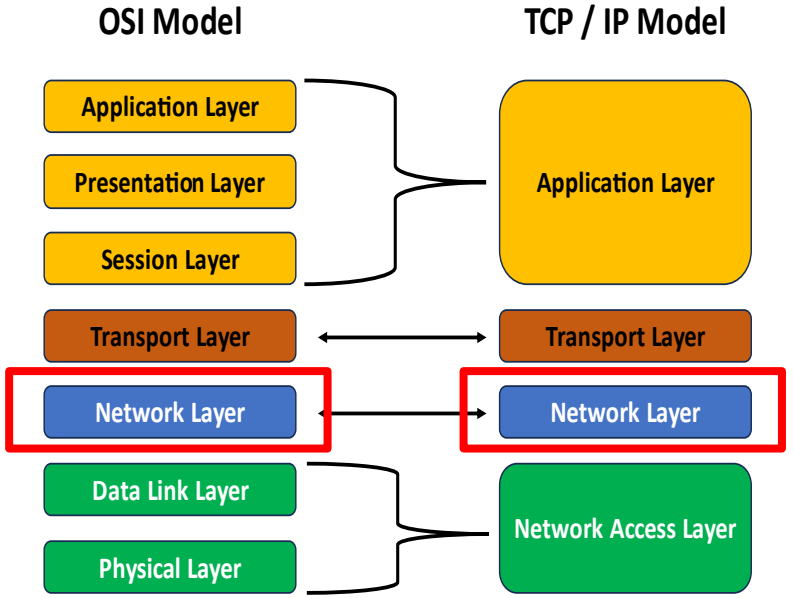


NETWORK SECURITY PROTOCOLS



IPSEC – OVERVIEW

- Standard solution for strengthening data privacy, particularly in wireless networks
- Objectives:
  - Create a shareable set of security protocols.
  - Allow key exchange for authentication.
  - Encrypt / Hash data for secure data transmission across a network.



IPSEC – FUNCTIONS

Internet Protocol Security

Core Protocols

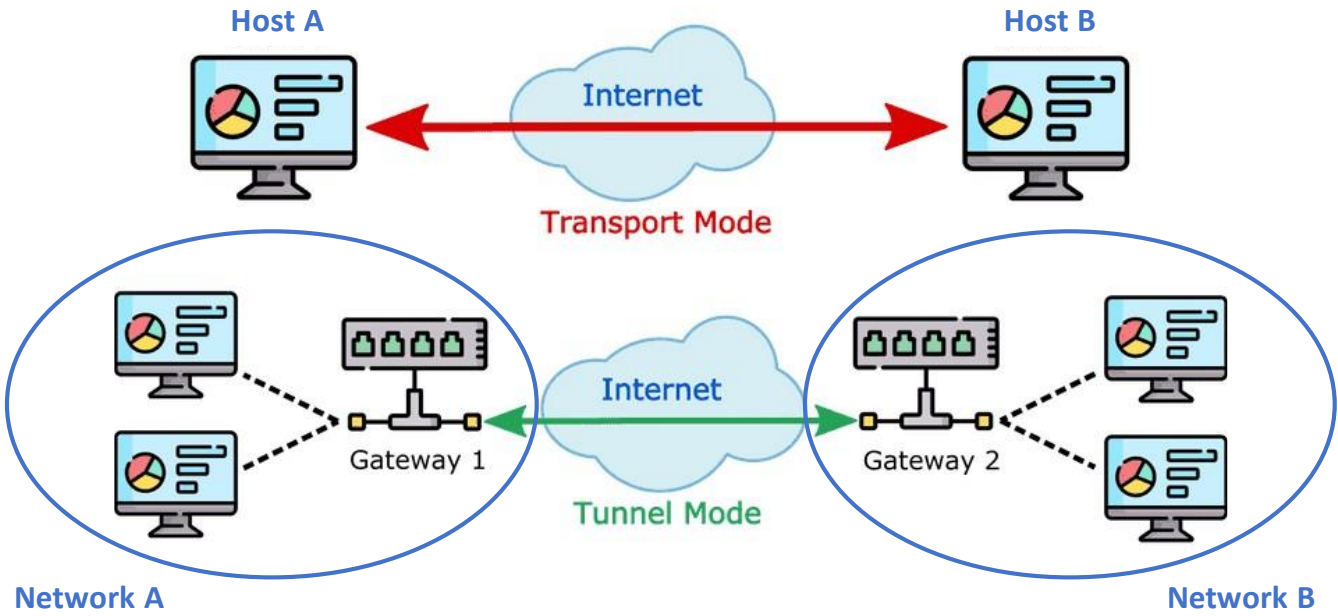
- IPSec Authentication Header
- Encapsulating Security Payload

Support Components

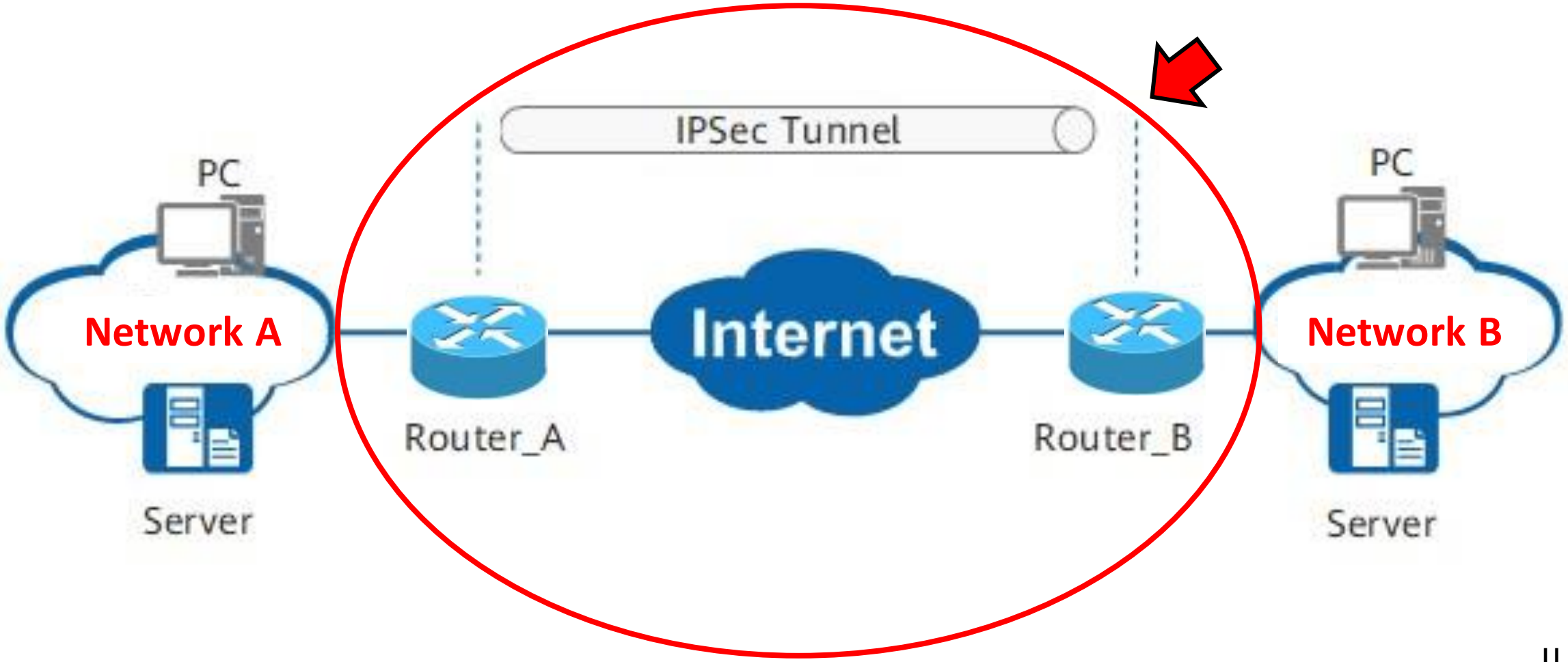
- Encryption / Hashing Algorithms
- Security Policies / Security Associations
- Internet Key Exchange / Key Management

IPSEC – OPERATION MODES

IPSec Tunnel Mode	New IP	IPSec	IP	TCP	Payload
IPSec Transport Mode		IP	IPSec	TCP	Payload
Without IPSec			IP	TCP	Payload

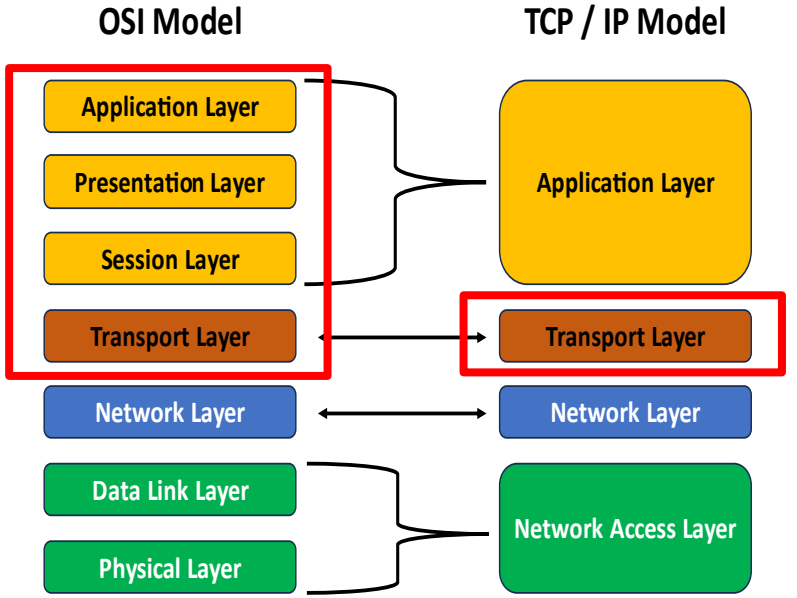


IPSEC – REAL-WORLD APPLICATION

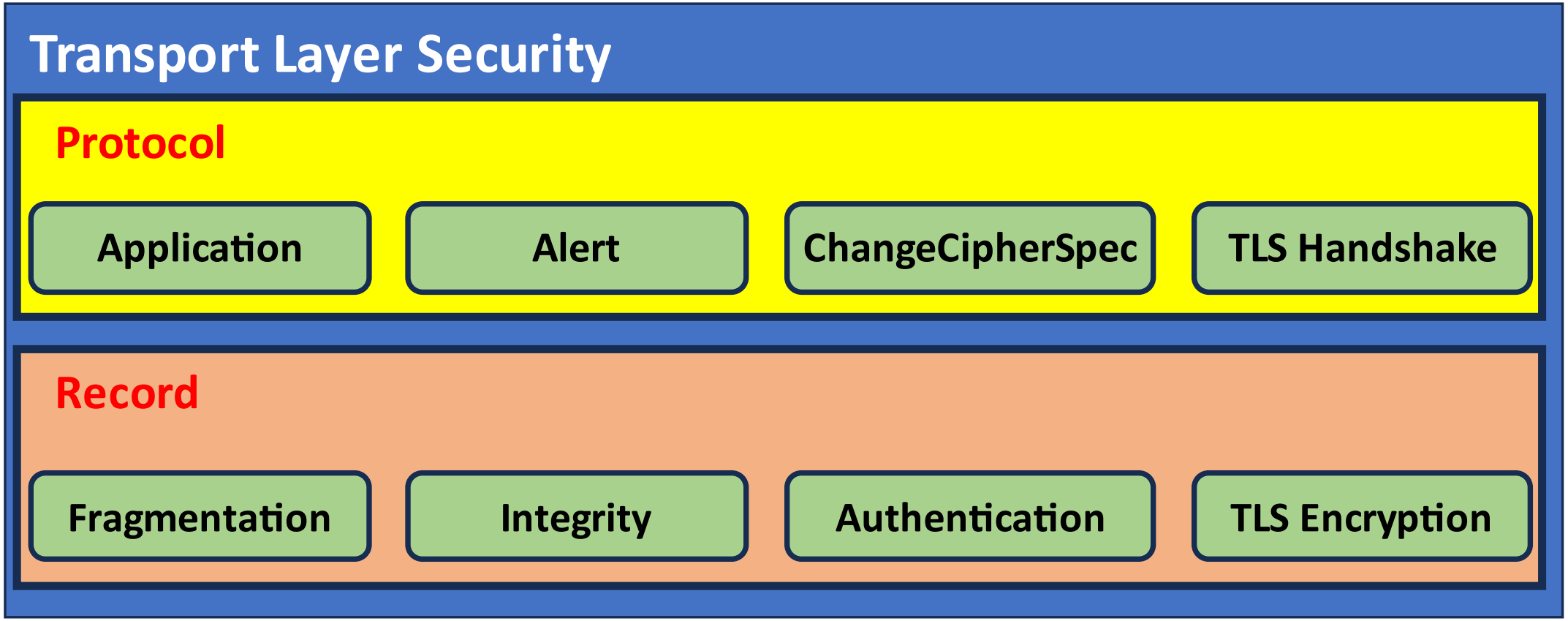


TLS – OVERVIEW

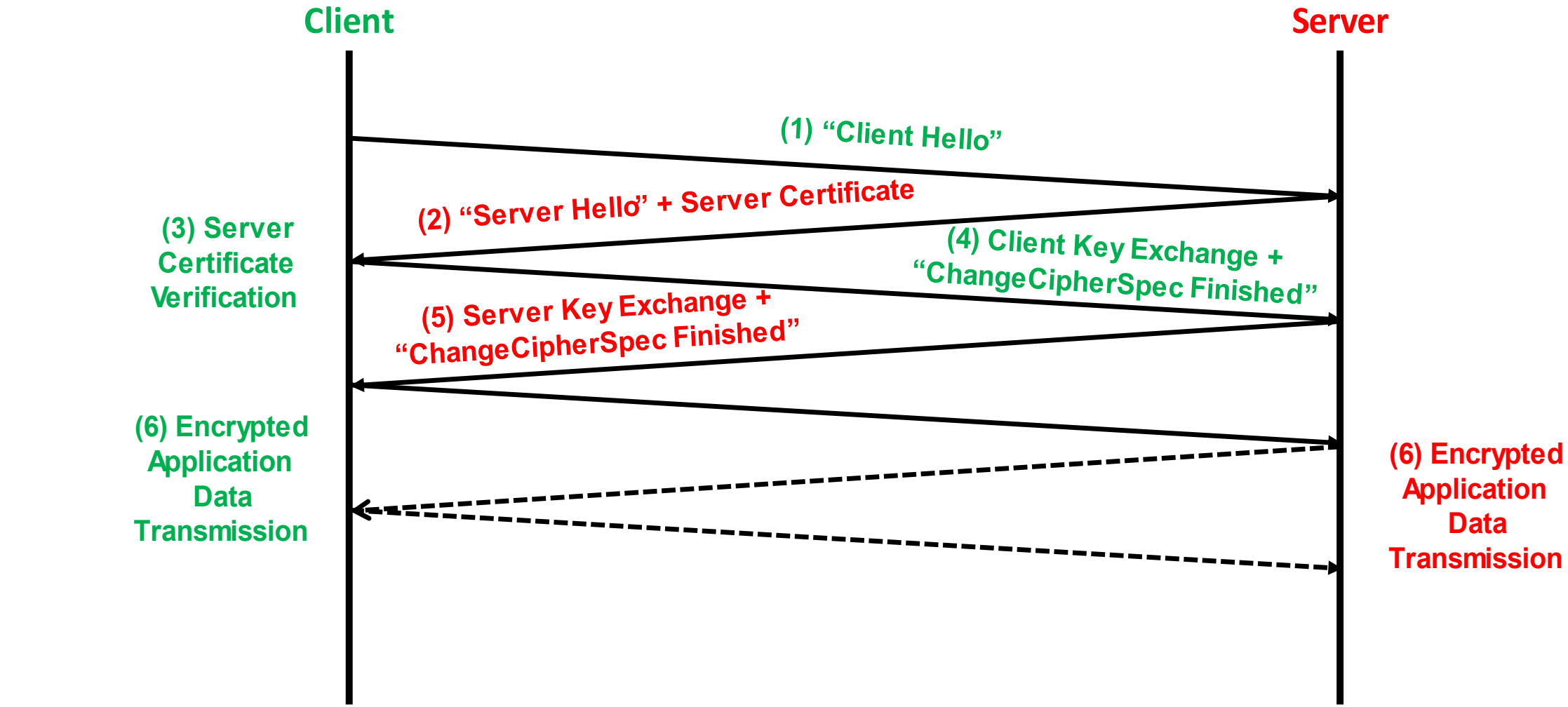
- Supersedes Secure Socket Layer (SSL) as the new security standard for web security today
- Latest version: **TLS 1.3** (since 2017)
- Objectives:
  - Authenticate and validate parties that are exchanging information with one another.
  - Encrypt data transmission between client and server for confidentiality.
  - Safeguard data integrity between client and server.



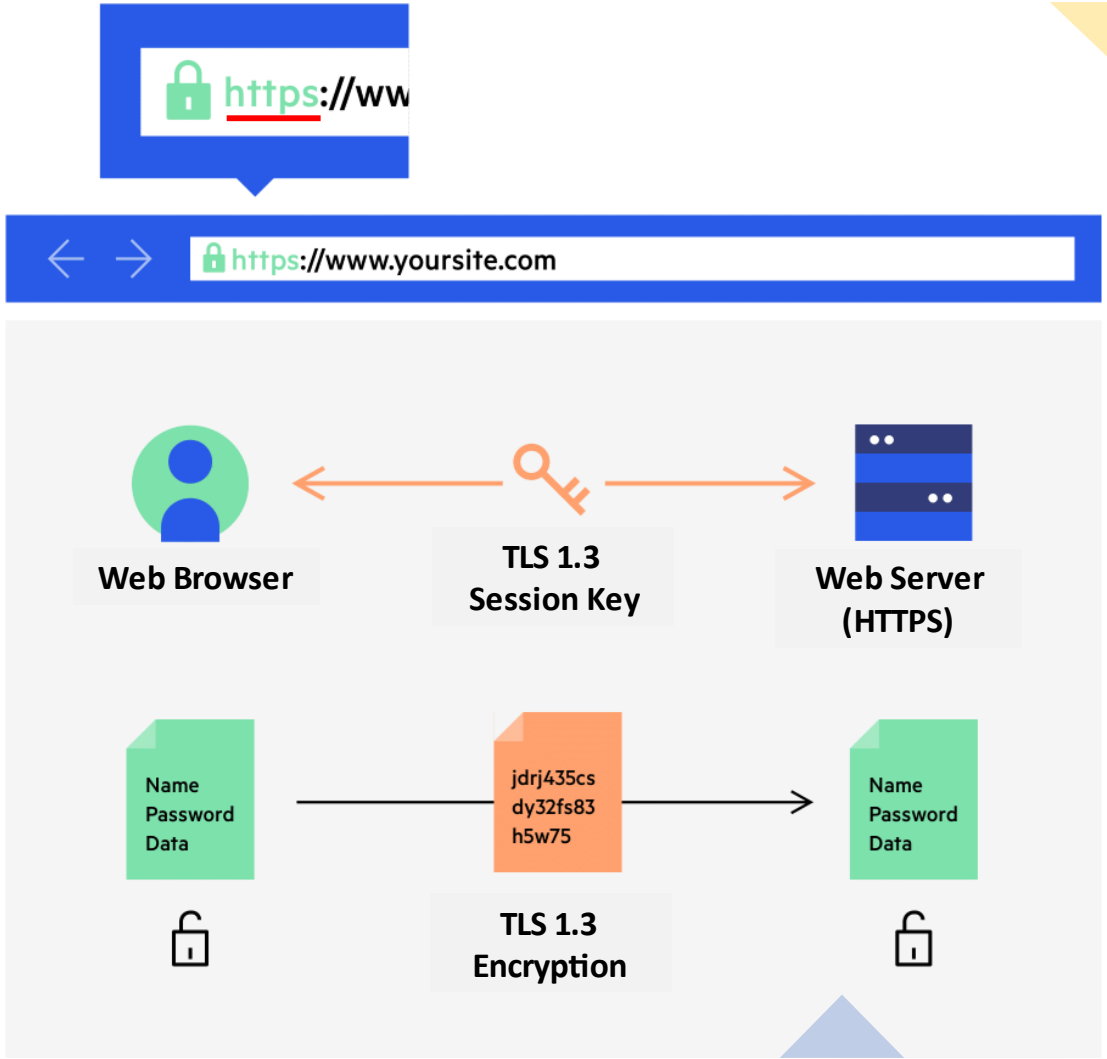
TLS - FUNCTIONS



TLS – TLS HANDSHAKE



TLS – REAL-WORLD APPLICATION



IPSEC VS TLS

	IPSec	TLS
Advantages	• Transparent to end users • Independent of the applications used with only operating system modifications needed	• More secure compared to IPSec • Lower latency and overhead than IPSec
Disadvantages	• Higher latency and overhead than TLS • Less secure than TLS	• Few platforms support TLS 1.3 • Requires modification to applications and operating system
Types of Attacks the Protocol is Vulnerable To	• Man-in-the-Middle (MitM) • DoS • VPN tunnel compromise • Cross-protocol attack	• Application Layer Protocol Confusion Attack (ALPCA) • Reflection ("Selfie") attack • Bleichenbacher's attack • Forced downgrade attacks

FUTURE OF NETWORK SECURITY

- Security infrastructure must be more robust and adaptable than before
- Integration of Artificial Intelligence and Machine Learning into Network Security

END