Daffodil International University

Topic 3: Web Security

Topic 3 – Lecture 1:

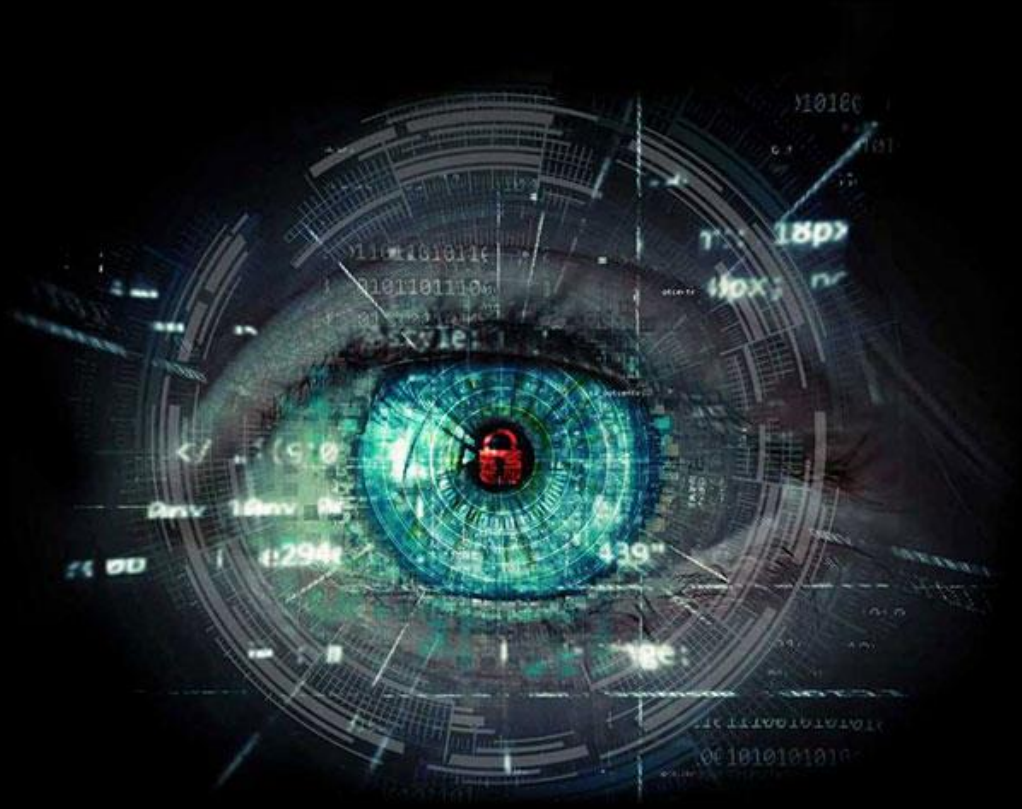
Web Security & IPSEC

Network Security and Cryptography

Web Security Topic 3 - 3.2

Scope and Coverage

This topic will cover:



01 Overview of web security

02 IPSEC

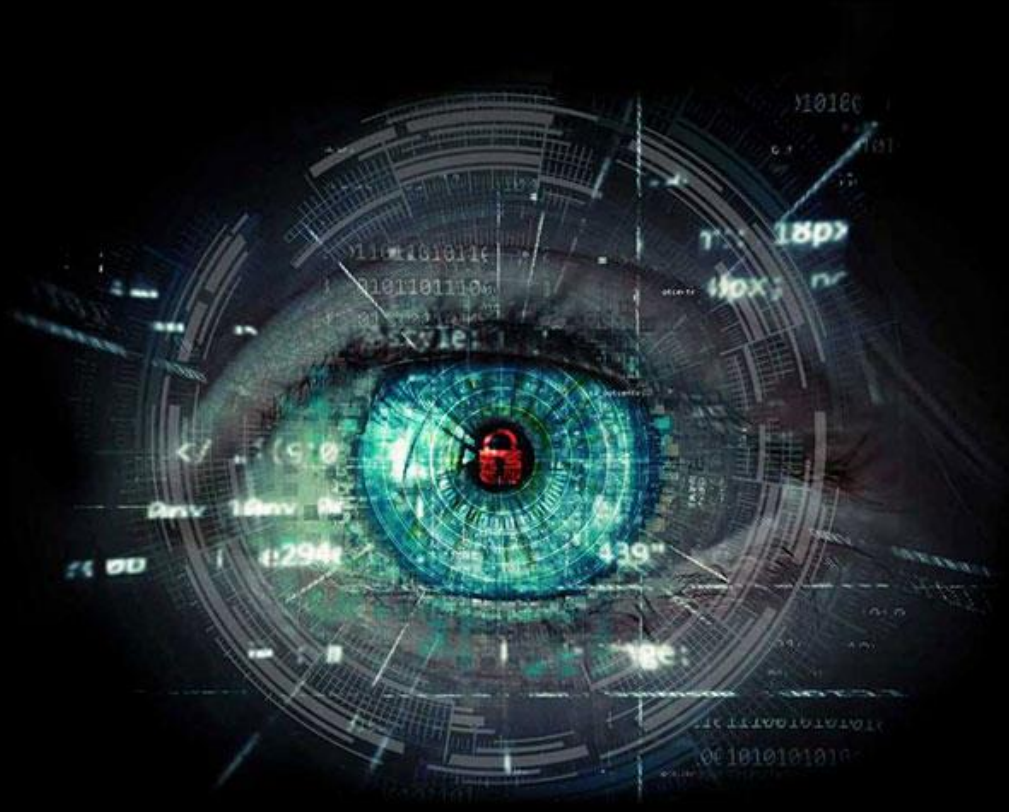
03 SSL/TLS

04 HTTPS

Web Security Topic 3 - 3.3

Learning Outcomes

By the end of this topic students will be able to:



- Explain the concept of web security with SSL/TLS
- Demonstrate applying for and deploying a Digital Certificate

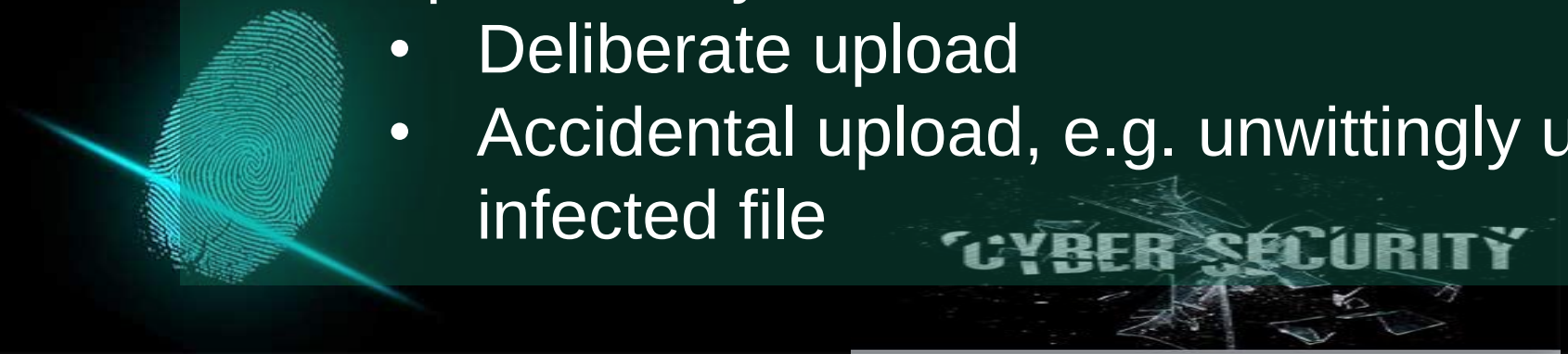
Web Security

- The Web presents us with some security issues that may not be present in other networks:
    - Two-way systems
    - Multiple types of communication
    - Importance to business
    - Complex software
    - Multiple connections to a server
    - Untrained users

Two-way Systems

- The Web works on a client-server model that allows communication in both directions:
  - Server sends files to clients
  - Clients send files to servers

- Servers must be protected from malicious content uploaded by clients:
  - Deliberate upload
  - Accidental upload, e.g. unwittingly uploading an infected file

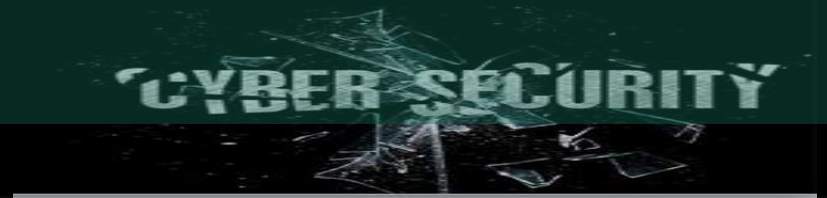


Multiple Types of Communication

- The web does not deal with a limited small number of file types:
  - Text
  - Image
  - Video
  - Sound …
- The web delivers real-time content.
- Multiple file types = multiple security threats

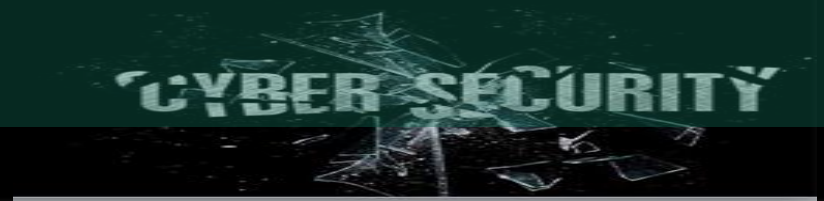
Importance to Business

- Used to supply corporate information
- Used to supply product/service information
- Used for business transactions including financial transactions
  - banking, online shops, ordering systems, etc.
- If web servers are compromised, there may be very serious consequences to a business.
  - Loss of money & trade
  - Loss of reputation



Complex Software

- Servers are relatively easy to set up and configure.
- It is simple to create web content.
  - Even complex looking web applications are often simple to create
- This simplicity is made possible by complex underlying software.
- Complex software often has undetected security holes.
  - You can be sure that someone will detect them!

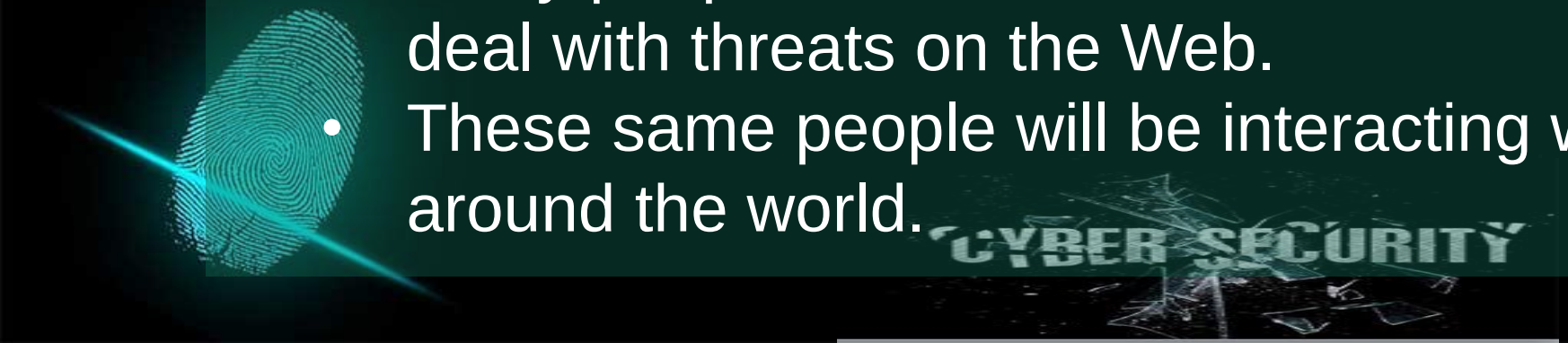


Multiple Connections

- The Web works because there are multiple connections to a server.
- Different servers are connected to each other.
- What happens if a server is subverted and a malicious attacker gains control?
  - How many clients will be affected?
  - How many other servers will be affected?
- An attack could have widespread consequences.

Untrained Users

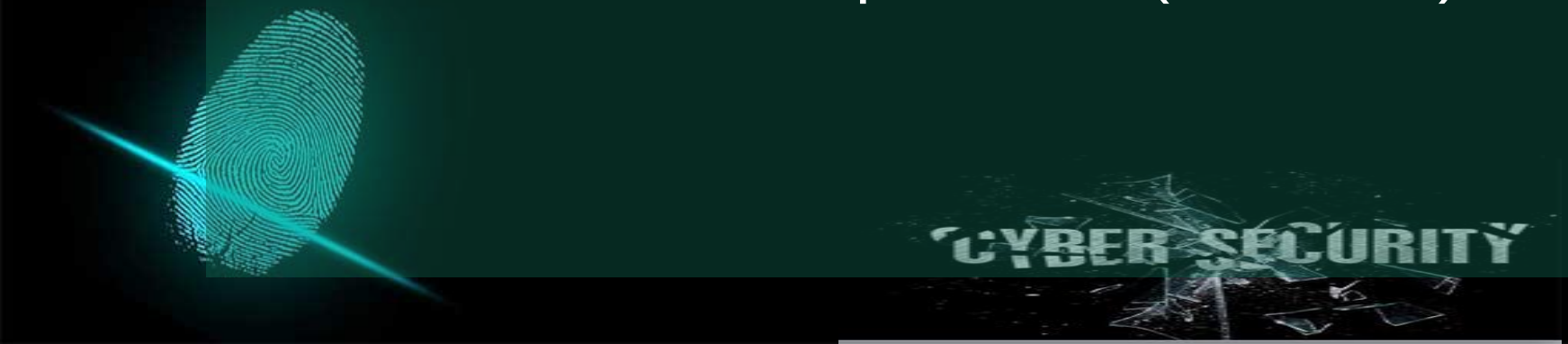
- The Web is used by many, many clients with no training or understanding of security issues.
  - How many people surf the Internet without antivirus software?
  - Add in the people who have out of date virus definitions
- Many people do not have the tools or knowledge to deal with threats on the Web.
- These same people will be interacting with servers around the world.



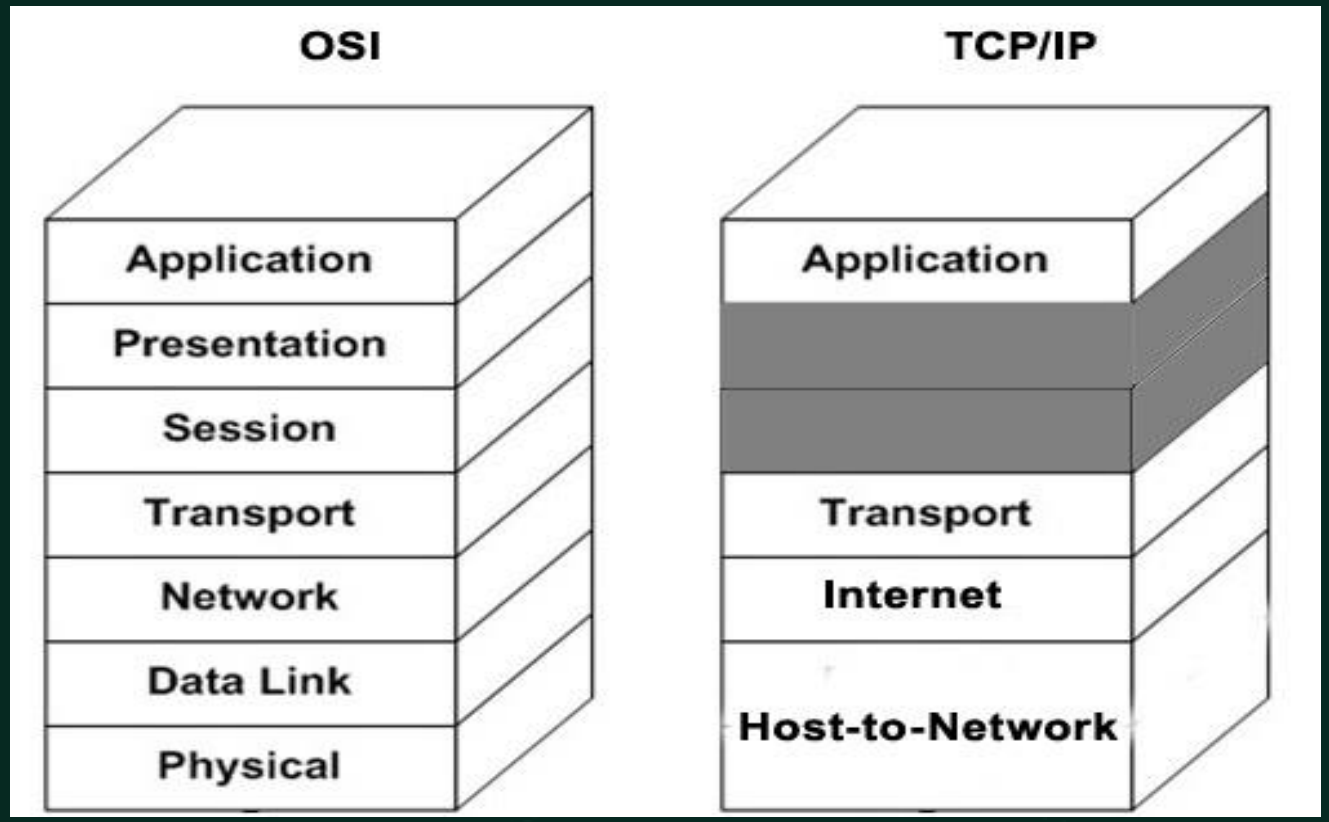
Traffic Security

- Maintaining the security of a server as a piece of hardware is not fundamentally different to general computer security.

- We will concentrate on the security of Web traffic
  - At the Network level (IPSec)
  - At the Transport level (SSL/TLS)

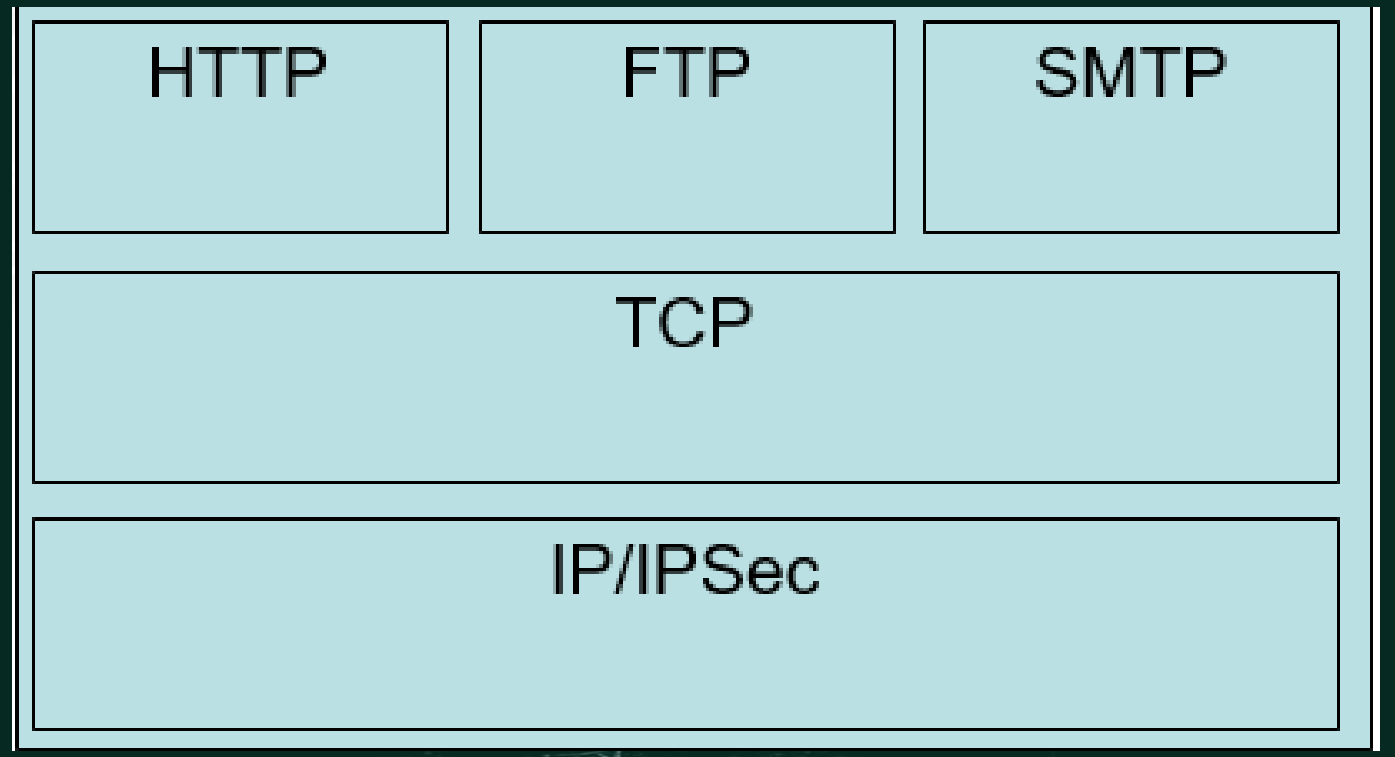


TCP/IP and the OSI Model



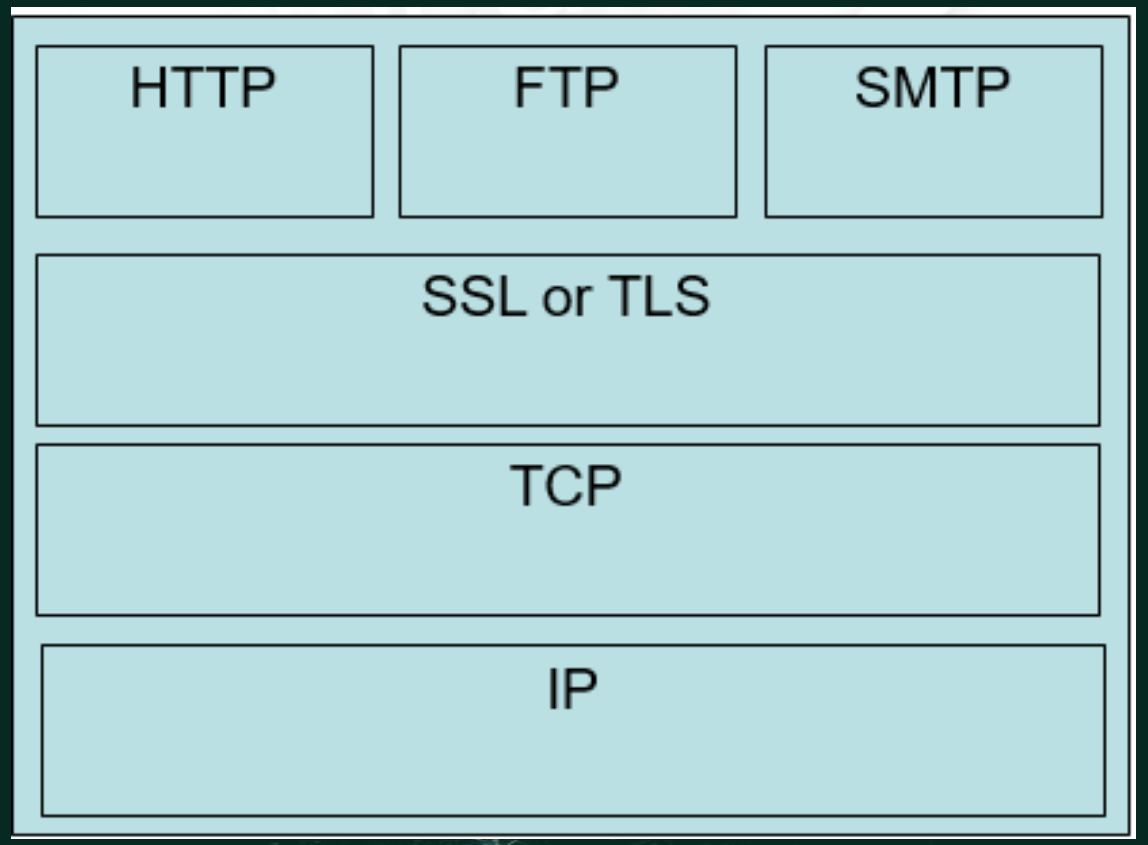
Network Level Security

IPSec



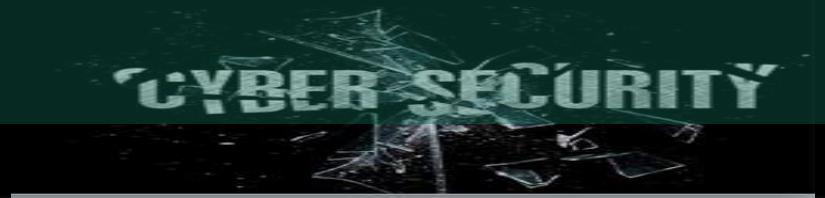
Digital Signature

SSL/TLS



IP Security (IPSec)

- Provides security services at the IP layer for other TCP/IP protocols and applications to use
- Provides the tools that devices on a TCP/IP network need in order to communicate securely
  - When two devices wish to securely communicate, they create a secure path between themselves that may traverse across many insecure intermediate systems.



Steps for an IPSec Connection

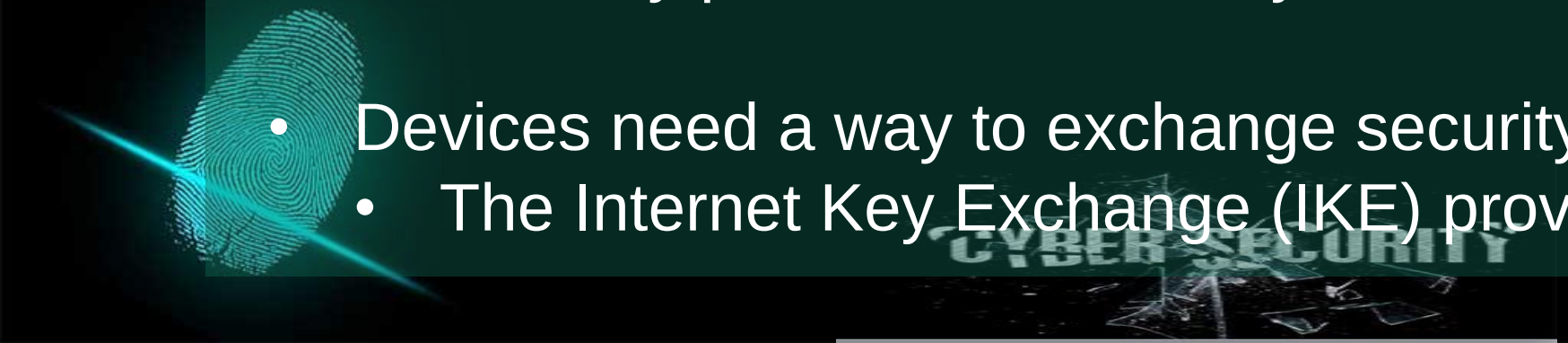
1. Agree on a set of security protocols to use so that data is in a format both parties can understand.
2. Decide on an encryption algorithm to use in encoding data.
3. Exchange the keys that are used to decrypt the cryptographically encoded data.
4. Use the protocols, methods and keys agreed upon to encode data and send it across the network.

IPSec Core Protocols

- IPSec Authentication Header (AH)
  - Provides authentication services
  - Verifies the originator of a message
  - Verifies that the data has not been changed on route
  - Provides protection against replay attacks
- Encapsulating Security Payload (ESP)
  - AH ensures integrity but not privacy
  - Datagram can be further protected using ESP
  - Encrypts the payload of the IP datagram

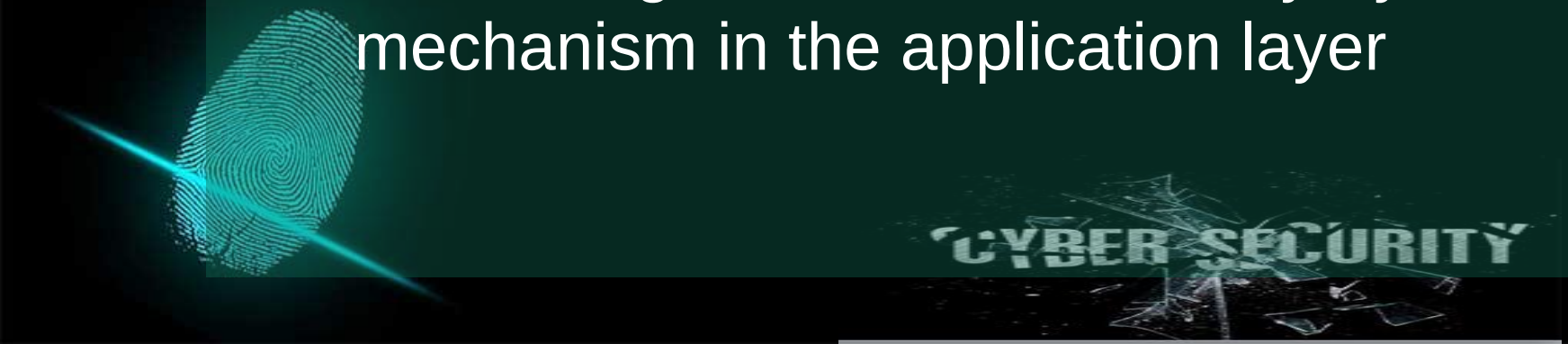
Support Protocols & Mechanisms

- The core protocols are quite generic and rely on other protocols and mechanisms to be agreed.
- Common algorithms used are MD5 and SHA-1
- IPSec provides flexibility in letting devices decide how they want to implement security.
  - Security policies and security associations are created.
- Devices need a way to exchange security information.
  - The Internet Key Exchange (IKE) provides this.



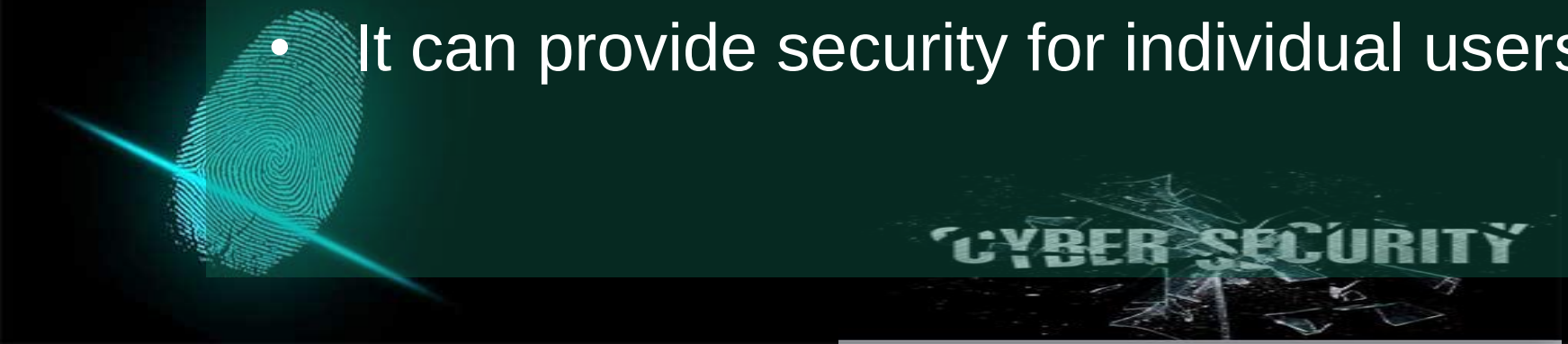
IPSec Applications

- Securing a company's Virtual Private network (VPN) over the Internet
- Securing remote access over the Internet
- Establishing connections with partners via an extranet
- Enhancing eCommerce security by adding to the security mechanism in the application layer



IPSec Advantages

- Can be applied to a firewall or router and apply to all traffic across that boundary
- It is transparent to applications.
- It is transparent to end users.
- It can provide security for individual users if required.



Break

Daffodil International University

Topic 3: Web Security

Topic 3 – Lecture 2:

SSL/TLS & HTTPS

Network Security and Cryptography

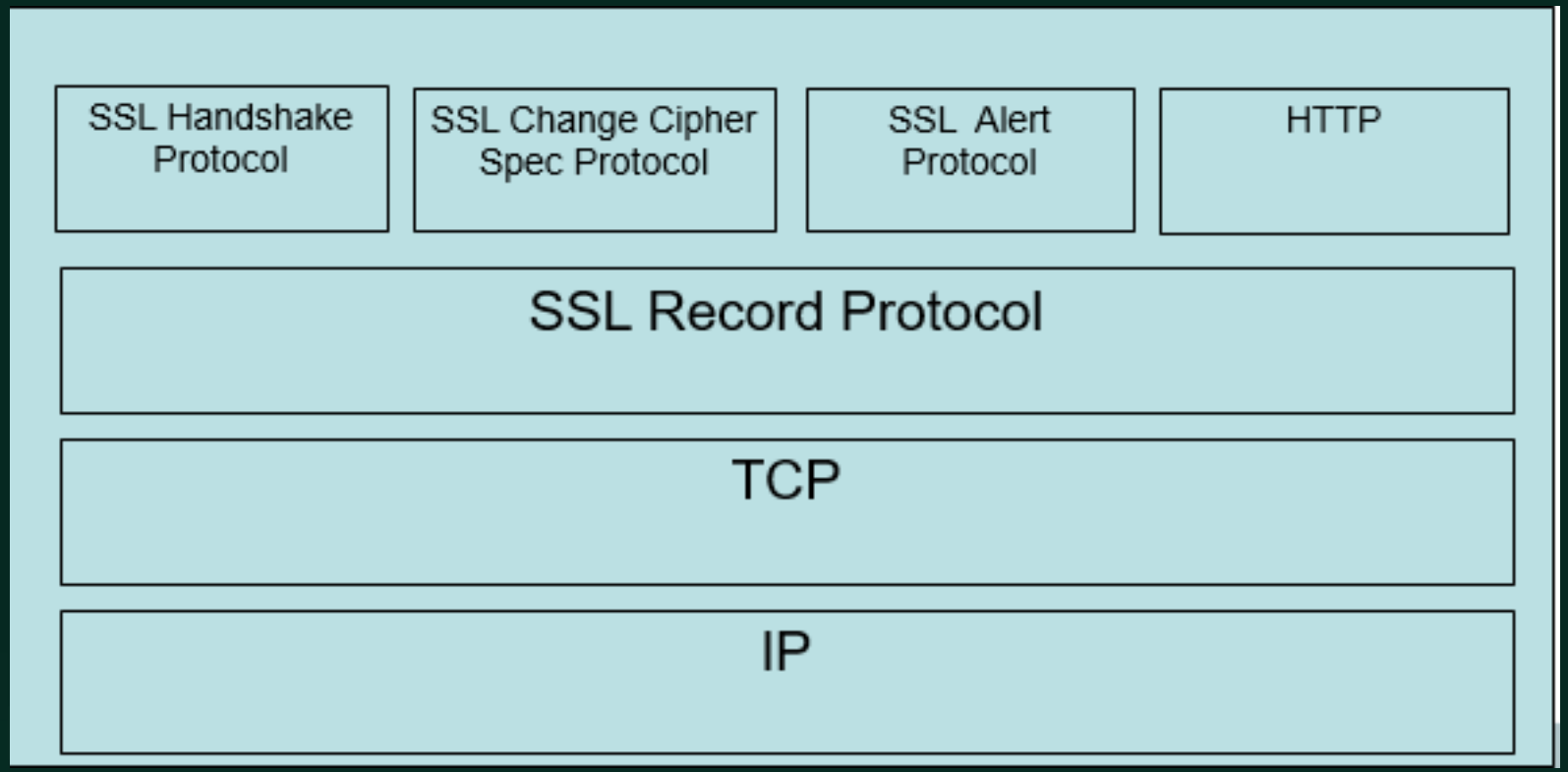
Secure Socket Layer (SSL)

- Originally developed by Netscape in 1995 to provide secure and authenticated connections between browsers and servers
- Provides transport layer security
- Transport Layer Security (TLS) Version 1 is essentially SSLv3.1

SSL Architecture

- SSL uses TCP to provide a reliable and secure end-to-end service.
- It is not a single protocol but two layers of protocols (see next slide).
- The Hypertext Transfer Protocol (HTTP) used for server/client interaction on the Internet can operate on top of the SSL Record Protocol.

SSL Architecture



SSL Connections

- A connection is a transport* that provides a suitable service.
- SSL connections are peer-to-peer relationships.
- These SSL connections are transient.
  -They only last for a certain length of time.
- Each connection is associated with a session.

**as defined by the OSI model*

SSL Sessions

- A session in SSL is an association between a client and a server.
- Such sessions are created by the SSL Handshake Protocol.
- A session defines the security parameters.
- A session may be shared by multiple connections.
  - Allows the same settings to be used by many connections without the need for repeatedly sending the security parameters

SSL Record Protocol - 1

- Provides two services for SSL connections
  - Confidentiality
  - Integrity

- Transmitted data:
  - Fragmented into manageable blocks
  - Compressed (optional)
  - Encrypted
  - Header added and transmitted in a TCP segment

SSL Record Protocol - 2

- Received data:
  - Decrypted
  - Verified
  - Decompressed
  - Reassembled
  - Delivered to higher level users

SSL Change Cipher Spec Protocol

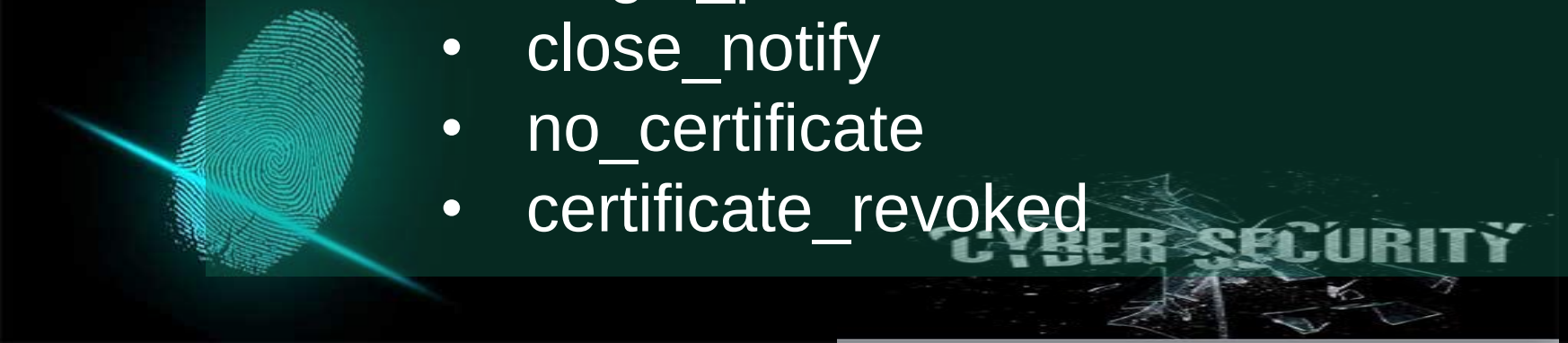
- Very simple
- One single byte containing the value 1
- Has one single purpose:
  - Causes the pending state to be copied into the current state
  - This updates the cipher suite to be used on a connection.

SSL Alert Protocol

- Used to convey SSL alerts to the peer entity
- Alert messages are compressed and encrypted as specified by the session.
- Each message consists of two bytes:
  - The first values indicates a warning or fatal alert
  - The second indicates the type of alert
- A fatal alert will cause SSL to immediately terminate the connection, but not other connections on the same session.

SSL Alert Types

- There are a number of alerts including the following. The top four are fatal:
  - unexpected_message
  - decompression_failure
  - handshake_failure
  - illegal_parameter
  - close_notify
  - no_certificate
  - certificate_revoked



SSL Handshake Protocol - 1

- The most complex part of SSL
- Allows server and client to authenticate each other
- Allows server and client to negotiate the encryption algorithms and keys that be used to protect data in an SSL record
- This protocol is used before any application data is sent.

SSL Handshake Protocol - 2

- Consists of a series of messages, all with the same format

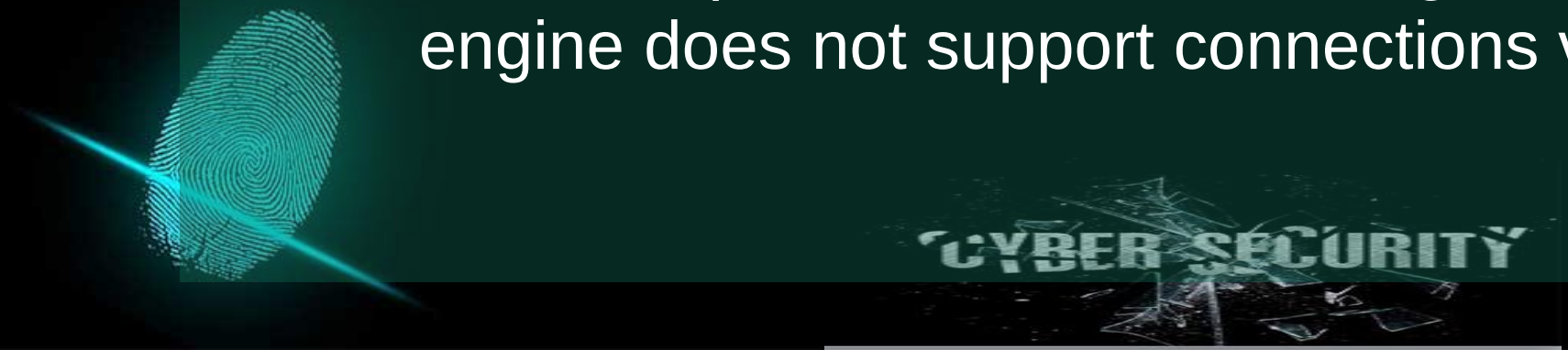
- Each message has 3 fields
  - Type (1 byte) – indicates 1 of 10 message types
  - Length (3 bytes) – the length of the message in bytes
  - Content (0 or more bytes) – parameters associated with the message

Messages

- The series of messages are initiated by the client.
- The first phase establishes the security credentials.
- The second phase involves authenticating the server and exchanging keys.
- The third phase involves authentication the client and exchanging keys.
- The fourth phase is completing the exchange.

HTTPS

- HTTP over SSL/TLS
- Used to create secure communications between a Web browser and Web server
- Built into modern browsers
- Requires server to support HTTPS communication
  - For example, at the time of writing, the Google search engine does not support connections via HTTPS

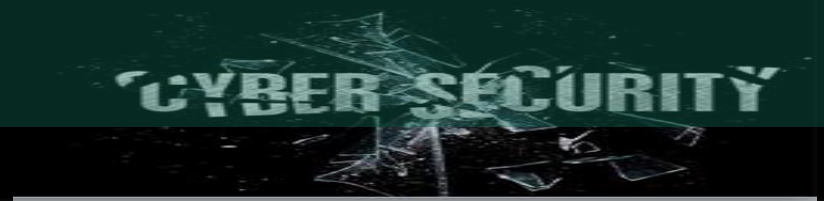


HTTPS Compared to HTTP

- URL begins with https:// rather than http://
- HTTPS connections use port 443 whereas HTTP uses port 80.
  - Port 443 invokes SSL
- If all is well, the browser will typically show a padlock or some other symbol to indicate the use of SSL/TLS.

HTTPS and Encryption

- The following elements of an HTTPS communication are encrypted:
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms
    - The fields filled in by the user in the browser
  - Cookies
    - From server to browser
    - From browser to server
  - Contents of the HTTP header



SSL Advantages

- It is independent of the applications once a connection has been created.
  - After the initiating handshake, it acts as a secure tunnel through which you can send almost anything.
- Has several implementation packages, both commercial and freely available
  - All major platforms (Windows, Linux, etc.) support SSL
  - No requirement for extra software packages

SSL Disadvantages

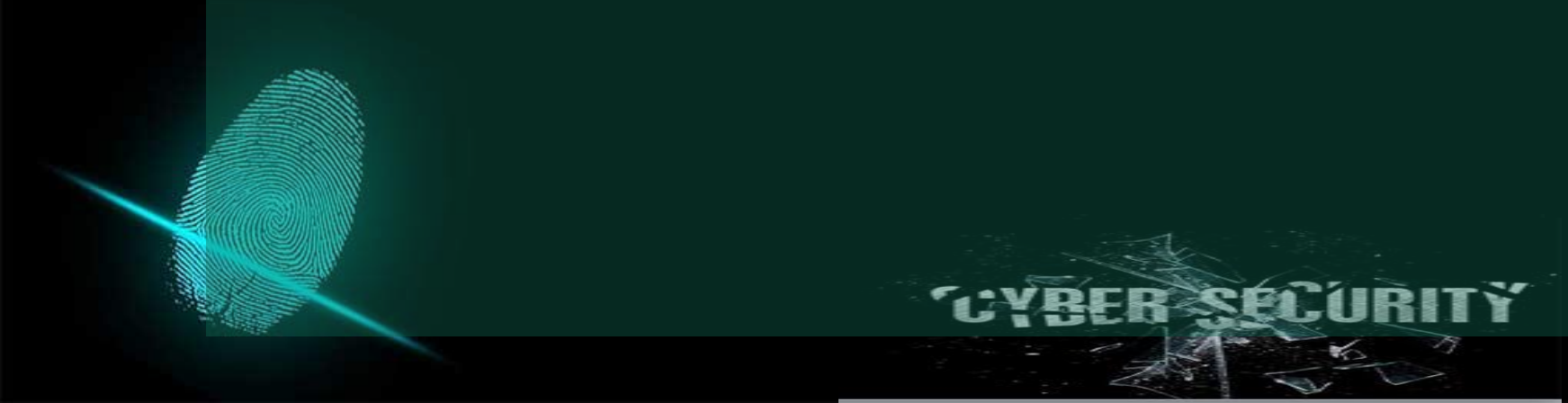
- The extra security comes with extra processing overhead.
- This overhead is largely at the server end.
- Means communications using SSL/TLS are a slower than those without it
  - Some sources suggest that HTTPS communication can be up to three time slower than HTTP.
  - With modern browsers, servers and connection speeds, this should not cause significant problems

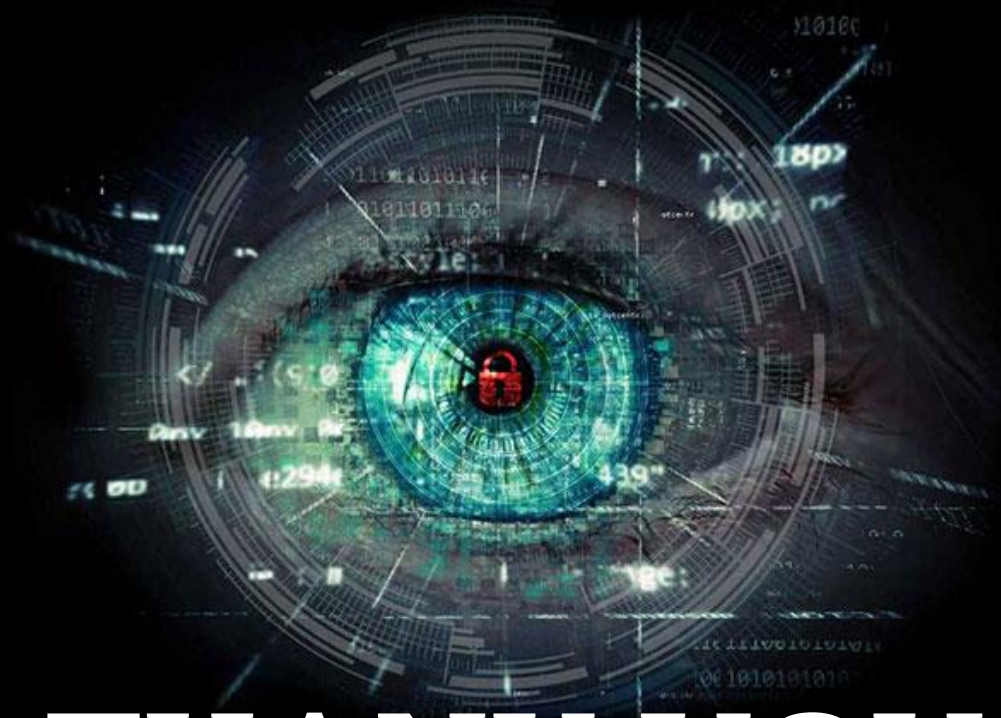
SSL/TLS Broken

- September 2011 - appears SSL/TLS cryptography has been broken by researchers
- This has major implications for the secure communications via the Internet
  - Reference for news emerging (September 2011):
  - http://www.computerweekly.com/Articles/2011/09/22/247969/Researchers-claim-to-have-broken-SSLTLS-encryption.htm

References

- Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
- Thomas, S.A. (2000). *SSL & TLS Essentials: Securing the Web*. Wiley.





THANK YOU
Any Question?

Topic3 – Web Security