TSSM™
Creating VCE Success

Software Development Teach Yourself Series

Topic 9: Networks and Cybersecurity Unit 4

A: Level 14, 474 Flinders Street Melbourne VIC 3000
T: 1300 134 518 **W:** tssm.com.au **E:** info@tssm.com.au

Contents

CASE STUDY

All Teach Yourself Series in this package will refer to the following case study.

Tariq Mulner is the manager of a school canteen. He manages how many lunches are going to be prepared each day. It is difficult to tell how many lunches will be sold, so he would like a software solution that students can use to order lunches. This application would provide him with a complete list of orders.
Most of the students have smart phones, so Tariq is suggesting the solution is a phone app that can read in the lunch order, and send it to his device so he can print out the order list.

Photo by Tirachard Kumtanom from Pexels used with permission

Networks

Most software applications rely on networks to transfer data between devices. We work and live in a world reliant on mobile devices so networks are crucial aspects of software application design and development.

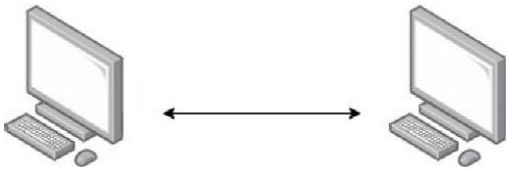
Local Area Network (LAN)

A LAN is a network defined by a small area, such as a home, a set of buildings or a small campus. All devices are directly linked together primarily by cabled connections.

Wide Area Network (WAN)

A WAN used the architecture of the internet to allow access to shared resources over a larger geographical area. An Intranet is a software restriction across a WAN that allows members of an organization to access shared resources such as email or data on servers. Your school portal is an example of an intranet.

Peer to Peer Network Architecture



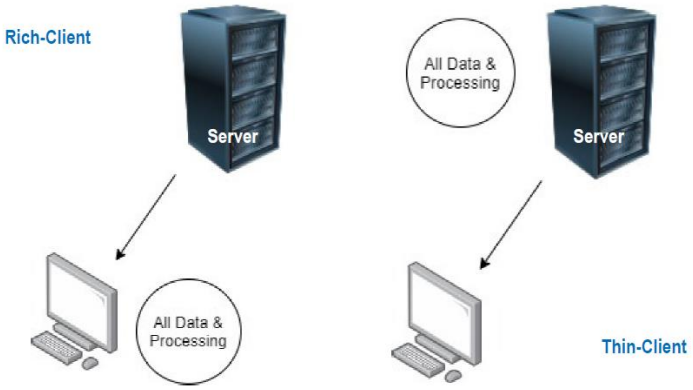
P2P is the direct exchange of data from one machine to another. Installing printer drivers and software relies on a peer to peer connection between your device and the printer. When you use torrenting software you are making direct connections to the devices of others to download files.

In the Case Study of U4O2 you will be required to recognize or recommend one of these two software architectures:

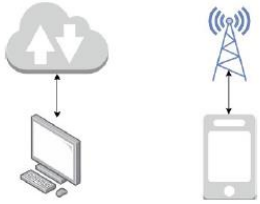
- Rich Client
- Thin Client

A Rich Client is a software architecture where a network connection is required for the software to work but all the data is stored and processed on the client not the server. This makes it easy to run if the internet access is slow, but the sue of the software may be interrupted at time by updates.

A Thin Client relies on the server to store all the data and to do the processing while the client merely displays the output and provides an interface. This runs faster, but requires fast internet access.



Mobile architecture relies on the network access via mobile phone technology, and the radio wave transmission to cell towers to access the internet.



Internet architecture relies on web page interfaces. Your school intranet is an internet architecture that uses a browser to access the interface.

Servers and Protocols

Ethernet Protocol is the rules governing the transfer of data via packets across at LAN. Carrier Sense Multiple Access/ Collision Detection is the process that Ethernet uses to "listen" for traffic on the network before sending packets.

Wi-Fi protocols are called 802.11x (x indicate4s the various transfer speeds) which uses a method called Request to Send/ Clear to Send – data is transferred by radio waves and encryption is used to protect the data while in transfer.

File Transfer Protocol governs the transfer of whole files from one device to another across a network. Uploading or download files from websites such as Google Drive, uses FTP.

Email protocols manage emails from a remote server to a local client. Both Internet Message Access protocol and Post Office Protocol allow the user to store their emails on the server or download them on their local device.

Web Protocols include TCP/IP which governs the way data packets are transferred across the internet to the correct device. HTTP governs the way web pages are accessed and displayed in browsers. HTTPS indicates when a website is protected by SSL.

Secure Sockets Layer (SSL) ensures internet connections are secure and safeguards any sensitive data that is being sent between two systems, preventing interference.

Transport Layer Security (TLS) is commonly called a 'certificate' and is an updated version of SSL. It makes sure data shared between two systems is impossible to read from unauthorized interlopers.

Network Devices

A lot of advances have occurred in network hardware and fewer devices are now required. Router Modems have replaced all modem devices as they have become more powerful and affordable. Routers are designed to connect networks, such as a LAN to the internet.

Switches are used to connect multiple device onto a LAN so they can share access to servers, printers and internet access.

Transmission Media

Cables

- Ethernet commonly known as CAT5 or CAT6 connect devices directly within LAN configurations.
- Unshielded Twisted Pair is the generic term for most copper wire cables including Ethernet and telephone wires.
- Optical fibre – make of glass and transports light signals rather than electrical pulses.

Wireless

- Radio Waves are used in Wi-Fi and mobile phone connections
- Microwaves are used for large data transfers. Examples include: live TV broadcasts to transmission towers, satellite uplinks and downlinks.

Cybersecurity

With the increase of digital technology being integrated into so many aspects of our lives, it is crucial that the digital systems and the data therein are protected from threats.

Physical Barriers

Locked doors, fences and other barriers to servers or devices with network access.

Biometrics include: voice recognition and thumb scan.

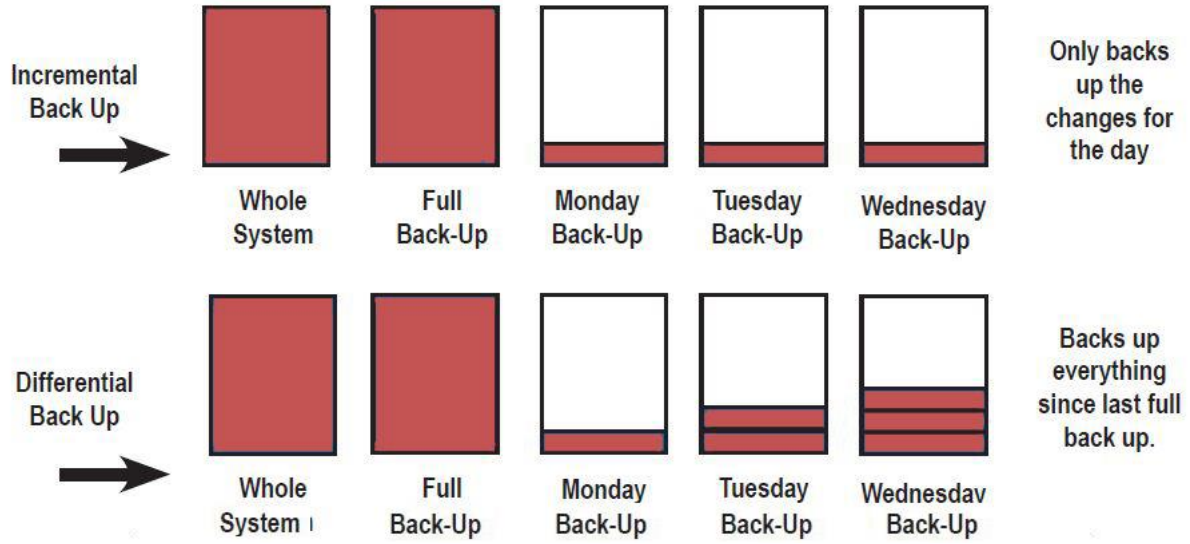
Security Appliances

Routers can include intrusion prevention, encryption and VPN capabilities.

Firewalls can include router capabilities and network management and analysis features.

Back-Up

A Back-up system integrates regular incremental or differential back-ups on a daily basis with full back-ups on a weekly or monthly basis.



Software Security Controls

User Authentication – using passwords for access limits who has access to the system. If each person has limited access incorporated into their network profiles, this controls who in the organisation has access to the data.

Firewalls

- Firewalls monitor the traffic in and out of a system. Network and Transport Layer Firewalls filter IP address.
- Context-Aware Application Firewalls limit malicious code from being downloaded into the system.
- Proxy Servers filter website requests against a list of restricted URLs and keywords.

Anti-Malware

Software to find and remove malicious software is the only way to protect a device or network from viruses and other malware.

Encryption

Uses a cypher to convert data into an unreadable file. This can protect data from being intercepted in transit or while stored on a server. There three types:

- Symmetric Encryption – where both the sender and receiver have the encryption and decryption key. Can be vulnerable when sharing the keys.
- Asymmetrical Encryption uses a public key that anyone can use to encrypt their data to send to the receiver who holds the private key that decrypts it. Vulnerable to Man in the Middle Attack.
- End to End Encryption uses a hybrid of both and is the most secure.

Version Control Systems

When developing software solutions many versions are produced and changes made to test different aspects of the program. GitHub is an online version control system that allows system developers to back up each version, and access each version if they need to roll back their work.

Software Updates

All systems require updates in response to hackers identifying vulnerabilities in the software. Keeping all systems up to date means they will have fewer vulnerabilities to threats.

Systems that need updating include:

- Operating Systems
- Network Operating Systems
- Anti-Malware
- Security Software
- Browsers
- Web Plugins
- Applications

Software Auditing and Testing

Auditing software has a three stage approach:

1. Predicting potential problems before they occur,
2. Monitoring errors, omission and malicious attacks
3. Minimising the impacts of threats.

Non Validated Input

A key online software vulnerability is the input forms on websites. If input is not thoroughly validated, any data can be typed in to take advantage of the live access to the databases and other software elements. SQL injection is a threat to software with an online interface. This is where a hacker can control access to the data server with the use of structured query language. Thorough testing of data entry validation is an auditing strategy.

Buffer Overflow

If data is allowed to be written beyond the limits of the allocated areas of memory this can produce a vulnerability that can be exploited. Software developers need to ensure all variables and data structures are allocated enough resources for the processing so as to keep the software secure.

Race Conditions

When a large complex software package is forced to run two or more operations at the same time, a vulnerability is created. An attacker can exploit the time it takes for the system to re-awaken and continue to monitor and run security controls.

Threats

Malware

Malware is software that is malicious in design with the intention of destroying, corrupting or stealing data. There are many types of malware:

- Spyware – monitors keystrokes, or takes over web cam.
- Trojan Horse – downloaded unintentionally with non-executable files
- Viruses – attached to legitimate executable files
- Malicious Auto Bots – spiders, crawlers, web bots, DoS attacks.
- Worms – bots that self-replicate across networks.
- Rootkit – creates a 'back-door' access for unauthorised entry to system
- Ransomware – encrypts data on servers until money is paid for decryption key

Hacking

Hacking is the attack conducted by a person directly. There are two key types we look at in this study design:

Man in the Middle Attacks – when encrypted data is transmitted, the hacker intercepts the transmission and eavesdrop on the communication. They do this by impersonating one of the receivers so as to get the decryption key. MitM attacks allow hackers to access sensitive data in banks and other organisations.

Cross Site Scripting (XSS) and SQLi – Server XSS is performed by using hypertext transfer protocol requests to access data on servers. Structures Query Language injection is a hacking technique used to access data on databases. With limited validation in place, a hacker can use the structure of a query to return key sensitive data such as passwords and usernames by simply typing into an interface input object.

Social Engineering

The least secure element of any digital system is the human element. The only way we can ensure humans do not create vulnerabilities is to educate users and put policies in place that users must agree to before use. There are four types of social engineering that we investigate in this study:

1. Pretexting: an attacker uses an email to an authorized user to give the impression that they are an employee, to encourage the user to provide usernames and passwords.
2. Phishing: Sending an email to authorized users posing as an organisation. The email encourages the user to click on a link which may infect the user's device or network.
3. Baiting: An attacker uses personal information about an authorized user (such as a personal interest) to tempt the user to provide sensitive data.
4. Quid Pro Quo: Attackers impersonate IT staff and offer assistance in return for access to the system to remove security software.

Risk Management Frameworks

There are many frameworks and models that can be implemented to ensure network and system security. A widely used framework is the National Institute for Standards and Technology (NIST) Framework Model. The model ensures all aspects of security are covered in five core functions:

1. Identify all vulnerabilities to the system.
2. Protect the system by removing vulnerabilities or putting in place protection measures.
3. Detecting threats through the everyday operation of the system using monitoring systems.
4. Response Plans are developed to ensure that all systems are threat free, to inform all stakeholders about the threats and to update all protection systems.
5. Recovering the system after a threat has been detected so that all the data and system is returned to operation.

Review Questions

Applied Questions

Tariq has asked you to produce an app. The Analysis is available in TOPIC 1. You have 3 weeks to develop the app to hand over. Ideally Tariq should have the solution for 2 weeks before evaluation begins.

1. The Bureau of Meteorology has a mobile phone app that delivers daily temperatures and weather forecasts. The App architecture is most likely:

A. Peer to Peer

B. Thin Client

C. Rich Client

2. Which of the following is a protocol that governs the transport of data packets across the internet?

A. HTTP

B. FTP

C. TCP

3. Which of the following only makes copies of data edited or created at the end of each day.

A. Full Back-Up

B. Incremental Back-Up

C. Differential Back-Up

4. Which of the following is TRUE about firewalls.

A. Firewalls monitor traffic in and out of the network.

B. Firewalls filter URL request responses

C. Firewalls restrict malicious software

5. What type of threat is a Trojan Horse?

A. Social Engineering

B. Malware

C. Hacking

6. The NIST Framework is a cybersecurity Model. What is a response plan?

A. A plan to protect the data on the system.

B. A Back-Up Plan if data is corrupted.

C. A plan on what to do in case of a threat.

Solutions to Review Questions

1. B. Thin Client

2. C. TCP

3. B. Incremental Back-Up

4. A. Firewalls monitor traffic in and out of the network.

5. B. Malware

6. C. A plan on what to do in case of a threat.