========================================================================

Q1

========================================================================

1. HTTP: Hypertext Transfer Protocol.

2. Network Standards permit interoperability among vendors which creates competition. Competition lowers prices and encourages growth in functionality.

3. Painless upgrades, lower initial costs.

4. (1)Retain state information. (2)Track usage of a particular site.

5. 25.

6. (1)Connet tablet to the Internet at home. (2) Connect laptop to the Internet at school.

7. 255.255.255.240.

8. an active attack.

9. ns13.dnsmadeeasy.com, 2600:1801:13::1.

10. Tom's private key.

========================================================================

Q2

========================================================================

1. If persistent connections are supported by both ends, then there is no need to create a new TCP session for every request and thus making it possible to send multiple requests back-to-back, futher reducing the propagation delay.

2. (1)advantages: low transmission power, no interference with 802.11; (2)security issues: eavesdroppers can read information and perform data modification and jam dns attacks. (3) (a)payment of bus fares; (b)door entry control; (c) retail payments.

3. NAT: network address translation. It is used to send false external IP addresses that are different from internal addresses.

NAT translates the IP address of client1.anu.edu.au into another IP address.

NAT box/firewall would keep a translation table which can translate an incoming IP address to an outgoing IP address and vice versa, and the translation is consistent. Therefore, packets sent in response from originserver.com can reach client1.anu.edu.au correctly.

4. Assume Bob has the contract initially and he would sign first.

Cryptography:

(1) Bob signs the contract with his private key;

(2) Bob encrypts the contract with Tom's public key;

(3) Bob sends the contract to Tom;

(4) Tom decrypts the contract with his private key;

(5) Tom signs the contract with his private key;

(6) Tom encrypts the contract with Alice's public key;

(7) Tom sends the contract to Alice.

Verification(by Alice):

(1) Alice decrypts the contract using Tom's public key;

(2) 。。。

Q4

Possible course of action 1: to follow my supervisor's instruction and put the system into production. It is possible that the “user ID reported to be from the PRN Secret Police” is actually a hoax, the system was actually hacked by Nussia, instead of PRN; and I am not competent enough to tell that it is a hoax. Actually, how can the Secret Police be so stupid not to use proxy to cover the access. In this case, Competence in Code of Ethics is relevant, because I cannot tell the different between a real access from PRN Secret Police and a hoax. I should not only continue to upgrade your knowledge and skills, but also make yourself aware of relevant standards and legislation, and act accordingly.

Possible course of action 2: to be a whistle- blower and to report this matter to *Canberra Times*, if I am confident that PRN government did hack the system, and both my supervisor and OzU legal service denied that. In this case, the Primacy of the Public Interest and Professionalism are relevant. Admitted, I should not put my employer (OzU) and my supervisor into bad light/ publicity. However, the Public Interest has the highest priority in the Code of Ethics. Privacy of staff and students should be properly protected. I am obliged to raise the students, staff and the general public's attention of this matter. Moreover, my supervisor may have breached the Code, I have to take appropriate action against him or her.

Q3

3.1

Key features of P2P architecture:

P2P is a network architecture in which each node is capable of performing each of the functions necessary to support the network, and in practice many nodes do perform many of the function.

Difference between P2P and Client-Server:

In P2P architecture, each node is both client and server; in Client-Server architecture, each node is either client or server.

(not sure if relevant)

The advantage of P2P over Client-Server is:

* reduced dependence on individual node/subnet
* avoided single point-of -failure
* inbuilt redundancy
* resistance to DoS attack
* service growth is proportionate to demand growth.

3.2

**for each item,to me, Roger's Blabla + wikipedia is enough pick something very different to each other, so differences among the different categories will be self-evident, then ctrl c + v**

3 kinds of mobile devices:

1 hand-held computing devices like iPad and MS surface.

2 processing capabilities in other 'form factor' like debit / credit card (pay pass / pay wave)

3 wearable computing devices like activity tracker (fitbit, vivofit)

3 kinds of wireless communications technologies:

1 WiMax (IEEE 802.16)

2 Digital Cellular (GSM, CDMA)

3 WiFi(IEEE 802.11)

3.3

(I am not sure if we are expected to memorize that many items, however, quiz 3 does require them)

3 threat-vulnerability combinations **(mobile payment)**

1 Unauthorised Conduct of Transactions

2 Interference with Legitimate Transactions

3 Acquisition of Identity Authenticators

e.g. Cr-Card Details (card-number as identifier,

plus the associated identity authenticators)

e.g. Username (identifier) plus Password/PIN/

Passphrase/Private Signing Key (id authenticator)

e.g. Biometrics capture and comparison

Safeguards that can be used to address those risks:

10 Absolute-Minimum

Physical Safeuguards

Access Control

Malware Detection and Eradication

Patching Procedures

Firewalls

Incident Management Processes

Logging

Backup and Recovery Plans, Procedures

Training

Responsibility

10 Beyond

Data Communications Encryption

Data Storage Encryption

Vulnerability Testing

Standard Operating Environments

Application Whitelisting

Device Authentication and Authorisation

Use of Virtual Private Networks

Intrusion Detection and Prevention

User Authentication

Firewall Configurations, Outbound

3.4

Malware

(1) uses a 'Vector'

(2) to deliver a 'Payload'

which performs

(3) a function that is 'Invoked'

by some means ...

... and is harmful to some party

vector: whereby undesired content reaches a device

I.e.engineering exploit

payload: The active code delivered to the target device

in order to perform some function or functions. The scope may extend to functions ancillary to

the ultimate purpose, e.g. means of obscuring

the existence or operation of the malware.

I.e.unexpected functionality that

facilitates unauthorised remote access to the device

Both I.e.s are about Trojan