



**Complete, fold and seal
(see note 2 below)**

Ridley

Liam James

12 Pages

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold over and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. **Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.**

List the numbers of the questions you have attempted	Office Use
2	20
3	14
4	23
Total	57

76%

Q.2) i) Internet of Things and Smart City Security Issues

The internet of things ^(IoT) is a concept that involves making everyday objects interactive and connected to the internet. These objects are then able to communicate and interact with other objects. ~~A concept~~ A concept that falls under the IoT banner is called Smart cities. Smart cities are formed when infrastructure within the city becomes interconnected and connected to a network, this includes: city-wide wifi, smart car parks, smart bus stops, and automated waste collection. These cities are ~~built~~ built on top of Wireless Sensor Networks (WSN). The rise in popularity of these technologies means the rise in the number of threats that they face. This report covers the potential threats and how they could impact a university campus network.

The first set of threats that will be highlighted relate to the internet of things. IoT will play a major part in the university campus. ~~To~~ To implement it, a wireless sensor network must be created. Sensors play a major role in IoT as the data collected by these sensors influence decisions made by other devices such as air conditioning, lighting. With all sensors being connected to one network, it opens up a number of threats. One of these threats is DDoS attacks. A DDoS attack is when a user with malicious intent floods a network with requests to overwhelm and bring it down to restrict.

continues on next page

access to it by genuine users. As a wireless sensor network already has to process large amounts of traffic, launching a DDOS attack becomes easier. If the WSN is brought down, it can stop essential tasks from taking place such as turning on lights, opening windows, etc. Another major threat to IOT are man-in-the-middle attacks (MitM). A MitM attack is when a user mimicks a destination device so that data is sent to them instead of the real destination. This data can then be copied, deleted and modified, and is then sent on to the ~~actual~~ intended destination. This type of attack can be very damaging because the ~~no~~ mitm can inject viruses into the packet which can infect the network, the attacker can also read private and confidential information, and delete data to cause errors on the network.

~~The next Set~~

The next Set of threats come from the Smart City Concept. As stated, Smart cities use ~~wsn's~~ WSN's to connect devices and accomodate communication. One of the main aspects of WSN's is that they process and store data from the sensors. This data can include irrelevant data, ~~some~~ ~~as~~ ~~is~~ and very confidential information such as device location, ~~vs~~ personal user information, etc. This makes WSN's prime targets for hackers looking to gain access to the information. ^{Some} ~~one~~ of the ways in which they gain this information ~~is~~ ~~to~~ are: Scan for and attack open ports, brute force attacks to crack passwords, mitm to intercept data, etc. Hacking a WSN can lead to major...



Breaches in not only ethical rules but also actual laws such as the data protection act. Another major threat to ~~sm~~ Smart cities and campuses is DDOS attacks. Bringing the network down could cause considerable problems within a Smart cities. Such as: bringing essential services to a stand still, restricting the use of traffic lights, etc. for campuses it means that infrastructure may become un-usable.
~~The first major~~

The BYOD (Bring your own device) policy that is to be introduced in this scenario can also ~~cause~~ cause security threats to arise. One of the biggest threats is allowing hackers inside access to the network. They can gain this through the personal devices of staff and students. Should they gain access, they could potentially gain access to and control of IoT devices and sensors, causing considerable damage.

As discussed, there are many threats that the Smart campus may face. However there are ways to stop these threats. To stop DDOS attacks, authentication servers may be used. These ensure that the request and communication is legitimate, or else the packet is dropped. Another way to stop DDOS is to ~~ensure~~ ensure the network has enough bandwidth to deal with large attacks. To stop MITM attacks, ~~good~~ strong encryption should be used, which means that if the packets were intercepted, an attacker would be unable to read...

The contents of the packet, authentication such as the two-way ~~that~~ hand shake can also be used to ~~ensure~~ ensure communication is with a legitimate device. To stop hacking of the network. Strong passwords should be used to stop the effects of brute-force, all devices should be encrypted so data cannot be read, and all database servers must be password protected and encrypted. All devices should be updated to the latest security patches. To stop internal breaches through BYOD. ~~See~~ A strong BYOD ~~needs~~ ~~to~~ policy needs to be written and enforced.

In conclusion, there are many threats the new campus will face. However, ~~to~~ the benefits of IOT such as less environmental impact, cost savings, more efficiency, means the benefits ~~are~~ outweigh the negatives.

Symmetric encryption

- 2-3. a). Symmetric encryption is one of the oldest and most well-known methods of encryption. It uses a secret key which scrambles a piece of text to a ^{defined} ~~required~~ format. Such as re-ordering the alphabet, to make the text unreadable. Symmetric uses a shared-key which is used by both the sender and receiver. This allows anyone with the same key to encrypt and decrypt the data. Symmetric encryption is commonly used between two ~~end~~ sides of a VPN link.

Some of the characteristics of Symmetric encryption include:

- Both sender and receiver share the same key.
- Key length is from 80 bits to 256 bits.
- Encryption process is fast due to the low computational requirements and simple mathematic operations.
- Examples of Symmetric encryption are: DES, 3DES, AES.

Symmetric encryption comes in two forms:

- Block cipher - Splits encryption into 64-bit blocks and processes it one block at a time.
- Stream cipher - Encryption in one block, processed one bit at a time.

Asymmetric

Asymmetric encryption

- The main issue with Symmetric encryption is that if the shared-key falls into the wrong hands, the hacker can decrypt all data using that particular key. ~~As~~ Asymmetric encryption solves this problem by using a ~~shared~~ key pair...

The contents of the packet, authentication such as the two-way ~~that~~ hand shake can also be used to ~~ensure~~ ensure communication is with a legitimate device. To stop hacking of the network. Strong passwords should be used to stop the effects of brute-force, all devices should be encrypted so data cannot be read, and all database servers must be password protected and encrypted. All devices should be updated to the latest security patches. To stop internal breaches through BYOD, ~~Strong~~ a strong BYOD ~~needs to~~ policy needs to be written and enforced.

In conclusion, there are many threats the new campus will face. However, ~~to~~ the benefits of IOT such as less environmental impact, cost savings, more efficiency, means the benefits ~~are~~ outweigh the negatives.

The first key is called a private key, which is known only by the source host, it is also unique, and the second key is a public key, which is ~~known~~ publicly available to view from the ~~source~~ destination address. If the source and server want to establish a secure encrypted link, the host sends a query ~~packet~~ packet to the server which ~~for~~ replies with a copy of its ~~packet~~ digital certificate, which the host ~~uses~~ uses to extract the public key. Asymmetric keys are used in secure HTTPS applications.

Some of the characteristics of asymmetric include:-

- key length of 512 bits to ~~4096~~ 4096 bits.
- Slower communication due to complex encryption and equations.
- key used for encryption is different from the one used for decryption.
- examples include: RSA, elliptic curve, DH.

3.) 5) - An example of a cryptography attack is a dictionary attack. This attack scans the data and runs it through a dictionary to find potential ~~key~~ key words, passwords, etc.

- Another example of a cryptography attack is a man-in-the-middle attack. This is used to intercept packets being sent. Once the packet is received the attacker can try to decrypt the data. One way of doing this is to try to gain access to the encryption key. This is easier when symmetric encryption has been used.



- Hacking is another threat to cryptography. This can allow the attacker to gain access to the encryption keys.

- Another threat is Spoofing. Spoofing is when an attacker pretends to be a genuine host / server, mimicking the legitimate devices information. An attacker could mimick a genuine public-key, to gain the knowledge of a hosts private-key.

14

14

Q.4. a). Android is a mobile platform which includes an operating system, middleware, and pre-installed apps. It is created and updated by Google. Some of the features of android include:-

- Application framework which allows reverse and replacement of components
- integrated web browser based on the webkit kernel.
- Audio, video, Sound Support.
- Rich development environment which includes a device emulator, debugging tools, eclipse ide plugin.

Android devices can be 'rooted' which is a process that allows users privileged access to the android system, allowing custom apps, GUI, and the removal of carrier information and apps. However, this process opens many risks such as bricking, voiding the warranty, hacking, etc.

As the mobile device acts like a computer, it is vulnerable to many of the same threats, such as, Hacking, viruses, spoofing, phishing, etc. However it can also be defended in the same way such as:-

- password protection
- don't install App files from unknown sources.
- ~~A~~ ~~is~~ install anti-virus software.
- regularly update the security patches.

4) ~~2~~ 5) below is a step by step penetration test procedure for an android device. A pen test is the process of scanning, attacking, and assessing a device to find and fix security flaws within the device.

1. Root the android device - This can be done using ~~the~~ many third party apps.
2. Perform a Dos and DDoS attack on the device. - This is to see how the device copes, and can be done using the AnDOSid tool.
3. Check for vulnerabilities in the internet browser. - This ~~see~~ is to check whether connections are secure.
4. Check for ~~vulnerabilities~~ vulnerabilities in the SQLite database. - to ~~see~~ check if the database is secure especially against SQL injection attacks.
5. Test for data leakage. - This test is to check whether data can easily be accessed and removed.
6. Check overall OS for security vulnerabilities - This checks application frameworks and installed applications.

3