LEVEL 5

NETWORK SECURITY AND CRYPTOGRAPHY

Lecturer Guide

Modification History

Version	Date	Revision Description
V1.0	October 2011	For release
V1.1	November 2015	Assessment Methodology Updated

Published by: NCC Education Limited, The Towers, Towers Business Park, Wilmslow Road, Didsbury, Manchester M20 2EZ, UK.

Tel: +44 (0) 161 438 6200 Fax: +44 (0) 161 438 6240 Email: info@nccedu.com
http://www.nccedu.com

CONTENTS

1. Module Overview and Objectives

This unit will provide the learner with the underlying theory and practical skills required to secure networks and to send data safely and securely over network communications (including securing the most common Internet services).

This module provides a look at the technologies employed to secure a network. It is designed to provide students with knowledge of the fundamental principles and techniques employed in securing information and networks. The module will allow students to assess the security risks inherent in computer networks and the technologies that can be employed to counter such risks. It covers cryptographic algorithms from a mathematical point of view, including practical examples of breaking codes.

Once the students have knowledge of the different types of algorithm, cryptographic protocols are introduced for accomplishing a varied set of tasks, including authentication, secure message exchange, digital signatures, etc. Other aspects of network security are then dealt with, such as access control devices and firewalls, VPN, NAT, malware, vulnerability assessment, Intrusion Detection Systems (IDS), etc.

2. Learning Outcomes and Assessment Criteria

Learning Outcomes; The Learner will:	**Assessment Criteria;** The Learner can:
1. Understand the most common types of cryptographic algorithm	1.1 Explain the most common types of cryptographic algorithm (i.e. block ciphers, public-key ciphers and hash algorithms) 1.2 Select and justify an appropriate algorithm for a particular purpose
2. Understand the Public-key Infrastructure	2.1 Describe the Public-key Infrastructure 2.2 Explain the role of Certification Authorities
3. Understand security protocols for protecting data on networks	3.1 Explain the concept of web security with TLS 3.2 Describe email security mechanisms 3.3 Describe disk encryption mechanisms 3.4 Deploy file encryption mechanisms
4. Be able to digitally sign emails and files	4.1 Explain digital signatures 4.2 Demonstrate applying for and deploying a Digital Certificate 4.3 Digitally sign an email
5. Understand vulnerability assessments and the weakness of using passwords for authentication	5.1 Explain the need for vulnerability assessments 5.2 Interpret a vulnerability assessment report 5.3 Explain the different authentication mechanisms 5.4 Describe multifactor authentication 5.5 Describe biometrics and their issues

6. Be able to perform simple vulnerability assessments and password audits	6.1 Use port scanners to highlight open ports 6.2 Perform password cracking using dictionary and brute-force methods
7. Be able to configure simple firewall architectures	7.1 Configure access control mechanisms 7.2 Describe the components of a firewall 7.3 Configure a DMZ firewall 7.4 Evaluate the limitations of firewalls 7.5 Apply and manage port forwarding rules
8. Understand Virtual Private Networks	8.1 Explain Virtual Private Networks 8.2 Select an appropriate remote access solution
9. Be able to deploy wireless security	9.1 Explain the vulnerabilities inherent in wireless networks 9.2 Deploy a secure network architecture for wireless access 9.3 Configure Access Control Lists 9.4 Encrypt and protect the wireless link

3. Syllabus

Syllabus			
Topic No	Title	Proportion	Content
1	Cryptography Fundamentals	1/12 3 hours of lectures 2 hours of tutorials	• Cryptographic algorithms including: – AES block cipher – RSA public-key code – SHA hash algorithm ***Learning Outcome: 1***
2	PKI	1/12 2 hours of lectures 1 hour of tutorials 2 hours of laboratory sessions	• The Public-Key Infrastructure • Certification Authorities and Digital Signatures ***Learning Outcome: 2, 4***

3	Web Security	1/12 2 hours of lectures 1 hour of tutorials 2 hours of laboratory sessions	• Browser security and SSL/TLS for encrypted browsing ***Learning Outcome: 3, 4***
4	Email Security	1/12 2 hours of lectures 1 hour of tutorials 2 hours of laboratory sessions	• PGP and S/MIME for encrypted and authenticated email ***Learning Outcome: 3, 4***
5	Data Protection	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• File, disk and portable encryption technologies ***Learning Outcome: 3, 4***
6	Vulnerability Assessment	1/12 2 hours of lectures 1 hour of tutorials 2 hours of laboratory sessions	• Vulnerability assessment terms and tools: – Port scanners – Password crackers ***Learning Outcome: 5, 6***
7	Authentication	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Passwords • Multi-factor authentication • Biometrics ***Learning Outcome: 5***

8	Access Control	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Packet filtering • Access control lists • NAT • IDS ***Learning Outcome: 7***
9	Firewalls	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Firewall architectures and their limitations • The DMZ firewall and its limitations ***Learning Outcome: 7***
10	VPN	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Virtual Private Network technologies and issues ***Learning Outcome: 7, 8***
11	Remote Access	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Alternative remote access technologies: – Remote desktops – Web applications ***Learning Outcome: 7, 8***
12	Wireless Security	1/12 2 hours of lectures 2 hours of tutorials 1 hour of laboratory sessions	• Wireless security (WEP, WPA, WPA2) • Secure network architectures for wireless deployments ***Learning Outcome: 9***

4. Related National Occupational Standards

The UK National Occupational Standards describe the skills that professionals are expected to demonstrate in their jobs in order to carry them out effectively. They are developed by employers and this information can be helpful in explaining the practical skills that students have covered in this module.

Related National Occupational Standards (NOS)
Sector Subject Area: 6.1 ICT Professionals **Related NOS:** 6.2.A.1 - Contribute to IT/technology security management activities; 6.2.A.2 - Document IT/technology security management processes; 6.2.A.3 - Assist the management with IT/technology security systems; 6.2.P.1 - Manage the IT/technology security requirements; 6.2.P.2 - Carry out IT/technology security management activities

5. Resources

Lecturer Guide:	This guide contains notes for lecturers on the organisation of each topic, and suggested use of the resources. It also contains all of the suggested exercises and model answers.
PowerPoint Slides:	These are presented for each topic for use in the lectures. They contain many examples which can be used to explain the key concepts. Handout versions of the slides are also available; it is recommended that these are distributed to students for revision purposes as it is important that students learn to take their own notes during lectures.
Student Guide:	This contains the topic overviews and all of the suggested exercises. Each student will need access to this and should bring it to all of the taught hours for the module.

5.1 Additional Hardware and Software Requirements

Hardware:	Centres require access to number of networked computers with peripheral devices, such as printers and scanners, plus Internet access, routers, and firewalls. Wireless devices are also required that that can be added to this network or used to create a standalone wireless network.
Software:	Centres must have network/server software available plus relevant security software. Students will also need access to image manipulation software such as Abode Photoshop, VPN server and client software, and a remote desktop application (e.g. www.logmein.com). Suitable open source software may also be used.

6. Pedagogic Approach

Suggested Learning Hours					
Lectures:	**Tutorial:**	**Seminar:**	**Laboratory:**	**Private Study:**	**Total:**
25	20	-	15	90	150

The teacher-led time for this module is comprised of lectures, laboratory sessions and tutorials. The breakdown of the hours is also given at the start of each topic, with 5 hours of contact time per topic.

6.1 Lectures

Lectures are designed to introduce students to each topic; PowerPoint slides are presented for use during these sessions. Students should also be encouraged to be active during this time and to discuss and/or practice the concepts covered. Lecturers should encourage active participation and field questions wherever possible.

6.2 Tutorials

Tutorials provide tasks to involve group work, investigation and independent learning for certain topics. The details of these tasks are provided in this guide and also in the Student Guide. They are also designed to deal with the questions arising from the lectures, laboratory sessions and private study sessions.

6.3 Laboratory Sessions

During these sessions, students are required to work through practical tutorials and various exercises. The details of these are provided in this guide and also in the Student Guide. Some sessions will require more support than others as well as IT resources. More detail is given in this guide.

6.4 Private Study

In addition to the taught portion of the module, students will also be expected to undertake private study. Exercises are provided in the Student Guide for students to complete during this time. Teachers will need to set deadlines for the completion of this work. These should ideally be before the tutorial session for each topic, when Private Study Exercises are usually reviewed.

7. Assessment

This module will be assessed by means of an assignment worth 50% of the total mark and an examination worth 50% of the total mark. These assessments will cover the learning outcomes and assessment criteria given above. Samples assessments are available through the NCC Education Campus (http:campus.nccedu.com) for your reference.

Assignments for this module will include topics covered up to and including Topic 7. Questions for the examination will be drawn from the complete syllabus. Please refer to the Academic Handbook for the programme for further details.

8. Further Reading List

A selection of sources of further reading around the content of this module must be available in your Accredited Partner Centre’s library. The following list provides suggestions of some suitable sources:

Bishop, M. (2012). *Computer Security: Art and Science*. Pearson Addison Wesley.
ISBN-10: 0321712331
ISBN-13: 978-0321712332
(Please note that this edition is hard copy but earlier paperback editions are also available).

Pfleeger, C., Pfleeger, S, and Margulies. (2015). *Security in Computing,* 5th edition*.* Pearson Prentice Hall.
ISBN-10: 0134085043
ISBN-13: 978-0134085043

Schneier, B. (1995). *Applied Cryptography*. John Wiley and Sons.
ISBN-10: 0471117099
ISBN-13: 978-0471117094

Stallings, W. (2013). *Cryptography and Network Security: Principles and Practice*, 6th edition. Pearson Education.
ISBN-10: 0133354695
ISBN-13: 978-0133354690

Topic 1: Cryptography Fundamentals

1.1 Learning Objectives

This topic provides an overview of the most common types of cryptographic algorithms and demonstrates examples of them in use today (e.g. AES, RSA and SHA-1). The basics of cryptographic protocols will also be covered to serve as an introduction to further topics presented later in the module.

It is critical that students understand the three different types of algorithm presented in these slides, i.e. block cipher, public-key cipher and hash algorithms. If their understanding is lacking here, then they will struggle in future topics. They should also understand that no system is 100% secure and cannot be made to be.

On completion of the topic, students will be able to:

- Explain the most common types of cryptographic algorithm (i.e. block ciphers, public-key ciphers and hash algorithms);
- Select and justify an appropriate algorithm for a particular purpose.

1.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the tutorial sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

1.3 Timings

Lectures:	3 hours
Private Study:	7.5 hours
Tutorials:	2 hours

1.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Introduction to module
- Overview of security
- Overview of cryptography
- Block ciphers
- Public-key ciphers
- Hash algorithms

1.4.1 Guidance on the Use of the Slides

The slides are divided into three lectures, each lasting 1 hour. These may be delivered as separate lectures or you may combine them into longer sessions.

1.4.2 Lecture 1

Slides 3-4: An overview of Topic 1.

Slide 5-10: An overview of the Network Security & Cryptography module is presented here. Go through the details with students to give them a wider understanding of what they can expect in this module.

Slide 11: This slide gives a definition of computer security from the (American) National Institute of Standards and Technology (NIST). Before showing the slide, ask the students for their ideas on what computer security is. It is likely that you will receive answers relating to “protecting from threats”; try to get students to think about exactly what it is they are protecting.

Slide 12: We now move on to a definition of cryptography from the National Institute of Standards and Technology. Before showing the slide, ask the students for their understanding of cryptography. Their knowledge may be very limited but it will provide an insight into their background knowledge of the subject.

Slides13-14: The first slide gives definitions of security objectives as defined by NIST and the second slide briefly outlines the consequences of not meeting these objectives.

Slide 15: Before showing this slide, ask the students if they think the NIST objectives omit any important objectives. If possible, try to group their conclusions into similar objectives that can be included under the two extra objectives given on the slide. Point students to Private Study Exercise 2 in their Student Guides, where they will research critiques of the CIA triad.

Slide 16: Authenticity involves verifying and trusting the entities involved in a transmission. Essentially it involves confirming that any message comes from the entity that claims to have sent it and that it has not been tampered with in any way during transmission.

Slide 17: Accountability simply means that the actions of a person or system can be traced back to the person or system carrying out those actions. If this can be done, then it is not possible for a person or system to claim they have not carried out an action and has a number of consequences. It acts as a deterrent to malicious acts; it allows the isolation of the source of faults and recovery from faults; it aids intrusion detection and prevention; and, where deliberate action has been taken, it aids legal action by providing accurate records.

Slides 18-19: An overview of the OSI security architecture and the key concepts as given in ITU-T Recommendation X.800 are provided here.

Slides 20-22: A brief outline of passive and active attacks as defined by X.800.

Slide 23: This slide provides a brief outline of security services as defined by X.800. Students should be directed to Private Study Exercise 3 to examine these in more detail.

Slide 24: A brief outline of security mechanisms as defined by X.800. Students should be directed to Private Study Exercise 4 to examine these in more detail.

Slides 25-28: Some basic number theory that is required later. At this stage, use simple examples such as 3 is a divisor of 12 as **12** = 4 x **3**; 7 is a prime number as is only has 1, -1, 7 and -7 as its divisors. You could perhaps also ask the students to provide the divisors of 8, 15, 24 and 30, plus all prime numbers between 10 and 20.

1.4.3 Lecture 2

Slide 30: You may like to begin this section by re-eliciting from students their understanding of cryptography based on the definition given earlier in the lecture, before showing them this slide, which presents an overview of cryptography and a brief introduction to the concepts of symmetric encryption and asymmetric encryption. These concepts will be expanded in the following slides.

Slide 31: Use the diagram to explain symmetric encryption.

Slide 32: The elements of the symmetric encryption process are plaintext, the original message in standard readable form; the encryption algorithm, the mathematical technique used to encrypt the message; the secret key, known only to the sender and receiver that is used to encrypt the message; the ciphertext, the message after it has been encrypted; and the decryption algorithm, the reverse mathematical technique that is used to decrypt the ciphertext back into plaintext.

Slide 33-34: The algorithms used in symmetric encryption are not secret but it is vital that the secret key remains so as this is what prevents the message from being read by attackers. The algorithm used should be sufficiently strong that an attacker cannot decode messages easily.

Slide 35: Cryptography systems (cryptosystems) can also be classified by the type of mathematical operation used to transform the plaintext to ciphertext, either via substitutions where each character is mapped to another character or via transposition where characters are transposed based upon their position in the plaintext. There is a further distinction between block ciphers where a block of the plaintext is encrypted as one and stream ciphers where the plaintext is encrypted element by element.

Slides 36-37: Simple examples of substitution and transformation are provided to help the students to understand the difference.

Slide 38: Modern cryptosystems are much more complex than the examples given and rely on the use of keys and multiple, interleaved layers of substitution and transposition when converting plaintext to ciphertext.

Slide 39: The main aim of an attacker is to determine the encryption key rather than to decrypt a single message as this opens the door to decrypting many messages. For such cryptanalysis attacks to have a chance of success, it is usually required to have some knowledge of the nature of the encryption algorithm used plus either some knowledge of the general characteristics of the plaintext or access to some plaintext/ciphertext combinations.

Slide 40: An alternative method is to simply try every possible key on a piece of ciphertext until some readable plaintext is produced. Whilst by luck the first attempt could be successful, statistically an attacker would need on average to use half of the possible keys before successfully decrypting the ciphertext. A key size of 32 bits gives over 4 billion possible keys. This may sound like a lot but a powerful computer could discover the key in a couple of milliseconds.

Slide 41: Some examples are given here for using larger keys. Students should recognise that larger keys increase security.

Slide 42: Use this slide to recap the difference between block ciphers and stream ciphers. A little extra detail is also provided.

Slides 43-44: The Feistel cipher is the basis for most modern symmetric cyphers. The input plaintext is split into two equal blocks called left and right. On each cycle, a function is applied to the right block and the key and this is XORed with the left block. XOR means when bits are compared and if both are different the result is 1, if both are the same the result is 0. You could get the students to produce a truth table that shows the four possible combinations of two input bits and gives the XOR result to check their understanding here. The blocks are then swapped so left becomes right and right becomes left. The process is repeated a number of times. Go through the diagram and ensure that students understand the process.

Slide 45: The Data Encryption Standard (DES) was the standard block cipher using a 56 bit key but by 1998 this could be cracked within 3 days making it unsuitable for sensitive messages.

Slides 46-54: The Advanced Encryption Standard (AES) replaced DES and has multiple key lengths and block sizes available to allow for greater security when required. The slides give a high level overview of the algorithm; use the diagrams to further explain each of the four steps used in each round (cycle).

1.4.4 Lecture 3

Slides 56-60: These slides cover the theory of public key encryption and provide a simple analogy using a locked mailbox. Use the diagram on Slide 60 to ensure that students understand how this works.

Slide 61: This slide briefly describes three ways in which public key cryptosystems can be used.

Slides 62-66: The RSA algorithm is explained as a simplified process first and then as a mathematical process. Students should be pointed towards the lab exercise where a simplified example is given using small prime numbers. They will be asked to create their own versions using different prime numbers.

Slide 67: An overview of RSA security is given here.

Slide 68: Hash functions can transform a large amount of data into a small amount of data. Hash functions can deal with varying sizes of data input.

Slide 69: This slide lists the properties of hash functions that are suitable for authentication purposes.

Slide 70: Explain to students that one-way hash functions are relatively easy to compute but difficult to compute in reverse, thus removing the need for any kind of private key.

Slides 71-72: These slides introduce the SHA-1 hash function, with an example (a common English expression using every letter of the alphabet), showing how a very small change in input makes a great difference to the output.

Slide 73: References

Slide 74: Questions

1.5 Tutorial Sessions

The time allocation for this topic is 2 hours.

Lecturers' Notes:

Students have copies of the tutorial exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Work through the following example and ensure you understand the maths and the process. Work through each line of calculation by yourself to ensure that you understand fully.

Generating Public and Private Keys

1. Pick two prime numbers. We'll pick p = 3 and q = 11
2. Calculate n = p * q = 3 * 11 = 33
3. Calculate z = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20
4. Choose a prime number k, such that k is co-prime to z, i.e., z is not divisible by k.
   We have several choices for k: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5).
   Let's pick k=7.
5. So, the numbers n = 33 and k = 7 become the public key.
6. Calculate the private key. Here is how:
   k * j = 1 (mod z)
   7 * j = 1 (mod 20)
   (7 * j) / 20 = ? with the remainder of 1 (are only interested in the remainder).

Since we selected to work with small numbers, we can easily conclude that 21/20 gives the remainder of 1. So, 7 * j = 21, and j = 3. This is our secret key. We MUST NOT give this key away.

Now, we can begin our message transmission from our browser to the server. First, the browser requests the public key from the server, which the server sends, i.e. it sends n=33 and k=7 back to the browser.

Now, we assume that the browser has a plain message P=14, and it wants to encrypt it before sending it to the server.

Encrypting the message

Here is the encryption maths that browser executes:

P ^ k = E (mod n)

"^" means "to the power of"
P is the plain message we want to encrypt
n and k are server's public key
E is our encrypted message we want to generate

This equation is solved as follows:

$$14 ^\wedge 7 = E \ (\bmod 33)$$

This equation in English says:

“raise 14 to the power of 7, divide this by 33, giving the remainder E”

105413504 / 33 = 3194348.606
3194348 * 33 = 10541348
E = 105413504 - 10541348 = 20

The encrypted message is **E=20**. This is the value that the browser is going to send to the server.

When the server receives this message, it then proceeds to decrypt it, as follows.

Decrypting the Message

Here is the decryption maths the server executes to recover the original plain text message which the browser started with.

$$E ^\wedge j = P \ (\bmod n)$$

E is the encrypted message just received
j is the server's secret key
P is the plain message we are trying to recover
n is server's public key

Plugging in the values:

20 ^ 3 = P (mod 33)
8000 / 33 = ? with the remainder of P
8000 / 33 = 242.424242...
242 * 33 = 7986
P = 8000 - 7986 = 14

This is exactly the plain text message that the browser started with!

Suggested Answer:

There is no answer required here; the next exercise will ensure that students have understood this.

Exercise 2:

Work in pairs and use the methods in Exercise 1 as follows:

- Person 1 generates public and private keys using different prime numbers.
- Person 1 passes the public key to Person 2.
- Person 2 chooses a number between 1 and 50 as the message.
- Person 2 encrypts the message and passes the encrypted message to Person 1.
- Person 1 decrypts the message.

- Check the messages match.

Change roles and repeat the exercise with different prime numbers and a different message.

Exercise 3:

See if you can decrypt the message below. It uses a simple substitution cipher where the letters of the alphabet have been shifted a number of places in a similar way to this:

Alphabet: A B C … Z

Cipher: B C … A

The message is:

GPC HDNB IPT ECSSBEEKCYYG OBSVGQRBO RHB WBEEDFB

Answer:

YOU HAVE NOW SUCCESSFULLY DECRYPTED THE MESSAGE

1.6 Private Study

The time allocation for private study in this topic is expected to be 7.5 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide. They are expected to also use private study time to review the content of this unit.

You may wish to ask students to complete the private study exercises after relevant lecture has been delivered and then allow time for review of their answers in the next lecture or tutorial session. Alternatively you may prefer to review the answers during Topic 2 or to collect in written work for one or more exercises as you feel is appropriate.

Exercise 1:

Neatly write out the calculations you made in Tutorial Exercise 2, showing all of the working out. These will be discussed during the tutorial session for this topic.

Suggested Answer:

Two sets of calculations showing all working out for the generation of keys, encryption of the message and decryption.

Exercise 2:

Research critiques of the CIA triad using several different sources for your information. Briefly describe areas where critics suggest that the CIA triad is insufficient for complete security. List the sources you have used.

Suggested Answer:

Alongside the requirements for authenticity and accountability given in the lecture slides, students should include the following areas:

- The CIA triad is information-centric and does not really deal with people – this may be covered in part by the additional requirements for authenticity and accountability.
- There are organisational issues that are not covered; therefore it should be expanded to cover ethical, social and organisational issues. One such approach by Dhillon & Backhouse suggests four new principles; responsibility, integrity, trust and ethicality (RITE). These can be considered when managing information security in organisations. Responsibility means having knowledge of rules and understanding of responsibilities so that members of an organisation are able to develop their own security practices when needed and that these practices are in line with overall organisational rules. Integrity means being morally sound and loyal to the organisation. Trust means that relationships within organisations should be built on confidence rather than control; employees have to be trusted to act according to the organisation's norms and employees have to feel confident that their privacy will not be compromised by too strict security controls. Ethicality means that members of an organisation should act according to ethical principles instead of strictly follow formal rules.
- It does not include responsibility to external partners.

- It is not the sum total of a good security policy; it is only a starting point. It appears to be a tempting holistic security model, but it should never be treated as the end.

Exercise 3:

Research the following security services as defined by X.800.

a. Authentication

b. Access control

c. Data confidentiality

d. Data integrity

e. Non-repudiation

Explain each one, giving examples where appropriate.

Suggested Answer:

a. Authentication is concerned with assuring that a communication is authentic. The recipient of the message should be sure that the message came from the source that it claims to be from; all communicating parties should be sure that the connection is not interfered with by any unauthorised party.

   For example, a person is using an online banking service. Both the user and the bank should be assured of the identities of the other.

b. This service controls who can have access to a resource, under what conditions access can occur, and what those accessing are allowed to do.

   For example, in online banking a user may be allowed to see her balance, but not allowed to make any transactions for some of the accounts.

c. The protection of data from unauthorized disclosure (from passive attacks). This includes:

   - Connection confidentiality – the protection of all user data on a connection.
   - Connectionless confidentiality – the protection of all user data in a single block.
   - Selective field confidentiality – the confidentiality of selected fields within the user data.
   - Traffic-flow confidentiality – the protection of information that might be derived from the observation of traffic flows.

d. The assurance that data received are exactly as sent by an authorized entity. This means they do not contain any modification, insertion, deletion or replay.

e. Protection against denial by one of the entities involved that they have participated in the communication. Nonrepudiation can include proof that the message was sent by the specified party and that the message was received by the specified party.

For example, a user of online banking has made a transaction, but later denied it. The bank needs to protect itself by ensuring it records who made the transaction.

Exercise 4:

Explain the following security mechanisms as defined by X.800.

a. Encipherment

b. Digital signature

c. Access Control mechanisms

d. Data Integrity mechanisms

e. Authentication Exchange

f. Traffic Padding

g. Routing Control

h. Notarization

Suggested Answer:

a. Using mathematical algorithms to transform data into a form that is not readily intelligible. This transformation and the recovery of the data at the receiving end depend upon an algorithm and zero or more encryption keys.

b. Data added or cryptographic transformation of a data unit allowing the recipient to prove the source and integrity of the data unit.

c. A range of mechanisms that enforce access rights to resources.

d. A range of mechanisms that assure the integrity of transmitted data.

e. A mechanism that aims to ensure the identity of an entity via the exchange of information.

f. The insertion of bits into empty spaces in a data stream to prevent attempts at traffic analysis.

g. Allows the selection of physically secure routes for data transmission and the changing of routes, especially when a breach of security is suspected.

h. The use of a trusted third party to assure certain properties of a data exchange.

Exercise 5:

Find three real-world applications where block ciphers are used for cryptography.

Suggested Answer:

Answers could include email privacy, secure remote access and ATMs (cash machines).

Topic 2: PKI

2.1 Learning Objectives

This topic provides an overview of the public key infrastructure including digital certificates and digital signatures. These topics will be expanded upon in later units and it is therefore vital that students understand the key concepts at this stage.

On completion of the topic, students will be able to:

- Describe the Public Key Infrastructure;
- Explain digital signatures;
- Explain the role of Certification Authorities.

2.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

2.3 Timings

Lectures:	2 hours
Laboratory Sessions:	2 hours
Private Study:	7.5 hours
Tutorials:	1 hour

2.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- The Public Key Infrastructure
- Digital Signatures
- Certification Authorities
- Digital Certificates

2.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

2.4.2 Lecture 1

Slides 3-5: An overview of Topic 2.

Slide 6: This slide provides a brief explanation of PKI including two ways in which it is commonly defined.

Slide 7: The benefits of using PKI are providing certainty as to the quality, the source, the destination and the privacy of information. It also provides assurance as to the timing of information and can provide evidence in legal cases.

Slide 8: PKI was primarily developed to support the transfer of data over insecure networks. The growth of the Internet and its use for data transfer made this a priority. However PKI is also suitable for and is used regularly in private networks such as the internal transfer of secure and private data within a corporation’s internal networks. PKI is also suitable for the secure transfer of cryptographic keys between users and is important in facilitating other services that rely on cryptography.

Slide 9: PKI utilises public key cryptography via a pair of related cryptographic keys. It verifies the identity of the sender via digitally signing the message and ensures privacy via the encryption of the message.

Slide 10: Before showing this slide, ask the students to give a brief overview of public key cryptography which was covered in Topic 1. The slide outlines the key points: there are two mathematically related keys but the private key cannot be easily calculated from the public key. One key is used to encrypt the data and the other to decrypt.

Slide 11: This slide describes the difference between public and private keys; you could again try to elicit this from students before showing the slide. Public keys are freely distributed and, therefore, in the public domain. Private keys must be kept secret, if a private key is known publicly then the system is no longer secure. It is this secret private key that proves the identity of the message sender.

Slide 12: Next, we revise the key difference between asymmetric and symmetric encryption. This key difference is that in asymmetric encryption only one party knows the secret private key and, therefore, this party can be uniquely identified.

Slides 13-14: These slides cover public key encryption followed by private key decryption. It is normal that symmetric encryption is also involved in the process as it is used to generate a random session key, which is then used to encrypt the data. Symmetric encryption is significantly faster than asymmetric encryption. This session key is then encrypted using the public key and both are then sent to the intended recipient. The recipient cannot read the message without first decrypting the session key and they must have the secret private key in order to do this. Once this random session key has been decrypted, the actual message can be decrypted.

In essence, symmetric encryption is used for the message and asymmetric encryption is used to encrypt the symmetric encryption.

Slide 15: An overview of digital signatures is introduced here. They are encrypted numerical values generated by a hashing function that are unique to a specific document.

Slide 16: A secret, private key is used to encrypt the numerical value generated by the hashing function. This encrypted value is then sent at the end of the file or as a separate file and the public key may also be sent along with this. Make sure that students understand that digitally signing a document authenticates the sender but it does not provide anonymity.

Slides 17-18: The receiver uses the public key to decrypt the hashing value and this value is used to calculate the hash value of the data. If the value calculated by sender and receiver match, this proves that the sender is who they say they are and that the data has not been tampered with in transit. If a public key certificate was sent, then this is validated via the Certificate Authority. Lecture 2 will deal with digital certificates in more detail.

Slide 19: This slide provides a very brief example of how this works when receiving a document via email.

Slide 20: A brief summary of public key encryption is provided to conclude the lecture.

2.4.3 Lecture 2

Slides 22-24: This section begins with an overview of Digital Certificates, including an introduction to Certificate Authorities. Digital Certificates, for example a certificate to guarantee the security of an online shop, are issued with restrictions on what they are used for and this means that the recipient of a digitally signed file must check that it is being used for a purpose for which it is validated. Inform the students that there will be more detail on Certificate Authorities later in this lecture and more on PGP in Topic 4.

Slide 25: Whilst Digital Certificates do not have to adhere to any standards, most issued by Certificate Authorities adhere to the ITU (IETF) standard X.509.This means the certificate includes information on the private key, the hashing algorithm, the dates when the certificate is valid and the actions the key can be used for.

Slide 26: The six components of a PKI system are listed. These are expanded upon in the following slides.

Slide 27: The Certification Authority (CA) issues certificates and verifies the identity of the owner to a certain standard and signs the certificate.

Slide 28: The matching private and public key pair may be generated by the CA or alternatively by the individual requesting the certificate. When an individual generates the key pair themselves, there is an element of enhanced security as the private key has not been transmitted to the CA.

Slides 29-30: The CA will make checks as to the identity of the person or organisation requesting the certificate. These checks can be carried out with different levels of rigour and robustness and there are different levels of certificate that reflect the confidence in which the certificate holder’s identity has been proven. Students will investigate this in more detail in the private study exercises.

Slide 31: It is possible for an individual or organisation to hold a large number of certificates from many CAs. Some web applications may insist that a certificate comes from a CA that they have authorised, thus limiting from where it can be obtained. In general, certificates can be issued by authorities within your own organisation, another organisation or commonly by an independent authority such as Verisign.

Slide 32: By signing a certificate, the CA prevents its modification. Signature validation occurs automatically via the public certificate which is held in a Root CA list.

Slide 33: Lists exist of digital certificates that are no longer valid (revocation lists). These exist outside of the system that stores certificate information. Students can think of it as similar to a list of expired or stolen credit cards that are not valid. They may be public as certificates may be distributed outside of the original organisations involved.

Slide 34: A Registration Authority (RA) is a third party employed by a CA to carry out the checks on the person or organisation requesting the certificate. RAs may appear to be a CA to the certificate requestor but the key difference is that they do not sign the certificate.

Slide 35-38: In order for certificates to be used, they must be made available to all those requiring access. There are a number of methods to ensure this, including public directories that make all information available to those with access, private directories that limit access to within an organisation, proprietary databases that are used to store the certificates within an organisation, and the transfer of certificates via electronic media such as email and portable storage devices.

Slide 39: Certificate management systems are usually maintained by CAs to track certificates and their responsibility to clients. They are used to publish, temporarily or permanently suspend, revoke and renew digital certificates. Such systems do not normally delete certificates as they may be requred in future disputes including legal actions.

Slide 40: PKI aware applications have in-built toolkits from specific CAs, thus allowing them to use that CA’s PKI functions.

Slide 41: References

Slide 42: Questions

2.5 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will need to provide support and advice for students while they undertake Exercise 1 and ensure that appropriate digital signatures have been produced. Students can then work in small groups to undertake the research in Exercise 2.

Exercise 1:

Create your own digital signature for a file created by yourself on your laboratory network. (Microsoft Office documents can be digitally signed with your own digital signature.)

Take notes of the steps you follow to do this and note any sources of information you have used in researching the process. Also note any issues that could arise as a result of creating your own digital signature.

You will be required to write a formal report on this work (Private Study Exercise 1).

Exercise 2:

Research a Certificate Authority and compare the different levels of certificate they provide. For each level, note details of:

- Cost
- Class
- How identity of owner is attested
- Examples of use

You will be required to write a formal report of this work (Private Study Exercise 1).

Suggested Answer:

Costs will vary depending upon supplier; typical answers could include:

Class 1: Verifies email address of owner, used to sign emails and office documents.

Class 2: Verifies email address and personal identity documents, used to sign emails and office documents where an individual is not associated with a larger trusted organisation.

Class 3: Verifies email address plus identity of individual plus identity of organisation, used by identities who represent an organisation and are required to sign documents with a high level of security.

2.6 Private Study

The time allocation for private study in this topic is expected to be 7.5 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1: Laboratory Reports

Neatly write up the Laboratory Exercises in a formal report. Your reports should include all steps carried out in the laboratory work, as well as a discussion of any problems encountered and solutions attempted to deal with problems. These will be discussed during the tutorial for this topic.

Your report should include:

Laboratory Exercise 1

- Source of information
- Steps required to creating your own digital signature
- Problems encountered and solutions (if any)
- Issues with producing your own digital signature

Laboratory Exercise 2

- Source of information
- Costs
- Classes
- How identity of owner is attested
- Examples of use

Suggested Answer:

Formal reports including the above information.

Exercise 2: Hash Functions

Investigate practical hash functions.

a. What are the most popular hash functions?
b. How big a hash value do they produce?
c. Provide a brief overview of each one.

Suggested Answer:

Students may include any number of hash functions but some of the key ones are:

GOST processes variable-length messages into fixed-length output of 256 bits. The input message is broken up into units of 256-bit blocks; the message is padded by appending as many zeros to it as are required to bring the length of the message up to 256 bits. The remaining bits are filled up with a 256-bit integer arithmetic sum of all previously hashed blocks and then a 256-bit integer representing the length of the original message, in bits.

The **MD5 Message-Digest Algorithm** produces a hash value that is usually expressed in hexadecimal form as a 32-digit number. As each hexadecimal digit is expressed as 4-bits the hash value has 128 bits. The MD5 algorithm has been employed in many security applications, and is often used to check data integrity as well. However, it is now known that MD5 is not suitable for applications like SSL certificates or digital signatures as it possible to create the same output from several different inputs.

SHA-1 is one of a series of “secure hash algorithms” with SHA 0, SHA-1 and SHA-2 being the main variants. SHA 0 had a serious weakness and SHA-1 was developed by the U.S. National Security Agency to overcome this. This NIST published algorithm has been widely used in a number of protocols. However, security flaws were discovered in 2005 due to a mathematical weakness in the algorithm and as a result stronger hash functions were required in order to provide stronger security.

Whirlpool is a hash function that operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits.

Exercise 3: Digital Signature Providers

Research a commercial provider of digital signatures available in your country and note detail on:

a. The file types that can be signed
b. Price of the service

Suggested Answer:

This will very much depend upon the service provide that the student researches.

2.7 Tutorial Notes

The time allowance for tutorials in this topic is 1 hour.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercises. You may also wish to collect in the students' lab reports for marking and more formal feedback.

You could ask students to work in pairs or small groups to prepare short presentation on one of the hash functions and/or digital signature providers they researched. Students should then augment their own notes while listening to other students' presentations.

You should also allow some time for any questions students may have about the contents of this topic.

Topic 3: Web Security

3.1 Learning Objectives

This topic provides an overview of the issues that are specific to web security and mechanisms for securing web traffic including SSL/TLS.

On completion of the topic, students will be able to:

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

3.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

3.3 Timings

Lectures:	2 hours
Laboratory Sessions:	2 hours
Private Study:	7.5 hours
Tutorials:	1 hour

3.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Overview of web security
- IPSEC
- SSL/TLS
- HTTPS

3.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

3.4.2 Lecture 1

Slides 3-4: An overview of Topic 3.

Slide 5: This slide gives a list of some security issues that apply to the Web but may not apply to other networks. Prior to showing the slide, ask the students to give examples of security issues that relate to the web and if any are not on the list discuss these with the class.

Slide 6: The Web uses a client server model where communications are two-way with messages and files passing from server to client and client to server. It is therefore possible for clients to pass files to servers that contain harmful content either as a malicious act or without knowing that the file they are passing is infected.

Slide 7: File transfer on the Web includes numerous file types for numerous types of content including text, image, video, sound and much more including real-time streaming of media files. The fact that multiple file types are used means there are many different threats that must be dealt with.

Slide 8: The Web has become increasingly important to business, not just as a means of advertising a business and their products and service, but as a means of carrying out business transactions including payment, ordering and invoicing systems. If the web-based systems of a company are compromised, there will be major consequences to that organisation in terms of its reputation but there may also be serious financial consequences in terms of the loss of future business, the direct loss of cash and compensation claims from clients.

Slide 9: Anyone who uses the Web will know that, in general, it easy to navigate around and use the applications it presents. Those who develop such applications also know that many are quite simple to develop if you have the underlying knowledge and skill set. The price for having such an accessible network is that the underlying software that makes it possible must be complex and with complexity comes risk. Complex software often has security holes that have not been detected by those creating it – but you can be sure that at some point a hacker will discover the flaw. There are cases where new Web software has been correctly installed and configured but is open to attack via a number of security flaws.

Slide 10: The Web is made up of millions of connections - clients to servers, servers to servers, etc - and this poses a threat when a server is compromised. The massive number of connections greatly increases the opportunity for a virus to spread or a hacker to gain access to clients or other servers. In theory, there is no limit to the spread of the problem.

Slide 11: Most people who use the Web are not trained in security issues and many have very limited or no knowledge of how to protect their computers and their communications. Millions of people connect to the Internet with no security software at all and many who have anti-virus software run it with out of date virus definitions. You might like to ask students to explain why this is problematic - these people do not pose a deliberate threat but many will have virus infections on their machines and be sending infected message throughout the Web without knowing they are doing so.

Slide 12: Securing the server as a piece of hardware requires the same steps as securing any computer. For the Web, the key component that is different is securing the traffic over a public network and this unit concentrates on that element of Web security. We will examine both IP Security that operates at the Network level and SSL/TLS which operates at the Transport level, plus touch on HTTPS. At this point it would be useful to ask the students to list the layers of the OSI model and get them to put them in the correct order and then compare this to the TCP/IP stack.

Slide 13: A diagram showing the relationship between the OSI model and TCP/IP is given here.

Slides 14-15: These slides show how the security protocols relate to other Web protocols.

Slide 16: IPSec provides security services for TCP and IP protocols to use and they can be used to create a secure path even when travelling through unsecured networks.

Slide 17: In order to create an IPSec connection, both parties must first agree on the protocols to be used along with the encryption and decryption algorithms. These protocols and algorithms must then be used in any communication between the parties.

Slide 18: There are two core protocols to IPSec. The IPSec Authentication header authenticates the message sender and verifies that the data has not been tampered with. The Encapsulating Security Payload encrypts the message payload to provide privacy.

Slide 19: IPSec does not specify encryption algorithms, policies and key exchange mechanisms but provides a framework in which these can be used. Both MD5 and SHA-1 are commonly used hashing algorithms used for encryption with IPSec and there is scope for organisations to create their own security policies as required. One important element is the requirement to securely exchange security information and this is done using the Internet Key Exchange (IKE) protocol which uses UDP packets to transfer the information.

Slide 20: There are a number of applications that use IPSec. The creation of a company VPN using the Internet to provide secure connections will reduce costs; remote staff can securely connect to a company via the Internet; partner companies may securely connect to each other via an extranet; and it may be used to enhance the security of eCommerce systems.

Slide 21: There are many advantages to the use of IPSec including protecting a network by using it in a firewall or router so that all traffic passing through the boundary is secure. IPSec is transparent to both applications and users so that there is no need to neither change software, nor train users in systems using it. IPSec may also be applied to individual users wherever required.

3.4.3 Lecture 2

Slide 23: An introduction to SSL and how it historically relates to TLS.

Slides 24-25: SLL is comprised of two layers of protocols that use TCP to create a reliable and secure end-to-end connection. The bottom layer is the SSL Record Protocol with the SSL Handshake, Cipher Spec and Alert protocols running on the higher layer. HTTP which is used for communication between client and server on the Internet can operate on top of the SSL Record Protocol.

Slide 26: A connection is simply a transport, as defined in the OSI model, that provides a service. Ask the students for a definition of a transport at this point. In other words it provides suitable end-to-end communication services for applications. In SSL this means creating suitable peer-to-peer relationships between clients and servers. These connections are not permanent but only last for a required period of time (they are transient). Each connection is associated with a session.

Slide 27: An SSL session is an association between a client and a server. It is the role of the SSL Handshake Protocol to create sessions. A session may be shared by multiple connections and involves agreeing security parameters such as a session identifier, compression methods, cipher specification and the master secret shared between client and server.

Slides 28-29: The SSL Record Protocol provides two main services to a SSL connection, namely confidentiality and integrity. When transmitting a message, the protocol fragments the message into blocks of 2^{14} bytes or less; the message may then be compressed but this is optional; it is encrypted; the relevant information is added as a header, and then it is transmitted in a TCP segment. For received messages, the protocol first decrypts the message, then verifies the sender, decompresses the message if it has been compressed, reassembles the blocks in the correct order, and passes it up the protocol stack for higher level users.

Slide 30: The Change Cipher Spec Protocol is a single byte containing the value 1. Its purpose is to cause the pending state to become the current state, thus updating the cipher suite on a connection.

Slide 31: The SSL Alert Protocol is used to provide alerts to the client. It consists of two bits with the first giving the severity of the alert - either a warning or fatal. If the alert is fatal, the connection will be closed but other connections using the same session may continue. However, no new connections on this session will be made. The second value indicates the type of alert.

Slide 32: There are a number of alerts and some are listed here. Some of these are automatically fatal and cause the connection to close and these generally relate to failures of the handshake or decompression, unexpected messages and illegal parameters. Other messages are the close_notify message, notifying that a party is closing the write side of a connection and a range of messages relating to problems with the security certificate.

Slides 33-34: The SSL Handshake Protocol is the most complex part of SSL and involves the authentication of both client and server, and the negotiation between them of the encryption and algorithm keys that will be used in a session. The handshake process must take place before any application data is transferred. The protocol involves a series of messages containing the same three fields but populated with different values. The type filed is a single byte that indicates the types of message. The length field is three bytes and indicates the number of bytes in the message. The content field is of variable length and holds the message content.

Slides 35: The exchange of messages is initiated by the client and begins with the establishment of security credentials such as the ciphers to be used and compression methods. Then the server is authenticated and its key exchanged; the client is then authenticated and its key exchanged. Finally the exchange is ended and a secure connection is set up.

Slide 36: The use of HTTP over SSL (or TLS) is known as HTTPS. It is the standard method of creating secure communications between a Web server and a Web browser. HTTPS capabilities are built into modern browsers but, in order to work, it must also be supported by the server.

Slide 37: There are a number of differences between HTTPS and HTTP alongside the increased security. The first is that when running a HTTPS connection, the browser will show the URL beginning with https:// rather than http://. The connection will also use port 443, which invokes SSL, rather than port 80 as used by HTTP. If all is well with the HTTPS connection, the browser will also indicate this via a symbol such as a padlock.

Slide 38: HTTPS encrypts a number of elements of a communication. The URL of the requested document and its content are encrypted along with the HTTP header and any cookies. An important element for the security of websites is that any forms displayed and the contents of those forms are also encrypted. This means that when a person fills in a form on a browser running HTTPS, the elements filled in by the user are encrypted. This protects usernames, passwords, credit card details, etc.

Slide 39: One of the key advantages to using SSL/TLS is that once a connection has been created, it is independent of the application wishing to use it and therefore, allows for the transfer of a wide range of file types. SSL/TLS is also included with all major platforms making it readily available for use.

Slide 40: The downside to using SSL/TLS is the increase in processing overhead as a result of implementing security and this largely falls upon the server. In modern systems with fast servers and data transfer speeds, this should not be a major issue as long as the server is suitably configured and has the capacity to deal with the load.

Slide 41: September 2011 - researchers appear to have broken the SSL/TLS cryptographic technique and this will have major implications for secure Internet communications. Fixes proposed by major organisations do not close this security hole according to the researchers who have made the breakthrough. Ask students about the implications this has for conducting business over the Internet. If fixes are successful you could ask students for their thoughts on this happening again.

Slide 42: References.

Slide 43: Questions.

3.5 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will require access to a server and a website that allows the students to set up a digital certificate – this can be one very basic website that all students use.

You will need to provide support and advice for students while they undertake Exercises 1 and 2 and ensure that digital certificates have been obtained and installed correctly. You may organise Exercise 1 as a class exercise providing a single certificate that can be installed by students working in small groups.

Exercise 1:

Apply for a digital certificate from a Certificate Authority (CA). You may need to research the availability of free trial digital certificates and your tutor will advise you on how to proceed. There are usually a number of CAs offering free trials.

Note the steps you have followed in obtaining the certificate and information you had to supply. You will be required to write this up as a formal report in the Private Study exercises.

Suggested Answer:

The exact details will depend upon the information requested by the CA. Information provided should include:

- Details of the CA
- The information requested by the CA
- The uses the certificate is authorised for
- The certificate code

Exercise 2:

Install the digital certificate on a server of your choice to secure a specific domain name. Test that it works correctly by accessing the site from a browser. Your tutor will provide you with details of where to install the certificate.

Note the steps you have followed in installing and testing. You will be required to write this up as a formal report in the Private Study exercises.

Suggested Answer:

The exact details will depend upon the certificate and server. Information provided should include:

- Server type
- The installation process
- Testing via browser
- Any errors or problems and how these were resolved.

3.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Lecturers' Notes

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Write up both of the laboratory exercises in a formal report, ensuring you include all relevant detail.

Suggested Answer:

The report should be of professional standard and include all of the detail listed in the Laboratory Exercise answers.

Exercise 2:

Research Internet Key Exchange (IKE) as used in IPSec and note its purpose and key features.

Suggested Answer:

A general outline is expected that covers the following points:

- IPsec does not use Public Key Infrastructure and exchanging keys before an IPsec connection is established as a problem.
- IKE solves generation of a symmetric key for a session of IPsec but without PKI, man-in-the-middle attack is possible.
- IKE (Internet Key Exchange) creates Security Associations (SA). That is, parties in IKE negotiate keys for the SA.
- SA is a data structure containing keys and other relevant information for the connection.
- IKE is a general purpose key exchange protocol. It is used by IPsec, but it can be used by other protocols that need SAs as well.
- Thus IPsec SA is not directly IKE SA, but IKE SA can be converted to IPsec SA (or to SA of some other protocol).
- IKE is a formally checked cryptoprotocol. IKE is rather complicated; usually a secure cryptoprotocol is complicated.

If tutors wish to delve a little deeper into the IKE protocol, then the following points can also be discussed with the students:

- IKE creates SA, refreshes them and deletes them.
- IKE has the following exchanges:
    - Phase one (creation of IKE SA): There are two modes for phase one: main mode or aggressive mode
    - Phase two (creation of IPSec SA): there is only one mode: quick mode
    - Maintenance of IKE SA

- Negotiation of private Diffie-Hellman groups

- What the last exchange means is that in the phase one there are several predefined ways to use Diffie-Hellman, but one can define your own ways.
- IKE protocol initial message exchanges are not encrypted.
- IKE uses (normally) the UDP port 500

Exercise 3:

Research the SSL handshake in detail and make notes on the details of the messages passed and their sequence.

Suggested Answer:

A general outline similar to the following is expected:

1. A client "hello" message is first sent to initiate the protocol and this lists the cryptographic capabilities of the client including an order of preference, which gives the version of SSL used, the cipher suites supported by the client, and data compression methods that the client supports. The message also contains a 28-byte random number.

2. The response from the server is its own "hello" message containing the cryptographic method (cipher suite) and data compression method it wishes to use, the session ID, and another random number.

   The handshake fails if the client and the server cannot support at least one common cipher suite. The server will usually choose the strongest common cipher suite.

3. The server sends its digital certificate.

   If the server is using SSL V3, and also requires a digital certificate in order to authenticate the client, the server will send a “digital certificate request” message. This message contains a list of the types of digital certificates supported and the names of acceptable certificate authorities.

4. The server sends a “hello done” message and then awaits a client response.

5. The client, the Web browser, verifies that the server's digital certificate is valid and checks that the server's “hello” parameters are acceptable.

   If the server has requested a digital certificate from the client, this is sent, or if no digital certificate is available, the client sends a “no digital certificate” alert. This is only a warning and does not automatically close the communication, but this may occur if client authentication is mandatory.

6. The client sends a “client key exchange” message. This message contains a 46-byte random number known as the pre-master secret which is used to generate the symmetric encryption key and the message authentication code (MAC) keys that are encrypted using the public key of the server.

   Where a client has sent a digital certificate, the client also sends a “digital certificate verify” message that has been signed with the client's private key. This allows the server to verify the ownership of the client digital certificate.

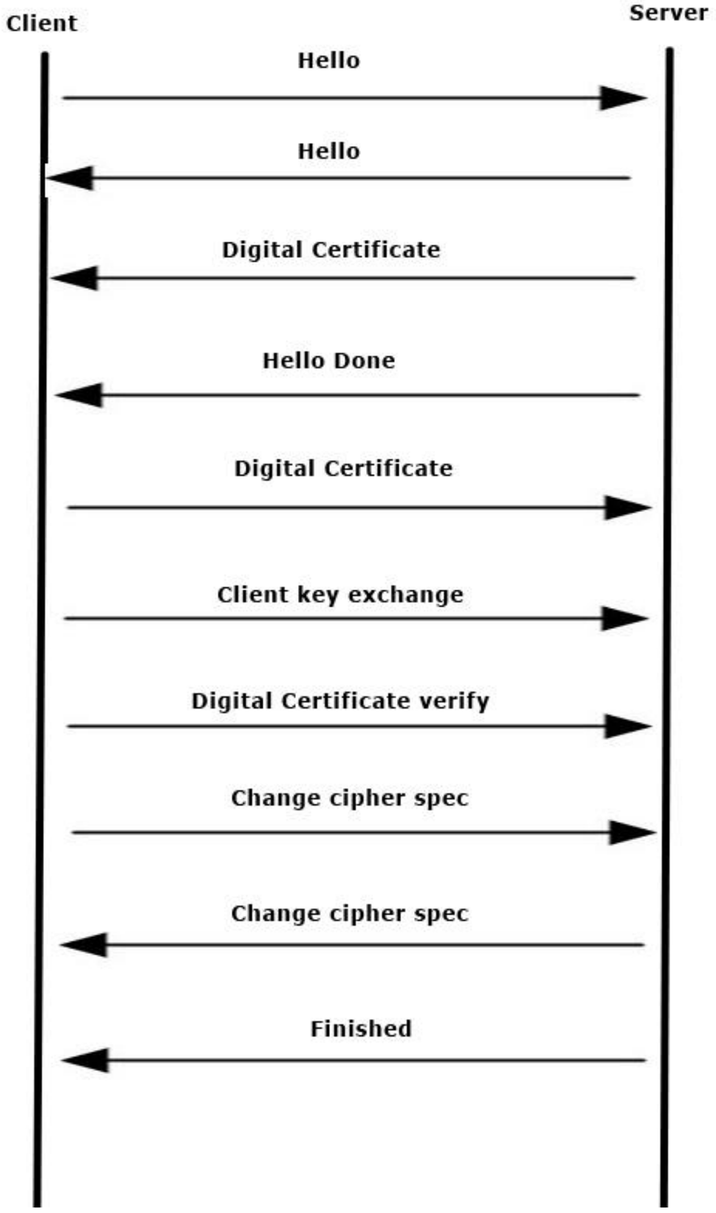
There is no need to verify the server digital certificate, if the server does not have the relevant private key it cannot decrypt the pre-master secret nor create the correct keys for symmetric encryption and the handshake will fail.

7. A series of cryptographic operations are used by the client to convert the pre-master secret into a master secret and all keys for encryption and message authentication are derived from this. The client sends a “change cipher spec” message to make the server switch to the newly negotiated cipher suite. The client sends the “finished” message which is the first message encrypted with this new cipher suite.

8. The server responds with its own “change cipher spec” and a “finished” message.

9. The SSL handshake ends and encrypted data can be transmitted.

This process is shown diagrammatically below.



3.7 Tutorial Notes

The time allowance for tutorials in this topic is 1 hour.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercises. You may also wish to collect in the students' lab reports for marking and more formal feedback.

You could ask students to work in small groups to prepare a short presentation on the SSL Handshake messages. Students should then augment their own notes while listening to other students' presentations.

You should also allow some time for any questions students may have about the contents of this topic.

Topic 4: Email Security

4.1 Learning Objectives

This topic provides an overview of email security including security threats and protection with emphasis on PGP and S/MIME.

On completion of the topic, students will be able to:

- Describe email security mechanisms;
- Digitally sign an email.

4.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

4.3 Timings

Lectures:	2 hours
Laboratory Sessions:	2 hours
Private Study:	7.5 hours
Tutorials:	1 hour

4.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Email security threats
- Email security solutions
- PGP
- S/MIME

4.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

4.4.2 Lecture 1

Slides 3-4: An overview of Topic 4.

Slide 5: An overview of the importance of email to business organisations. Email is the main method of communicating in writing in a business setting and also for the transfer of documents due to its simplicity, speed and cost effectiveness.

Slide 6: Before showing the slide ask the students to quickly list the security threats that apply to email communication. Make a compiled list of all of their suggestions and hold a discussion on the problems they cause, which threats are the most important, etc. There are many security threats and, as a result of the widespread use of email, these can have major consequences for mission critical business software and systems. Key threats come from viruses, hackers and also the increasing volumes of spam which use up network resources.

Slides 7-8: Viruses often appear as harmless email content such as jokes, promotional material and can be embedded in images and video files. In many cases the recipient has to open a file attachment in order to activate the malicious code but others launch as soon as the email is opened thus making it important that such emails are filtered out before reaching the inbox and policies are implemented that ensure that emails from unknown recipients are not opened. Most off-the-shelf email security solutions automatically inspect all outgoing and incoming email plus any attachments they contain and automatically update to deal with new attack signatures.

Slides 9-10: Spam is in essence “junk email” offering products and services you don’t want. Studies suggest that around 90% of all email is spam and that this costs billions of dollars per year in productivity and systems slowdowns. Whilst the majority of spam is simply annoying and takes time to remove, there is a proportion of spam that contains malicious code within it. Modern email security systems recognise spam in a number of ways including the use of certain words or phrases, the email size or format and the sender’s email address. Options are provided for dealing with messages identified as spam including moving them into a separate spam folder or deleting them directly from the server. Options are usually available to block email addresses or IP addresses that have been the source of spam.

Slides 11-12: Phishing is the process of sending emails that appear to originate from a trusted and respected source, such as a bank, with the aim of tricking the recipient into disclosing personal and financial details such as the details of their bank account. They range from the very obviously fake to cleverly crafted html emails that are formatted to look exactly the same as those from the supposed source. Most phishing emails are aimed at individuals but there have been attempts to target small businesses. Anti-phishing measures are generally included in email security software and these include authenticating senders, detecting spam messages, isolating or deleting spam messages and reporting procedures that notify others of the threat.

Slides 13-14: Spyware is software that dynamically records activities and data on an infected computer, having been installed without the user’s knowledge, often via downloaded freeware or shareware applications. The spyware normally transmits the information to the attacker via an Internet connection. Firewalls are insufficient protection against the threat of spyware but email security packages do usually block known spyware and regularly check the system for spyware activity.

Slide 15: One of the first steps in protecting against email security threats is authenticating the sender of the message. Verification of an email address and/or originating IP address plays a part in preventing spam, viruses and spyware. The Simple Mail Transfer Protocol (SMTP) was originally created to enable message transfer between academics or government bodies only and did not, therefore, have an inbuilt authentication method. Digitally signing emails provides a method of authenticating a sender but it does not tell the recipient if the sender is to be trusted.

Slide 16: TCP (Transmission Control Protocol) allows the automatic authentication of a source IP address, but this does not necessarily mean that the message was sent from the email address in the header. Attackers can easily modify an email header and copy email content from genuine emails to produce a phishing attack. Ask the students what a ’zombie’ is - if the sending computer has been compromised by a trojan horse and is under the control of an attacker, then the IP address an email was sent from will appear genuine.

Slide 17: One method used to protect email is the blacklisting of IP addresses where unwanted email has originated and then preventing future email from these addresses from reaching users by either quarantining or deleting the messages. This does not prevent a lot of spam as the system for allocating IP addresses ensures that many of these are allocated dynamically as and when they are needed. Organisations are allocated a block of IP addresses and when a user connects to the Internet they are allocated an available IP address. This means that a spammer may have a different IP address the next time they send an email and this may not be blacklisted.

Slide 18: Some Internet Service Providers have introduced methods that may help prevent their customers spamming. These methods include enforcing the use of port 587, instead of port 25, which requires authentication; limiting the number of received headers in email that is being relayed; cleaning and patching any computers that have been infected by viruses and trojans (this can be done remotely); and monitoring email for sudden spikes in traffic that often signify a flood of spam messages.

Slides 19-20: There are a number of threats we have not considered so far that relate to the content and communication of a valid email message. For secure email, mechanisms must be in place to prevent the alteration and reading of messages between sending and receiving, to authenticate users, and to encrypt information sent in the email body and header. Secure email systems that include the use of digital signatures to authenticate senders and encryption to protect the privacy of messages and headers will be discussed in the next lecture.

4.4.3 Lecture 2

Slide 22: Cryptography is used in email communication for three main purposes: to digitally sign a message to authenticate a sender and ensure message integrity; to encrypt a message body for privacy; to encrypt the communications between mail servers to protect the confidentiality of a message header and body.

Slide 23: Message signing is often combined with the encryption of the message body to provide authentication and privacy. It is common to digitally sign an email message that is being encrypted but digitally signed messages are only encrypted when the message is in some way confidential.

Slide 24: The transmissions of emails can be completely protected by creating a virtual private network (VPN), encrypting entire email messages or headers to encrypt details of sender, receiver and message subject. This is only normal when regular messages between two organisations require privacy.

Slide 25: Most emails are protected on an individual basis rather than using a VPN. Protected email messages are digitally signed with the option to encrypt the body of the message if this is required. The two most commonly used standards for signing and encrypting email messages are Open Pretty Good Privacy (OpenPGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME).

Slide 26: OpenPGP is a commonly used protocol for encrypting and digitally signing email messages. It is based on the earlier PGP protocol which was a proprietary protocol that had intellectual property right issues that prevented it from being used widely. OpenPGP is essentially PGP Version 5 and was released in 1991.

Slides 27-28: Many OpenPGP implementations use NIST recommended algorithms including 3DES and AES for data encryption, DSA and RSA for digital signatures and SHA for hashing, but there are implementations that utilise other algorithms. The 3DES and DSA algorithms are explored further in the private study exercises for this topic. The OpenPGP standard uses both public key and symmetric encryption techniques, with public key cryptography being used to create digitally signed message digests and symmetric key encryption being used to encrypt the message body. The reason for using symmetric keys is to reduce the overhead required for the encryption/decryption process.

Slides 29-30: There are a number of steps involved in creating a signed and encrypted email message using OpenPGP, and the order that these are performed in can vary for different implementations. The plaintext is compressed which helps reduce the likelihood of a successful cryptanalysis attack by removing commonly searched for patterns. This also reduces file size and therefore reduces transmission time. A random session key is generated and in some implementations this is done by getting the user to move their mouse within a window. A digital signature is generated for the message using the sender’s private key, and then added to the message. The message and signature are then encrypted using the session key and a symmetric algorithm, typically 3DES or AES. The session key is encrypted using the recipient’s public key and added to the beginning of the encrypted message. Finally, the encrypted message is sent to the recipient who reverses the steps to recover the session key, decrypt the message, and verify the signature.

Slide 31: Many popular mail clients require a plug-in in order to enable a user to both send and receive OpenPGP encrypted messages. There are a number of websites with details of how to apply these plug-ins to specific email clients.

Slide 32: Multipurpose Internet Mail Extensions (MIME) is a standard that supports the extension of text that includes non-ASCII characters both in the body and header of the message, the use of multi-part messages, and the attachment of multiple different file types including images, video, sound, etc.

Slide 33: Secure/MIME is a secure version of the MIME protocol that was developed by a group of software vendors and can, therefore, be easily integrated into existing email products. It, like OpenPGP, supports authentication and encryption of email messages.

Slide 34: The function of S/MIME is to provide cryptographic service to electronic messages via signing to provide authentication, message integrity and non-repudiation plus encryption to provide privacy and data security.

Slide 35: Many email clients support S/MIME and in theory this makes it simple for users using different operating systems with different mail clients to communicate securely via email. However there are different levels of support for the protocol in different mail clients.

Slide 36: Digital certificates are required from a Certificate Authority to operate S/MIME. It is recommended that different private keys are used for encryption and signature as this allows authentication of the encryption key whilst maintaining non-repudiation of the signature key. The receiver's certificate must be stored in order to do this.

Slide 37: The process of creating a signed and encrypted message in S/MIME is similar to that of OpenPGP. Two standard symmetric key algorithms are supported and it is recommended that AES is used as this is deemed to be more secure than 3DES.

Slide 38: Both OpenPGP and S/MIME use digital certificates in order to manage keys. The digital certificate attests to the identity of the user it was issued to, identifies the public key, gives other information such as expiry date, and is signed by a trusted party. There are, however, differences in how the two protocols manage keys.

Slide 39: OpenPGP uses the "web of trust" which allows individual users to make their own decisions on management and control. This works very well for individuals and for small organisations but in larger organisations it becomes extremely difficult to maintain a consistent policy and is therefore unworkable. Some organisations work around this problem by having keyservers that are repositories of user keys. This still means that the organisation has to largely trust individual members of the organisation and many organisations do not believe that such a system is sufficiently robust in terms of assuring the identity of individuals.

Slide 40: S/MIME uses a hierarchical structure of Certificate Authorities. At the top of the hierarchy is a highly trusted master CA that issues certificates to itself and subordinate CAs. Subordinate CAs can issue certificates directly to users and their subordinate CAs and so on. This allows any pair of users holding valid certificates to establish a chain of trust.

Slide 41: There are third-party services available that allow two organisations to exchange secure email via their services. This removes the need to establish a relationship of trust directly between the two parties and also eliminates the need for the two parties to have compatible email systems. It does, however, add a different trust issue between both users and the third-party provider as emails will reside on their mail server.

Slide 42: References

Slide 43: Questions

4.5 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will require email accounts for the students and also require the ability to obtain a digital certificate for email and the ability to install this. There are certificates available that are free for personal use and you should suggest that your students use your preferred provider of these.

You will need to provide support and advice for students while they undertake Exercises 1 and 2 and ensure that digital certificates have been obtained and installed correctly. Allow time and opportunity for students to feedback to the group once Exercise 2 has been completed.

Please note that you will need to confirm which algorithms students should research in Private Study Exercise 3 before the end of the laboratory session.

Exercise 1:

In pairs, send an email to each other. Examine the email header, make a note of each part and determine the information this gives you. Now use the remaining time to write a short report of your findings. Ask your tutor questions as necessary as you are writing up your findings.

Suggested Answer:

Details should be given of each element of the header and an explanation of the information this provides. A genuine header should be used and the explanations below should use the values in the header.

The message header must include at least the following fields:

From: The sender's email address; may also contain the name of the author or authors.

Date: The time and date at the sender's location when the message was written. Some email clients fill this in when sending but the receiver's client may then convert this to its local time.

The message header should include the following fields:

Message-ID: An auto-generated field that is used to prevent multiple deliveries

In-Reply-To: Message-ID of the message that this is a reply to, so that related messages are linked together. This field is only used for reply messages.

Common header fields include:

To: The address and possibly name of the message's recipient(s).

Subject: A brief summary of what the message is about.

Bcc: Blind Carbon Copy; addresses that were added to the delivery list but not listed for other recipients to see.

Cc: Carbon copy; addresses of those copied into the message who are not the primary recipients.

Content-Type: Information the message type, usually a MIME type.

Precedence: usually has a value such as "bulk", "junk", or "list"; used for example to prevent notices that a recipient is on vacation from being replied to or transmitted to other recipients.

Received: Tracking information showing which mail servers have handled the message (last handler first).

Reply-To: Email address that should be used to reply to the message – this does not have to be the same as the sending address.

Sender: Address of the sending email account.

Archived-At: A link to any archived form of a single email message.

Exercise 2:

Obtain a free digital certificate for use with personal email – your tutor will advise of the email address to use and provide the URL of a website where a free certificate can be obtained. Install the certificate and send an email to your lab partner.

You will be required to take notes and feedback to the group, describing the process of obtaining the certificate, installing it and sending a secure email message. Include details of any problems encountered and explain how you overcame those problems.

Suggested Answer:

The answer should include the following details:

- Details of the CA
- Process of obtaining the certificate
- Process of installing the certificate
- Process of sending a secure email
- Problems encountered and solutions to those problems

4.6 Private Study

The time allocation for private study in this topic is expected to be 7.5 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Although the use of OpenPGP and S/MIME improves the security of email transmission, there are costs associated with this. Research the negative aspects of using secure email and note the key points.

Suggested Answer:

Students should find several issues that may have a negative impact on an organisation as a result of implementing secure email protocols and these include:

- Firewall and mail server security services such as scanning for malware and viruses is made significantly more difficult by encryption. The firewall or mail server requires a method for decrypting the email so it can read and act upon the message contents.
- Encryption and decryption require extra processor time in comparison to unencrypted emails. Equipment may need upgrading if it is not capable of supporting the load.
- Extra administrative tasks may have to be carried out within an organisation such as key distribution, key recovery, and revocation of encryption keys.
- Email encryption can make it difficult for law enforcement agencies or internal investigators to investigate cybercrime or system abuses in the workplace.
- Encrypted emails sent to or received from other organisations may be insufficiently protected if those organisations do not support the use of strong encryption algorithms and key sizes. It may be necessary to get other organisations to strengthen their encryption mechanisms to meet the standards you require.

Exercise 2:

The lectures did not deal with securing the mail-server operating system (OS). Research the steps required to secure a mail-server OS and make notes on your findings.

Suggested Answer:

Students should define a number of key tasks to carry out such as:

- Planning the installation and deployment of the host operating system and components of the mail server
- Patching and updating the operating system as updates appear
- Configuring the operating system correctly to address security issues
- Installing and configuring other security software
- Testing the operating system to ensure that it is as secure as planned

These should be expanded on to some extent:

Security should be considered at the beginning of the systems development life cycle to maximise security and remove the need for expansive changes at a later date. Developing a plan in the early stages enables organisations to compromise between usability, performance, and risk.

After installation, an OS will need patches and/or upgrades to correct for known vulnerabilities. All OS's have known vulnerabilities that should be corrected before using them to host a mail server.

When configuring the OS, all services should be disabled and applications enabled only if required by the mail server.

The authorised users who can configure the operating system should be limited to a very small number of designated mail server administrators.

Mail server users will be a much larger group of people. In order to enforce policy restrictions the administrators must configure the OS to authenticate any new user by requiring proof that the user is authorised for such access.

Modern server OS allow an administrator to set access privileges to files, directories, devices, and other computational resources. By setting access controls correctly the mail server administrator can reduce the likelihood of security breaches.

OS's don't usually include all of the security controls necessary to secure applications fully. Administrators should install, and configure additional software to provide the missing controls (firewalls, etc.).

Exercise 3:

Research the 3DES and DSA algorithms and make notes on each. Prepare a short presentation on one of the algorithms – your tutor will inform you which one.

Suggested Answer:

Students should prepare a short presentation on one of the algorithms and the class should have half of the students preparing a presentation on each algorithm. The main points that should be presented are:

3DES

- 3DES is based upon the DES algorithm
- Developed as DES had become open to brute force attacks
- Applies DES three times, hence the name
- Also known as Triple DES (TDES)
- Uses three different keys, one for each DES application
- Gives an effective key size of 168 bits
- As it runs DES three times it uses three times the processor time which is a high overhead
- It is generally slower than AES and NIST has AES replacing 3DES as the standard algorithm over the coming years

DSA

- Digital Signature Algorithm
- An alternative to RSA
- Both RSA and DSA are included in the Digital Signature Standard (DSS)
- RSA is more commonly used
- DSA signatures are shorter than RSA
- Encryption is faster with DSA
- Verification however is much faster with RSA

4.7 Tutorial Notes

The time allowance for tutorials in this topic is 1 hour.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study exercises. You may also wish to collect the students' lab reports for marking and more formal feedback.

Students should be selected to present their findings on the 3DES and DSA algorithms. You may want students to initially work in groups with other students who have research the same algorithm and then give a group presentation to the rest of the class. Each presentation should be followed up with discussions on each of the algorithms and students should take notes to supplement their own research and to provide them with an understanding of both algorithms.

You should also allow some time for any questions students may have about the content of this topic.

Topic 5: Data Protection

5.1 Learning Objectives

This topic provides an overview of protecting data via disk and file encryption mechanisms. On completion of the topic, students will be able to:

- Describe disk encryption mechanisms;
- Deploy file encryption mechanisms.

5.2 Pedagogic Approach

Information and theory of the topic will be presented to the students during lectures. They will then practise the skills during the Laboratory sessions. Students are expected to undertake their own private study to understand the theory fully and put the lectures in context.

5.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

5.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Overview of data protection
- File encryption technologies
- Disk encryption technologies

5.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

5.4.2 Lecture 1

Slides 3-4: An overview of Topic 5.

Slide 5: Any networked system is open to unauthorised access to the data held within the system or data transmitted across the network. This unauthorised access may be the result of a malicious act to gain information that can be used to harm the organisation, or for the personal gain of the attacker, or it may simply be an exercise by a hacker to prove they are capable of accessing data on your system. Such threats generally come from outside of the organisation, but may also come from people within an organisation who attempt to access data that they do not have privileges to access.

Slide 6: All kinds of data may be of interest to a hacker but some data is particularly sensitive, including payment details such as credit card numbers, research and development information where a company is developing a new product, commercially sensitive information such as marketing plans, salary details, planned acquisitions, etc., and personal data relating to employees, clients and contacts that could be used maliciously against them, or simply to discredit the data security of the organisation storing the data.

Slide 7: The response from an organisation after it has been hacked largely depends upon the nature of the hacking. The response will be different depending on whether the data has been used to commit fraud (law enforcement agencies will be involved), or data has been amended or deleted (data recovery procedures will be needed), or the hacking was done as a prank with no long term consequences other than fixing the security hole. Other factors will have an effect such as the length of time that the hacking has been going on for, the nature of the data that has been accessed, who is aware that the data has been accessed, and whether there will be any evidence that must be saved in order to carry out a full investigation into the hacking or for any future legal action.

Slide 8: There are three strands to a strategy for preventing hacking. Firstly, a plan that lays out what is done, who is responsible for doing it and the tools and procedures that will be used; secondly, the use of suitable security technology including both hardware and software tools; and thirdly, ensuring that all users of a network are vigilant and are a key part of protecting the network they are using.

Slide 9: Any plan should include details of software, hardware and people. Responsibilities should be allocated to specific job roles and procedures laid out as to when log files are checked, how often updates and patches are applied and how often the procedures and plans should be reviewed.

Slide 10: A wide range of tools should be used to protect the network including firewalls, intrusion detection systems, virus and content scanning software, tools that assess the vulnerability of the network and any patches and fixes for security holes.

Slide 11: One of the most effective tools in protecting your network and the data it holds is by having staff that are fully committed to and trained in data protection. Hardware and software is ideal for running repetitive tasks that apply rules to the network security system, but they are not so good at noticing something new or unusual – this is something that only people can do.

Slide 12: Using methods to protect your data is a key security measure that complements the tools used to prevent unauthorised access to a network. The key elements to a data protection poily are backing up data to allow recovery, having strong access control mechanisms, using passwords to protect individual documents, encrypting individual files, and encrypting disks.

Slide 13: Any plan to protect data should include details of what data will be backed-up and when the back-up procedures will be run. All enterprise databases allow for the automated back-up of data and if tools are not available in an OS there are commercial software packages available that will do this for other file types. An important part of data back-up is the secure storage of this data including the storage of copies off-site, and ensuring that this data can be used easily to restore lost and damaged records.

Slide 14: Strong access control mechanisms can be used to protect data. These mechanisms can be applied to folders, sub-folders and individual files with access rights granted to groups of users, individual people and other network resources.

Slide 15: Individual files can be password protected and many common software packages have mechanisms for doing this, including MS Office and Adobe Acrobat. This method will not prevent a serious hacker from gaining access to the data but will often prevent the opportunistic hacker who, for example, could be a work colleague who is using your workstation.

Slide 16: Most operating systems support mechanisms for encrypting files, for example MS Windows has the Encrypting File System (EFS) tool, which allows a user to store information on a hard disk in an encrypted format but does not protect if it is transmitted over the network.

Slides 17-18: Packages are available to encrypt the entire contents of a disk or disk partition, which lock the whole content of that disk or partition. These packages automatically encrypt data when it is written to disk and automatically decrypt it before it is loaded into memory. Some of these packages create invisible folders or partitions that hide the data. Usually portable drives such as USB drives and flash drives can be encrypted as well.

5.4.3 Lecture 2

Slide 20: File encryption systems also allow for the encryption of folders. For most operating systems this is a very simple process to carry out, usually by an action in the user interface such as checking a box.

Slide 21: There are a number of advantages to using file encryption. Files can be encrypted individually and this means that if a hacker manages to crack the key for one file this does not provide access to other files as they use a different key. Encrypted files can be managed on a file by file basis, such as granting user access rights to specific files rather than a whole directory. Access control mechanisms can be provided via public key cryptography and the cryptographic keys are only available in memory whilst the file that has been decrypted is open.

Slide 22: Most file encryption systems that come with normal file management systems embedded in an operating system encrypt the file contents, but do not encrypt the metadata. This means that information such as the file name, file size, directory structures and timestamps for file edits are not encrypted and a hacker could determine the file's existence and location even if they cannot read the contents.

Slide 23: Specialised systems are available for the encryption of files and folders that encrypt contents and metadata. These files offer extra features such as deniable encryption, the ability to provide read-only access to encrypted files and the ability to provide different views of the files depending upon the user or key used.

Slide 24: There are a number of features that may be available in file encryption systems that provide deniable encryption. Usually the ciphertext can be decrypted into more than one readable plaintext version depending upon which key is used to decrypt it. Deniable encryption also makes it impossible to verify the existence of a file without the proper encryption key. An attacker will not know if the data was encrypted or if the owner has an encrypted file or even if the encrypted file can be decrypted by the owner.

Slides 25-26: Modern versions of Microsoft's Windows OS utilise the Encrypting File System (EFS) where a file or folder can be encrypted simply by checking the relevant checkbox. The EFS tool features an encryption method using certificates issued by a Windows certification authority, or self-signed, to protect individual files or folders. The system uses a combination of asymmetric and symmetric cryptography to encrypt files so they can be opened by the user who encrypted them, a designated recovery agent, and give the option to provide access to other user accounts.

Slide 27: Disk encryption uses software or hardware tools to encrypt a whole disk or part of a disk with the aim of preventing unauthorised access to the data it holds. Where everything on a disk is encrypted this is known as full disk encryption or whole disk encryption.

Slide 28: In full disk encryption, everything is encrypted including the blocks that hold the bootable section of the operating system, as well as any data stored. Some solutions will leave the master boot record unencrypted and therefore they do not really encrypt the whole disk. Ask the students what the master boot record is – it is the starting point the basic input/output system (BIOS) looks to when starting up the machine and holds the details of how to boot the disk and load the operating system, including information on disk partitions and the initial boot program. Some hardware disk encryption systems will also encrypt the master boot record providing greater security.

Slide 29: Often the same key is used for encrypting every partition on a disk but some solutions allow for the encryption of different partitions with different keys, which is more secure.

Slide 30: Disk encryption has a number of advantages over file encryption. Temporary files are encrypted and this is an important feature as a hacker could glean some important information from unencrypted temporary files. Any files saved to disk are automatically encrypted and this removes the possibility of a user simply forgetting to encrypt an important individual file. When a cryptographic key is destroyed it makes all of the encrypted data unusable and therefore useless when viewed. However, this does not remove the encrypted files, and for greater security tools should be used that purge or overwrite this data.

Slide 31: There are both software and hardware disk encryption tools available with externally based hardware tools providing some extra security features, e.g. the key is stored externally thus protecting it from any malicious code on the computer. External hardware tools also have little or no effect on system performance whereas software tools on the host computer will have performance overhead.

Slide 32: Disk encryption systems rely on the use of authentication methods including passwords. Therefore, it is important to have systems in place that allow passwords to be recovered in the event that they become unavailable. Such a situation could arise when an employee leaves an organisation quickly or simply forgets a complex password. In large organisations there could be a large amount of mission critical data stored on encrypted disks and the recovery system is vital. Any method used for the recovery of lost passwords should be simple to use but also secure in order to prevent unauthorised access to passwords.

Slide 33: A common password recovery system is to use the common ‘challenge/response’ systems that all students should be familiar with. Ask them for examples – they should be familiar with username/password, security question/answer (e.g. name of first pet) and other versions commonly in use. The advantages of this approach are that there is no need to store any passwords as the user knows the required response, there is no need for the secure exchange of secret data in the process, and it is not open to attacks via sniffers that can capture network traffic.

Slide 34-35: When full disk encryption is used the disk sectors that hold the operating boot system are also encrypted, meaning some decryption is required before the operating can boot up. A common method of dealing with this is to have a separate, small and secure pre-boot operating system that allows for user authentication that will decrypt the main boot system. There are a range of external keys that can be used to authenticate the user in this pre-boot OS. Before showing Slide 35, ask the students to come up with some examples.

Slide 36: References

Slide 37: Questions

5.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will require access to the file encryption systems available with your operating systems or other software that you use, with permission for the students to use these for this session. Students should have access to their own folder and the folders of their partners in order to test the effects of file and folder encryption.

Exercise 1:

You should work in conjunction with a lab partner for this exercise and the following exercise. Your tutor will advise you of the folders to use and files to create for the exercises. You should make notes of all steps carried out as you will be required to write a formal report of your laboratory work in Private Study Exercise 1.

1. Each person should create two simple files (for example two different word processed documents containing a small amount of text). Save both files in the folder allocated by your tutor.

2. Use the file encryption tools available in your operating system to encrypt one file but not the other. It is your decision as to how this is done. You could encrypt the file, or the file and the root folder for example.

3. Ensure that you have noted all the steps you have followed, the location and file names used, all messages from the system and the options you were provided with and have chosen.

Suggested Answer:

The exact answer will depend upon the file encryption system used but should include:

- File names
- Directory where file was stored
- Details of how file encryption is enabled including:
    - Dialog boxes shown
    - Action required
    - Options for folder encryption and options chosen
    - Any file sharing settings
    - Options for storage/copying of encryption key and options chosen
- Any other relevant data

Exercise 2:

Try to access both of your laboratory partner’s files as follows:

1. Open the files with a standard package for those file types
2. Move the files to another location
3. Copy and paste the files

Try to determine if/how each file has been encrypted from the results of your actions and check this with your partner.

Suggested Answer:

Students should be able to determine which file was encrypted and how. Their formal reports (Private Study Exercise 1) should in a description of what happened and the system messages received for each action.

5.6 Private Study

The time allocation for private study in this topic is expected to be 7.5 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Write up both of the laboratory exercises in formal reports ensuring you include all relevant detail.

Suggested Answer:

The reports should be of professional standard and include all of the detail listed in the laboratory exercises.

Exercise 2:

In small groups of 2 or 3, research a commercially available full disk encryption package. Make notes on the following:

- Manufacturer and package name
- The advertised benefits of using the package
- The features it provides
- Operating systems it is compatible with
- Languages supported
- Provide an assessment of the benefits of this package

Create a short 5 minute presentation on the package you have researched, you will be expected to present your findings in the tutorial session.

Suggested Answer:

The answer will be dependent upon the package researched but should include some detail on the information requested above.

Exercise 3:

Research ONE of the following methods as a means of pre-boot authentication:

- Smartcard and PIN
- Biometric method
- Dongle

Make notes on how the method you have chosen works, including some detail of the authentication process.

Suggested Answer:

The answer will be dependent upon the method researched but a brief outline of the key points is below.

Smartcard and PIN

- Credit card-sized card
- Usually tamper-resistant
- Used in conjunction with a card reader
- Card holder required to also input PIN (just like ATM)
- Can be used for multiple machines with same combination of card and PIN
- Can securely hold an encryption key but this is not activated without PIN

Biometrics

- Fingerprints are commonly used for pre-boot authentication, even in home user laptops
- Thought of as a strong authentication technique – often easy to guess a password or use brute-force to crack a password but not possible with a fingerprint
- No need to remember anything to authenticate
- Systems used to be expensive, but cost is not much of an issue now
- Can be used for multiple devices
- Means of "cracking the code" are rather gruesome!

Dongle

- A small piece of hardware that plugs into the system
- This device stores the key
- Can be used in combination with passwords or other authentication tools
- Simply having the dongle can authenticate the user
- Dongle itself can be encrypted
- Relies on the user keeping the dongle safe

5.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercises. You may also wish to collect in the students' lab reports for marking and more formal feedback.

You should also allow some time for any questions students may have about the contents of this topic.

Exercise 1:

Present your findings from Private Study Exercise 2 to the rest of the class.

You should note any key differences between the package you have researched and those from the other groups.

Exercise 2:

Work in a group with other students who have researched the same method in Private Study Exercise 3. Prepare a short presentation to give to the rest of the class.

You should then make notes on the other methods while listening to the presentations from the other groups.

Topic 6: Vulnerability Assessment

6.1 Learning Objectives

This topic provides an overview of assessing networks for vulnerability to attack, including the cracking of passwords via dictionary and brute force attacks.

On completion of the topic, students will be able to:

- Use port scanners to highlight open ports;
- Perform password cracking using dictionary and brute-force methods.

6.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

6.3 Timings

Lectures:	2 hours
Laboratory Sessions	2 hours
Private Study:	7.5 hours
Tutorials:	1 hour

6.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time and should be read in conjunction with the slides provided.

The structure of this topic is as follows:

- Overview of network vulnerability
- Port scanners
- Password crackers

6.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

6.4.2 Lecture 1

Slides 3-4: An overview of Topic 6.

Slides 5-6: Ask students for their definition of a security vulnerability before showing the slide. A security vulnerability in a network is a weakness or flaw in the network that allows an attack to damage the network in some way; such as providing a hacker with unauthorised access as a user of the network, causing the network performance to deteriorate in some way or damaging the data, software or hardware of the network. The vulnerability may be an inherent feature of the network, the result of poor design or a result of insufficient testing of one of its components. Another possible cause is the incorrect deployment or configuration of the network or one of its components or alternatively due to errors in the operation or management of the network and its resources.

Slide 7: There are a number of areas that can introduce vulnerabilities into the system. This includes the introduction of new software that has an inherent vulnerability or the incorrect configuration of new software; hardware may be placed in an environment that makes it vulnerable due to dust or humidity, or there may be access by unauthorised personnel; organisational procedures may not include the requirement for secure passwords that regularly change and there may not be audit procedures for regular software updates and patching; the organisation may not recruit suitable personnel or may not train its staff sufficiently; the physical environment which holds key network equipment may not be secured. There could be a combination of these and other factors.

Slide 8: Modern networks are very large and complex and this size and complexity makes security flaws more probable. It also makes complete network testing impossible, as the time required to test every service and every connection would be huge.

Slide 9: Networks are made up of many components including operating systems, hardware and software. Many of these components are used throughout the world and knowledge of their make-up and operation is widespread. This means that if vulnerability is discovered it will be quickly exploited and the knowledge of it will be spread quickly via the Internet. However, so will the fix.

Slide 10: The simple fact that a network provides many services means that there will be many connections, many users, a large number of different protocols and many different ports in use. Each one of these could be potential security vulnerability.

Slide 11: Passwords provide an opportunity for hackers to crack them and thus appear to the system as a legitimate user. The cracking of passwords will be examined in greater detail in the next lecture (or second part of this lecture, if not separating the lectures). Examples are given from a survey in the UK from 2006 where the passwords “123”, “Password” and “Liverpool” accounted for more than 20% of passwords used. This shows the need to enforce the use of strong passwords which should be allied to the need for regular changes to passwords.

Slide 12: Operating systems provide another potential security flaw, via default settings that may grant full access to all users or via administrators that do not use the OS to set suitable access privileges to users. It is also true that all operating systems come with undiscovered flaws.

Slide 13: Access to the Internet provides a huge potential security hole in a network. There are many websites with malicious code, including viruses, spyware and other malware. If malicious code becomes active on a network it could cause major problems. Standard security practices including firewalls, anti-virus software, staff training and acceptable use policies play a large part in protecting networks from these threats.

Slide 14: Most complex software packages will come with a few bugs, especially when first released. These are not malicious attempts to create vulnerabilities but are simply due to the complexity of the software. Patches and fixes are regularly issued and should be applied. Such updates can usually be applied automatically to genuine copies of the software.

Slide 15: Human action provides the greatest threat to a network, whether by malicious action or by accident. One key security hole, if software is not coded correctly to validate user input, is the insertion of malicious code in user-entered input such as when completing text boxes on a web form. Two such attacks are the SQL Insertion attack and the Buffer Overflow attack and you can inform the students that they will research these as part of their Private Study.

Slide 16: It is common in modern programming methods to reuse code and libraries from past programs. It is, therefore, important to remove any security flaws from old code before reusing it. There are organisations that publish known vulnerabilities to help programmers and system designers from repeating past mistakes and the Open Web Application Security Project (OWASP) is one such source.

Slides 17-18: Every operating system has been found to have vulnerabilities. The best method of dealing with these vulnerabilities is to operate good security practices. This includes auditing and testing your security. Software is available that can be used to test your network for vulnerabilities and in some instances fix those vulnerabilities. Whilst this is a very important tool, the vigilance of the human users cannot be replaced.

6.4.3 Lecture 2

Slide 20: Network administrators have to accept the fact that their network will contain vulnerabilities. This means that an important task of network security management is the management of these vulnerabilities. This process includes prioritising vulnerabilities (in order to deal with those posing the greatest threat to the network), fixing vulnerabilities, reducing the consequences of any breach of the network by backing up data etc. and monitoring the network so that new vulnerabilities are detected and any attacks are dealt with in the appropriate manner.

Slide 21: Documentation exists on known vulnerabilities of software, hardware and operating systems. This is used in tools that test for known vulnerabilities. There will also be vulnerabilities that have not yet been discovered and the best defence is to have good security policies and follow sound security practices.

Slide 22: Penetration testing involves using the methods of malicious attackers from inside and outside the network to exploit vulnerabilities in the network. The aim is to uncover any network vulnerabilities that could be discovered by an attacker and then deal with those vulnerabilities in an appropriate manner. By operating in the same way as an attacker, information about system vulnerabilities is gained. In addition, the effectiveness of current defences is also measured and information on the potential effects of any security breaches is collated. This will allow those managing the network to take a view on where network upgrades are required and to make decisions on investment in network security.

Slides 23-24: A vulnerability scanner is a program used to test for known vulnerabilities in some part of a network, as part of a penetration test. There are different types that scan different elements of a network and scanners are available for ports, databases, web applications, network traffic etc.

Slide 25: Port scanners are software devices that probe a host for open ports. They are used both by network administrators and attackers to discover vulnerabilities. In the TCP/IP protocol suite each service from a host is identified by an address and a port number. There are 65536 possible port numbers but each service only uses a limited number.

Slide 26: Depending on the message received from a port, the scanner will determine whether a port is open (the host is listening and the port is open for communications), closed (where communication is not allowed on this port) or it is filtered (where some device such as a firewall is controlling the traffic).

Slides 27-35: An overview of common port scans is given with most using a TCP segment for the scan but a brief overview of a UDP scan is given. A brief explanation of the TCP three-way handshake is included (on Slide 29).

Slide 36: By cracking a password an attacker may gain access to an individual file, a computer or a whole network or system. As we have seen earlier many users have very simple passwords which make this easier. There are even many instances where users write down their passwords and store them near their workstations, or even write passwords on post-it notes and stick them to screens!

Slide 37: A dictionary attack relies on the use of weak passwords that use common words and as ‘password’ is a very common password it is easy to see why this technique will be successful. A list of common words is stored in a dictionary file and password cracking software runs all of these against the desired password until a match is found.

Slide 38: A brute force attack does not rely on the use of common words but the software runs all possible combinations of characters until a match is found. The average length of time this takes depends on the password complexity. The best defence is to use complex passwords together with cryptographic functions.

Slide 39: There are a number of common password-cracking applications available and their success is often based upon a combination of dictionary and brute-force attacks.

Slide 40: References

Slide 41: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

6.5 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will require port scanner software, such as Nmap, installed with student access to the software and the ability to scan at least one other computer on your network.

You will also require password cracking software and dictionary files that the students can download or that are already loaded for them to use (spell checking dictionaries can be used for this). It is necessary to direct the students to a particular folder or directory where passwords are held that they are to crack. Ideally this will hold dummy passwords rather than important passwords for the system. These could be set up specifically for this exercise with two or three set up for a dictionary attack and one or two more complex passwords for a brute force attack.

It is the tutor's responsibility to ensure that all required software is available, that scanning and password cracking is allowed, and that the network is configured to allow this, at least during the laboratory sessions. You will need to provide support to students as they work through these exercises.

At the end of the laboratory session, you should divide students into small groups to work in during the private study time to complete Exercise 2 and inform each group as to which attack they should research.

Exercise 1:

Your tutor will direct you to the port scanning program installed on your system and provide the necessary details of which computer to scan.

- Read any instruction manuals or user guides that come with the port scanner
- Scan the ports of the computer you have been directed to scan according to your tutor's instructions
- Print out the log/results produced by the port scanner
- You are required to produce a formal report as part of the Private Study Exercises and this should include:
    - A description of how the scan was carried out
    - Details of the scanning processes utilised by the software
    - The log/report file
    - A detailed explanation of the information produced by the log/report file

Suggested Answer:

A formal report should be produced by each student, which includes all of the detail above.

Exercise 2:

Your tutor will direct you to the password cracking program installed on your system and provide the necessary details of which folder or directory you will be accessing.

- Read any instruction manuals or user guides that come with the password cracking program
- Try to crack all the passwords in the folder your tutor has directed you to
- Print out the results produced by the password scanner
- You are required to produce a formal report as part of the Private Study Exercises and this should include:
    - A description of how the password cracker works
    - The log/report files produced
    - A detailed explanation of the information produced by the log/report file which should include:
        - Usernames
        - Hashed version of passwords (if hashing is used)
        - Plaintext versions of passwords

Suggested Answer:

A formal report should be produced by each student, which includes all of the detail above.

6.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Students need to be divided into small groups for Exercise 2 and informed as to which attack they should research.

Exercise 1:

Write up both of your laboratory exercises as formal reports, ensuring you include all relevant detail.

Suggested Answer:

The reports should be of professional standard and include all of the detail listed in the laboratory exercises.

Exercise 2:

Research either SQL Injection attacks or Buffer Overflow attacks, as directed by your tutor. You will be required to prepare a brief presentation of approximately 5 minutes for the tutorial session.

Suggested Answer:

Students should cover the key points of each attack type.

SQL Injection

- Allows an attacker to gain access to a database that underlies a website or online system
- Allows an attacker to potentially modify, add and delete data that is not meant to be available to users
- Where filtering of strings is not done correctly this makes it easy to gain access for example:
    - A simple login system with no filtering could allow access via an SQL statement
      SELECT password FROM users WHERE password = '' OR 1 = 1
      In this case the hacker has simply entered ' OR 1 = 1 as their password
      As 1 = 1 this is always true
- There are other versions using similar themes
- It is important that sql error messages are not shown to users as this gives further clues as to table names etc.

Buffer Overflow

- A buffer is a contiguous section of memory allocated for a specific purpose, such as an array
- There may not be any check on the amount of data a user can write to a buffer and this can therefore go out of the bounds of the buffer, an overflow

- A program that writes beyond the allocated memory for the buffer might result in unexpected behaviour
- The extra data may be written into memory areas that are allocated for program instructions rather than data and the program will attempt to execute these commands
- A hacker can inject malicious code into this overflow area and thus get a program to execute their commands rather than those originally planned by the programmer

Exercise 3:

Research port numbers used by common protocols over TCP/IP and UDP. Make a list of common protocols and port numbers used.

Suggested Answer:

Students' lists of common protocols and port numbers used should include:

- FTP port 20/21
- SMTP port 25
- DNS port 53
- HTTP port 80
- POP3 port110
- IMAP port 143/port 220
- SQL Server port 156
- BGP port 179
- IRC port 194
- HTTPS port 443

6.7 Tutorial Notes

The time allowance for tutorials in this topic is 1 hour.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercises. You may also wish to collect the students' lab reports for marking and more formal feedback.

Students should be selected to present their findings on SQL Injection and buffer overflow attacks. Each presentation should be followed up with discussions on each of the attacks and students should be encouraged to take notes to supplement their own research and to provide them with an understanding of both attacks.

You should also allow some time for any questions students may have about the content of this topic.

Exercise 1: Review of Private Study Exercises

Show your two lab reports (and also your research on port numbers used by common protocols over TCP/IP and UDP) to your tutor and discuss any problems you encountered on these exercises.

Give your presentation on SQL Injection attacks/Buffer Overflow attacks to the group. Answer any questions from your tutor or from the other students.

Topic 7: Authentication

7.1 Learning Objectives

This topic provides an overview of authentication techniques, including passwords, modern biometric authentication methods, and the use of multiple authentication methods. Some of these concepts have been introduced in earlier topics and this topic will reinforce these lessons and develop them further.

On completion of the topic, students will be able to:

- Explain the different authentication mechanisms;
- Describe multifactor authentication;
- Describe biometrics and their issues.

7.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

7.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

7.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Overview of Authentication
- Passwords
- Multi-factor Authentication
- Biometrics

7.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

7.4.2 Lecture 1

Slides 3-4: An overview of Topic 7.

Slide 5: We will concentrate on network user authentication rather than authentication for an individual computer or message authentication. User authentication is the primary form of defence for a network, to prevent unauthorised access to the network. By identifying authorised users the network administrator can set access controls for network resources and also make users accountable for their actions whilst logged into the network.

Slide 6: The authentication of a network user is a two step process. The first step involves identification where the user claims to be a specific identity to the network's security system (e.g. uses a username). The second step is the verification where the entity proves that they are the claimed user (e.g. uses a password) and thus binds them to the specific identity they have claimed to be. At this point they should have access to the network.

Slide 7: Before showing the slide, ask the students to list all the authentication methods they can think of. Then show the slide and group the students' answers into the four categories of: something they know, something they possess, something they are (static biometrics), something they do (dynamic biometrics).

Slide 8: There are potential problems with all authentication methods. Passwords, PIN, etc. can easily be forgotten, smartcards and other tokens can be lost, stolen or forged and biometric systems can produce false positives where an entity that shouldn't be authenticated is authenticated and false negatives where the genuine user is not authenticated. Most networks combine passwords with cryptographic methods for user authentication.

Slides 9-10: Smartcards are small electronic devices that typically have a small amount of memory and a small processor embedded in them. They are resistant to tampering and also are meant to be very difficult to duplicate. One big disadvantage is that they can be used by someone other than the intended user (they are transferable) but their use in combination with a password or PIN introduces a level of complexity that makes this more difficult. Before showing slide 10 ask the students for examples of the use of smartcards. Cards that are combined with a PIN have the problem that most PINs are 4-digit and therefore there are a limited number of combinations – ask the students to calculate the number of combinations – which is why ATMs limit the number of attempts to guess the correct PIN.

Slide 11: Passwords are the most commonly used authentication method and this is largely due to the fact that no specialised hardware or software is required to use them. A typical password authentication system involves the user typing a username and password combination, the security system then finds that user in a database and then checks that the password is the correct one, i.e. there is a username, password pair that matches in the database and then provides the relevant access privileges to the authenticated user.

Slide 12: The strength of the password is an issue for real-life systems, as users, when they are allowed to choose their own password, invariably pick an obvious combination of characters or use a person’s name or place name. Such passwords are very easy to crack via a dictionary attack. Where strong passwords are enforced, either by limiting the options available to the user or by supplying passwords to them, users will often write down the password and keep it near the computer thus providing an even greater security threat.

Slide 13: There are other means of obtaining passwords other than cracking or reading the piece of paper it is written. By eavesdropping on network traffic an attacker may determine what passwords are being used but encrypting traffic can greatly reduce the possibility of this occurring. Another common method is to gain access to the database storing the passwords which enables an attacker to learn all of the passwords on the system and change any at will. Individual sessions may be hijacked by an attacker who will allow a user to authenticate themselves and then disconnect the user leaving open the connection with the hijacker who then appears as the authenticated user.

Slide 14: It is common for users to forget their password, especially where strong passwords are used. A system that changes passwords at regular intervals overcomes this to a certain extent as new passwords will be supplied regularly. Password generators can be used that use a master secret to generate new passwords for all users of a system.

Slide 15: Many systems do not use a whole password or pass phrase to authenticate a user but request several specific characters from the password. The aim is to make it more difficult for an eavesdropper who would need many sessions in order to obtain the complete password.

Slides 16-17: Passwords should not be stored as plaintext in a database but should be encrypted before being stored. The recent hacking of Sony networks allowed hackers to easily obtain millions of username and password combinations as they were stored in plaintext. Hashing functions such as MD5 and SHA-1 are commonly used to encrypt passwords before they are stored in a database. These hashing functions are publically available and relatively simple to use but it is also difficult to obtain the password from the hashed result. Usually the system will store a plaintext username along with the result of hashing the password.

Slide 18: Whilst hashing a password provides a level of security from the time that is required to work out a password that would generate the hashing result this is not the case for a weak password. A weak password is still very open to the use of a dictionary attack where the dictionary file contents are hashed to produce the required result.

7.4.3 Lecture 2

Slides 20-21: In multi-factor authentication two or more verification methods are used. This is commonly used with ATM transactions where the user possesses a token (the card) and knows something (the PIN). Using several passwords is not multi-factor authentication as all of the verification methods used are something the user knows. A system employing usernames and passwords only is single-method verification as the username is the identification process not part of the verification process. Two factor authentication typically involves something the user possesses along with something they know. Three-factor authentication typically uses something the user possesses along with something they know and a biometric method.

Slide 22: There are disadvantages to multi-factor authentication systems, with cost being the primary disadvantage. A careful balance must be struck between the need for security and the associated costs of equipping users with tokens and purchasing the hardware and software required for processing tokens and biometric data. The nature and importance of the protected data should be the deciding factor.

Slide 23: By combining two or more verification methods, there is a very large decrease in the probability of “cracking” the verification methods.

Slides 24-25: Biometrics is the study and use of automated methods to recognise the unique characteristics of humans. These “unique” characteristics include physical features such as fingerprints, eye patterns (both iris and retina), hand measurements, facial features and also behavioural characteristics such as the way a signature is written, the speed of typing, voice patterns, etc. The aim of biometrics is to provide a verification method that is non-transferable. Passwords and PINs can be communicated to other users; smartcards can be passed to other users – ask the students to discuss how biometrics can be transferred to another user or somehow “cracked”.

Slide 26: In order to register biometric data with the system the user has measurements taken via suitable hardware and software. It is possible to take several biometric measurements of the same feature and/or different features. Some algorithm is applied to the data and it is converted into a template that is stored in the system database.

Slide 27: To authenticate a user the same biometric measurements are taken and the algorithm is applied to produce another template. This new template is compared to the template in the database and if there is a sufficient match the user is allowed access.

Slide 28: When two biometric measurements are taken from the same person it is very unlikely that there will be an exact match. For this reason tolerances are built into the matching algorithms to allow a close match to be accepted.

Slides 29-35: There are a range of biometric authentication methods.

Fingerprints have been used for this purpose by law enforcement agencies long before the invention of the hardware and software that allows this to be done by computer systems. The ridges and valleys that form a fingerprint are thought to be unique to an individual fingertip. The use of fingerprint recognition as an authentication method has become common.

Face recognition has two main forms, one uses the visible spectrum and the other uses the infra-red spectrum to record the heat signature of a face. Such systems are widely accepted by users but do suffer from problems under different lighting conditions and the use of masks can further confuse matters.

Speech recognition may be used as studies suggest that there are patterns of speech that differ between users. The physical anatomy of a speaker, such as mouth size, affects this, as do cultural factors in the language used, region they come from and the way they have learned to speak.

Iris patterns, the patterns in the coloured area surrounding the pupil of the eye, are thought to be unique for each person. The patterns are recorded via video cameras and the systems work when the user is wearing standard glasses or contact lenses. The equipment required for iris recognition systems is coming down in price and such systems may become more widespread as a result.

As well as fingerprints, other elements of hand and finger geometry can be used to identify an individual, including measures of length, width and surface area. Such systems have become commercially available and are in use for building access control mechanisms.

Written signatures have long been used in non-computerised systems but allied to suitable technology it is not just the final signature that is measured but also the way it is written, including writing speed, pressure and the angle of writing. These systems are in use in areas of business where signatures are an accepted means of identification.

In a similar way measuring the way a password is typed, via the speed of typing and interval time between individual characters, allied to the actual password itself, provides a biometric measure that can identify a user.

Slide 36: There are errors inherent in biometric authentications due to the need to allow tolerances in the matching algorithm. This results in both false positives, where a person is incorrectly authenticated, and false negatives where the system does not authenticate a genuine user. In some systems the rates of each of these errors can be varied by altering some of the system parameters and the error rates are generally very low anyway.

Slide 37: There are three main areas of concern with the use of biometric systems: privacy, injury and exclusion. The privacy issue relates to the fact that if such systems are in widespread use, all of the transactions of an individual in disparate systems can be attributed to that unique individual. Simpler systems do not allow this as a user can assume multiple identities using a different identity in each system. Injury concerns have two main strands, one is the hygiene of equipment used for the biometric measurement of many users and the other is the methods by which criminals could get the biometric “keys” to hack into a system. The exclusion issue relates to people with disabilities who may be missing a part of the body required for biometric authentication.

Slide 38: Fingerprints are now very widely used and fingerprint readers are now commonly supplied with new notebook computers. The cost of such systems is low and by combining them with a password or PIN a genuine two-factor authentication system is created.

Slide 39: References

Slide 40: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

7.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

You will require an image scanner and software and image manipulation software such as Adobe Photoshop. For the first exercise, ensure that you have your prepared signature scanned into the computer. The copying, scanning and observation of similarities and differences can be done as a whole group or with smaller groups/individuals, as you see fit. You may want to take a class vote on the best student forgery.

Exercise 1:

1. Your tutor will have written the word "Signature" in his/her own hand-writing and scanned it into the computer as an image. Examine this image and attempt to copy this signature on a piece of paper. Scan this into the folder containing the tutor's image of the signature.

2. Your tutor will also write the word "Signature" again on another piece of paper and scan this into the same folder. You should now use image manipulation software to compare and/or overlay images to compare your version and the tutor's new version with the original.

3. Note where there are obvious differences and similarities between your signature and the original.

4. Note where there are differences between your tutor's new signature and the old one.

You will be required to write a report on this in the private study exercises. Your report should include details of how the experiment was carried out, your findings and implications for signature recognition as a verification method.

Suggested Answer:

A formal report is required in the private study exercises. Students should have therefore compiled notes on the following:

- The process they carried out to create, store and compare signatures
- Whether any forgeries were close to the original
- Common differences between forgeries and originals
- Differences between the original and the real signature provided by the tutor
- An opinion as to whether any forgeries would be accepted
- An opinion as to whether the real signature would be accepted
- Implications of their findings.

7.6 Private Study

The time allocation for private study in this topic is expected to be 7 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Write up your laboratory exercise in a formal report ensuring you include all relevant detail.

Suggested Answer:

The report should be of professional standard and include all of the detail listed in the laboratory exercise.

Exercise 2:

Research and make a note of the twenty most common passwords used in common applications (replace any rude words or swearing with ***).

Suggested Answer:

Answers will vary depending upon the applications surveyed but there should be some common themes including:

- 123456
- 12345
- 123456789
- Password
- iloveyou
- princess
- ****you
- 1234567
- 12345678
- abc123
- Nicole (or other names)
- Daniel
- babygirl
- monkey
- Jessica
- Lovely
- michael
- Ashley

- 654321
- Qwerty

Exercise 3:

Research a commercially available biometric authentication system. Make notes on the biometric methods used and other key features such as:

- hardware required
- cost
- operating systems supported
- error rates
- other relevant information such as different applications the system is/may be used with

Suggested Answer:

Answers will vary depending upon the systems researched and some of the information requested above may not be available.

7.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercise. You may also wish to collect the students' lab reports for marking and more formal feedback.

You should also allow some time for any questions students may have about the content of this topic.

At this stage of the module, you should also take time to introduce the assessed assignment to students. Assignments for the relevant assessment cycle are available from the NCC Education Campus (http://campus.nccedu.com). You will need to ensure that each student has a copy of the assignment and understands the requirements. Assignments would normally be submitted for marking during Topic 9 or 10, depending on how much time you feel you need for marking.

Exercise 1: Review of Private Study and Laboratory Exercises

As a group you will review the tutorial and laboratory exercises from this topic and you should be prepared to discuss your own work and to hand in your lab report if necessary. Make sure you ask questions if there is anything you are not sure about from this topic.

Your lecturer will also introduce your assignment. You should make sure you have a copy of the task and fully understand what is required and when the assignment needs to be handed in.

Topic 8: Access Control

8.1 Learning Objectives

This topic provides an overview of access control methods via access control lists, packet filtering and the translation of network addresses, plus the monitoring of these methods via intrusion detection systems.

On completion of the topic, students will be able to:

- Configure access control mechanisms;
- Apply and manage port forwarding rules.

8.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

8.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

8.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides. The structure of this topic is as follows:

- Packet filtering
- Access control lists
- NAT
- IDS

8.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

8.4.2 Lecture 1

Slides 3-4: An overview of Topic 8.

Slide 5: Messages move around a network using three main protocols, IP, TCP and UDP. Ask the students for a brief explanation of the purpose of each of these protocols. Messages are broken up into packets with each packet having a header (or headers) that includes the addresses of the source and the destination, thus allowing routing devices to route the packet so that it reaches its final destination. As the header has source and destination addresses this can be used to create traffic control rules based upon source address, destination address or a combination of both. This topic examines the creation, application and monitoring of these rules.

Slide 6: A routing device examines a packet header to determine what it does with the packet and packet filtering simply adds an extra layer to this process. When a routing device examines the destination address and determines that it should process the packet, instead of forwarding it to the next node on the network it first applies a set of filtering rules to determine what happens. Such rules do not require the routing device to read the payload of the packet - only the header - and they can be applied to packets travelling both into and out of a network or section of a network.

Slide 7: Packet filtering rules implement the security policies of a network by either allowing or disallowing network services. The rules can be applied in a general way, such as preventing all traffic into a network, or in a more specific way so that they only apply to a specific machine or even a single port.

Slide 8: Most routers have inbuilt packet filtering capabilities and these are used to provide a first line of defence for a network. This approach is inexpensive and allows for strong protection but it is not sufficient on its own to fully protect a network.

Slide 9: Rules can be applied to single machines, to individual ports or to combinations of ports and machines, thus allowing for some complexity in the rules.

Slides 10-11: The simplest form of packet filtering is stateless filtering, which operates by using a set of rules created by an administrator. This is easy to create but has limitations on flexibility, as the rules are applied to every packet and no information regarding prior traffic (that could be used to “learn” whether a packet should be allowed through) is stored. The rules are in an Access Control List where rules are processed in a specific order. The first rule that matches the packet being inspected is applied to it and it is either blocked or allowed through. The default rule is that if a packet is not explicitly allowed then it should be blocked.

Slide 12: Stateful packet filtering is more complex, as details are held of previous traffic that was allowed through; including details of IP addresses, ports, handshake status, routes used and time. Packets are compared with previous packet traffic and can be allowed to flow in both directions, as decisions are based upon connections rather than an individual on-way rule.

Slides 13-15: In order to configure a packet filter the first step is to determine what traffic should be allowed or not at a conceptual level. This will include items such as connections to the Internet, email connections and internal network connections. The second step is to convert these into a set of rules that include IP addresses and ports or protocols. Thirdly these are converted into a format that is readable by the routing device carrying out the packet filtering. This third step may involve using an interface that is specific to the device and will not be covered in the lecture.

Determining the rules that are required involves considering (or mixing) the needs of the business and an assessment of the risks in allowing certain traffic into or out of the network. It is good security practise to block all traffic that has not been specifically allowed, in this way only the services essential for the running of the organisation are allowed and there is less risk of threats coming from unforeseen traffic.

The rules are created in an Access Control List which should include the IP addresses of source and destination to which the rule applies, ports to which the rule applies, the action to be taken (either to allow or block the packet), and some brief textual explanation of the rule.

Slides 16-17: It is important to note that the access control rules are applied in order. Each rule is applied to the packet until a match is found and the action is applied. All the following rules are then ignored so care must be taken to create the rules in the correct order. Typically this means rules that are more specific must be placed before more general rules. As an example, if Internet access is going to be blocked for the network except on one machine the rule allowing connection for the single machine must be placed ahead of the rule blocking Internet access. Slide 17 asks some questions relating to the simple rule table on the slide and this should be discussed with the class.

8.4.3 Lecture 2

Slide 19: Network Address Translation (NAT) allows multiple client computers on a network to use the same IP address when connecting to an external network such as the Internet. There are three advantages to this: the reuse of IP addresses allows more computers to connect to the Internet than there are IP addresses available, there are some security advantages and it simplifies some network management tasks.

Slide 20: Under IPv4 there were insufficient IP addresses to meet the needs of users on the Internet, though IPv6 has changed this. The main reason for the use of NAT was to overcome this problem of scarce IP addresses.

Slides 21-23: Each IP address consists of a network part to the left and a host part to the right. The exact length of each part depends upon the size of the network. The network number identifies the network and the host number identifies the individual computer on that network. There are four main classes of IP address, named A, B, C, D, with network size determining the class. Class A networks can have around 17 million hosts, Class B 65,000 hosts, Class C 256 hosts, the rest are class D hosts or reserved for special functions.

Slide 24: Internet Service Providers usually assign a unique IP address to individual customers but this may be done dynamically so that the IP address may be different every time a client connects.

Slide 25: A NAT gateway allows multiple computers to connect to an external network such as the Internet with all computers using the same single IP address. To the outside world it appears as if all this traffic comes from the same computer. The downside to using NAT is that a genuine end to end connection is not created between the network computer and the computer outside of the network and this may prevent certain protocols from working.

Slide 26: Dynamic NAT allows for a small number of public IP addresses, rather than a single IP address, to be dynamically allocated to a large number of private IP addresses within the internal network. Port Address Translation (PAT) is a variant of NAT commonly used in small businesses that allows one or more private networks to share a single IP address. In order to do this the PAT device translates internal IP addresses and port numbers and stores these mappings so that reverse translation can be done for incoming packets.

Slide 27: NAT can provide security by only allowing outgoing connection and only allowing inbound connections for specific services via mapping specific ports to specific internal IP addresses. Messages are initially received by the NAT gateway using its own protocol stack, thus providing a buffer between the client machines on the network and the outside world.

Slide 28: Network administration can be made simpler by some of the tools that are included with modern NAT devices and these include: Dynamic Host Configuration Protocol (DHCP) servers (see Private Study), methods for restricting access to the Internet, the ability to divide a network into sub-networks, and tools for logging network traffic.

Slides 29-30: NAT works by translating every IP address within the network into a public IP address and also renumbering source ports to be unique, thus allowing for identification of individual clients. A port mapping table holds details of the unique port of every client computer. This process can be reversed in order to route incoming packets to the correct client computer. Slide 30 shows this operation through a Port Address Translation device.

Slide 31: Intrusion Detection Systems (IDS) monitor network traffic and alert the network administrator or user if there is any suspicious activity. There are a number of different types available and some will take action if suspicious activity is detected, for example blocking the network user or IP address that is the source of the suspicious traffic.

Slides 32-36: The available IDS types include:

Network Intrusions Detections Systems (NIDS) are placed in strategic locations in the network to monitor network traffic across a whole network or section of the network. Traffic in and out of all devices can be monitored and ideally all traffic would be monitored. However, this can create bottleneck that significantly slows the network.

Host based Intrusion Detection Systems (HIDS) monitor all traffic into and out of the single device that they operate on. The device user and/or network administrator is informed when suspicious activity is found.

Signature-based IDS compare packets against a database of known threats, to determine if there is a match between the two. Where a match exists the network administrator is informed. This approach suffers from a lag between new threats appearing and those threats being added to the database, resulting in a period of time when they do not protect the network from any new threat (as with antivirus software).

Anomaly-based IDS use a baseline of network activity that includes bandwidth, protocols, ports and devices and compares current activity to this baseline. If there is any significant change in any parameters in comparison to the baseline, the network administrator is alerted.

Slide 37: In general IDS are a very useful tool for monitoring and protecting a network but they are prone to false alarms. In the first instance IDS must be configured correctly so that they do not miss suspicious activity and also to reduce the potential for false alarms. They rely on having a network administrator that understands the nature and importance of each alarm and who also knows what the appropriate course of action is upon receiving an alarm.

Slide 38: References

Slide 39: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

Before leaving students should be provided with details of the router/firewall they will be using in the laboratory exercise and the rules they will set up, so that they can research how the device is programmed plus any protocols and port numbers they will require. See the laboratory exercise for more detail.

Lecturers' Notes:

At the end of the lectures, students should be provided with details of the firewall/routing device, the conceptual rules and the IP addresses of all devices that will be used in the laboratory exercise. You should instruct the students that they need to carry out Private Study Exercise 1 before the laboratory session for this topic.

8.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

A section of the laboratory network should be available for the students to work with. This section should be separated from the rest of the network via a router or firewall that can have packet filtering rules applied to it. Students will require access to this device and be able to create packet filtering rules and then test those rules by sending suitable test messages through the device.

The tutor is required to produce a small set of conceptual rules that will be applied to this section of the laboratory network, e.g. no http access, access denied from a specific computer (IP address) outside of this section of the network, etc.

Exercise 1:

Your tutor will provide you with details of the network device that you will be using, the conceptual rules that will be applied to your network and the IP addresses of all devices that will be involved in the exercise.

You should have completed Private Study Exercise 1 before beginning this exercise, to gain all of the necessary preliminary information. You should:

- Create an access control list for your packet filtering rules based upon the requirements of your firewall or router.
- Program the firewall or router so that these rules are applied to traffic passing through the router.
- Where possible, test these rules to ensure that they have been applied correctly.

You will write up this laboratory exercise (including the preliminary work) in Private Study Exercise 2. Your report should include:

- Details of the router/firewall used
- Detail of the conceptual rules
- A list of the protocols and ports that these rules would apply to
- An access control list in a suitable format with an explanation of why you have chosen this order
- Detail of how these rules were added to the firewall or router.
- Details of any testing carried out

Suggested Answer:

Students should produce a clearly written report which contains all of the above data.

8.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

It is important that students complete Exercise 1 before attending the laboratory session.

Exercise 1:

This is preparatory work that must be carried out before attempting the laboratory exercise for this unit. Read through the details your tutor has provided you with for the laboratory exercise. Now you should:

- Find and read the relevant manual or user guide for creating packet filtering rules on the router or firewall you will be using. Familiarise yourself with the detail of this.
- Note any IP addresses and services/protocols/network services that the tutor mentions in the hand-out for the laboratory exercise.
- Research the protocols and ports that will form part of any packet filtering rules.
- Determine the order in which to apply the conceptual rules for packet filtering

Suggested Answer:

This will depend upon the equipment to be used and the rules set by the tutor but students should be familiar with the process they will follow to create the rules on the firewall or router, plus have written details of:

- IP addresses involved
- Protocols and ports involved
- An order in which to apply the rules

Exercise 2:

Write up your laboratory exercise in a formal report, ensuring that you include all relevant detail.

Suggested Answer:

The report should be of professional standard and include all of the detail listed in the laboratory exercise.

Exercise 3:

Research DHCP. Write notes explaining what DHCP is and how a DHCP server works.

Suggested Answer:

DHCP is the Dynamic Host Configuration Protocol. Its purpose is to enable individual computers on an IP network to extract their configurations from a server. The server has no exact information about the individual computer until they request the information from the server. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force. The definition of DHCP is recorded in an Internet RFC.

The protocol is used to assign IP addresses to hosts or workstations on the network. Usually, a DHCP server on the network performs this function. It leases out addresses for specific times to the various hosts. If a host does not use a given address for some period of time, that IP address can then be assigned to another machine by the DHCP server. When assignments are made or changed, the DHCP server must update the information in the DNS server.

A DHCP client uses DHCP to obtain configuration parameters from a DHCP server. The configuration parameters are “bound” to the DHCP client and managed by the DHCP server.

In order for a client to lease an IP address, the steps are:

- Lease Request - The client sends a broadcast requesting an IP address
- Lease Offer - The server sends the above information and marks the offered address as unavailable. The message sent is a DHCPOFFER broadcast message.
- Lease Acceptance - The first offer received by the client is accepted. The acceptance is sent from the client as a broadcast (DHCPREQUEST message) including the IP address of the DNS server that sent the accepted offer. Other DHCP servers retract their offers and mark the offered address as available and the accepted address as unavailable.
- Server lease acknowledgement - The server sends a DHCPACK or a DHCPNACK if an unavailable address was requested.

DHCP discover message - The initial broadcast sent by the client to obtain a DHCP lease. It contains the client MAC address and computer name. This is a broadcast using 255.255.255.255 as the destination address and 0.0.0.0 as the source address. The request is sent, and the client waits one second for an offer. The request is repeated at 9, 13, and 16 second intervals with additional 0 to 1000 milliseconds of randomness. The attempt is repeated every 5 minutes thereafter.

The client uses its own port 68 as the source port with port 67 as the destination port on the server, to send the request to the server. The server uses its own port 67 as the source port with port 68 as the destination port on the client, to reply to the client. Therefore the server is listening and sending on its own port 67 and the client is listening and sending on its own port 68. This can be confusing when you consider which way the message is going. RFC 1531 states ‘DHCP messages from a client to a server are sent to the 'DHCP server' port (67), and DHCP messages from a server to a client are sent to the 'DHCP client' port (68).’

After 50% of the lease time has passed the client will attempt to renew the lease with the original DHCP server it was obtained from, using a DHCPREQUEST message. Any time the client boots and the lease is 50% or more passed, the client will attempt to renew the lease. At 87.5% of the lease completion, the client will attempt to contact any DHCP server for a new lease. If the lease expires, the client will send a request as in the initial boot when the client had no IP address. If this fails, the client TCP/IP stack will cease functioning.

DHCP relay agents may be placed in routers or subnets that don't have a DHCP server to forward DHCP requests.

Client Reservation is used to ensure that a computer gets the same IP address all the time. Therefore, since DHCP IP address assignments use MAC addresses to control assignments, the following are required for client reservation:

- MAC (hardware) address
- IP address

Exclusion ranges are used to reserve a bank of IP addresses so computers with static IP addresses, such as servers, may use the assigned addresses in this range. These addresses are not assigned by the DHCP server.

The DHCP protocol does not include any authentication mechanism and is therefore open to a number of security breaches.

8.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercise from this topic with some emphasis on the laboratory exercise. You may also wish to collect the students' lab reports for marking and more formal feedback. You should also address any questions students may have about the content of this topic.

You should also allow time during the tutorial session to check that students are working on their assignments and answer any general questions on the expected scope of the work. You may wish to remind them of the submission deadline and documentation requirements.

Exercise 1: Review of Private Study and Laboratory Exercises

As a group you will review the tutorial and laboratory exercises from this topic and you should be prepared to discuss your own work and to hand in your lab report if necessary. Make sure you ask questions if there is anything you are not sure about from this topic.

Your tutor will talk about the assignment and check your progress with this. You should use the tutorial as an opportunity to ask any questions you have on the scope of your assignment, the deadline and documentation requirements.

Topic 9: Firewalls

9.1 Learning Objectives

This topic provides an overview of firewall operation and architecture and its limitations. On completion of the topic, students will be able to:

- Describe the components of a firewall;
- Configure a DMZ firewall;
- Evaluate the limitations of firewalls.

9.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

9.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

9.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Firewall architectures and their limitations
- The DMZ firewall and its limitations

9.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

9.4.2 Lecture 1

Slides 3-4: An overview of Topic 9.

Slide 5: A firewall is a network's first line of defence, as its purpose is to prevent access by unwanted hackers and traffic. It checks incoming and outgoing traffic from a network and blocks traffic in both directions based upon the rules it is using. A simple explanation is that it forms a semi-porous barrier between a network and the outside world (Internet), by only letting certain traffic through.

Slide 6: A firewall examines the data passing through it. If the data seems to be legitimate, based upon the rules it has been provided with, it is allowed through. If the data is not legitimate, it is prevented from passing through. The rules can be determined by the network administrator or another authorised person.

Side 7: The firewall rules are created in order to allow or deny traffic through the firewall, based upon the needs of the organisation and an assessment of security risks. It is important to remember that some of the rules may then block legitimate traffic.

Slide 8: Firewalls come as both software and hardware. Typically, software firewalls are located on individual computers and protect only that computer; hardware firewalls typically reside in routers and protect the whole network or part of a network. Ideally a network will utilise both.

Slide 9: Software firewalls are usually easy to install and come with an easy to use interface that allows a user to configure them in a highly flexible way. They often have pre-set levels that can be used for quick set up.

Slide 10: Hardware firewalls protect a whole network or a section of a network by setting up network wide traffic filters. They also protect network devices that are not capable of having their own software firewall.

Slide 11: Firewalls can be divided into three main categories based upon how they work: packet filters (you can remind students that these were covered in the last topic), application gateways and firewalls that inspect the content of packets. Extra features are offered by vendors (sellers) of firewalls with their packages.

Slides 12-14: Application gateways (or application layer firewalls) act at Layer 7 of the OSI model and apply rules to all traffic on an application (e.g. all FTP traffic). You can ask the students to explain what layer 7 is (Layer 7, the Application Layer, is the user interface to your computer programs for example, word processor, e-mail application, telnet, and so on). Rules are applied that determine whether a packet is allowed through or not. An example of such a firewall is one that blocks access to websites based upon keywords contained in the request.

Application gateways provide a buffer between the real application and a client. Another advantage is that in the event of patching the software to plug a hole in security, it can be done quickly on the gateway and this may not be the case on every networked machine. Application level firewalls are very useful with common applications, but for bespoke applications they may struggle to deal with the specifics of the application. They also slow down the transmission process.

Slides 15-19: Packet inspection firewalls are capable of inspecting the payload of a packet. They examine the session data associated with a packet and use this to determine whether a packet is allowed to pass through or not. This technology is often referred to as stateful packet inspection because the firewall maintains records of connections made through it. This allows it to determine whether each packet is part of an existing connection, is a new connection or is an invalid packet. A simple example of connecting to a web server through a packet inspection firewall is provided on the slides. These firewalls operate relatively quickly and at the same time allow inspection of the packet payload. One disadvantage is a vulnerability to certain types of denial of service attack, which can fill the connection tables it uses with connections that should not be legitimate.

9.4.3 Lecture 2

Slide 21: Firewalls are used at the perimeter of a network or the perimeter of a section of network, to protect that network or section. The position of firewalls in relation to the network and the outside world is known as the firewall architecture and this has security implications for the whole network. This module will not look at the other security technologies, such as IDS, that should be included as part of a complete network security package.

Slide 22: A closer look will be taken at some common architectures.

Slides 23-25: The simplest firewall architecture is to use a screening router between the internal trusted network and the outside un-trusted network. All traffic must pass through a router with packet filtering capabilities, which is usually placed at the network perimeter. This configuration may be used to create a Demilitarised Zone (DMZ) and it is best to use this configuration with other firewall technologies. This architecture has the advantages of being very simple and cheap but the disadvantages are no logging facilities, no user authentication methods and difficulty hiding the internal network structure from would-be attackers.

Slides 26-27: A Demilitarised Zone (DMZ) is part of the internal network that is protected from the outside world via a firewall but is also isolated from the rest of the internal network by a firewall. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. DMZs are sometimes useful for organisations with hosts that need all traffic destined for the host to bypass some of the firewall's policies, but need traffic coming from the host to other systems on the organisation's network to go through the firewall. It is common to put public-facing servers, such as web and email servers, on the DMZ. A simple network layout of a firewall with a DMZ (the mail server) is shown. Traffic from the Internet goes into the firewall and is routed to systems on the firewall's protected side or to systems on the DMZ. Traffic between the DMZ and systems on the protected network goes through the firewall, and can have firewall policies applied.

Slides 28-30: A screened host architecture places a bastion host between the router and the trusted internal network. The bastion host is a specially configured computer acting as a server for traffic coming between networks and thus providing an extra layer of security between trusted and un-trusted networks. The bastion host has two network interface cards, one for the internal network and one for external, and is protected itself by the router which performs packet filtering on incoming traffic. The bastion host can be used to set further rules regarding traffic into the trusted network. This architecture provides greater security than a screening router as two different devices are providing security features. It also provides transparent access from the trusted network out to the public network but limits the traffic into the trusted network. As with screening routers, this architecture does not hide the internal structure of the network and there is only one path between the trusted network and the outside world and if this fails network connectivity is removed or all security is compromised.

Slides 31-32: The dual-homed host places the bastion host between packet filtering routers. This means all traffic to and from the bastion host, which has no routing capabilities itself, is filtered by the routers as well as having the protection of the bastion host. This configuration hides the internal network structure from would be attackers but has the disadvantage that it requires proxy servers or each user to log in to the bastion host before connecting to the outside network. Multi-homed hosts can be configured where the bastion host connects to the outside network and multiple internal networks with a packet filtering router between it and each network.

Slides 33-34: In a screened subnet demilitarised zone architecture, the bastion host is surrounded by packet filters, as in a dual homed architecture, but there is a separate sub-network that is a demilitarised zone. Traffic between the DMZ and the trusted network must pass through the bastion host and a packet filtering router thus providing a greater level of protection. The DMZ allows services from the network to be provided to the public network in a more secure manner as it is isolated from the trusted network and also hides the internal network structure from the outside world. There is still a single path between all of the internal networks and the public network.

Slide 35: Multiple screened DMZ subnets can be used, with each providing a different service to the un-trusted public network. This allows for different levels of security between the outside network and individual DMZs, between different DMZs, and between the internal network and different DMZs providing greater flexibility.

Slide 36: Multiple firewalls can be used to produce multiple layers of protection. By placing a bastion host between a demilitarised zone and both the outside un-trusted network and the trusted internal network, an extra layer of security is provided. If security devices from different vendors are used this also enhances security as it is unlikely that vulnerabilities present in a firewall from one vendor are replicated in the device from another vendor.

Slide 37: References

Slide 38: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

9.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

A section of the laboratory network should be available for the students to work with. This section should be separated from the rest of the network via a router and firewall that can be configured by the students. Students will require permission to connect devices in such a way that they can create a protected network and a demilitarised zone. The network and DMZ may consist of a single device in each if equipment is limited.

The tutor is required to produce details of the devices to use and an outline of the firewall architecture that will be created but this must include a DMZ and protected network using a suitable architecture, e.g. screened subnet DMZ. This should be given to the students at the start of the laboratory exercise. The exact detail of this is left to you so that it can be tailored to your own laboratory and equipment.

Exercise 1:

Read the details in the document provided by your tutor regarding the devices and architecture you are required to produce.

Create the architecture outlined in the document, which should include a demilitarised zone (DMZ) and a protected network.

You are required to produce a formal report on this work in Private Study Exercise 1. This report should include:

- All hardware used
- The firewall architecture used including a diagram of the architecture
- An explanation of how the architecture works
- Detail of how this architecture was practically created
- Any problems encountered

Suggested Answer:

A formal report containing all of the above detail.

9.6 Private Study

The time allocation for private study in this topic is expected to be 7 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Write up your laboratory exercise in a formal report ensuring that you include all relevant detail.

Suggested Answer:

The report should be of professional standard and include all of the detail listed in the laboratory exercise.

Exercise 2:

Complete your assignment work and take your assignment to the tutorial session to discuss progress and any issues or concerns with your tutor.

Suggested Answer:

A completed assignment or one very close to completion so that any final improvements can be discussed with the tutor.

9.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the laboratory exercise from this topic. You may also wish to collect the students' lab reports for marking and more formal feedback. You should also deal with any questions students may have about the content of this topic.

You should also allow time during the tutorial session to check that students are working on their assignments, are close to completion and review their assignment work to date. You may also wish to remind them of the submission deadline and documentation requirements.

Exercise 1: Review of Private Study and Laboratory Exercises

You will review and discuss the laboratory exercise and your report. Use this time to ask your tutor any questions you have about this topic.

Your tutor will ask you for an update on your assignment. You should use this tutorial as an opportunity to ask any final questions you have on the scope of your assignment, the deadline and documentation requirements.

Topic 10: VPN

10.1 Learning Objectives

This topic provides an overview of Virtual Private Networks (VPN) and issues with the use of VPN. On completion of the topic, students will be able to:

- Configure access control mechanisms;
- Explain Virtual Private Networks.

10.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

10.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

10.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Virtual Private Network technologies
- Issues with Virtual Private Networks

10.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

10.4.2 Lecture 1

Slides 3-4: An overview of Topic 10.

Slide 5: True private networks utilise dedicated communication lines leased by an organisation to provide a private communications channel. Virtual private networks do not use a dedicated communications line but send private communications over shared networks, typically the Internet. In this way it is a virtual private network; although the communication is private the network is not truly private. Such connections are used by organisations that wish to communicate privately using the Internet. There are two main sections to the VPN; the internal network which should be genuinely private and secure; and the external part (the Internet) which may be a little less secure.

Slide 6: From a user's perspective a VPN appears to be a dedicated private connection. The tunnelling gives the appearance of a private connection and the data is encrypted so that the data is private.

Slide 7: There are four elements to a VPN: The connections to the Internet and the virtual private network; the datagrams that contain the data plus the source and destination information; firewalls that determine what is allowed to pass through and traverse the connection; and protocols that create the VPN tunnels which are the virtual private connections through the Internet.

Slide 8: This slide presents a diagram of VPN.

Slide 9: The key functions of VPN are authenticating that the data was sent by the stated sender; allowing only authenticating users to access the network and preventing unauthorised access; maintaining the confidentiality of messages passed over the network by preventing them from being read or copied during transmission; and ensuring that the message received is exactly the same as the message sent.

Slide 10: Public key encryption and digital signatures are used for encryption and authentication. A VPN sends datagrams along a virtual connection, usually over the Internet. There are two parts to each datagram, an outer header and the inner payload. The header may or may not be encrypted but the payload is encrypted.

Slide 11: A network can be created by utilising multiple VPN tunnels between different points.

Slide 12: There are three key protocols used in VPN that are explored in more detail in the following slides.

Slides 13-15: Internet Protocol Security (IPsec) is an open standard protocol suite that provides privacy and authentication services. It has a transport mode where the data in the payload is encrypted but the header is not, and a tunnel mode where both header and payload are encrypted. An IPsec connection is known as a security association (SA). An SA has a security identifier which is carried in the packets and used to look up encryption keys when a secure packet arrives at its destination. The security identifier applies to traffic in only one direction so for a secure two-way communication over a VPN two security associations are required.

In IPsec transport mode the IPsec header is inserted just after the IP header, as the IP header is not encrypted. The outer IP header has a modified protocol field to indicate that the IPsec header follows. The IPsec header contains security information, including the security identifier and a sequence number. It may also include integrity checks on the enclosed data.

In IPsec tunnel mode the whole IP packet is encapsulated by a new IP packet with an IPsec header. This method is particularly useful when the tunnel ends at a device which is not the final destination. It is normal to have a firewall between the devices sending and receiving the messages and the tunnel through the Internet. Using tunnel mode allows the firewalls to encapsulate the IP packets at the sending end and then remove this encapsulation at the receiving end. The devices inside the firewalls on the trusted network do not then have to be aware of IPsec as they only deal with IP packets.

Slide 16: The Point to Point Tunnelling Protocol (PPTP) establishes a direct connection between two networking nodes and can provide encryption, authentication and compression services.

Slide 17: In the Layer 2 Tunnelling Protocol (L2TP) the whole datagram is sent within a UDP packet. It does not provide any encryption or confidentiality and this is provided by another protocol passed along the tunnel created.

Slide 18: PPTP sessions are commonly carried along a L2TP tunnel with PPTP providing the confidentiality and authentication functions. Some systems use IPsec to provide confidentiality, authentication and integrity with L2TP and this combination is commonly known as L2TP/IPsec.

Slide 19: There are a number of advantages to using VPN rather than a leased private connection and chief among these is cost. There is no need for expensive, leased, long distance lines or any call charge costs. VPN is also easily scalable, providing sufficient bandwidth is available over broadband connections. It is also very easy to add and remove users and can greatly increase the flexibility and efficiency of a business by allowing employees access to the company network from remote locations.

Slide 20: In order to securely implement a VPN a good understanding of security issues relating to the use of public networks is required, along with the deployment of proper precautions. There is some cost involved with this. The network will also be dependent upon the availability of Internet connections and this is to a certain extent outside the control of the organisation implementing the VPN, and therefore unpredictable. There can also be interoperability issues with equipment from different vendors, along with the requirements to operate with existing technology used on the internal networks of the organisation.

10.4.3 Lecture 2

Slide 22: A brief recap of what a VPN connection is. Before showing the slide ask the students to provide a brief outline of what a VPN is.

Slide 23: There are a number of ways of categorising and classifying the different types of VPN available. Here we divide them into two categories based upon architecture: client-initiated VPNs and network access server initiated (NAS-initiated) VPNs.

Slide 24: Client-initiated VPNs are controlled by client VPN software that initiates the secure tunnel. They create a secure connection between the client and the network of the Internet Service Provider but are not scalable.

Slide 25: VPNs that are initiated by the network access server (NAS) do not require any client VPN software as it is the ISP's NAS that initiates the tunnel to the private network. Clients use the public telephone network to connect to the ISP NAS and this section of the connection is not secure.

Slide 26: In business VPNs are used to connect individual computers to a company network (remote access), to connect multiple offices within the organisation (intranet) or to connect to other selected organisations who are partners of the business (extranet).

Slide 27: A true extranet involves a company connecting to a number of business partners via one or two ISPs. The partners could be suppliers, customers, collaborative partners or contractors. Security is extremely important as there are connections between different organisations. Breaches could result in changes to transactions that involve huge sums of money.

Slide 28: An intranet extends VPN access to other remote offices and can potentially connect large numbers of workplaces together (but all from the same organisation). It is likely that this will involve a single service provider and it is therefore much easier to have a consistent security policy and quality of service throughout the whole VPN. Where multiple ISPs are used across the Internet there is little control of the connections as no single organisation is in control of the Internet.

Slides 29-30: Remote users can access a corporate network via a VPN by making a local call to an ISP rather than a long distance call to their base office. This allows mobile staff to gain access to the corporate network over fast broadband connections. Typically this uses the Point to Point Protocol (PPP) and tunnels that extend from the access server to the corporate network. When using a Microsoft VPN the Point-to-Point Tunnelling (PPTP) protocol is used to tunnel from the access server through to the client PC.

Slide 31: Virtual Private Dial-up Networking (VPDN) relies upon ISPs to tunnel remote traffic securely. Remote users can dial-up local ISPs who then forward the traffic. The configuration and security functions remain with the client. The dial-up service provider simply provides the secure tunnel between sites.

Slide 32: Before showing the slides ask the students for examples of where VPN is used in business and what it is used for. This slide lists a few general examples which students may be invited to add to if there were very suggestions before showing the slide.

Slide 33: Small businesses often use the simple VPN options that are provided via operating systems. These are often not very secure, simply relying on usernames and passwords for security rather than public key cryptography. Standard VPN solutions require investment in extra hardware and/or software plus administration, costing both time and money. A cost effective alternative for a small business is to use Secure Sockets Layer (SSL) VPNs that are easy to install and use ports commonly used for secure e-commerce transactions with websites.

Slides 34-35: SSL VPNs allow access control mechanisms based upon user identity, device and/or protocol with a secure connection being created via a standard web browser. Any traffic between the web browser and the SSL VPN device is encrypted via the SSL/TLS protocol. Data is encrypted via the public-key cryptography of the SSL protocol and authentication of both client and server is achieved via the SSL handshake.

Slides 36-37: There are two main types of SSL VPN.

A SSL Portal VPN allows a single secure connection to a website. The user connects to the website using a standard web browser and is authenticated by a method acceptable to the website. The user then has access to a web page that acts as a secure portal to many other network services.

A SSL Tunnel VPN requires a browser that can support active content via java, ActiveX, etc., and this can provide content that is not available via a SSL Portal VPN. The browser can access multiple secure network services through a tunnel running under SSL.

Slide 38: There are some initial costs associated with obtaining SSL certificates in order to run SSL VPNs but these are recouped from the savings made from having a secure network, as is the case with other VPNs, plus the reduced cost in time to manage and administer the SSL VPN once it is running. It is a viable option for small and medium sized businesses.

Slide 39: References

Slide 40: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

Lecturers’ Notes:

You will need to point out to students that they need to have completed Private Study Exercise 1 prior to the laboratory session.

10.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

Students should have completed Private Study Exercise 1 prior to the laboratory session and utilise the user guide they have created.

Your network requires a server and client that are available for use by students to create a VPN. Exercise 1 should be extended where facilities and permissions allow. This may involve students being given permission to configure a VPN server and for this it would be ideal if there was a network for student use that is isolated from the rest of the college.

During private study time, you may want to ask students to work in pairs or small groups for Exercise 3, depending on how easy this is to arrange with your group. You should advise students of the necessary arrangements during the laboratory session if so.

Exercise 1:

Create a VPN connection from a client computer to the college or laboratory network. You should follow the steps you have noted in Private Study Exercise 1. Make notes on any problems you encountered when setting up the VPN. Make notes on how the server is set up to allow the VPN connection and the protocols used. You are required to write a report including all relevant details in Private Study Exercise 2. This should be combined with the manual requested in Private Study Exercise 1.

Suggested Answer:

The answer will depend upon the server and client software but students should create a report that gives information on:

- Problems encountered on setting up the VPN and solutions to those problems
- The configuration of the VPN server
- The protocols used in the VPN connection

10.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Students should complete Private Study Exercise 1 prior to the laboratory session.

Exercise 1:

Find details of both the server and client VPN software available for use in your computer laboratory. Research how to create a VPN connection from a client computer in the laboratory. Make notes and create a short user manual that shows how to set up a VPN connection from a client.

You will use your user manual during the laboratory session for this topic.

Suggested Answer:

The answer will depend upon the server and client software but a short user manual should be created that would allow a new person to set up a VPN connection from a client computer.

Exercise 2:

Complete your report for the laboratory exercise.

Suggested Answer:

Student should produce a professional report providing the detail given in the laboratory exercise.

Exercise 3:

As directed by your tutor (you may be asked to work with one or two other students), research a commercial SSL VPN application and make notes on how the application operates. Your notes should include details of operating systems and browsers that the software is compatible with, the protocols utilised, services it can provide and a brief description of how a connection is made.

You are required to produce a short presentation of your findings in the tutorial session.

Suggested Answer:

The answer will depend upon the application researched but the presentation should give information on:

- The operating systems and browsers the application is compatible with
- Protocols used
- Services it can provide
- A general description of how the connections are made

10.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercise. You may also wish to collect the students' lab reports for marking and more formal feedback.

Students should be selected to present their findings on SSL VPNs. Each presentation should be followed up with discussions on each of the applications and students should take notes to supplement their own research and to enhance their understanding of the topic.

You should also allow some time for any questions students may have about the content of this topic.

Exercise 1: Review of Private Study and Laboratory Exercises

You will present your findings from your private study on SSL VPNs. You will also review and discuss the laboratory exercise as well as your private study research.

Topic 11: Remote Access

11.1 Learning Objectives

This topic provides an overview of remote access technologies including remote desktops and web applications. On completion of the topic, students will be able to:

- Configure access control mechanisms;
- Select an appropriate remote access solution.

11.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

11.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

11.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Alternative remote access technologies:
    - Web applications
    - Remote desktops

11.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

11.4.2 Lecture 1

Slides 3-4: An overview of Topic 11.

Slide 5: Remote access involves accessing a computer without having physical access to it. This is achieved via another device over a network, typically the Internet. This is commonly used in many businesses and many consumers allow computer manufacturers to have remote access to their desktop computers and notebooks, to enable remote troubleshooting in the event of problems.

Slide 6: In businesses remote access has allowed huge changes in the way that they operate. It allows for flexible working so that staff are able to work from home, when mobile and when wishing to work outside of normal office hours. This makes business incredibly flexible for dealing with customers in different locations and different time zones. It also provides flexibility in employing people who do not wish to work to traditional working patterns. This enables greater adherence to equal opportunities regulations.

Slide 7: Remote access comes in two general forms: file access and application access. In the former a remote user can gain access to individual files, for instance a remote salesperson could access a contract or a price list for a customer. With application access a remote user can also process files and data as if they were on the internal network. This enables them to do much more, such as amend prices or place an order.

Slides 8-11: In order to create remote access functionality, an understanding of the internal application architecture (the way in which clients interact with software, data and files) is required.

A client/database architecture has complete applications installed and running on client computers. These applications interact with a database server in order to obtain the data to process but the business logic is applied on the client computer. This architecture is generally used where the network only has a small number of clients.

A client/server architecture has footprint applications installed on the client computers. These are stripped down applications that are sufficient only to connect to the complete application which is installed on a server. The server application runs the business logic, connects to the database server and presents the results to the client.

In a web-based architecture the browser is used as the client, resulting in very little software being required on the client computer in order to operate. The browser connects to a server that provides a user interface in the browser. The server may communicate with many other application servers to provide the applications required by the client and all results are displayed in the browser.

Slide 12: There are several ways of creating a remote access connection and the security and bandwidth implications of each should be considered. You may wish to elicit students' views on the security and bandwidth issues of each.

Slide 13: Before showing the slide ask the students to explain what a VPN is. A VPN provides remote access by creating a secure tunnel over the Internet between the remote user and the internal network. Once a session has been created this allows the remote user to interact with the network and data can be transmitted in both directions. There can be bandwidth issues with some applications and bandwidth limits can come from either end of the connection, though this is likely to be at the remote user's end as the bandwidth available at a business is likely to be much greater than that of a mobile or home user.

Slide 14: With a remote desktop connection (RDC) the applications are hosted on a remote server and they send screenshots back to the user. Inputs via mouse and keyboard on the client computer are forwarded to the server and the results are sent back to the client in a screenshot. The screenshots are compressed providing a remote solution that uses a constant and small bandwidth.

Slide 15: Application hosting involves the use of a specialist third party organisation to host your applications on their own servers on their network. Use of the software is licensed from the external partner who also manages the system and charges for this service. This removes the need for large in-house IT departments as much of this work will have been outsourced. In reality this model means that staff in the company office are remotely accessing applications in the same way as a genuine remote user.

Slide 16: Web-based applications work from a standard web browser and no other software is required. Software vendors provide direct access to their applications over the Internet and this operates through the browser window, this is known as Software-as-a-Service (SaaS). All data is passed over the Internet, usually in encrypted format.

Slide 17: Where remote access is allowed, standard network security best practice should be followed. Before showing the slide ask the students to list the features of good network security – discuss the features they have suggested and highlight any omissions.

11.4.3 Lecture 2

Slide 19: A remote desktop allows applications to be run on a remote server but displayed locally and this is achieved via software installed specifically for this purpose or via features supplied by the operating system. Modern versions of Microsoft Windows provide this functionality. Applications can be run directly from the command line in the controlling computer or via a graphical user interface (GUI).

Slides 20-21: The controlling computer displays an image that has been transmitted by the remote computer that it is controlling (the controlled computer). This image is updated at regular intervals or when changes have been made that are detected by the remote access software. Actions are carried out using input devices, such as mouse and keyboard, of the controlling computer and these actions are transmitted to the controlled computer. The controlled computer treats these actions as though they were input directly into itself and the application it is running behaves accordingly.

Changes to the display are then transmitted as an image to the controlling computer and the image on its screen is changed to match. The net effect is that, to the user, the controlling computer operates as though it was the controlled computer but with the inevitable delays of protocol processing and transmission times. The controlled computer may have its input devices and screen disabled whilst the remote session is taking place, to prevent any interference whilst the remote session is ongoing.

Slide 22: Remote acces software has been used maliciously to gain control over computers of unsuspecting users. A typical scenario involves the user receiving a telephone call from a person pretending to be from a major, trusted corporation such as Microsoft or a computer manufacturer. They offer to fix their system or improve its performance and then gain access to the computer. This has resulted in deliberate damage to operating systems, where a fee has then been required to fix it or the computer is then used (as a ’zombie’) for malicious activity.

Slide 23: There are a number of protocols used in remote desktop applications. We will take a look at Virtual Network Computing (VNC) and the Remote Desktop Protocol (RDP). Inform the students that the others are covered in a Private Study Exercise.

Slide 24: VNC is a graphical desktop sharing application that provides remote access to a GUI. The source code from the original development and many of the packages derived from it are open source. This operates by transmitting input device actions in one direction and graphical screen updates in the other direction.

Slide 25: VNC is platform indepent and allows for remote connections between devices using different operating systems. There are implentations of VNC for most operating systems and it also allows for connections from multiple clients to one server simultaneously.

Slide 26: There are three components to VNC: client, server and protocol. The VNC server is the program that runs on the server and allows a client to take control. The VNC client is the program that controls the server and is also known as the viewer. The remote framebuffer (RFB) protocol sends simple graphical messages to the client and input device actions to the server, which does not need a physical display.

Slide 27: A framebuffer is a memory buffer that drives video display and is common to systems that use windows – that is windows, with no capital W (i.e. a window on the display screen, not specifically Microsoft Windows). A framebuffer stores information regarding the colour and position of every pixel in a display and can be used to transmit the display information of rectangles that will be displayed on a screen.

Slide 28: The RFB protocol sends colour information about a rectangle to display in the form of a framebuffer. The protocol itself includes security and compression techniques and it is usual for a client and server to agree which version to use, the one that gives the best compression and security. The client uses port 5900 to access a server, or port 5800 for a browser, but the server may use port 5500 for listening mode.

Slide 29: Even though VNC does not use plaintext passwords it is thought to be insecure. This is due to it being vulnerable to sniffing attacks that would allow the encryption key and password to be discovered. SSL or VPN tunnelling can be used to provide greater security and SSH clients are available for most platforms.

Slide 30: RDP is Microsoft's own protocol for remote access but RDP clients are available for most operating systems. It allows input to (and display from) a remote computer, thus allowing complete GUI control. It is an extension of the ITU T.120 family of protocols and is compatible with a number of applications and LAN protocols. Inform students that the T.120 family of protocols is the subject of a Private Study Exercise.

Slide 31: RDP has its own video driver and on-screen events drivers. The video driver is used to convert rendering information into packets that are sent to the client device via the network. The protocol receives these packets at the client and converts them into calls to the Microsoft Windows Graphic Device Interface (GDI) API. Mouse and keyboard events on the client are transmitted to the server and it uses its own driver to receive and apply these.

Slide 32: RDP comes with a number of standard features. A stream cipher that can use a 56-bit or 128-bit key is used to encrypt data. Bitmap caching and data compression techniques are used to reduce the amount of bandwidth required by the protocol. A roaming disconnect feature is included, allowing a user to disconnect without logging off so that they can reconnect to the session later when they log back in, even from a different machine or location. Clipboard facilities are available that allow copying between client and server and between different sessions. Print and sound redirection is possible, where printing can be carried out on the client and sounds made on the server can be heard on the client. Authentication via Smart Card is possible and 24-bit colour is also supported by the protocol.

Slide 33: References

Slide 34: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

11.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

Your network is required to have remote desktop capabilities, server and client, including student permission to use these. The exact details are left to up to you so that you can use suitable solutions based upon your operating systems and network capabilities.

The tutor is required to support the student throughout this process and provide them with details of how to set up the remote access connection at both the client and server end of the connection and set a small series of simple tasks that will be performed remotely from the client computer.

During private study time, you may want to ask students to work in pairs or small groups for Exercise 2, depending on how easy this is to arrange with your group. You should advise students of the necessary arrangements during the laboratory session if so.

Exercise 1:

Create a remote desktop connection between a client and server on your network. Your tutor will provide you with details of the options available in your laboratory.

You should test the connection by carrying out a small number of simple tasks from the client computer as directed by your tutor.

You will be required to produce a formal laboratory report in Private Study Exercise 1 and you should note all of the required detail for this report during the laboratory exercise. Your report should include:

- The remote access application used
- Protocols utilised by the application
- The process of creating the connection
- The tasks performed remotely
- Security settings for the connection
- Any problems or issues during the laboratory exercise

Suggested Answer:

Notes for the formal report should be produced by each student, covering all of the elements listed above.

11.6 Private Study

The time allocation for private study in this topic is expected to be 8 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Complete your report for the laboratory exercise. Your tutor will ask to see your report, and may collect it for marking, during the tutorial.

Suggested Answer:

A professionally produced report providing the detail given in the laboratory exercise.

Exercise 2:

Research one of the following on your own or in a pair/group, as directed by your tutor:

- Apple Remote Desktop (ARD)
- Independent Computing Architecture (ICA)
- Appliance Link Protocol (ALP)

Prepare a brief presentation of approximately 5 minutes for the tutorial session. Your presentation should cover the key points/features of the protocol you have chosen.

Suggested Answer:

Students should cover the following key points for each:

Apple Remote Desktop (ARD)

- Mainly for computer administrators who control many computers
- Users can remotely control or monitor other computers over a network.
- Supports third party VNC clients and servers
- Latest version uses AES 128-bit encryption
- Has a number of powerful tools in the latest version including:
    - Auto-install of updates to remote computers
    - Remote drag and drop facilities
    - A dashboard for an overview of remote computers
    - Application usage reports
    - User history reports

Independent Computing Architecture (ICA)

- A proprietary protocol for an application server from Citrix Systems
- Works with most operating systems – is platform independent
- Transmits high-level window display information
- It is graphically intensive so bandwidth can be an issue
- Needs a great deal of data compression and optimization to be useable on low bandwidth networks
- Can send data as bitmaps where GUIs are not compatible between client and server

Appliance Link Protocol (ALP)

- Proprietary protocol for use with Sun Ray from Oracle
- Used with ultra-thin clients which are networked display devices
- Applications run on the server
- Usually uses smart cards for user authentication
- Users can move between thin clients and continue sessions even without closing programs
- Can be used with a thin client to access a Windows desktop
- Low energy clients
- Uses both UDP and TCP

Exercise 3:

Research the ITU T.120 family of recommendations.

- Make notes that provide an overview of this family of recommendations
- Create a list of the individual recommendations stating what they relate to.

Suggested Answer:

In general, T.120 covers a set of protocols for multi-user communications and aims to provide the following benefits:

- Multi-point data delivery
- Reliable data delivery
- Interoperability
- Platform, application and network independence
- Scalability
- Co-existence with other standards
- Extendibility

The recommendations include:

- T.120 - Data protocols for multimedia conferencing
- T.121 - Generic application template
- T.122 - Multipoint communication service - Service definition

- T.123 - Network-specific data protocol stacks for multimedia conferencing
- T.124 - Generic Conference Control
- T.125 - Multipoint communication service protocol specification
- T.126 - Multipoint still image and annotation protocol
- T.127 - Multipoint binary file transfer protocol
- T.128 - Multipoint application sharing
- T.134 - Text chat application entity
- T.135 - User-to-reservation system transactions within T.120 conferences
- T.136 - Remote device control application protocol
- T.137 - Virtual meeting room management - services and protocol

11.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic, with some emphasis on the laboratory exercises. You may also wish to collect the students' lab reports for marking and more formal feedback.

Students should be selected to present their findings on the remote desktop protocols. Each presentation should be followed up with discussions on each of the protocols and students should take notes to supplement their own research and to provide them with an understanding of all protocols.

You should also allow some time for any questions students may have about the content of this topic.

Topic 12: Wireless Security

12.1 Learning Objectives

This topic provides an overview of security issues that are specific to wireless networks and examines the standards, protocols and architectures used to address these issues.

On completion of the topic, students will be able to:

- Explain the vulnerabilities inherent in wireless networks;
- Deploy a secure network architecture for wireless access;
- Configure Access Control Lists;
- Encrypt and protect the wireless link.

12.2 Pedagogic Approach

Information will be transmitted to the students during the lectures. They will then practise the skills during the laboratory sessions and extend their understanding during private study time. The tutorial will then provide an opportunity to review the key ideas and obtain further guidance and support.

12.3 Timings

Lectures:	2 hours
Laboratory Sessions:	1 hour
Private Study:	7.5 hours
Tutorials:	2 hours

12.4 Lecture Notes

The following is an outline of the material to be covered during the lecture time. Please also refer to the slides.

The structure of this topic is as follows:

- Security issues specific to wireless networks
- Wireless security (WEP, WPA, WPA2)
- Secure network architectures for wireless deployments

12.4.1 Guidance on the Use of the Slides

The slides are divided into two lectures, each lasting 1 hour. These may be delivered as two separate lectures or you may combine them into one longer session.

12.4.2 Lecture 1

Slides 3-4: These slides present an overview of Topic 12.

Slide 5: A typical wireless network has a number of wireless enabled devices connecting to an access point. The access point connects to a wider network which may be the Internet in a home network but is more likely to be a LAN in a commercial organisation. By their nature, wireless networks are less secure than the equivalent wired network.

Slide 6: A typically Wireless LAN (WLAN) has a number of devices (e.g. laptops) connecting to an access point which in turn connects to a wired network providing access to internal servers such as file servers and printer servers, and also Internet access.

Slide 7: Before showing the slide, ask the students to list the security issues that are specific to wireless networks and discuss these briefly with the group. A wireless network broadcasts signals from the access point and these signals are detected by wireless enabled devices. Because the signal is broadcast the network boundary is determined by the signal strength with the network ending where the signal is no longer detectable. This means that wireless transmissions are usually detectable outside of the building where they are housed allowing attackers to access the signal undetected. In order to have a fully secure wireless network, access must be restricted and transmissions must be encrypted. However, some wireless networks are public so this is not an option.

Slide 8: There are three general approaches to wireless network security. For closed networks where there are limited, known users with authorised access, such as a home or office network, the simple solution is to implement access controls at the access point and encrypt transmissions to prevent eavesdropping. Where fully public networks are implemented with no access controls, such as those provided in some cities, cafes, etc. the open wireless network is isolated from any private networks. For a wireless network that mixes both private and public features it is possible to utilise end-to-end encryption techniques to protect the private traffic.

Slides 9-10: The IEEE approved the WLAN standard in 1997 (IEEE 802.11) and there have been a number of revisions since this time. A typical LAN has access controls that only allow authorised devices to connect to the access point (AP). One method of doing this is via MAC address filtering where a list of permitted MAC addresses is created. A permitted list is the normal way of creating the access control list but it is also possible to create a blocked list as an alternative.

Slide 11: Wired Equivalent Privacy (WEP) is the original security component of the IEEE 802.11 standard. Its aim was to prevent unauthorised parties from viewing wireless traffic by encrypting the traffic. It was designed as an efficient and fairly strong encryption algorithm but in reality it is weak and has now been superseded by Wi-Fi Protected Access (WPA).

Slides 12-13: WEP encryption uses the RC4 stream cipher for confidentiality and the CRC-32 checksum for integrity – inform students that they will research these as a Private Study Exercise. Secret keys are usually 64 or 128 bits long, though some versions do have 256 bit keys, and this small key size makes WEP easier to crack. An access point and the connecting devices can share up to 4 secret keys with one of these keys being nominated as the default key. The encryption keys are made up of the key in the form of 10 or 26 hexadecimal characters (40 or 104 bit) plus a pseudorandom initialisation vector (IV) of 24 bits. The use of an IV is common in cryptographic schemes as this continually changes thus preventing a repeat of the same input from creating the same output. The random nature of the IV means that the actual input into an algorithm is different each time even if the 40 or 104 bit secret key is the same.

Slides 14-16: WEP has two main authentication methods: open system authentication and shared key authentication. Open system authentication effectively does not authenticate the client device upon connection to the access point. It relies on the fact that data packets transmitted over the wireless network are encrypted and, whilst any wireless enabled device can connect, the encryption keys are required in order to communicate. The shared key authentication method has a handshake process to authenticate clients upon connecting to the AP. This process starts with an authentication request from the client which then receives a clear text challenge from the AP. The client then encrypts the challenge using the WEP key and then includes this in another authentication request. The AP decrypts this and compares it with original challenge, if there is a match the client is authenticated. After authentication the data frames transmitted over the network are encrypted using the WEP key with the RC4 stream cipher. It is intuitive to think that the shared key authentication method is more secure than open system authentication but this is not the case as the key being used can be derived if the frames used in the challenge process during handshake are captured. In reality both methods do not offer sufficient security and WEP has been replaced by WPA and WPA2.

Slide 17: One of the main flaws with WEP is the use of the 24-bit IV. For a secure system the IV should never repeat but 24-bits is too short and there is a 50% chance that the IV will be repeated every 5000 packets. Another major security flaw is that replaying packets can cause the AP to retransmit the IVs. With the correct equipment WEP can be cracked in a very short time, a matter of seconds in some instances.

12.4.3 Lecture 2

Slide 19: Wi-Fi Protected Access (WPA) was developed in response to the security flaws in WEP with a view to protecting current and future wireless networks via the use of authentication and encryption mechanisms. WPA was an interim solution and implements most of the IEEE 802.11i standard whereas WPA2 fully implements this standard, which has now been incorporated into IEEE 802.11-2007, the base standard for Wi-Fi devices.

Slide 20: The IEEE 802.11i standard has been fully implemented as WPA2. It uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, also known as CCM mode Protocol or CCMP for simplicity. This is a block cipher encryption method based upon AES and replaces the less secure RC4 stream cipher of WEP and Temporal Key Integrity Protocol (TKIP) of WPA. This standard has been mandatory for all new Wi-Fi certified devices since 2006.

Slide 21: CCMP is an encryption protocol that is more secure than those used in WEP and WPA and uses a 128-bit key. It provides data confidentiality, user authentication and access control mechanisms.

Slides 22-23: Pre-shared Key (PSK) mode or personal mode is designed for home or small business use and utilises a pre-shared key between clients and access points. It does not require an authentication server as the clients authenticate directly with access points by using the same pre-shared key. The key is changed after a set period of time or can be changed when a client leaves the network. There are a number of weaknesses inherent with this mode, one being the insecure transmission of the key by people. Whenever the key is changed the new key must be manually added to every client and access point plus the key must be provided to any guest that is provided with access to the network. The key itself is a 64-bit hexadecimal number that is generated from a passphrase and if the passphrase uses common words or phrases this could be open to a dictionary attack.

Slide 24: Enterprise is, as its name suggests, designed for larger enterprises with greater resources at their disposal. Authentication is provided via IEEE802.1X and the Extensible Authentication Protocol (EAP). An authentication server is central to the authentication process and this is usually a Remote Authentication Dial In User Service (RADIUS) server. This is more complex than personal mode but does provide greater security.

Slide 25: 802.1X is the IEEE standard for port-based network access control (PNAC). There are three elements to this: the supplicant is the client device that wishes to connect to the network, the authenticator is the access point, and the authentication server is the server supporting RADIUS and EAP. A supplicant can only access the network through the authenticator once it has been validated and authorised.

Slide 26: The Extensible Authentication Protocol (EAP) is a framework used by wireless networks that supplies functions that allow the devices to negotiate their authentication methods (EAP methods). It provides a secure authentication method and negotiates a shared private key between authenticator and supplicant.

Slides 27-28: The 802.1X authentication process has four stages. Initialisation is when the authenticator detects a new supplicant and the relevant port is enabled and set to the unauthorised state. During the initiation phase the authenticator transmits EAP Request Identity frames. The listening supplicant responds with an EAP Response Identity frame which contains an identifier such as a user ID. The authenticator encapsulates this frame in a RADIUS Access Request packet and sends this to the authentication server. In the negotiation phase the authentication server sends the authenticator an EAP request specifying the EAP Method. This is encapsulated and transmitted to the supplicant. During the authentication phase, after the EAP

Method is agreed, EAP Requests and Responses are sent between supplicant and authentication server until the server sends an EAP Success message. At this point the authenticator changes the state of the port from unauthorised to authorised and normal traffic can flow from the supplicant via the authenticator across the network.

Slides 29-30 RADIUS is a protocol providing a centralised Authentication, Authorization, and Accounting (AAA) service; in other words it manages the authentication of clients wishing to connect to a network. It is a client-server protocol, operating at the Application Layer of the OSI model, that uses UDP for transport. There are 3 main functions of this protocol: authenticating users and/or devices and providing permission for them to access the network, authorising users and/or devices for specific services on the network, and accounting for usage of network services.

Slide 31: WPA2 provides each packet with a new session key adhering to good security practice by not reusing keys.

Slide 32: When creating or planning a wireless network, a suitable network architecture is required. The two main categories, standalone access points and centrally co-ordinated access points have benefits and are suited to different environments.

Slides 33-34: With standalone access points all access points in the network operate independently of each other, carry out encryption and decryption and have their own configuration file. Large networks will rely on a management application. The network configuration is static and does not respond to changing network conditions, e.g. failure of a neighbouring AP. This is an ideal architecture for a small network requiring few access points or where a wireless bridge is required between a main building and an outbuilding. The downside is that as the network grows there will be a large increase in the time required to manage the network.

Slides 35-37: An architecture utilising co-ordinated access points uses thin access points that are little more than radio receivers/transmitters. A centralised controller handles the entire authentication, encryption, monitoring and balancing tasks of the network. The configuration process is carried out only once on the central controller allowing new access points to be added by simply plugging them in. This configuration also allows for the implementation of redundancy by adding extra APs that will come into action should another, neighbouring AP fail. This architecture is ideal for large networks or in networks where redundancy or self-healing is required. Self-healing networks do not, in the eyes of an average user, appear to have faults. In-built redundancy and fail-safe systems seamlessly make a redundant device active in a situation where a device fails, thus maintaining network services at all times. Network administrators are made aware of the fault and can take the necessary corrective action.

Slide 38: In general a co-ordinated architecture is better in terms of ease of management, network resilience and quality of service. However the standalone architecture is good for small networks.

Slide 39: References

Slide 40: Invite students to ask any questions they have at this time and you may remind them that they will also have the opportunity to ask questions during the tutorial.

12.5 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

Lecturers' Notes:

Students have copies of the laboratory exercises in the Student Guide. Answers are not provided in their guide.

Your laboratory must have facilities for students to create and configure a wireless network, including the security settings of that network. The exact details are left up to you so that you can use suitable solutions based upon your equipment and network capabilities.

You will need to support the students throughout this process and provide them with any details they will require regarding connecting and configuring the wireless network.

During private study time, you may want to ask students to work in pairs or small groups for Exercise 2, depending on how easy this is to arrange with your group. You should advise students of the necessary arrangements during the laboratory session if so.

Exercise 1:

Create a small wireless network. Your tutor will provide you with details of the hardware, configuration and security options available in your laboratory.

You should test the network by connecting from a wireless enabled client device.

You will be required to produce a formal laboratory report in Private Study Exercise 1 and you should note all of the required detail for this report during the laboratory exercise. Your report should include:

- The architecture of the network including a schematic topology diagram
- A list of hardware included in the wireless portion of the network
- Reasons for choosing the network architecture you have implemented
- Security standards and protocols utilised by the wireless network
- Detail of access controls, services allowed, etc.
- The process of connecting a wireless enabled device to the wireless network you have created
- Any problems or issues during the laboratory exercise

Suggested Answer:

A formal report should be produced covering all of the elements listed above.

12.6 Private Study

The time allocation for private study in this topic is expected to be 7 hours.

Lecturers' Notes:

Students have copies of the private study exercises in the Student Guide. Answers are not provided in their guide.

Exercise 1:

Complete your report for the laboratory exercise.

Suggested Answer:

A professionally produced report providing the detail given in the laboratory exercise.

Exercise 2:

Research one of the following in groups of 2 or 3 students, as directed by your tutor:

- The RC4 stream cipher
- CRC-32 redundancy check
- The TKIP security protocol

You will be required to prepare a brief presentation of approximately 5 minutes for the tutorial session.

Suggested Answer:

Students should cover the key points of each.

RC4

- Used in SSL and WEP
- Quick and simple
- Main weakness when weak or repeating keys are used, e.g. in WEP
- Generates a keystream (pseudorandom stream of bits)
- Uses a table of all possible combinations of 256 bits in an 8 by 8 table along with two index pointers to create the pseudorandom number
- Main issue with WEP is the repeating nature of the keys which makes this insecure

CRC-32

- Error detection code designed to detect changes to raw data
- Data blocks get a short check value attached to them
- Check value is a short fixed length binary sequence
- Derived from the remainder obtained from polynomial division of the data block contents

- For CRC-32 the polynomial is 33 bits long
- On receiving the data block the calculation is repeated
- If check values do not match there has been some data corruption

TKIP

- Temporal Key Integrity Protocol
- Combines a secret key with an initialization vector
- Passes this to the RC4 stream cipher
- Implements a message integrity check
- Ensures every packet is sent with a unique encryption key
- The key used for encryption is 128 bits long
- Uses a 48-bit sequence number that removes the replay attack problem inherent in WEP

Exercise 3:

Research MAC addresses and make notes on what a MAC address is and how it is used.

Suggested Answer:

Notes should cover the main points:

- Media Access Control address
- A unique value that is associated with the network adapter of a device
- Sometimes called hardware addresses or physical addresses
- 12 digit hexadecimal numbers (48 bits)
- Written in the form MM:MM:MM:SS:SS:SS
- Ms represent the manufacturer number
- Ss represent the serial number of the device
- Operate on the data-link layer of the OSI model providing an identifier at a low level
- MAC addresses remain constant whereas IP addresses change when a device changes networks
- Networks map IP addresses to MAC addresses in order to identify individual devices.

Exercise 4: Revision

Review the material for the module. You should bring any specific questions about the module and revision for the examination to the tutorial session.

12.7 Tutorial Notes

The time allowance for tutorials in this topic is 2 hours.

Lecturers' Notes:

Tutorial time should be spent reviewing the private study and laboratory exercises from this topic with some emphasis on the laboratory exercise.

Students should be selected to present their findings on Private Study Exercise 2. Each presentation should be followed up with discussions on each item and students should take notes to supplement their own research and to enhance their understanding of the topic.

You should also allow some time for any questions students may have about the content of this topic or any other topic in this module and also provide some guidance regarding revision for the examination. You may also like to make use of the sample examination paper which is available on the NCC Education *Campus* (http://campus.nccedu.com).