LEVEL 5

NETWORK SECURITY AND CRYPTOGRAPHY

Student 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 you 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 you with knowledge of the fundamental principles and techniques employed in securing information and networks. The module will allow you 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 you 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 Outcomes: 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 you 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. Teaching and Learning

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. You will need to bring this student guide to all classes for this module. The breakdown of the hours is also given at the start of each topic.

5.1 Lectures

Your lecturer will be presenting the basic knowledge and the theoretical concepts required for the unit during this time. He/she will use PowerPoint slides during the lecture time and you will be expected to take notes.

You will also be encouraged to be active during this time and discuss and/or practice the concepts covered. Lectures will include question and answer elements to promote participation and to allow your lecturer to check whether you understand the concepts they are covering.

5.2 Tutorials

These are designed to deal with the questions arising from the lectures and private study sessions. You should think carefully beforehand about any areas in which you might need additional guidance and support and use this time to discuss these with your teacher.

5.3 Laboratory Sessions

During these sessions, you are required to work through practical tutorials and various exercises. The details of these are provided in this guide.

5.4 Private Study

This Student Guide also contains details of the private study exercises. You are expected to complete these exercises to improve your understanding. Your tutor will set deadlines for the completion of this work and go over the suggested answers with you. The deadlines will usually be before the scheduled tutorials for that topic. Some of the private study tasks may require you to work in a small group so you will need to plan your time carefully and ensure that you can meet with your group members to complete the work required before the deadline.

You should also use this time to revise the content of lectures to ensure understanding and conduct extra reading (using the supplementary textbooks or other materials available in the library or online). You should bring any questions to the tutorial for additional guidance and support.

6. 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.

7. Further Reading List

You will also be expected to undertake further reading to consolidate and extend your knowledge of the topics covered in this module. Your Accredited Partner Centre's library will contain a selection of useful sources of information and you can also make use of materials available online. The list below also provides suggestions of suitable reference books you may like to use:

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

On completion of the topic, you 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 Timings

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

1.3 Tutorial Sessions

The time allocation for this topic is 2 hours.

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:

$$P \wedge k = E \pmod{n}$$

"^" 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:

$$14 \wedge 7 = E \pmod{33}$$

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 ^ j = P (mod 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!

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

1.4 Private Study Exercises

You should spend approximately 7.5 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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.

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.

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.

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

Exercise 5:

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

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 you understand the key concepts at this stage.

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

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

2.2 Timings

Lectures: 2 hours

Laboratory Sessions: 2 hours

Private Study: 7.5 hours

Tutorials: 1 hour

2.3 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

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).

2.4 Private Study Exercises

You should spend approximately 7.5 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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

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.

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

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, you will be able to:

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

3.2 Timings

Lectures: 2 hours

Laboratory Sessions: 2 hours

Private Study: 7.5 hours

Tutorials: 1 hour

3.3 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

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.

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.

3.4 Private Study Exercises

You should spend approximately 7.5 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

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

Exercise 2:

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

Exercise 3:

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

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, you will be able to:

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

4.2 Timings

Lectures: 2 hours

Laboratory Sessions: 2 hours

Private Study: 7.5 hours

Tutorials: 1 hour

4.3 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

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.

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.

4.4 Private Study Exercises

You should spend approximately 7.5 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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.

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.

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.

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, you will be able to:

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

5.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

5.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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.

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.

5.4 Private Study Exercises

You should spend approximately 7.5 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

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

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.

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.

5.5 Tutorial Notes

The tutorial for this topic will last for 2 hours.

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, you will be able to:

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

6.2 Timings

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

6.3 Laboratory Sessions

The laboratory time allocation for this topic is 2 hours.

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

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

6.4 Private Study Exercises

You should spend approximately 8 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

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

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.

Exercise 3:

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

6.5 Tutorial Notes

The tutorials for this topic will last for 1 hour.

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, you will be able to:

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

7.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

7.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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.

7.4 Private Study Exercises

You should spend approximately 7 to 8 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

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

Exercise 2:

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

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

7.5 Tutorial Notes

The tutorials for this topic will last for 2 hours.

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, you will be able to:

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

8.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

8.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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

8.4 Private Study Exercises

You should spend approximately 8 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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

Exercise 2:

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

Exercise 3:

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

8.5 Tutorial Notes

The tutorials for this topic will last for 2 hours.

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, you will be able to:

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

9.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

9.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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

9.4 Private Study Exercises

You should spend approximately 7 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

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

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.

9.5 Tutorial Notes

The tutorials for this topic will last for 2 hours.

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, you will be able to:

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

10.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

10.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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.

10.4 Private Study Exercises

You should spend approximately 8 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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.

Exercise 2:

Complete your report for 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.

10.5 Tutorial Notes

The tutorials for this topic will last for 2 hours.

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, you will be able to:

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

11.2 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

11.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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

11.4 Private Study Exercises

You should spend approximately 8 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

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.

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.

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.

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, you 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 Timings

Lectures: 2 hours

Laboratory Sessions: 1 hour

Private Study: 7.5 hours

Tutorials: 2 hours

12.3 Laboratory Sessions

The laboratory time allocation for this topic is 1 hour.

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

12.4 Private Study Exercises

You should spend approximately 7 hours on the Private Study for this topic. You should use this time to complete the exercises below as directed by your lecturer and to review the contents of this topic.

Exercise 1:

Complete your report for 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.

Exercise 3:

Research MAC addresses and make notes on what a MAC address is and how it is used.

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.