Network Security and Cryptography

December 2015

Sample Exam Marking Scheme

This marking scheme has been prepared as a **guide only** to markers. This is not a set of model answers, or the exclusive answers to the questions, and there will frequently be alternative responses which will provide a valid answer. Markers are advised that, unless a question specifies that an answer be provided in a particular form, then an answer that is correct (factually or in practical terms) **must** be given the available marks.

If there is doubt as to the correctness of an answer, the relevant NCC Education materials should be the first authority.

Throughout the marking, please credit any valid alternative point.

Where markers award half marks in any part of a question, they should ensure that the total mark recorded for the question is rounded up to a whole mark.

Answer ALL questions

Marks

Question 1

a) Briefly describe the processes of *encryption* and *decryption* in relation to cryptography. **5**

Encryption is the process of converting readable clear-text/plain-text (1 mark) to cipher-text (1 mark). This text is an obscured / unrecognisable form (1 mark). Decryption is the reverse process. (1 mark) Encryption and Decryption both make use of a key and algorithm. (1 mark).

b) What is the difference between Symmetric and Asymmetric key encryption? **4**

Award 1 mark for each bullet point up to a maximum of 4 marks:

- ***Symmetric Key encryption uses the same key for encryption and decryption.***
- ***Asymmetric key encryption uses a pair of related keys (one for encryption and the other for decryption).***
- ***The keys cannot be derived from each other.***
- ***A message encrypted by one key can only be decrypted using the other.***

c) Suppose you decide to use a 10-bit key. How many combinations are there? **1**

- $2^{10} = 1024$

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 2

a) James and Alexander are having a debate about Public Key Infrastructure (PKI). James says that it is simply a way of authenticating users. However, Alexander argues that it is a type of encryption algorithm. They have asked you to decide who is correct. **6**

Briefly outline the purpose of PKI. You should also explain what is meant by a certificate authority and digital certificate.
The maximum number of marks awarded to the question is 6. Award up to 2 marks for the description of PKI:

Public Key Infrastructure (PKI) is security architecture/ framework that has been introduced to provide an increased level of confidence for exchanging information.

Award up to 2 marks for the explanation of Certificate Authority:

A Certificate Authority to verify applicants, issue and verify certificates.

Award up to 2 marks for the explanation of Digital Certificate:

Digital Certs which binds a public key to an identity that the issuing CA is willing to vouch for.

Note: Award 1 mark for partially correct answers.

b) Are James's and Alexander's opinions about Public Key Infrastructure correct or incorrect? For **each** opinion, you should provide ONE (1) reason for why it is either correct or incorrect. **4**
The maximum number of marks awarded to the question is 4. Award 1 mark for accurately stating whether an opinion is correct or incorrect up to a maximum of 2 marks. Award 1 mark for a relevant justification up to a maximum of 2 marks.

Alexander is incorrect. An algorithm is a set of instructions to carry out a task, PKI uses encryption, but it can use many different types of encryption algorithm, and it does much more – see (a)

James is incorrect. PKI enables a certificate holder to be authenticated, but PKI is much more, Certificates are not just issued to users.

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 3

a) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. **3**

Award 1 mark for each bullet up to a maximum of 3 marks:

- ***Confidentiality: through Encryption of data***
- ***Integrity: Routers at each end of the tunnel calculate checksum or hash. Integrity (sequence integrity): Anti-replay protection through sequence numbers.***
- ***Authentication: It involves Signatures and Certificates***

b) Briefly explain what is by an Authentication Header (AH) **and** an Encapsulating Security Payload (ESP). **6**
The maximum number of marks awarded to this question is 6. Award 1 mark for each bullet point up to a maximum of 3 marks:

<u>Authentication Header</u>

- ***Adds a new Header (inc New IP)***
- ***Provides authentication services***
- ***Verifies the originator of the message***
- ***Provides an integrity check of the entire packet, including the new L3 IP header.***
- ***Provides protection against replay attacks***

Award 1 mark for each bullet point up to a maximum of 3 marks:

<u>Encapsulating Security Payload</u>

- ***Adds a new Header (inc New IP)***
- ***Encrypts the original datagram***
- ***Provides protection against replay attacks***

c) Draw a diagram to show where IPSec fits in the TCP/IP model. **1**

Application (HTTP/ FTP etc)
TCP
IP/IPSec
Host to Network

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 4

a) Explain what is meant by a digital signature **and** describe how it is generated. **6**

Award 1 mark for each bullet point up to a maximum of 6 marks:

- ***<u>Definition:</u> a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.***
- ***The message is hashed with agreed algorithm) to form a message digest***
- ***The message digest is encrypted with the sender's private key.***
- ***The encrypted message digest is the signature which is added to the message and sent.***
- ***The recipient computes the message digest and also decrypts the signature with the sender's public key.***
- ***The recipient compares the MD with the decrypted signature. If they match, the message has not been tampered with.***

b) Does a digital signature ensure the entire message is encrypted? You should provide ONE (1) reason to support your answer. **2**

Award 1 mark for correctly stating 'No' and 1 mark for the justification up to a maximum of 2 marks.

No – it ensures integrity, authenticity and non-repudiation.

c) Name the IETF standard for email security **and** briefly outline what additional security it provides in addition to digital signatures. **2**

Award 1 mark for each bullet point up to a maximum of 2 marks.

- ***S/MIME***
- ***Encryption of the body of the message using symmetric key method (3DES/AES)***

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 5

a) Explain what is meant by the term *firewall* in network security **and** discuss how it is used in network architectures. **7**

The maximum number of marks awarded to this question is 7. Award up to 2 marks for the description:

A Firewall is a hardware or software device (1 mark) which inspects incoming and outgoing traffic (1 mark).

Award 1 mark for each bullet point up to a maximum of 5 marks:

- ***It allows or drops the packet depending on whether it meets one of a set of rules.***
- ***Firewalls often provide additional functions such as NAT and VPN gateway.***
- ***It provides functions of Proxy server and Reverse-proxy.***
- ***A firewall is normally positioned on the perimeter of a network.***
- ***It can also partition networks of differing security requirements (e.g. DMZ for services requiring direct connection from the internet)***

b) Firewalls use Access Control Lists (ACL). Explain what is meant by an ACL and typical contents. **3**

Award 1 mark for each bullet point up to a maximum of 3 marks:

- ***A rule determines conditions to drop or allow a packet executed in sequential order. Processing stops when a rule is matched.***
- ***Typical Contents: Source IP address/ Network and Destination IP address/ Network***
- ***Typical Contents: Action (block/allow) and Protocol***

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 6

a) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these FIVE (5) requirements. **5**

Award 1 mark for each bullet point up to a maximum of 5 marks:

- ***Authentication – validates that the data was sent from the sender.***
- ***Access Control – preventing unauthorized users from accessing the network.***
- ***Confidentiality – preventing the data from being read or copied as the data is being transported.***
- ***Data Integrity – ensuring that the data has not been altered.***
- ***Availability – ensuring that a connection can be made.***

b) There are several methods of achieving secure remote access. One important method is to use a VPN. Explain if/ how a VPN achieves each of the requirements in part (a) **5**

Award 1 mark for each bullet point up to a maximum of 5 marks:

- ***Authentication of the user, typically via RADIUS.***
- ***Access control – only authorized users can access, e.g. through access rights on the authentication server.***
- ***Confidentiality via encryption of data across the insecure network***
- ***Integrity –via MAP, replay attack prevention***
- ***Availability cannot be provided by a VPN through protocols, but by capacity and resilience of the architecture.***

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 7

a) Confidentiality, Integrity and Availability are core attributes in security. Identify THREE (3) threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. **6**

The maximum number of marks awarded to each question is 6. Award 1 mark for correctly stating a threat up to a maximum of 3 marks. Award 1 mark for correctly stating which area has been compromised up to a maximum of 3 marks.

<u>Threat – Compromised Area</u>

- ***Eavesdropping – Threatens Confidentiality.***
- ***Denial of Service – Threatens Availability.***
- ***Rogue Aps and Evil Twin Aps – Threaten Confidentiality and Integrity.***
- ***Misconfigured Aps – Threatens Confidentiality, Integrity and Availability.***
- ***Endpoint Attacks – Threatens Confidentiality, Integrity and Availability.***

b) Spell out the acronyms PSK and EAP. Briefly explain the difference between PSK and EAP for authenticating devices onto a Wireless network. **4**

Award 1 mark for each bullet point up to a maximum of 4 marks:

- ***PSK stands for Pre-shared key***
- ***It requires same secret key to be installed on all clients and the AP. As the number of clients grows, there is a risk of a key disclosure, and it is trivial to reveal the plaintext of the PSK on client devices.***
- ***EAP stands for Extensible Authentication Protocol***
- ***It uses an authentication server to process each client's request. Centrally managed, individual credentials.***

Note: Credit alternative valid points.

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 8

a) Briefly explain what is meant by a password audit. **2**

There are regular attempts to crack users' passwords using techniques such as a dictionary attack (1 mark) Passwords unchanged for a long period can be identified (though this should be controlled by technical security policy). An audit identifies weak passwords which are reported (1 mark).

b) Explain what is meant by the term *salt* in relation to cryptography. You should discuss how it is used to make it more difficult to crack passwords. **4**

Salt is the term used for randomizing the hashes by appending or prepending a random string to the password before hashing (1 mark). This makes the same password hash into a completely different string every time (1 mark) To check if a password is correct, we need the salt (1 mark) so it is usually stored in the user account database along with the hash, or as part of the hash string itself (1 mark).

c) Discuss TWO (2) alternative methods of authentication **and** outline ONE (1) advantage or disadvantage of each method. **4**

The maximum number of marks awarded to this question is 4. Award 1 mark for stating an alternative method up to a maximum of 2 marks. Award 1 mark for correctly stating an advantage/disadvantage of each method up to a maximum of 2 marks.

<u>Method – Advantage/Disadvantage</u>

- ***Smartcards - tamper resistant but easily transferrable***
- ***Biometrics (iris/ fingerprint/ voice). Weakness e.g. fingerprint (gummy finger) and a need for liveness detection.***
- ***2FA (eg PW + smartcard) – Reduces the chance of compromise.***

Note: Credit alternative valid points.

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 9

a) Briefly describe the term *vulnerability* in the context of network security **and** provide THREE (3) examples of vulnerabilities in a network. **5**

Award up to 2 marks for the description:

Vulnerability is a weakness of an asset or control that can be exploited by one or more threats.

Note: Award 1 mark for a partially correct definition

Award 1 mark for each bullet point up to a maximum of 3 marks:

- ***Open ports that should be closed***
- ***Unprotected sensitive traffic***
- ***Lack of id and authentication of sender/receiver***
- ***Insecure network architecture***
- ***Poor password mgt***
- ***Lack of effective change control***
- ***Uncontrolled downloading / use of software***
- ***Single point of failure***
- ***Lack of back-up copies***
- ***Unprotected password table***
- ***Immature or new software***
- ***Incomplete or unclear spec for developers***

b) Explain what is meant by a *vulnerability assessment* in the context of network security **and** provide THREE (3) reasons why it is important. **5**

Award up to 2 marks for the description:

A vulnerability assessment involves trying to detect network and system vulnerabilities and to test security by taking an "attacker" like approach in order to gain access.

Note: Award 1 mark for a partially correct definition

Award 1 mark for each bullet point up to a maximum of 3 marks:

<u>Importance</u>

- ***It determines susceptibility to an attack before networks are exploited,***
- ***Forces companies to take early corrective action.***
- ***It can show the consequences of an attack to your***
- ***Organization***
- ***Should be a part of regular audit.***

Total: 10 Marks

© NCC Education Limited 2015

Marks

Question 10

a) James and Alexander are having another debate about computer and network security. James says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with James? You should explain your answer with NINE (9) reasons. **10**

The objective of this question is to place security in context of the business and provide students with more opportunity to construct an argument. However, marks should be credited for bullet points, and not on the structure of their discussion.

The maximum number of marks awarded to this question is 10. Award 1 mark for stating that James is wrong.

Award 1 mark for each bullet point up to a maximum of 9 marks:

- ***It is not possible to find all vulnerabilities and threats***
- ***It is prohibitively expensive to mitigate all of them***
- ***Many threats and vulnerabilities are non-technical***
- ***A risk-based approach is needed***
- ***A risk-based approach examines the likelihood and impact of potential security incidents***
- ***A risk-based approach determines which the highest risks are.***
- ***Those identified as low risk can be accepted.***
- ***High risk can be controlled or transferred.***
- ***Estimating the cost of an incident against the cost of controlling it is one way of deciding.***

Note: Credit alternative valid points.

Total: 10 Marks

End of Examination Paper

© NCC Education Limited 2015

Learning Outcomes matrix

Question	Learning Outcomes assessed	Marker can differentiate between varying levels of achievement
1	1	Yes
2	2	Yes
3	3	Yes
4	4	Yes
5	7	Yes
6	8	Yes
7	9	Yes
8	5, 6	Yes
9	5, 6	Yes
10	5	Yes

© NCC Education Limited 2015

Grade descriptors

Learning Outcome	Pass	Merit	Distinction
Understand the most common types of cryptographic algorithm	Demonstrate adequate understanding of common types of cryptographic algorithm	Demonstrate robust understanding of common types of cryptographic algorithm	Demonstrate highly comprehensive understanding of common types of cryptographic algorithm
Understand the Public-key Infrastructure	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Understand security protocols for protecting data on networks	Demonstrate adequate understanding of security protocols	Demonstrate robust understanding of security protocols	Demonstrate highly comprehensive understanding of security protocols
Be able to digitally sign emails and files	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Understand Vulnerability Assessments and the weakness of using passwords for authentication	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to perform simple vulnerability assessments and password audits	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Be able to configure simple firewall architectures	Demonstrate adequate level of understanding and ability	Demonstrate robust level of understanding and ability	Demonstrate highly comprehensive level of understanding and ability
Understand Virtual Private Networks	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to deploy wireless security	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard

© NCC Education Limited 2015