Higher National Diploma in Information Technology

Second Year, First Semester Examination – 2015

IT 2003 – Operating Systems and Computer Security

Marking Scheme

Instructions to candidates

1. Answer any Four (04) questions.
2. All questions in carry equal marks – 25 Marks each.
3. Time allowed is two (02) hours.

Q1

i. List three security concepts. [03 Marks]

- ***Confidentiality***
- ***Integrity***
- ***Availability***

ii. Define "Security attack" and Security Mechanism" [04 Marks]

Security attack: any action that compromises the security of information owned by an organization

Security Mechanism: a mechanism that is designed to detect, prevent, or recover from a security attack

iii. Five major categories of security services are define in X.800 OSI security architecture. Briefly explain any three of them [06 Marks]

a. Authentication - assurance that the communicating entity is the one claimed

b. ***Access Control - prevention of the unauthorized use of a resource***

c. ***Data Confidentiality –protection of data from unauthorized disclosure***

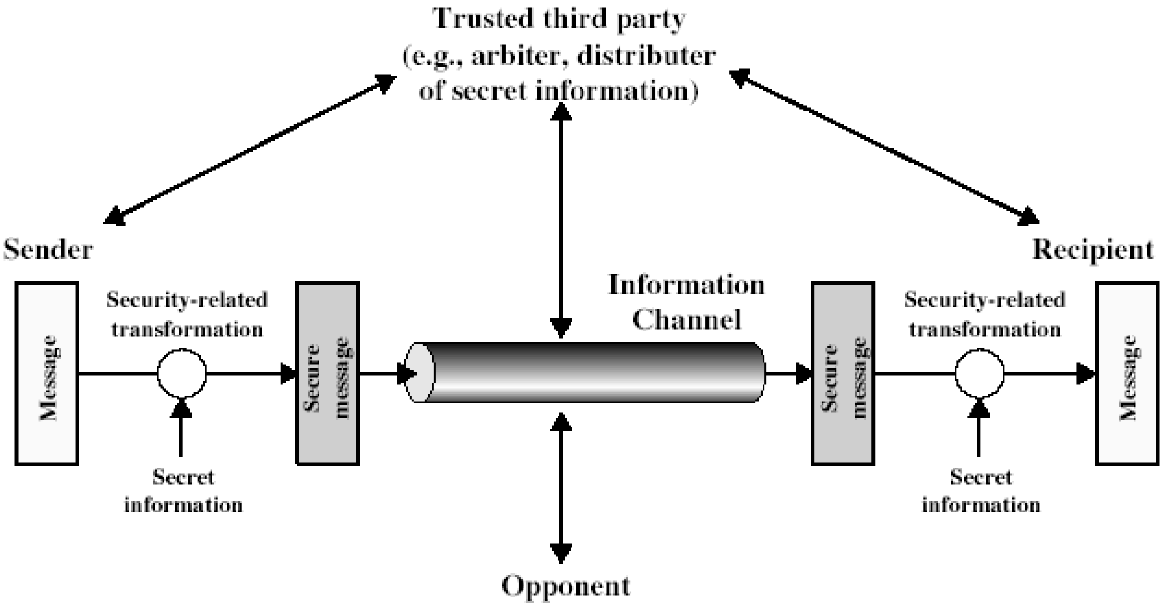
d. ***Data Integrity - assurance that data received is as sent by an authorized entity***

e. ***Non-Repudiation - protection against denial by one of the parties in a communication***

(any 3x02=06 marks)

iv. Briefly explain “Model for Network Security” with use of diagram [05 Marks]

This models information flowing over an insecure communications channel, in the presence of possible opponents. Hence an appropriate ***security transform (encryption algorithm)*** *can be used, with suitable* ***keys****, possibly negotiated using the presence of a* ***trusted third party****.*



v. Define "Information Security Policy" [03 Marks]

Documentation of measures accepted by the management as necessary to maintain confidentiality, Integrity and Availability of information

vi. Information Security Policy (ISP) is important to an organization. Are you agree with this statement? Justify your answer. [04 marks]

ISP gives Protection of the interest of those relying on information, and the information systems and communication that deliver the information, from harm resulting from failures of availability, integrity and confidentiality

Q2

i. Define the term cryptanalysis? [03 Marks]

The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key

ii. Briefly explain the following terms [05 Marks]

a. Encryption

The process of converting plaintext to cipher text

b. Decryption:-

The process of converting cipher text back into plaintext

c. Cipher:-

algorithm for transforming plaintext to ciphertext

d. Plane text

the original message

e. Key

info used in cipher known only to sender/receiver

iii. Encryption algorithms are categorized as Substitution Ciphers and Transposition Ciphers. Give two examples for each. [04 Marks]

Substitution Ciphers

Caesar Cipher, Monoalphabetic Cipher, One-Time Pad (any 2x01= 02 marks)

Transposition Ciphers

Rail Fence cipher, Row Transposition Ciphers (2x01= 02 marks)

iv. Compare characteristics of Block and Stream Ciphers [04 Marks]

- ***block ciphers process messages in into blocks, each of which is then en/decrypted***
- ***stream ciphers process messages a bit or byte at a time when en/decrypting***

v. Encrypt the message "easy question" using Caesar encryption algorithm defined as C=E(P)=(Pi+3) mod 26 [09 Marks]

e→7 mod 26 = 7 = H

a→3 mod 26 = 3 = D

s→21 mod 26 = 21 = S

y→27 mod 26 = 1 = B

q→19 mod 26 = 19 = T

u→23 mod 26 = 23 = X

e→7 mod 26 = 7 = H

s→21 mod 26 = 21 = V

t→22 mod 26 = 22 = W

i→11 mod 26 = 11 = L

o→17 mod 26 = 17 = R

n→16 mod 26 = 16 = Q

(0.5 x 12= 06 marks)

The encrypted message is HDVBTXHVWLRQ (02 marks for answer and 01 for writing it in capital letters)

Q3

i. Asymmetric encryption developed to address two key issues. Explain one briefly. [02 Marks]

- ***key distribution – how to have secure communications in general without having to trust a KDC with your key***
- ***digital signatures – how to verify a message comes intact from the claimed sender***

(any one of above, 02 marks)

ii. Public key algorithm rely on two keys. Briefly explain two characteristics of public key algorithm. [04 Marks]

- ***it is computationally infeasible to find decryption key knowing only algorithm & encryption key***
- ***it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known***
- ***either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)***
  (any 2 x02 =04 marks)

iii. Name two alternative function use in message authentication? [04 Marks]

- ***message encryption***
- ***message authentication code (MAC)***
- ***hash function (any 2x02= 04 marks)***

iv. What is a Digital Certificate? [02 Marks]

An electronic Document which provides the certification that a person is authorised to use the Public Key algorithm given to him by a trusted third party

v. Explain the role of a Key Distribution Centre in a Two Key Crypto System. [5 Marks]

The key distribution center is an independent third party organization that is involved in generating public key algorithms and facilitating procedures to generate corresponding

private key algorithms by the users of public key crypto systems. The digital certificate is also issued by such organizations when purchasing the public key algorithms by the users.

vi. The Digital Signature is a well-known modern security mechanism that assures confidentiality, integrity and availability of information. It uses a number of security techniques in performing its task. Discuss the benefits and limitations of Digital Signature. [08 Marks]

Benefits:

a. ***Provides Confidentiality, Integrity and Availability to information***
b. ***Acts as a signature placed on a manual documents***
c. ***Allows revelations of information disclosure, tampering documents and certain types of frauds.***
d. ***Can be configured and implemented fairly easily***
e. ***Users of the system does not have to understand complicated technological details to use the signature***
f. ***Provides a secure private channel in a public network***

Limitations:

a. ***The keys has to be exchanged prior to communication***
b. ***Need of a secure channel to exchange keys***
c. ***No provision in the system for compromising passwords and pin codes***

Q4

i. Malicious software is categorized in to two types. Name them and give two examples for each category. [04 Marks]

Host based:

Trap door, Trojan horse, logic bomb, virus (any 2 example) 02 marks

Independent:

Rabbit, zombie, worm ***(any 2 example)*** ***02 marks***

ii. State three common non-malicious program errors. [03 marks]

- ***Buffer overflows***
- ***Incomplete mediation***
- ***Time of check to time of user errors***

iii. List down the three authentication methods and give one example for each of these classes [03 Marks]

a. Something the user knows - Passwords, PIN numbers

b. Something the user has- A Plastic card with a chip

c. ***Something the user is –biometrics*** [01x3 Marks]

iv. Explain the phases of virus life cycle [04 Marks]

d. Dormant – waiting on trigger event

e. Propagation – replicating to programs/disks

f. Triggering – by event to execute payload

g. Execution – of payload

v. Explain methods use for buffer overflow protection. [04 marks]

Canaries: known values that are placed between a buffer and control data on the stack to monitor buffer overflow
Bounds checking: a compiler based technique that adds run time bounds information for each allocated block of memory
Tagging: tagging the memory of buffer as data memory. (any 2 methods: 2x2=4)

vi. Briefly explain “procedure based access control” and “role based access control” [04 marks]

procedure based access control

- ***Procedure that controls access to objects***
- ***Trusted interface to accesses object***
- ***Users or general operating system routines cant access***
- ***No simple, fast access(inefficient)***

role based access control

- ***Deferent users***
  - ***Administrators***
  - ***Users or guests***
- ***Associate privileges***
  - ***Users***
  - ***Groups***
  - ***Control access rights by job***

vii. State services available in Trusted Operating System [03 Marks]

a. Memory protection
b. File protection
c. General object access control
d. User authentication

*****Full marks be given to any three from the list***

Q5

Write the short notes on 5 (five) of the following topics. [5 * 5 marks =25 marks]

i. Firewall (hint: construct your answer by considering what is, limitations and types)

A choke point of contro; and monitoring. Used to interconnect network with different trust. Impose restriction on network service. Auditing and control acess.

Limitation of fire wall: cannot protect from attcks bypassing ,internal threats and transfer virus

Types: packet filter, stateful packet filter, application level gateway, circuit level gateway

ii. Intrusion techniques and Approaches to Intruder Detection

Intrusion technique:

Aim to gain access and increase privilege on a system. Key goal is often acquire password. Main techniques for that is password guessing and password capturing.

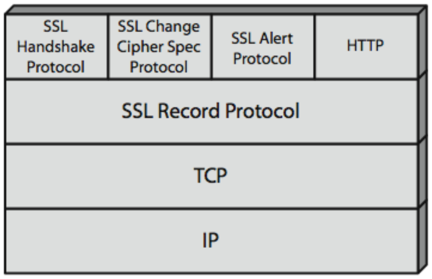
Approaches to Intruder Detection:

- ***statistical anomaly detection***
  - ***threshold***
  - ***profile based***
- ***rule-based detection***
  - ***anomaly***
  - ***penetration identification***

iii. Security Socket Layer protocol

transport layer security service

SSL has two layers of protocols



iv. IP Security

- ***general IP Security mechanisms***
- ***provides:***
  - ***authentication***
  - ***confidentiality***
  - ***key management***
- ***applicable to use over LANs, across*** public & private WANs, & for the Internet

benefits:

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

v. Database integrity

Data integrity is the accuracy & consistency of data stored in the database system. A condition or restriction that is applied to a particular set of data is commonly termed as integrity control on constrains. Constraints are used to ensure accuracy & consistency of data in a relational databse. Data integrity involves making sure Data is entered consistently, stored consistently in the database. Database normalization can also help provide data consistency since the occurrence of redundant data being reduced in the database.

There are 5 types of constraints in SQL. They are

- Not Null constraints
- Primary key constraints
- Unique constraints
- Foreign key constraints
- Check constraints

vi. Database Administrator

***Database Administrator* – Manager whose responsibilities are focused in management of the technical aspects of the database system**

Responsibilities of a DBA

- ***Establishing data definition***
- ***Developing programs to generate needed information***
- ***Adding data & deleting data from the database***
- ***Implementing security & integrity controls***
- ***Managing database operations***
- ***Database planning & Development***

vii. Database recovery

Database Recovery

All database systems must have second backup & recovery procedures to avoid inefficiencies & loss. Because information stored on computer media is subject to loss or corruption caused by a wide range of events. It is important to provide restoring correcting data to the database source of failures

1. ***System errors – The system has entered an undesirable state, such as deal lock, which prevent s\s th program form continuing with normal processing, The type of failure may or may not result in corruption of data files***
2. ***Hardware failures – Disk failure & loss of transformation capabilities***
3. ***Logical Errors – Bad data or missing data***

Recovery procedures

1. ***Aborted – A transaction may not always complete its process successfully such transactions must be aborted restoring the database to the state it was in before the transaction such restoration is achieved by roll back***

2. ***Committed – A transaction hat successfully complete its processing said to be committed***

END