KABARAK UNIVERSITY

UNIVERSITY EXAMINATIONS

2009/2010 ACADEMIC YEAR

FOR THE DEGREE OF BACHELOR OF BUSINESS MANAGEMENT & INFORMATION TECHNOLOGY

COURSE CODE:	**BMIT 416**
COURSE TITLE:	**IT SECURITY, AUDIT & ETHICS**
STREAM:	**Y4S1**
DAY:	**MONDAY**
TIME:	**9.00 – 11.00 A.M.**
DATE:	**07/12/2009**

INSTRUCTIONS:

- Answer question **ONE** and any other **THREE** questions
- Do **NOT** write anything on the question paper

PLEASE TURN OVER

SEDCTION A ANSWER *ALL* QUESTIONS IN THIS SECTION

QUESTION ONE (40 Marks)

a)

i). Outline EIGHT ways in which a security policy benefits a company [4 marks]

ii). Security assurance is what the business pays for and security controls are what it gets." Explain this statement. [4 marks]

iii). In RSA, assume e=3, p = 11 and q =23. Show that 147 is a possible value of d. [4 marks]

b)

i). Consider data that is stored over time in a mandatory access control based system. Will the contents of files containing highly classified ("top secret") information be necessarily more trustworthy than material stored in files marked unclassified? Justify your answer [3 marks]

ii). "Access control matrices can represent anything that is represented by access control lists."
State whether this statement is true or false and justify your answer: [2 marks]

iii). Which is generally safer (from a security point of view), a firewall with a .default deny. policy or a firewall with a default allow Policy? Explain [3 marks]

c)

i). Many spam filters can be configured to use either a whitelist or a blacklist. Name one advantage of using a whitelist (instead of a blacklist) for your spam filter. [2 marks]

ii). Name one disadvantage of using a whitelist (compared to a blacklist) for your spam filter [2 marks]

d)

i). Explain the terms "proof of submission" and "non-repudiation" in an electronic mail system [3 marks]

ii). Explain the importance of non-repudiation in a system of e-commerce [3 marks]

e) Distinguish between the following terms as applied in computer security

i). Security model and security policy [2 marks]

ii). Encryption and hash [2 marks]

f) The security handshake protocols are evaluated according to security & *pereformance*. The *performance* parameters are:

- Number of messages,
- Processing power required, and
- Compactness of messages.

Compare the following two protocols, P1 and P2, with respect to the above performance measures: [2 marks]

Alice Bob

P1: I'm Alice, *K{timestamp}* --- >

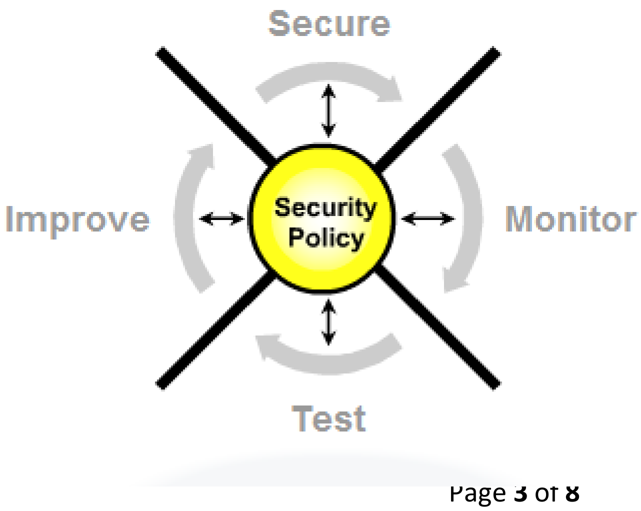
P2: I'm Alice, *timestamp, hash {K, timestamp}* >

g) Explain the rational behind the fact that most banks and credit card companies allow their Customers to access their accounts from ATM machines using only 4 digits as personal identification? [3 marks]

SECTION B ANSWER ANY THREE QUESTIONSTION

QUESTION TWO (20 Marks)

Study the following security wheel hence answer the question that follow



i). What security solutions would you implement to secure the network? [10 marks]

ii). What methods would you use to monitor the security? [4 marks]

iii). How would you test the security measures that you implemented in the Security and Monitoring Phases? [3 marks]

iv). What does the Improve Phase **actually** involve? [3 marks]

QUESTION THREE (20 Marks)

a)

i). In SSL, what is to be gained by "resuming" a session instead of starting a "new" session? [2 marks]

ii). In SSL, explain how the client and server mutually authenticate each other? [3 marks]

iii). In SSL, explain how to ensure that two identical plain messages will be transmitted as two different cipher messages? [2 marks]

iv). Assume that Alice likes to have a secure conversation with Bob and she wants a trusted 3rd party T to record the conversation. One possible scheme is to establish two SSL connections from Alice and Bob to T. How many times will a message typed by one person need to be encrypted/decrypted before the other person can read it? Explain? [3 marks]

b)

i). What is the principle of least privilege? Why is it important? [3 marks]

ii). Is a TCP connection secure against eavesdropping? Why or why not? [3 marks]

QUESTION FOUR (20 Marks)

a) Consider the following PEM message:

From: Alice
To: Bob
Subject: CS772 Final
Date: Mon Dec 4, 2006
-----BEGIN PRIVACY ENHANCED MESSAGE-----
Proc-Type: 4, ENCRYPTED
Content-Type: RFC822
DEK-Info: DES-CBC, **IV**
Originator-ID-Asymmetric: <***Alice*** certificate ID>
Key-Info: RSA, <encoded message key encrypted with ***Alice*** public key>
MIC-Info: RSA-MD5, RSA, <encoded ***encrypted*** MIC>
Recipient-ID-Asymmetric: <***Bob*** certificate ID>
Key-Info: RSA, <encoded message key encrypted with ***Bob*** public key>
<encoded encrypted message using DES-CBC>
-----END PRIVACY ENHANCED MESSAGE-----

i). Is it possible for Bob to prove that indeed Alice sent that message to him? Explain? [2 marks]

ii). Is it possible for Trudy to intercept and then read and modify the message? Explain? [2 marks]

b) You have a copy of Anthony Joseph's certificate chain: his certificate is signed by the EECS department; the EECS department's certificate is signed by UC Berkeley; UC Berkeley's certificate is signed by Verisign. Whose public keys do you need to know in advance in order to obtain the correct public key for Anthony? [2 marks]

c) Study the following digital certificate hence answer the questions that follow

Certificate Request:	**Certificate:**
Data: Version: 0 (0x0) Subject: C=US, ST=Virginia, L=Norfolk, =Old Dominion University, OU=Computer Science Department, CN=cs772 grader/emailAddress=cs772@cs.odu.edu Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:9b:5e:7d:fc:c8:73:4e:88:14:f8:d8:6f:d0:80:	Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: md5WithRSAEncryption Issuer: CN=Dr. Wahab, ST=Virginia, C=US/emailAddress=wahab@cs.odu.edu, O=Old Dominion University Validity Not Before: Oct 11 17:15:35 2006 GMT Not After : Oct 11 17:15:35 2007 GMT Subject: CN=cs772 grader, ST=Virginia,

d1:a5:d8:03:bb:fa:10:38:e8:2d:a3:67:87:c3:b1: b0:ef:1e:82:43:44:35:a0:d7:06:16:4a:5f:46:7a: ae:ca:96:ef:66:34:80:f9:88:e5:4c:fc:3b:fb:e3: 61:ed:02:d9:9d:9c:29:6b:b6:d8:82:63:f0:44:d6: d3:6a:79:48:a2:31:41:4a:bd:b0:9e:e4:c6:26:ca: 06:41:c6:0c:df:8c:d3:cd:63:11:2d:cd:7c:70:d0: 4d:7c:1d:1b:2b:60:2d:53:3f:4d:d0:f3:b5:31:7f: 25:53:35:fa:de:a7:b7:09:45 Exponent: 65537 (0x10001) Attributes: challengePassword :oducsc unstructuredName :cs772 class, fall 06 Signature Algorithm: md5WithRSAEncryption 45:bd:7d:8a:1b:b6:74:78:f2:36:f2:d8:46:f7:82:70:47:02: 1d:31:b4:60:91:6e:39:eb:a3:78:a2:da:ed:df:70:f3:c1:25: df:89:f3:ed:5d:ad:c5:e5:f7:77:2e:77:c4:fd:ad:21:1f:2f: f4:f8:cc:a5:01:60:c8:68:84:86:87:d7:d5:60:8c:ff:ef:39: 76:fc:7a:12:13:a0:ea:e2:e2:9b:b1:3a:93:4f:8f:31:78:62: b1:2b:ef:a2:3a:05:0f:11:5a:5e:16:8f:fe:14:8f:af:d8:60: f5:7d:01:7a:cd:26:bc:84:ee:0f:5e:5c:59:04:fc:c6:6c:92: aa:29	C=US/emailAddress=cs772@cs.odu.edu, O=Old Dominion University, OU=Computer Science Department Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:9b:5e:7d:fc:c8:73:4e:88:14:f8:d8:6f:d0:80: d1:a5:d8:03:bb:fa:10:38:e8:2d:a3:67:87:c3:b1: b0:ef:1e:82:43:44:35:a0:d7:06:16:4a:5f:46:7a: ae:ca:96:ef:66:34:80:f9:88:e5:4c:fc:3b:fb:e3: 61:ed:02:d9:9d:9c:29:6b:b6:d8:82:63:f0:44:d6: d3:6a:79:48:a2:31:41:4a:bd:b0:9e:e4:c6:26:ca: 06:41:c6:0c:df:8c:d3:cd:63:11:2d:cd:7c:70:d0: 4d:7c:1d:1b:2b:60:2d:53:3f:4d:d0:f3:b5:31:7f: 25:53:35:fa:de:a7:b7:09:45 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: CA:FALSE Signature Algorithm: md5WithRSAEncryption 58:f2:a7:7f:dd:93:99:ec:ce:2a:61:09:8d:c9:e0:8e:53:c8: 0d:85:a8:15:7c:0d:f9:8f:fb:1a:a8:86:a0:93:c0:13:21:d2: 4e:5a:22:a1:0c:d0:dc:71:a0:84:45:15:e8:1b:5f:7a:44:43: a0:4f:28:ca:b0:4a:34:61:8f:bd:ed:b4:2a:e4:8c:6f:15:43: ac:a3:5a:a3:5a:99:b4:d2:55:87:60:f2:79:7d:46:f9:7b:f0: 5b:85:ad:ef:d2:06:ce:34:cb:11:f4:1f:08:f9:26:e9:65:26: 2a:96:02:d8:7e:0b:f0:93:e4:74:62:85:85:71:7d:bf:e9:e9: 71:37

Considering the above listings of certificates:

i). Explain the meaning of the term certification authority (CA) in IT security context hence state the CA in this certificate [3 marks]

ii). How long the certificate is valid? Explain how you arrive at your answer [1 mark]

iii). What is the value of the subject public key <e, n>? [2 marks]

iv). What is the value of the issuer public key? [2 marks]

v). Why you think that the signed certificate indeed corresponds to the certificate request? [2 marks]

vi). Is it possible for the owner of the signed certificate to issue and sign other certificates? [2 marks]

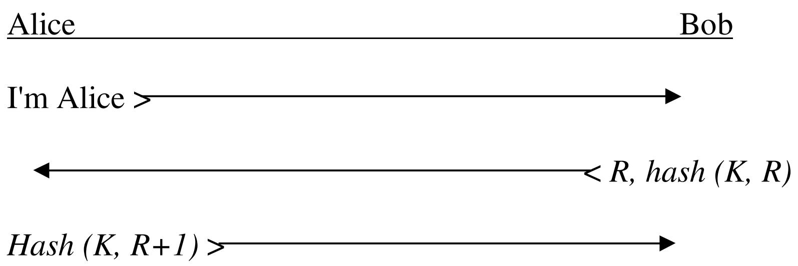
d) Which two security components make up the security solution of trust and identity?

[2 marks]

QUESTION FIVE (20 Marks)

a)

i). The following is a proposed mutual authentication protocol.



What are the possible flaws in this protocol? [2 marks]

ii). Propose how to fix the possible flaws with minimal modifications to the protocol. [3 marks]

iii). Explain how Trudy can exploit the "source routing" feature of the IP protocol? [2 marks]

b) Alice wants to send a cellphone text message to Bob securely, over an insecure communication network. Alice's cellphone has a RSA public key *KA* and matching private key *vA*; likewise, Bob's cellphone has *KB* and *vB*. The following is a cryptographic protocol for doing this, assuming both know each other's public keys.

Here is what Alice's cellphone will do to send the text message *m*:

1. Alice's phone randomly picks a new AES session key *k* and computes *c* = RSA-Encrypt(*KB*; *k*), *c*0 = AES-CBC-Encrypt(*k*;*m*), and *t* = RSA-Sign(*vA*; (*c*; *c*0)).
2. Alice's phone sends (*c*; *c*0; *t*) to Bob's phone.

And here is what Bob's cellphone will do, upon receiving (*c*; *c*0; *t*):
1. Bob's phone checks that *t* is a valid RSA signature on (*c*; *c*0) under public key *KA*. If not, abort.
2. Bob's phone computes *k*0 = RSA-Decrypt(*vB*; *c*) and *m*0 = AES-CBC-Decrypt(*k*0; *c*0).
3. Bob's phone informs Bob that Alice sent message *m*0.

i). Does this protocol ensure the confidentiality of Alice's messages? Why or why not? [3 marks]

ii). Does this protocol ensure authentication and data integrity for every text message Bob receives? Why or why not? [4 marks]

iii). Suppose that Bob is Alice's stockbroker. Bob hooks up the output of this protocol to an automatic stocktrading service, so if Alice sends a text message .Sell 100 shares MSFT. using the above protocol, then this trade will be immediately and automatically executed from Alice's account. Suggest THREE reasons why this might be a bad idea from a security point of view. [6 marks]

QUESTION SIX (20 Marks)

Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats.

(a) A firewall at the network perimeter. [7 marks]

(b) Firewalls on every end host machine. [7 marks]

(c) A network perimeter firewall and firewalls on every end host machine. [6 marks]