(*Knowledge for Development*)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2016/2017 ACADEMIC YEAR

SPECIAL EXAMINATIONS
YEAR ONE EXAMINATIONS

FOR THE DEGREE OF
MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY

COURSE CODE : MIT 824

COURSE TITLE : IT SECURITY ARCHITECTURE

DATE: 01/10/2017 TIME: 8.00A.M. – 10.00A.M.

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTION ONE AND ANY OTHER THREE **QUESTIONS.**

QUESTION ONE (40 MARKS)

a) Policies must be considered as the basis for all information security efforts. Hence the first step in compiling a security strategy is to review existing polices

i). Distinguish between policies standards and procedure and provide one example in each case [4 marks]

ii). Distinguish between proactive and reactive strategies in security planning [4 marks]

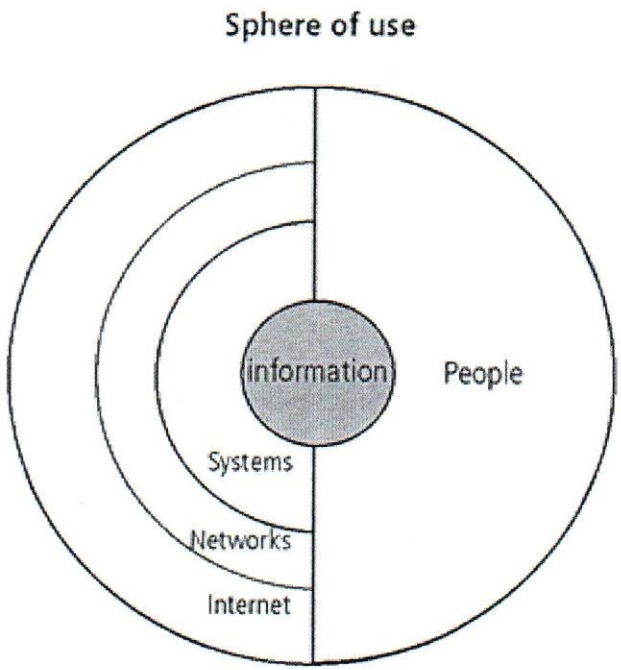
b)

i). Explain what a security model is [1 mark]

ii). Identify a security model that would be appropriate to implement an information integrity policy and explain how it works [4 marks]

iii). Identify a security model that would be appropriate to implement an information confidentiality policy and explain how it works [4 marks]

c) The diagram below illustrates the ways in which people can access information which is placed at the centre of the sphere of use.



i). Explain the connotation of this diagram with regard to access of information [3 marks]

ii). Generally speaking, the concept of the sphere as illustrated is to represent the 360 degrees of security necessary to protect information at all times. With aid of a diagram demonstrate the layers of security that overlay each of the layers of the sphere of use [7 marks]

d) Explain the meaning of the following terms with regard to design of secure systems.

i). Trusted computing base [2 marks]

ii). Reference monitor [2 marks]

e) Define the following system design and configuration principles and Explain how they promote security

i). Principle of least privileges [3 marks]

ii). Defense in depth [3 marks]

iii). Minimization principle [3 marks]

Section B (60 Marks) Answer Any THREE Questions

QUESTION TWO (20 MARKS)

a)

i). Identify and explain the constructs of the Clerk Wilson Security Model [6 marks]

ii). With aid of an appropriate example, explain the concept of well formed transaction as applied in clerk Wilson model [4 marks]

b) Consider the following confidentiality classification with the security levels from the most sensitive at the top and the least sensitive at the bottom and the associated categorization of users and documents grouped by their security clearances.

Confidentiality classification	***User categorization by security***	***Document categorization by***
TOP SECRET	Tamara	Personal Files
|	|	|
SECRET	Sally	Electronic Mail Files
|	|	|
CONFIDENTIAL	Claire	Activity Log Files
|	|	|
UNCLASSIFIED	Ursula	Telephone List Files

i). Sate the rule used by the confidentiality model to assign file read privileges to users. Hence state the read rights of Sally [2 marks]

ii). Explain the documents read privileges of Tamara and Claire assuming that the discretionary access control allows it. [2 marks]

iii). Supposing the star property rule (no writing down rule) does not apply and Tamara decides to write personal files content into the activity log files. Explain how this would affect secrecy assuming that discretionary access control is set appropriately. [2 marks]

iv). State the tranquility rule and explain its importance with respect to security [2 marks]

v). Explain one limitation of the confidentiality model [2 marks]

QUESTION THREE (20 MARKS)

a) The purpose of the security architecture blueprint is to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each domain. Explain the role of the following blue prints in security design and implementation

i) Stakeholders [2 marks]

ii) Risk management [2 marks]

iii) Policies and standards [2 marks]

iv) Security architecture [2 marks]

v) Assurance [2 marks]

b) Describe the *"Ring Model"* architecture of the x86 family of CPUs showing how it makes use of the layering concept to achieve security [3 marks]

c) Distinguish between a proxy server, a gateway and a packet filtering router hence illustrate the relative positioning of each with respect to LAN, ISP and the internet [7 marks]

QUESTION THREE (20 MARKS)

A company, example.org, has a webserver (ws.example.org) and several workers, each of which have a desktop computer. The company's network has the following hostnames and IP addresses:

Hostname	IP Address
router.example.org	192.168.223.1
ws.example.org	192.168.223.5
desktop1.example.org	192.168.223.8
desktop2.example.org	192.168.223.9

In the beginning, the company wanted to make sure that their webserver was accessible to potential customers over the Internet. To accomplish this, they purchased a leased line (or other permanent connection), put a router on their premises, and then hooked their webserver up to the Internet. Then their problems started. The first thing they noticed was that their webserver received lots of traffic, but much of that traffic was not to the web server process itself. They also noticed slowdowns on their server, and they found processes running on it that the System Administrators

were not familiar with. Furthermore, they noticed that their desktop systems suddenly got slower and started behaving erratically.

a) Explain the probable course of this problem [6 marks]

b) The System Administrators were not happy with the situation, though: while the only system that needed to be accessible to the Internet was the web server, internal systems were also visible to the Internet. They needed to somehow stop that access. After some searching, they found some layer 3 and layer 4 firewall products to solve their problems

   i) Identify an appropriate layer 3 firewall that the System admin may use and explain how it can be used to protect the internal systems (i.e., the desktop systems) [4 marks]

   ii) Explain how the layer 4 firewall would help the system administrator to do port filtering. Hence state to rule sets that the system administrator would set to restrict network traffic to just the web server [4 marks]

c) The users then called with a request: since the company's web server was such a vital resource, the users thought they should use the Internet, too. After all, they needed to find product information from other companies, and by looking on the Internet, they were able to research others' products faster. The system administrators discussed the problem, and determined that a safe firewall rule would allow the internal desktops to talk to a web server on the Internet, but not allow any other traffic. Thus, they came up with a set of rules like this:

   - allow desktop*.example.org to send to anyone on destination port 80
   - allow anyone to send to desktop*.example.org, but only if the source port is port 80

This almost worked, but there is one problem: An attacker can simply use port 80 as the source port and now scan the network.

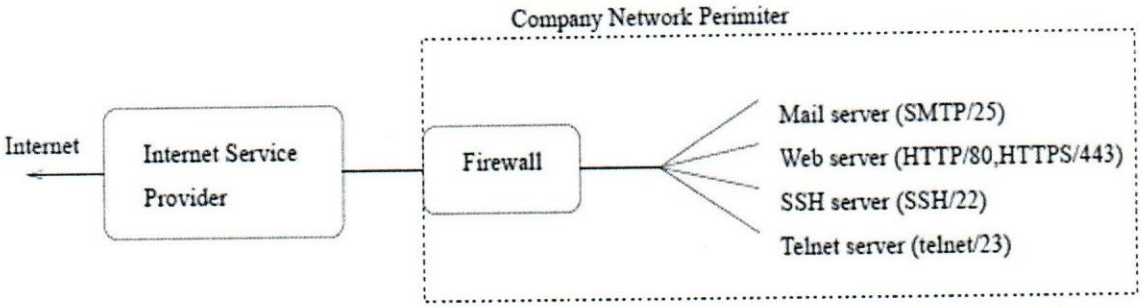
Explain how the TCP 3 way handshake may be used to address this problem?

Other than the TCP 3 way handshake solution state two other firewalls that can used to address this problem? [2 marks]

QUESTION FOUR (20 MARKS)

a) Suppose you are employed as an IT security officer in an organization and your first assignment is to evaluate the potential risk to IT facilities facility from threats. With aid of a risk matrix diagram explain how you would use a combination of the impact of loss rating and the vulnerability to threat to determine risk rating and prioritize countermeasures [5 marks]

b) The following diagram shows the architecture for your company's network and connection to the internet.



IP addresses:

ISP router	2.2.2.1
Mail server	1.2.3.5
Web server	1.2.3.4
SSH server	1.2.3.3
Telnet server	1.2.3.2

Example rules:

```
allow * *:*/in -> *:*/out
drop * *:* -> *:*
```

Your company is installing a packet filter firewall. Here is the proposed security policy for the firewall:

1. By default, block all inbound connections.
2. Allow all inbound TCP connections to SMTP on mail server.
3. Allow all inbound TCP connections to HTTP and HTTPS on web server.
4. Allow all inbound TCP connections to SSH on SSH server.
5. Allow all outbound connections.
6. Telnet access should not be allowed (because it sends passwords in cleartext).

i). Using the syntax from examples above, write the firewall ruleset for your company's firewall. For each rule, give a brief description of its purpose. [12 marks]

ii). Hackers target your company's network with repeated requests for large images on your company's webserver. The hackers' machines are on the 20.1.21.x subnet. How could you change your firewall ruleset to block these attacks? [3 marks]

c) We have an internal web server, used only for testing purposes, at IP address 5.6.7.8 on our internal corporate network. The packet filter is situated at a chokepoint between our internal network and the rest of the Internet. Can such a packet filter block all attempts by outside hosts to initiate a direct TCP connection to this internal web server? If yes, show a packet filtering rule set that provides this functionality; if no, explain why a (stateless) packet filter cannot do it. [3 marks]

d) Can a packet filter block all incoming email containing the phrase *"Make money fast"*? If yes, show a packet filtering rule set that provides this functionality; if no, explain why a (stateless) packet filter cannot do it. [2 marks]

QUESTION FOUR (20 MARKS)

ACME is an insurance and investment company that grew from a mainframe-only shop ten years ago to now integrating a client-server model. The integration of other architectural components like data, application, and infrastructure came after expanding and integrating different applications and systems in the client-server environment. Security was not an integral component from an architectural perspective. As such, many security components were either missing or lacking in security design and implementation, such as IDS, DMZ, VPN implementation, web architecture, system builds, patch management, hardware and software directions, data classifications, encryption policy and standards, firewalls design, operating systems security, etc.

a) Explain the roles of the following in network security

i). IDS [3 marks]

ii). DMZ [3 marks]

iii). VPN [3 marks]

b) Explain how the firewall limits the functionality of the IDS [4 marks]

c) You are asked to configure a DMZ in your company network with the web server as the gateway or the front door to the company network. Explain how you will do this [3 marks]

d)

i). What is a Security perimeter [1 marks]

ii). Usually user password or password file is essential to intruder describe TWO methods you can use to protect password file. [3 marks]

QUESTION FIVE (20 MARKS)

a) Crosscutting concerns are the features of an architectural design that may apply across all layers, components, and tiers. These are also the areas in which high-impact design mistakes are most often made. Identify SEVEN of these features. [7 Marks]

b) With aid of a diagram demonstrate the key security design decisions that you would document as part of a web application architecture [13 marks]

Question Six (20 marks)

You have been approached by company Z to analyze their network architecture and overall security posture. Company Z is involved with real estate and new business development in a mid-sized metropolitan area and consists of approximately 105 employees. Their line of work requires personnel to obtain, store, and process sensitive financial documents, such as bank loans and customer's credit history reports, as well as legal documentation, covering for example, property deeds and zoning ordinances. To facilitate these objectives, efficient and effective communication across boundaries is paramount. Company Z must have the ability to exchange information with a diverse array of stakeholders ranging from employees and clients, to banks and law firms, both locally and globally based. The IS Manager expressed to you that because of the nature of their business they were beginning to rely on electronic communications more and more. He mentioned that features such as e-mail and voice over IP (Internet Protocol) had significantly reduced their shipping, faxing, and phone costs and that overall; management was pleased with efficiencies gained in lower bidding and negotiation processes. As their reliance on electronic communication increased, Company Z's GroupWise email system quickly became an integral component of their daily business transactions. The IS Manager was concerned that as the company further entrusted their sensitive communications to technology, improvements in efficiency may come at the expense of increased network security risks. Specifically, he expressed a strong interest in preserving system availability and placed a great deal of emphasis on their GroupWise email system. He mentioned that a Denial of Service attack was a legitimate concern and that Company Z recently granted users Internet access in the absence of any type of acceptable use policy. In addition, he stated that of the few security policies they had managed to develop over the years, most were never effectively implemented much less enforced. This further served to legitimize the IS Manager's concerns over potential threats and vulnerabilities from outside the network and served as good fodder when considering the company's security posture.

The IS Manager asked you to conduct a low cost risk assessment that would assess their overall security posture by identifying gaps in their current network architecture. Your are advised to use the Survivable Systems Analysis (SSA) method for the task.

a) Explain the tenet of survivable systems and describe how you would use this tenet to focus your assessment [3 marks]

b) Describe the THREE primary capabilities that would help to achieve the objectives of system survivability and for each capability state relevant technologies, techniques or tools that you would advice company Z to use. [7 marks]

c) Outline the FOUR steps of the SSA method and for each explain what you would do and what the likely deliverables are while assessing the overall security posture of company Z. [10 marks]