COMPUTER NETWORK SECURITY

EXAMINATION MARKING SCHEME

INSTRUCTIONS:

Attempt QUESTION ONE and any other TWO questions

QUESTION ONE (COMPULSORY) (30 MARKS)

a. List three types of data confidentiality. (3 marks)
Connection Confidentiality — The protection of all user data on a connection.
• **Connectionless Confidentiality** — The protection of all user data in as single data block.
• **Selective-Field Confidentiality** — The confidentiality of selected fields within the user data on a connection or in a single data block.
• **Traffic-Flow Confidentiality** — The protection of the information that might be derived from observation of traffic flows.

b. Describe the term operational control and cite an example. (3 marks)
Operational Controls:
Focus on controls that are implemented and executed by people e.g.: training, education, user administration, software support, documentation etc.

c. Name three types of infosec policies that need to be made in order to produce a full infosec policy. (3 marks)
- Enterprise infosec program policy
- Issue-specific infosec policies
- Systems-specific infosec policies

d. Briefly describe the term cryptography. Hence list two cryptographic hash algorithms. (3 marks)
The art of secret writing. There are several common cryptographic hash algorithms, including MD5 (for Message Digest 5) and Secure Hash Algorithm 1 (SHA-1).

e. Describe the digital signature verification process. (3 marks)
Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

f. Suppose you discover that an intruder has warez in an FTP area that you are aware of. Describe three actions that you can take to discover the identity of the attacker as a forensics expert. (3 marks)
If they leave warez or tools in FTP area
- Log who retrieves them
- Replace warez with files of white noise
- Contact site admins at sites downloading the software

g. List three pros of a reasonably effective intrusion detection system. (3 marks)
- A reasonably effective IDS can identify
  - Internal hacking
  - External hacking attempts
- Allows the system administrator to quantify the level of attack the site is under
- May act as a backstop if a firewall or other security measures fail

h. Briefly describe three limitations of firewalls. (3 marks)

- cannot protect against attacks bypassing firewall
- may not protect fully against internal threats
- improperly secure wireless LAN
- laptop, PDA, portable storage device infected outside then used inside

i. Describe what a VPN protects over a public network. (3 marks)

A VPN carries private traffic over a public network using advanced encryption and tunnels to protect:
- Confidentiality of information
- Integrity of data
- Authentication of users

j. Describe (NOT list) any three ethical issues of the information age. (3 marks)
- Privacy - right of individual to control personal information
- Accuracy – who is responsible for the authenticity, fidelity, and accuracy of information?
- Property – Who owns the information? Who controls access? (e.g. buying the IP verses access to the IP)
- Accessibility – what information does an organization have the right to collect? Under what safeguards?
- Etc

QUESTION TWO (20 MARKS)

a. Describe the relationship between policies, standards, practices, guidelines and procedures. (5 marks)

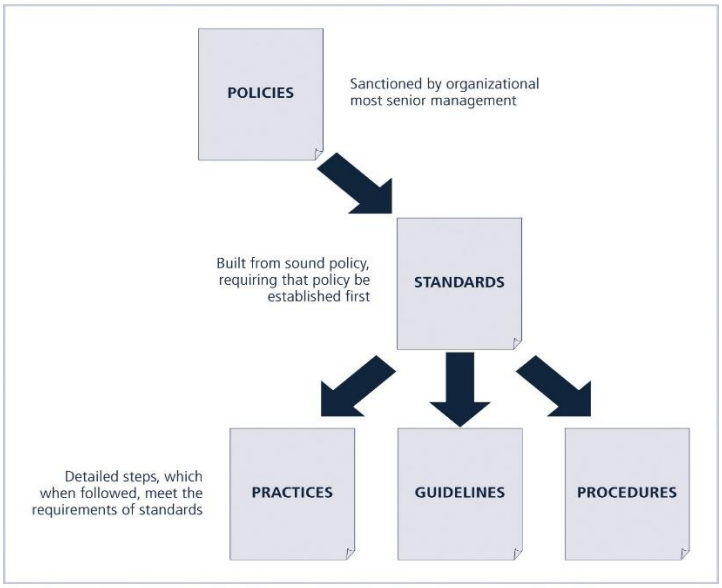

FIGURE 4-2 Policies, Standards, and Practices

b. You have been recently contracted by Bazuzu Logistics Inc management to look into the usage of ICT in their organization. The organization has five departments namely HR, finance, logistics, security and management. The management are concerned about privacy and wastage of resources in the organization. The organization has invested heavily in an expensive color line printer, a black and white printer, an internet server, a color line heavy duty printer, desktop devices in every department, and UPS as well as intelligent switches. Staff have been using the color line printers to print their work including documents of a personal nature. Further an

examination of the materials that are being downloaded from the Internet clearly indicates most of it is not work related. Management would like the color line printer for their own exclusive use, and the heavy duty line printer to be used for printing only documents that require color printing (and preferably company related work only). The logistics staff should have exclusive use of the heavy duty black and white printer after 4 pm as this is when they require to print materials for the transport officers to distribute to the drivers on dispatch. The finance department should also have priority printing enabled for them on all printers due to invoicing clients. The management would not like to block the Internet entirely but would like staff to practice fair usage when it comes to personal stuff. Lastly management would like the servers to log all printing being done and also require special permission for anyone to use the printing and internet services after 7 pm; they would like a report of who has accessed what after 7 pm. This report should be sent to the CEO Ms Muteti every Monday at 8 am.

i. What kind(s) of policies would you require to enforce the above requirements? (2 marks)
Require both ISSP and SySP.

ii. How many policies do you require to develop to fulfill the requirements? (3 marks)
Usage of internet (ISSP), usage of printers (SySP)

iii. Hence write down the relevant policies, and include the standards as well the steps that will fulfill the standards. (10 marks)
Give the name of the policy and what it will do; who will implement it.
How the policy will be implemented (standards and procedures)

QUESTION THREE (20 MARKS)

a. Describe the difference between a session key and pre-distribution key. (5 marks)
A session key is a key used to secure a single, relatively short episode of communication: a session. Each distinct session between a pair of participants uses a new session key, which is always a symmetric-key key for speed. In Pre-Distribution of Public Keys the algorithms to generate a matched pair of public and private keys are publicly known, and software that does it is widely available.

b. You have been invited as a security expert by Ngumi Moja Consultants to test their encryption software. They would like to know how easy/hard it is for a hacker to intercept a message from their system to one of their clients and decipher it. Cool. You get to work and the first message you intercept reads as follows:
OFM XRNX ILUVYNOCSKLZ YELXLXANRDD JYAL CVKLUBA.
You examine the cipher and based on your knowledge of breaking ciphers you can guess this is either a Caesar or Captain Midnight cipher or at least variant. You show the consultants that you can break the cipher by actually going ahead to do it. Write down what the cipher is in the format X →Y and send the following reply using the same cipher code: THE CIPHER CODE CAN BE IMPROVED. (15 marks)
X →Y (n = 10, 9, 8, 7, ..)

QUESTION FOUR (20 MARKS)

a. List four disadvantages of VPNs. (4 marks)
- The availability and performances of VPN networks are difficult to control
- VPN speeds are much slower than those experienced with a traditional connection
- VPN technologies from different creators may work poorly together. With time, this may improve. For now, however, this can cause frustration when implementing a VPN.

- One of the VPN's weakest links→ its users.

b. You are part of a team that is sub-contractor for VPN solutions. Most of the time you weigh between developing a VPN solution in-house for a client or have the client outsource the solution (which of course only gets you a small 'finder fee' for your team). Your most recent prospect is Summertime Investments a company that receives funds and instructions for investments from their clients in the diaspora. They are of the opinion that they should outsource the VPN service despite the fact that they have a state of the art server and communication equipment. Discuss at least four things they should consider before outsourcing. Finally recommend whether they should outsource or not, justifying your recommendation. (12 marks)
   Things to consider before outsourcing -
   - For connecting remote offices consider an ISP that also offers POP to connect to Internet as a local call
   - Redundancy of equipment, connections, and people
   - Provider policies, equipment, employee qualification to deal with outside hackers and viruses
   - On-site consulting assistance

c. Describe four steps you would undertake to protect your system and its data should you suspect you are under attack. (4 marks)
   - Complete system backup
   - Get a system with tcpdump running a complete packet log to disk
   - Sync the disks, and halt the system
   - Bring system back up to single user mode