COMPUTER NETWORK SECURITY

ASSIGNMENT MARKING SCHEME

INSTRUCTIONS:

Attempt ALL Questions

Question One (30 marks)

a. Define the following terminologies:
   i. Security attack. (1 mark)
   ii. Security service. (1 mark)
   iii. Security mechanism. (1 mark)
   - ✓ Security Attack: Any action that compromises the security of information exchanges and systems.
   - ✓ Security Service: A service that enhances the security of information exchanges and systems. A security service makes use of one or more security mechanisms.
   - ✓ Security Mechanism*: A mechanism that is designed to detect, prevent or recover from a security attack.

b. Differentiate between white hat hackers, grey hat hackers, and black hat hackers by describing them. (3 marks)
   - ✓ *Black hat (crackers) hackers*: for malicious reasons such as vandalism, credit card fraud, identity theft, piracy, or other types of illegal activity
   - ✓ *White hat hackers*: for non-malicious reasons, for instance testing their own security system
   - ✓ *Grey hat hackers*: combination of a Black Hat and a White Hat Hacker (repair the system for a small fee)

c. List three basic rules to follow when shaping policy. (3 marks)
   - ✓ Never conflict with law
   - ✓ Stand up in court
   - ✓ Properly supported and administered
   - ✓ Contribute to the success of the organization
   - ✓ Involve end users of information systems

d. Briefly describe the three degrees of freedom provided by IPSec. (3 marks)
   - ✓ First, it is highly modular, allowing users (or more likely, system administrators) to select from a variety of cryptographic algorithms and specialized security protocols.
   - ✓ Second, IPsec allows users to select from a large menu of security properties, including access control, integrity, authentication, originality, and confidentiality.
   - ✓ Third, IPsec can be used to protect "narrow" streams (e.g., packets belonging to a particular TCP connection being sent between a pair of hosts) or "wide" streams (e.g., all packets flowing between a pair of routers).

e. Describe two common reasons for applying a digital signature to communications. (4 marks)
   - ✓ Authentication

     Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures

can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

- ✓ Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

f. Describe three recommended courses of action to undertake should you discover your system is under attack. (3 marks)
   - ✓ *Do a complete system backup immediately*
   - ✓ 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

g. List three pros of a reasonably effective intrusion detection system. (3 marks)
   - ✓ A reasonably effective IDS can identify internal hacking and 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. List three critical functions provided by Virtual Private Networks. (3 marks)
   - ✓ **Confidentiality (encryption)** – The sender can encrypt the packets before transmitting them across a network.
   - ✓ **Data integrity** – The receiver can verify that the data was transmitted through the Internet without being altered.
   - ✓ **Origin authentication** – The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information

i. 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

j. Briefly explain rule-based ethics. (2 marks)
   - ✓Priority is given to following the rules without undue regard to the outcome
   - ✓Rules are often thought to codify principles like truth fulness, right to freedom, justice, etc.

- ✓Stress fidelity to a sense of duty and principle ("never tell a lie")
- ✓Exist for the benefit of society and should be followed

Question Two (20 marks)

a. List and describe the roles of the supporting organizations of computer security. (8 marks)
   - ✓Audit – Auditors are responsible for examining systems whether the system is meeting stated security requirements.
   - ✓Quality assurance – Responsible for improving the products and services, how computer security can be used to improve the quality.
   - ✓Training office – Responsible for training users, operators, managers in computer security.
   - ✓Risk Management – Responsible for studying all types of risks including computer security-related risks.

b. Describe the major controls of computer security, citing an example in each instance. (12 marks)
   - ✓ *Management Controls:*

     Focus on controls that can be characterized as managerial.

     e.g.: management of computer security program, management of risk within the organization, management of assurance etc.
   - ✓ *Operational Controls:*

     Focus on controls that are implemented and executed by people

     e.g.: training, education, user administration, software support, documentation etc.

     Often require technical or specialized expertise and rely upon management activities as well as technical controls
   - ✓ *Technical Controls:*

     Focus on security controls that the computer system executes.

     e.g.: identification, access control, other cryptographic technologies

Question Three (20 marks)

a. Define the following terminologies:
   i. Policy
   ii. Standard
   iii. Practices, procedures and guidelines

b. Hence, using a diagram and appropriate explanations describe how the above terminologies relate to each other. (5 marks)

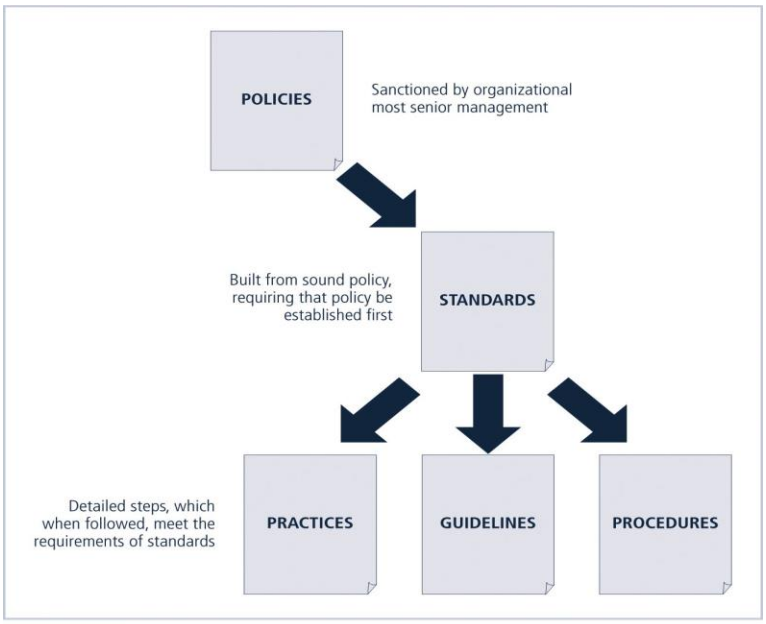

FIGURE 4-2 Policies, Standards, and Practices

c. Describe how the following systems work, paying attention to the dimensions of security each provides and any special features/capabilities of each:

i. Pretty Good Privacy (PGP). (4 marks)
ii. IPSec. (4 marks)
iii. Secure Shell. (4 marks)

- Pretty Good Privacy (PGP)

✓ Pretty Good Privacy (PGP) is a widely used approach to providing security for electronic mail. It provides authentication, confidentiality, data integrity, and nonrepudiation.
✓ Originally devised by Phil Zimmerman, it has evolved into an IETF standard known as OpenPGP
✓ PGP's confidentiality and receiver authentication depend on the receiver of an email message having a public key that is known to the sender.
✓ To provide sender authentication and nonrepudiation, the sender must have a public key that is known by the receiver.
✓ These public keys are pre-distributed using certificates and a web-of-trust PKI.
✓ PGP supports RSA and DSS for public key certificates.

- Secure Shell (SSH)

✓ The Secure Shell (SSH) protocol is used to provide a remote login service, and is intended to replace the less-secure Telnet and rlogin programs used in the early days of the Internet.
✓ SSH is most often used to provide strong client/server authentication/ message integrity—where the SSH client runs on the user's desktop machine and the SSH server runs on some remote machine that the user wants to log into—but it also supports confidentiality.
✓ Telnet and rlogin provide none of these capabilities.

- ✓ Note that "SSH" is often used to refer to both the SSH protocol and applications that use it; you need to figure out which from the context.

- IP Security (IPSec)

- ✓ Support for IPsec, as the architecture is called, is optional in IPv4 but mandatory in IPv6.
- ✓ IPsec is really a framework (as opposed to a single protocol or system) for providing all the security services discussed throughout this chapter.
- ✓ IPsec provides three degrees of freedom.
  - First, it is highly modular, allowing users (or more likely, system administrators) to select from a variety of cryptographic algorithms and specialized security protocols.
  - Second, IPsec allows users to select from a large menu of security properties, including access control, integrity, authentication, originality, and confidentiality.
  - Third, IPsec can be used to protect "narrow" streams (e.g., packets belonging to a particular TCP connection being sent between a pair of hosts) or "wide" streams (e.g., all packets flowing between a pair of routers).

Question Four (20 marks)

a. Describe three types of cryptography. (12 marks)

✓Public Key

- Two keys: public & private

✓Symmetric Key (aka "Secret Key")

- One key: secret (but possibly shared)

✓Hash Functions

- No keys

(4 marks each, with explanations and/or explanatory diagrams)

b. Describe two types of firewalls. (8 marks)