TED (10)-4079/5059 Reg. No...........................

(REVISION-2010) Signature.........................

MODEL EXAMINATION IN ENGINEERING/TECHNOLOGY

INFORMATION SECURITY

[*Time:* 3 hours

(Maximum marks: 100)

Marks

PART –A

I Answer the following questions in one or two sentences. Each question carries 2 marks

1. **Differentiate attack and threat.**

   Attack:

   An Action taken to harm an asset.

   Threat:

   A potential occurrence-malicious or otherwise-that may harm an asset

2. **State two methods of user authentication**

   Identification step: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

   Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier."

3. **Describe hackers**

   A hacker is someone who seeks and exploits weakness in a computer system or computer network.

   Hackers may be motivated by a multitude of reasons, such as profit, protest,challenge or enjoyment

4. **Outline spoofing**

   A common characteristics of packets used in many types of DoS attacks is the use of forged source addresses

5. **State two services of firewalls.**

Serve as an entry point into a network

Screens all packets entering the network

PART—B

II Answer *any five* of the following. Each question carries 6 marks.

1. **Differentiate passive attacks and Active attacks in network security**

Active Attack:

- The Attacker needs to gain physical control of a portion of the link and be able to insert and capture transmissions
- Medium could be telephone twisted pair, coaxial cable, or fiber optics

Passive attack:

- The attacker merely needs to be able to observe transmissions
- May be inductive taps**.**

2. **Summarize the requirements of hash functions**

- applied to any size data
- H produces a fixed-length output.
- H(*x*) is relatively easy to compute for any given *x*
- one-way property
  - computationally infeasible to find *x* such that H(*x*) = *h*
- weak collision resistance
  - computationally infeasible to find *y* ≠ *x* such that H(*y*) = H(*x*)
- strong collision resistance
  - computationally infeasible to find any pair (*x*, *y*) such that H(*x*) = H(*y*)

3. **Describe rainbow table and approaches for password cracking**

rainbow table attacks

precompute tables of hash values for all salts

a mammoth table of hash values

e.g. 1.4GB table cracks 99.9% of alphanumeric Windows passwords in 13.8 secs

not feasible if larger salt values used

Approaches:

Dictionary attacks

Rainbow table attacks

4. **Summarize the different access control policies.**

• **Discretionary access control (DAC):** based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. This policy is termed *discretionary* because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

• **Mandatory access control (MAC):** based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed *mandatory* because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource. See chapter 10.

• **Role-based access control (RBAC):** based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

5. **Classify the types of intruders**

Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access control to exploit a legitimate user's account
Misfeasor:A legitimate user who access data,programs, or resources for which such access is not authorized, or who is authorized for such access
Clandestine user: An individual who seizes supervisory control of the system and use this control to evade auditing and access control

6. **Describe the parts of virus**

• Infection mechanism:The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the infection vector.
• Trigger: event or condition determining when the payload is activated or delivered.
• Payload: What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.
A virus can be prepended or postpended to an executable program, or it can be embedded in some other fashion. The key to its operation is that the infected program, when invoked, will first execute the virus code and then execute the original code of the program.

Once a virus has gained entry to a system by infecting a single program, it is in a position to infect some or all other executable files on that system when the infected program executes

7. **Summarize reflection attacks.**

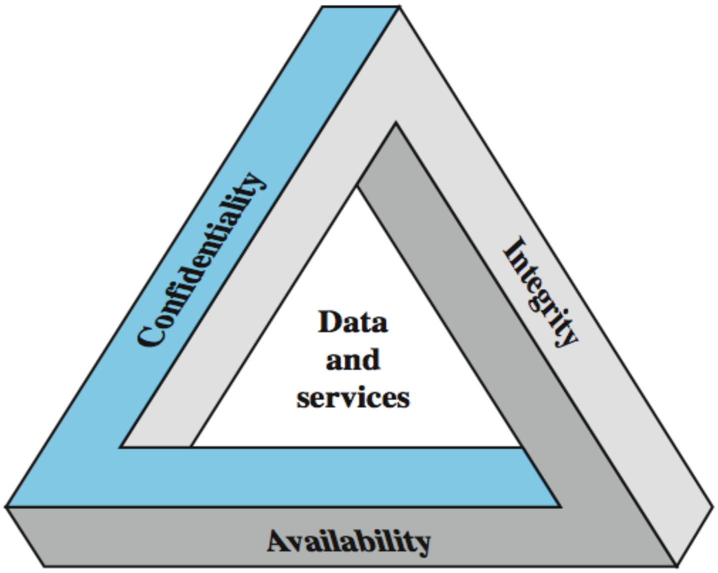
Reflection and amplification attacks use network systems functioning normally. The attacker sends a network packet with a spoofed source address to a service running on some network server, which responds to this packet, sending it to the spoofed source address that belongs to the actual attack target. If the attacker sends a number of requests to a number of servers, all with the same spoofed source address, the resulting flood of responses can overwhelm the target's network link. The fact that normal server systems are being used as intermediaries, and that their handling of the packets is entirely conventional, means these attacks can be easier to deploy, and harder to trace back to the actual attacker.

PART—C

(Answer one full question from each unit. Each question carries 15 marks.)

UNIT--I

III (a) Describe the security requirements triad **6**



• Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
• Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
• Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:
• Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. • Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

(b) Summarize the aspects for comprehensive security strategy **9**

- An overall strategy for providing security
  - Policy (specs): what security schemes are supposed to do
    - Assets and their values
    - Potential threats
    - Ease of use vs security
    - Cost of security vs cost of failure/recovery
  - Implementation/mechanism: how to enforce
    - Prevention
    - Detection
    - Response
    - Recovery
  - Correctness/assurance: does it really work (validation/review)

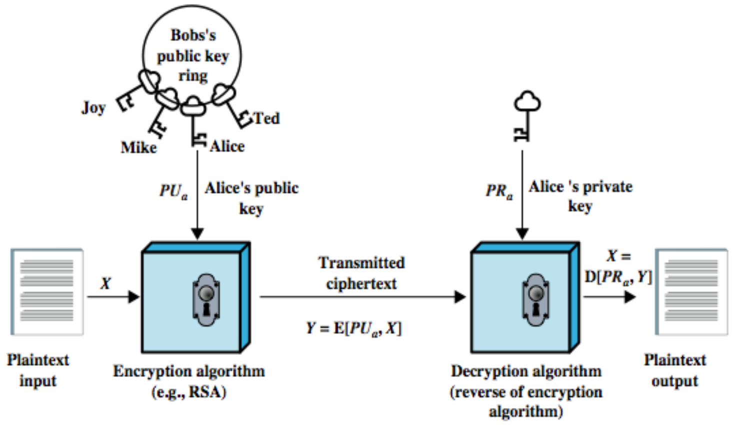
OR

IV (a) Illustrate one way hash function **7**

If strong collision resistance is required (and this is desirable for a general-purpose secure hash code), then the value $2^{n/2}$ determines the strength of the hash code against brute-force attacks. Oorschot and Wiener presented a design for a $10 million collision search machine for MD5, which has a 128-bit hash length, that could find a collision in 24 days. Thus a 128-bit code may be viewed as inadequate. With a hash length of 160 bits, the same search machine would require over four thousand years to find a collision. With today's technology, the time would be much shorter, so that 160 bits now appears suspect.

- When weaknesses were discovered in SHA, a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new versions of SHA, with hash value lengths of 256, 384, and 512 bits, known as SHA-256, SHA-384, and SHA-512. These new versions have the same underlying structure and use the same types of modular arithmetic and logical binary operations as SHA-1. In 2005, NIST announced the intention to phase out approval of SHA-1 and move to a reliance on the other SHA versions by 2010.

(b) Describe the public key encryption scheme **8**



(a) Confidentiality

A public-key encryption scheme has six ingredients

- Plaintext: the readable message or data that is fed into the algorithm as input.
- Encryption algorithm: performs various transformations on the plaintext.
- Public and private key: a pair of keys selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input.
- Ciphertext: the scrambled message produced as output that depends on the plaintext and key. For a given message, two different keys produce two different ciphertexts.
- Decryption algorithm: takes ciphertext and key to produces the original plaintext.

As the names suggest, the public key of the pair is made public for others to use, while the private key is known only to its owner. A public-key cryptographic algorithm relies on one key for encryption and a different but related key for decryption. All participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user protects his or her private key, incoming communication is secure.

UNIT II

V (a) Summarize the demerits of memory cards. **4**

Requires special reader: This increases the cost of using the token and creates the requirement to maintain the security of the reader's hardware and software.

- Token loss: A lost token temporarily prevents its owner from gaining system access. Thus there is an administrative cost in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary now need only determine the PIN to gain unauthorized access.
- User dissatisfaction: Although users may have no difficulty in accepting the use of a memory card for ATM access, its use for computer access may be deemed inconvenient

(b) Describe different types of physical characteristics in biometrics **11**

A biometric authentication system attempts to authenticate an individual based on unique physical characteristics.These include static characteristics, such as fingerprints, hand geometry, facial characteristics, and retinal and iris patterns; and dynamic characteristics, such as voiceprint and signature. Compared to passwords and tokens, biometric authentication is both technically complex and expensive, and have yet to mature as a standard tool for user authentication to computer systems

- Facial characteristics: define characteristics based on relative location and shape of key facial features, such as eyes, eyebrows, nose, lips, and chin shape.
- Fingerprints: the pattern of ridges and furrows on the surface of the fingertip, believed to be unique across the entire human population. Automated fingerprint systems extract a number of features to use as a surrogate for the full pattern.
- Hand geometry: identify features of hand,: e.g. shape, lengths & widths of fingers.
- Retinal pattern: formed by veins beneath the retinal surface is unique and therefore suitable for identification. Uses a digital image of the retinal pattern by projecting a low-intensity beam of visual or infrared light into the eye.
- Iris: Another unique physical characteristic is the detailed structure of the iris.

• Signature: each individual has a unique style of handwriting, esp in signature.
• Voice: patterns are more closely tied to physical and anatomical characteristics of the speaker, but still have a variation from sample to sample **over time from the same speaker,complicating the biometric recognition task.**

OR

VI (a) Summarize the user authentication attacks. **9**

Client attacks are those in which an adversary attempts to achieve user authentication without access to the remote host or to the intervening communications path. The adversary attempts to masquerade as a legitimate user. e.g. in a password-based system, the adversary may attempt to guess the likely user password.

Host attacks are directed at the user file at the host where passwords,token passcodes, or biometric templates are stored.

Eavesdropping refers to an adversary's attempt to learn the password by observing the user, finding a written copy of the password, keystroke logging, etc.

Replay attacks involve an adversary repeating a previously captured user response. The most common countermeasure to such attacks is the challenge-response protocol.

In a **Trojan horse attack**, an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric. The adversary can then use the captured information to masquerade as a legitimate user.

A **denial-of-service** attack attempts to disable a user authentication service by flooding the service with numerous authentication attempts.

(b) Describe the different access rights. **6**

An access right describes the way in which a subject may access an object. Access rights could include the following: read, write, execute, delete, create, search

- Read: user may view information in a system resource
- Write:User may add, modify, or delete data in a system.
- Execute: User may execute Specified programs.

- Delete:user may delete certain system resources.
- Craete: user may create new files, records
- Search: user may list the files in a directory

UNIT III

VII (a) List examples of intrusion **7**

Performing a remote root compromise of an e-mail server
• Defacing a Web server
• Guessing and cracking passwords
• Copying a database containing credit card numbers
• Viewing sensitive data, including payroll records and medical information, without authorization
• Running a packet sniffer on a workstation to capture usernames and passwords
• Using a permission error on an anonymous FTP server to distribute pirated software and music files
• Dialing into an unsecured modem and gaining internal network access
• Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
• Using an unattended, logged-in workstation without permission

(b) Describe the methods of signature detection **8**

Signature techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. In very general terms, we can characterize all approaches as focusing on either anomaly detection or penetration identification, although there is some overlap in these approaches.
Rule-based anomaly detection is similar in terms of its approach and strengths to statistical anomaly detection. With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.
Rule-based penetration identification takes a very different approach to intrusion detection. The key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known

weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. The most fruitful approach to developing such rules is to analyze attack tools and scripts collected on the Internet. These rules can be supplemented with rules generated by knowledgeable security personnel. In this latter case, the normal procedure is to interview system administrators and security analysts to collect a suite of known penetration scenarios and key events that threaten the security of the target system.

OR

VIII(a) State (i) Virus $(\mathbf{4}\times \mathbf{2} = \mathbf{8})$

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. A virus can do anything that other programs do. The difference is that a virus attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs. Most viruses carry out their work in a manner that is specific to a particular operating system and, in some cases, specific to a particular hardware platform. Thus, they are designed to take advantage of the details and weaknesses of particular systems

(ii) Backdoor

A backdoor in a computer system is a method of bye passing normal authentication. securing unauthorized remote access to a computer obtaining access to plaintext**.**

(iii) Flooders and

Is an individual who make to access the system resources without the permissions of the administrator by overloading the path

(iv) Adware

Adware or advertising-supported software, is any software which automatically renders advertisements in order to generate revenue for its author

(b) Differentiate Bots and Rootkits **7**

- **A bot (robot),** also known as a zombie or drone, is a program that secretly takes over hundreds or thousands of Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the bot's creator. The collection of bots often is capable of acting in a coordinated manner; referred to as a botnet. A botnet exhibits three characteristics: the bot functionality, a remote control facility, and a spreading mechanism to propagate the bots and construct the botnet. Some uses of bots include: distributed denial-of-service attacks, spamming, sniffing traffic, keylogging, spreading new malware, installing advertisement add-ons and browser helper objects (bhos), attacking irc chat networks, manipulating online polls/games.

The remote control facility is what distinguishes a bot from a worm

- A **rootkit** is a set of programs installed on a system to maintain administrator (or root) access to all the functions and services of the operating system. The rootkit alters the host's standard functionality in a malicious and stealthy way. A rootkit can make many changes to a system to hide its existence, making it difficult for the user to determine that the rootkit is present and to identify what changes have been made. Done by subverting the mechanisms that report on processes, files, and registries

UNIT IV

IX (a) Describe different flooding attacks **8**

Flooding attacks take a variety of forms, based on which network protocol is being used to implement the attack. Common flooding attacks use any of the ICMP, UDP or TCP SYN packet types.

- An ICMP flooding attack uses an ICMP packet, such as ICMP echo request packets in a ping flood. This type of ICMP packet was chosen since traditionally network administrators allowed such packets into their networks. More recently, many organizations have restricted the ability of these packets to pass through their firewalls. In response, attackers have started using other ICMP packet types. Since some of these should be handled to allow the correct operation of TCP/IP, they are much more likely to be allowed through an organization’s firewall.
- An alternative to using ICMP packets is to use UDP packets directed to some port number, and hence potential service, on the target system. Spoofed source addresses are normally used if the attack is generated using a single source system, for the same reasons as with ICMP attacks.
- Another alternative is to send TCP packets to the target system. Most likely these would be normal TCP connection requests, with either real or spoofed source addresses. In this case, it is the total volume of packets that is the aim of the attack, rather than specifically targeting

the system code. This is the difference between a SYN spoofing attack and a SYN flooding attack.

(b) Describe the counter measures of DDoS attacks **7**

A critical component of many denial of service attacks, is the use of spoofed source addresses. One of the fundamental, and longest standing, recommendations for defense against these attacks is to limit the ability of systems to send packets with spoofed source addresses, cf. RFC 2827. This filtering needs to be done as close to the source as possible, by routers or gateways knowing the valid address ranges of incoming packets.

. The filters must be applied to traffic before it leaves the ISP's network, or even at the point of entry to their network. Some attacks using particular packet types, such as ICMP floods, or UDP floods to diagnostic services, can be throttled by imposing limits on the rate at which these packets will be accepted.

It is possible to specifically defend against the SYN spoofing attack by using a modified version of the TCP connection handling code. Instead of saving the connection details on the server, critical information about the requested connection is cryptographically encoded in a "cookie" that is sent as the server's initial sequence number an entry for an incomplete connection from the TCP connections table when it overflows, allowing a new connection attempt to proceed.

OR

X (a) Summarize the security policies of firewall **8**

The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet: source IP address, destination IP address, source and destination transport-level address (port number), IP protocol field, interface (on firewall packet came from or is destined for). One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast.

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

The default discard policy is more conservative. Initially, everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. The default forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known.

(b) Illustrate application proxy firewall **7**

- Examines packets and their contents at the Application Layer
- Can cause delay due to additional processing
- May strip info on internal servers, server version on outgoing messages (e.g., email)
- May allow only certain types of sessions through:
    - FTP: May permit receives, no sends. Or sends of specific files only.
    - Email: Encrypts email between all of company's offices
    - HTTP: May filter PUT commands, URL names. Can cache replies.
- Authentication: Perform extra authentication for external access (via dialup or internet)