TED (10)-4079/5059 Reg. No………………………

(REVISION-2010) Signature……………………

FIFTH/SIXTH SEMESTER DIPLOMA EXAMINATION IN ENGINEERING/ TECHNOLOGY-OCTOBER,2013

INFORMATION SECURITY

(For Vth semester CT and for VIth semester CM and IF)

[*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. **State a method to prevent brute-force attack.**

   One common method to prevent brute force attacks are called captchas.these are an additional question-response that a log in attempt must satisfy in order to send the login request to all
2. **Describe 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.
3. **Describe masquerader**

   An Individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
4. **What is source address spoofing?**

   A common characteristic of packets used in many types of denial of service attacks, is the use of forged source addresses. This is known as source address spoofing.
5. **Describe amplification attack.**

   Amplification attacks are a variant of reflector attacks, that differ in generating multiple response packets for each original packet sent. This can be achieved by directing the original request to the broadcast address for some network. As a result, all hosts on that network can potentially respond to the request, generating a flood of responses

PART B

(Maximum marks:30)

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

1. **Differentiate private and public key cryptosystems.**

   Private key encryption:

   The universal technique for providing confidentiality for transmitted data is symmetric encryption. Symmetric encryption, also referred to as conventional encryption or single-key encryption

   public key:

   . Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns. More important, public-key cryptography is **asymmetric**, involving the use of two separate keys, in contrast to the symmetric conventional encryption, which uses only one key.

2. **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.

3. **Describe different forms of eaves dropping.**

   Dictionary attacks

   try each word then obvious variants in large dictionary against hash in password file

   Rainbow table attacks

   precompute tables of hash values for all salts

   a mammoth table of hash values

4. **Illustrate the concepts of UNIX File Access Control.**

   If the “set user ID”(SetUID) and “set group ID”(SetGID) are set on an executable file, the operating system functions as follows. When a user (with execute privileges for this file) executes the file,the system temporarily allocates the rights of the user’s ID of the file creator, or the file’s group, respectively, to those of the user executing the file. These are known as the “effective user ID”and “effective group ID” and are used in addition to the “real user ID” and “real group ID” of the executing user when making access control decisions for this program. This change is only effective while the program is being executed. This feature enables the creation and use of privileged programs that may use files normally inaccessible to other users

5. **Describe inline and passive network sensors.**

Inline sensor:

An inline senor is inserted into a network segment so that the traffic that it is monitoring must pass through the sensor

Passive Network sensor:

It monitors a copy of network traffic; the actual traffic does not pass through the device. Passive sensor is more efficient than inline sensor

6. **Describe the functions of honey pots**

Honeypots are designed to divert an attacker from accessing critical systems, collect information about the attacker's activity, and to encourage the attacker to stay on the system long enough for administrators to respond. These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect. The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities. Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems. Initial efforts involved a single honeypot computer with IP addresses designed to attract hackers.

7. **Summarise 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. Ideally the attacker would like to use a service that created a larger response packet than the original request.

PART C

(Maximum marks:60)

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

UNIT--I

III Describe the OSI security architecture. 15

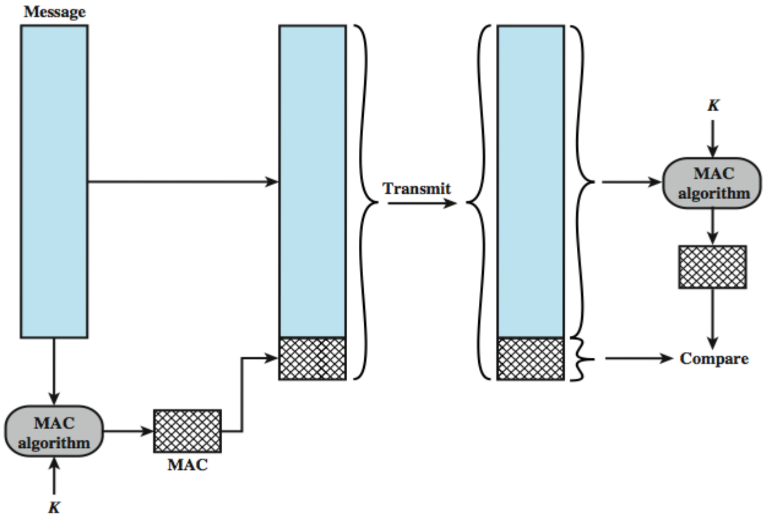
ITU-T Recommendation X.800, *Security Architecture for OSI*, defines a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture is useful to managers as a way of

organizing the task of providing security. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as:
• Security attack: Any action that compromises the security of information owned by an organization. cf. network security attacks slide earlier
• Security mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack. cf. functional requirements from previous slide or Table 1.6 in text.
• Security service: A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

- ➢ Authentication services
    - ♦ Peer entity authentication
    - ♦ Data origin Authentication
- ➢ Access Control
- ➢ Data Confidentiality
    - ♦ Connection confidentiality
    - ♦ Connectionless confidentiality
    - ♦ Selective field confidentiality
    - ♦ Traffic flow confidentiality
- ➢ Availability
- ➢ Data Integrity
- ➢ Non Repudiation

OR

IV Illustrate message authentication using Message Authentication code 15



- One authentication technique involves the use of a secret key to generate a small block of data, known as a message authentication code, that is appended to the message.

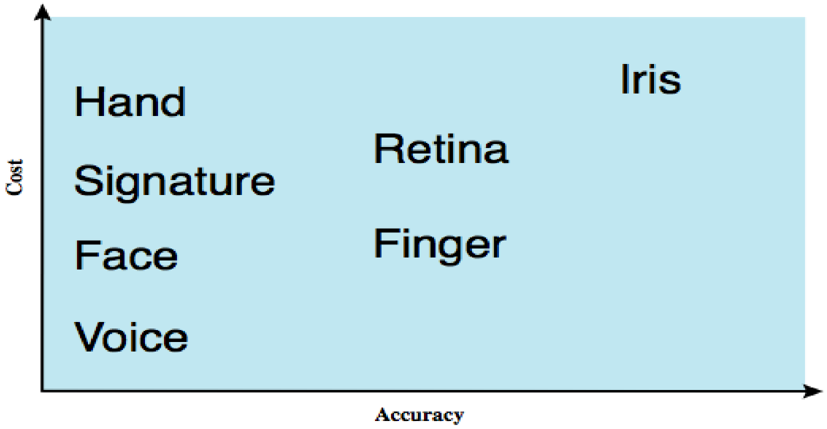
- This technique assumes that two communicating parties, say A and B, share a common secret key K_{AB}. When A has a message to send to B, it calculates the message authentication code as a function of the message and the key: $\text{MAC}_M = \text{F}(K_{AB}, M)$. The message plus code are transmitted to the intended recipient.
- The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code, as shown in figure .
- If we assume that only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then:

1. The receiver is assured that the message has not been altered.
2. The receiver is assured that the message is from the alleged sender.
3. If the message includes a sequence number, then the receiver can be assured of the proper sequence.

A number of algorithms could be used to generate the code. The NIST specification, FIPS PUB 113, recommends the use of DES. DES is used to generate an encrypted version of the message, and the last number of bits of ciphertext are used as the code. A 16- or 32-bit code is typical.

UNIT II

V Explain biometrics and the different types of physical characteristics in biometrics. 15



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. Figure gives a rough indication of the relative cost and accuracy of the most common biometric measures:

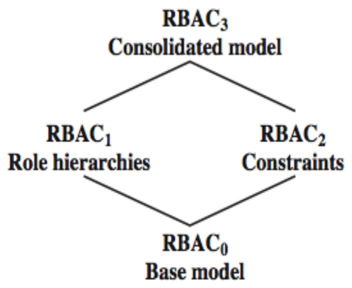
- **Facial characteristics:** define characteristics based on relative location and shape of key facial features, such as eyes, eyebrows, nose, lips, and chin shape.
- **Fingerprints**: the pattern of ridges and furrows on the surface of the fingertip, believed to be unique across the entire human population. 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

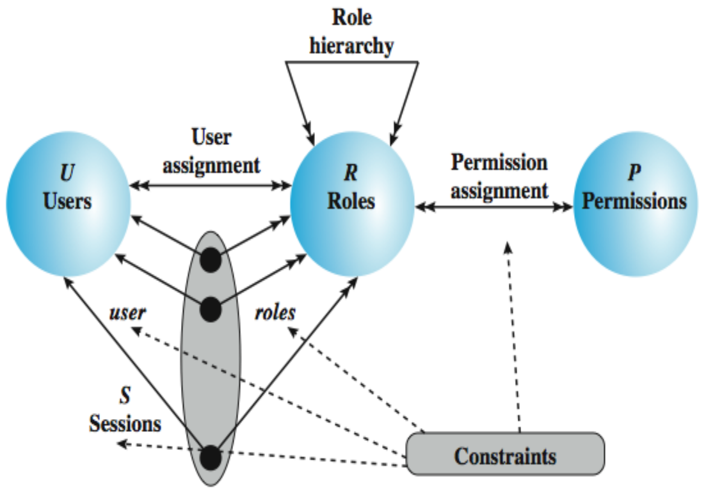
VI Illustrate Role Based Access Control reference model **15**

A variety of functions and services can be included under the general RBAC approach. [SAND 96] defines a family of reference models, that consists of four models that are related to each other as shown in Figure 4.9a. and in Table 4.3 in the text. $RBAC_0$ is contains the minimum functionality for an RBAC system. $RBAC_1$ includes the $RBAC_0$ functionality and adds role hierarchies, which enable one role to inherit permissions from another role. $RBAC_2$ includes $RBAC_0$ and adds constraints, which restricts the ways in which the components of a RBAC system may be configured. $RBAC_3$ includes $RBAC_0$ plus the added functionality of both $RBAC_1$ and $RBAC_2$. An $RBAC_0$ system contains the four types of entities:

- User: An individuals that has access to this computer system, & associated user ID.
- Role: A named job function within the organization that controls this computer system. Typically, associated with each role is a description of the authority and responsibility conferred on this role, and on any user who assumes this role.
- Permission: An approval of a particular mode of access to one or more objects. Equivalent terms are *access right*, *privilege*, and *authorization*.
- Session: A mapping between a user and an activated subset of the set of roles to which the user is assigned.



(a) Relationship among RBAC models

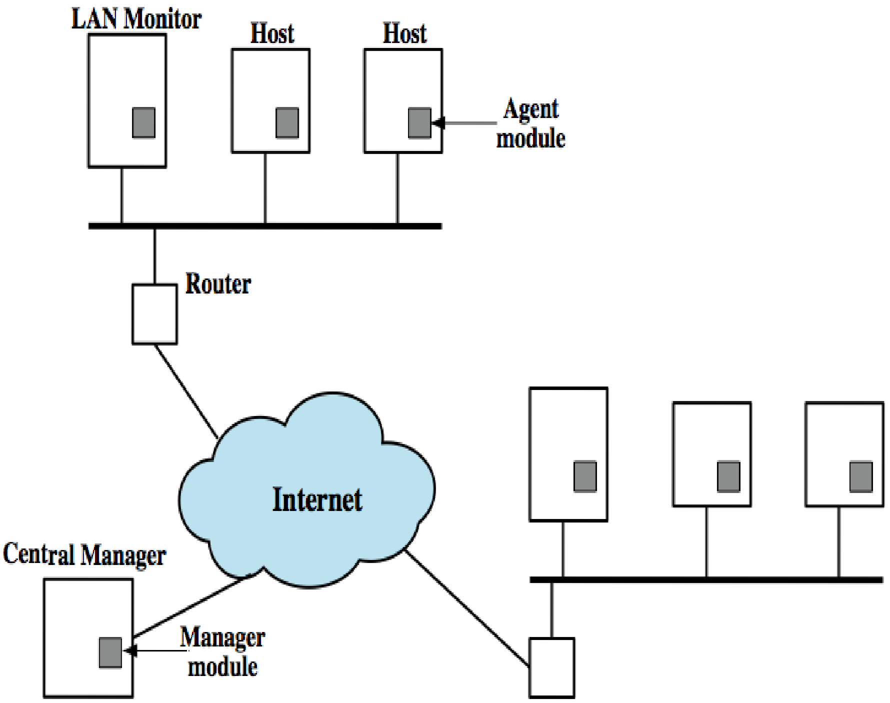


(b) RBAC models

The solid lines in figure indicate relationships, or mappings, with a single arrowhead indicating one and a double arrowhead indicating many. Thus, there is a many-to-many relationship between users and roles: one user may have multiple roles, and multiple users may be assigned to a single role. Similarly, there is a many-to-many relationship between roles and permissions.

UNIT--III

VII Illustrate the architecture of Distributed Host based Intrusion Detection System. 15



Traditionally, work on host-based IDSs focused on single-system stand-alone facilities. A more effective defense of a distributed collection of hosts supported by a LAN or internetwork can be achieved by coordination and cooperation among IDSs across the network. A good example of a distributed IDS is one developed at the University of California at Davis. The scheme is designed to be independent of any operating system or system auditing implementation. Figure 6.2 here shows the overall architecture, which consists of three main components:

- Host agent module: An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security-related events on the host and transmit these to the central manager.
- LAN monitor agent module: Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

OR

VIII a) Describe how bots are used by attackers. **9**

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 typical means of implementing the remote control facility is on an IRC (Internet relay chat) server. More recent botnets tend to avoid IRC mechanisms and use covert communication channels via protocols such as HTTP. Once a communications path is established between a control module and the bots, the control module can activate the bots, and even issue update commands that to download a file from some Internet location and execute it, making a more general-purpose tool that can be used for multiple attacks.

The first step in a botnet attack is for the attacker to infect a number of machines with bot software that will ultimately be used to carry out the attack. The essential ingredients in this phase of the attack are: Software that can carry out the attack; A vulnerability in a large number of systems; A strategy for locating vulnerable machines, a process known as scanning.

A number of the countermeasures discussed in this and the preceding chapter make sense against bots, including IDSs, honeypots, and digital immune systems.

VIII (b) List the requirements of an IDS **6**

- run continually with minimal human supervision.
- be fault tolerant in the sense that it must be able to recover from system crashes and reinitializations.
- resist subversion. The IDS must be able to monitor itself and detect if it has been modified by an attacker.
- impose a minimal overhead on the system where it is running.
- be able to be configured according to the security policies of the system that is being monitored.
- be able to adapt to changes in system and user behavior over time.
- be able to scale to monitor a large number of hosts.
- provide graceful degradation of service in the sense that if some components of the IDS stop working for any reason, the rest of them should be affected as little as possible.
- allow dynamic reconfiguration; that is, the ability to reconfigure the IDS without having to restart it.

UNIT-- IV

IX (a) Describe different flooding attacks. **9**

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.

IX (b) Describe the classic denial of service attack. **6**

The simplest classical denial of service attack is a flooding attack on an organization. The aim of this attack is to overwhelm the capacity of the network connection to the target organization. If the attacker has access to a system with a higher capacity network connection, then this system can likely generate a higher volume of traffic than the lower capacity target connection can handle. The attack might be as simple as using a flooding ping command directed at the target network. This traffic can be handled by the higher capacity links on the path between them, until the final router in the Internet cloud is reached. At this point some packets must be discarded, with the remainder consuming most of the capacity on the link to the medium sized company. Other valid traffic will have little chance of surviving discard, as the router responds to the resulting congestion on this link.

In this classic ping flood attack, the source of the attack is clearly identified since its address is used as the source address in the ICMP echo request packets. This has two disadvantages from the attacker's perspective. Firstly the source of the attack is explicitly identified, increasing the chance that the attacker can be identified, and legal action taken in response. Secondly, the targeted system will attempt to respond to the packets being sent.

OR

IX (a) Describe the methods used by the network intrusion prevention system to identify malicious packets. **9**

A network-based IPS (NIPS) is in essence an inline NIDS with the authority to discard packets and tear down TCP connections. As with a NIDS, a NIPS makes use of techniques such as signature detection and anomaly detection. Among the techniques used in a NIPS but not commonly found in a firewall is flow data protection. This requires that the application payload in a sequence of packets be reassembled. The IPS device applies filters to the full content of the flow every time a new packet for the flow arrives. When a flow is determined to be malicious, the latest and all subsequent packets belonging to the suspect flow are dropped. In terms of the general methods used by a NIPS device to identify malicious packets, the following are typical:

- Pattern matching: Scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.
- Stateful matching: Scans for attack signatures in the context of a traffic stream rather than individual packets.
- Protocol anomaly: Looks for deviation from standards set forth in RFCs.
- Traffic anomaly: Watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.
- Statistical anomaly: Develops baselines of normal traffic activity and throughput, and alerts on deviations from those baselines.

A modified version of Snort (Snort Inline) gives Snort an intrusion prevention capability. Snort Inline includes a replace option, which allows Snort user modify packets rather than drop them. This feature is useful in a honeypot implementation.

X (b) List the limitations of firewalls. 6

The firewall cannot protect against attacks that bypass the firewall, e.g. from dial-out, or a modem pool dial-in capability for traveling employees and telecommuters.
2. The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. An improperly secured wireless LAN may be accessed from outside the org
4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network and then attached and used internally.