

Internal Assessment Test – III July 2021

Sub:	Cyptography, Network Security & Cyber Law					Code:	17CS61
Date:	29 / 07 / 2021	Duration:	90 mins	Max Marks:	50	Sem:	VI-17scheme
Note: Answer any 5 full questions						Branch:	CSE&ISE

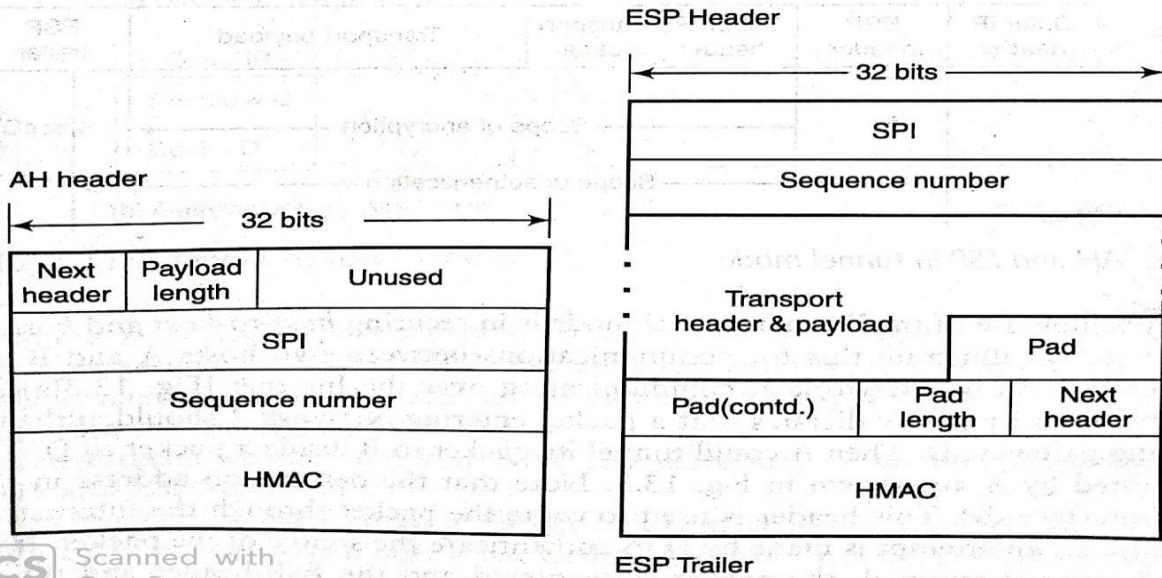
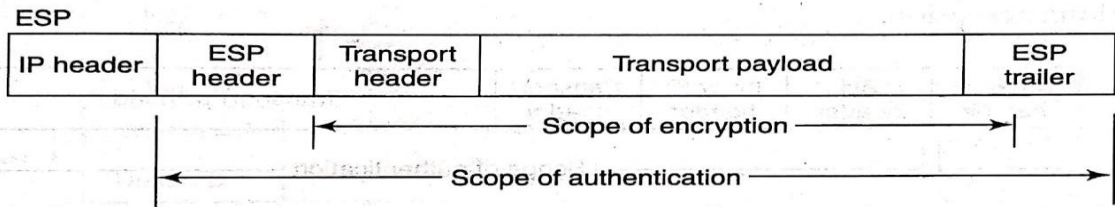
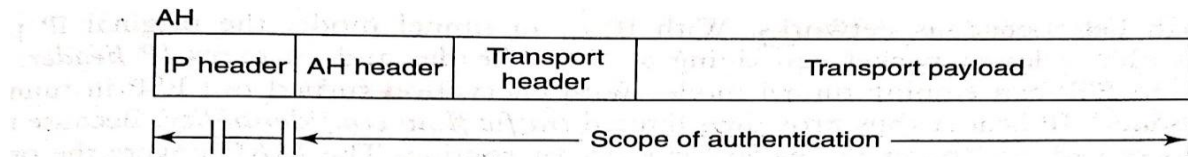
		Marks	OBE	
			CO	RBT
1.	What is IP Security? How Confidentiality and Authentication is enabled at network layer?	[10]	CO4	L2
2.	What are the different attacks on WEP? Explain how these attacks are mitigated in TKIP and CCMP?	[10]	CO5	L2
3.	Explain the different types of Firewalls.	[10]	CO5	L1
4.	Explain types of IDS with their tasks.	[5+5]	CO5	L1
5.	What is Code Red? Explain the following propagation model of Code Red. i). Simple epidemic Model ii) Kermack- McKendrick model	[10]	CO5	L2
6.	Define the following terms under the Information Technology Act, 2000 i) Certifying authority ii). Cyber Appellate Tribunal iii). Digital Signature iv). Secure System v). Controller	[2*5]	CO6	L1
7.	Explain various offences and punishments of cyber crime.	[10]	CO6	L1

1. What is IP Security? How Confidentiality and Authentication is enabled at network layer?

IP security is mainly designed to protect the applications against sniffing, spoofing, hijacking and DoS attacks

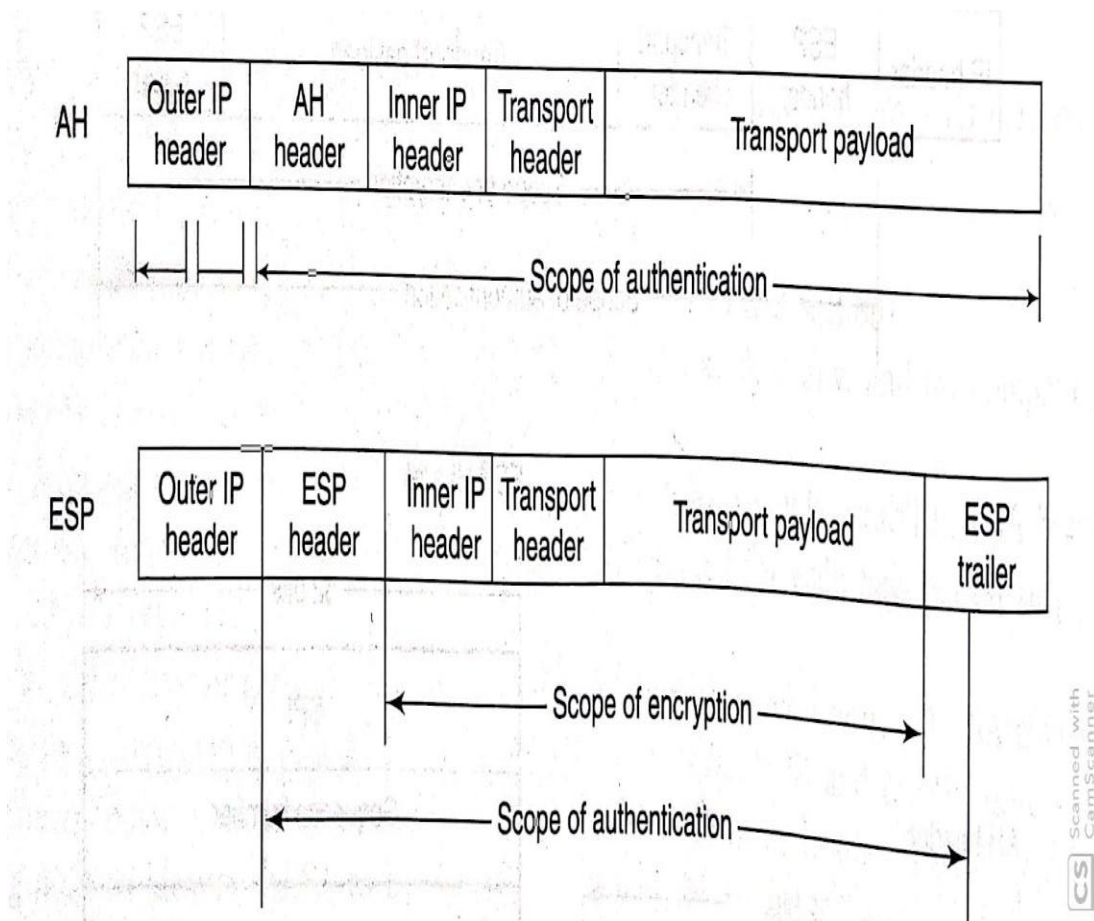
It provides the following security services

- Data origin authentication and data integrity
- Protection from Replay attacks
- Data Confidentiality



- Security header is placed in between IP and TCP headers.
- Message authentication and integrity is achieved by adding the MAC in both the cases.
- MAC is a part of AH header where as MAC is added as the trailer part in the ESP header
- SHA-1 or MD-5 are used to compute MAC for enforcing IP security.
- In AH, integrity check is computed on parts of IP header such as Source and destination Ip address. Hence uses even IP header also for integrity check.
- In case of ESP, IP header is excluded from providing security.
- Both AH and ESP headers will add extra 32 bit SPI field and a sequence number to the header.

- ESP and AH in Tunnel mode:



With IP Security in Tunnel Mode, the original IP packets are encapsulated within outer packet having IP security header and a outer IP header

- ESP in the Tunnel Mode, encrypts the inner IP header providing limited traffic flow confidentiality
- Inner IP header is encapsulated and outer ip header is used for routing
- MAC covers inner IP address in its entirety
- In AH, MAC covers entire inner IP Header and the selected parts of the outer Ip header for generating MAC to ensure the authentication os communication entities.
- In both the cases, the the source and destination addresses would be the addresses of gateways connecting source and destination networks
- Gateways TUNNEL the inner ip packets by applying end-to-endencapsulation

2. What are the different attacks on WEP? Explain how these attacks are mitigated in TKIP and CCMP?

Different Types of attacks on WEP are:

Known plaintext attack:

- The first problem with WEP is the possibility of keystream reuse.
- Since the IV is 24 bits in length, there are only 2^{24} distinct key streams that could be constructed given a secret S.
- Suppose an attacker finds two frames which were encrypted using the same IV.

$$P \oplus P' = C \oplus C'$$

$$P' = P \oplus C \oplus C'$$

- Let their ciphertexts be C and C'.
- Let the corresponding plaintexts be P and P'.

Message Modification Attack:

- Consider an attacker who wishes to modify a message sent by a legitimate user.
- Let the sender's plaintext (not including the CRC checksum) be $M_1 F M_2$ where M_1 , F, and M_2 are each binary strings.
- The attacker wishes to substitute the substring F, with another substring F' ,
- so that the decrypted message seen by the receiver is $M_1 F' M_2$. The attacker does not need to know the values, M_1 and M_2 . However, we assume that he knows F and F' .
- Ideally, the message integrity check should detect any modification to an existing message. Can the attacker modify the message (including checksum) in such a way so that the modification is undetected at the receiver end?
- For the above plaintext, the ciphertext computed by the sender is :

Thus knowing c, c' , and p , we can obtain p' which is called as known plaintext attack.

$$((M_1 F M_2) \parallel \text{CRC}(M_1 F M_2)) \oplus KS$$

The attacker intercepts the ciphertext and performs the following operations:

1. He first constructs the string, $0^{l_{M_1}} \parallel (F \oplus F') \parallel 0^{l_{M_2}}$. Here, $0^{l_{M_1}}$ is a string of $|M_1|$ zeros where $|x|$ is the length of the substring x .
2. He then computes the CRC on this string, $\text{CRC}(0^{l_{M_1}} \parallel (F \oplus F') \parallel 0^{l_{M_2}})$.
3. He finally XORs the original ciphertext with $0^{l_{M_1}} \parallel (F \oplus F') \parallel 0^{l_{M_2}} \parallel \text{CRC}(0^{l_{M_1}} \parallel (F \oplus F') \parallel 0^{l_{M_2}})$.

The last step follows from the fact that the CRC is a linear operation, i.e.,

$$\text{CRC}(m_1 \oplus m_2) = \text{CRC}(m_1) \oplus \text{CRC}(m_2)$$

The receiver, on decrypting the ciphertext, obtains

$$(M_1 F' M_2) \parallel \text{CRC}(M_1 F' M_2)$$

The modified message has a valid CRC and so passes the integrity check at the receiver.

- Hence, the receiver accepts the message, unaware that it has been modified by an attacker.

Data Protection in TKIP using Two Phase Key Mixing

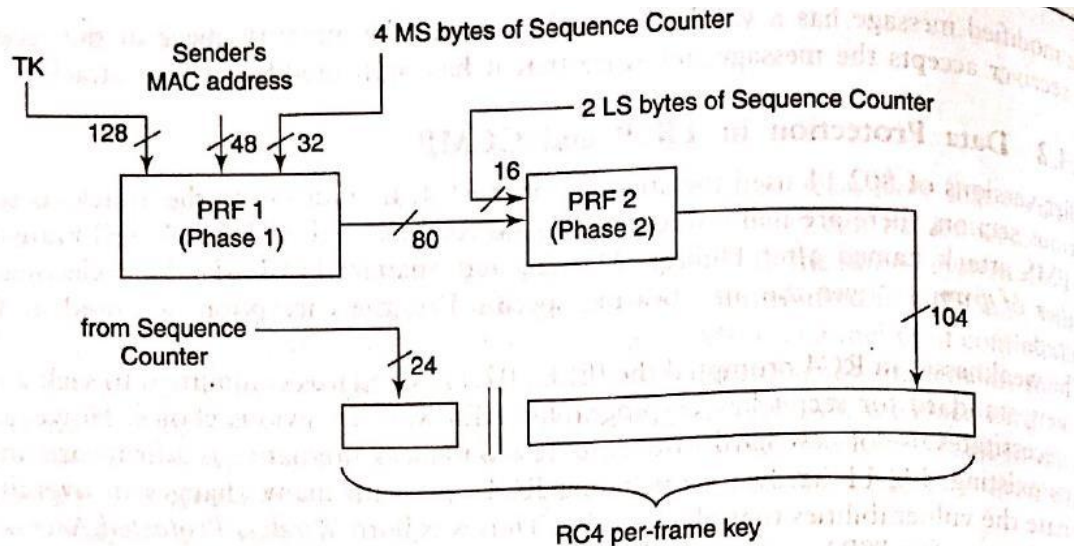


Figure 15.6 Two-phase key mixing in TKIP

TKIP generates a random and different encryption key(TK), for each frame sent. It employs a process called two-phase key mixing.

- The inputs to this process are the 128-bit temporal key, TK, computed as part of the four-way handshake ,the sender's MAC address and the four most significant bytes of a 48-bit frame sequence counter.
- The randomizing capability of the key mixing function and the large size of the key space virtually guarantee that "keystream collisions" never occur.
- Thus, known plaintext attacks that could be successfully launched on WEP have no chance of success with TKIP.
- The sequence counter is incremented for each frame sent.
- It is also carried in the header of each frame.

This helps protect the receiver from replay attacks.

- Figure given above, shows the two phases used in generating the RC4 key.
- Two pseudo-random function (PRF1 and PRF2) are employed in the two phases.
- The 32 most Significant bits of the sequence counter are input to PRF1.
- The least significant 16 bits of the sequence counter are inputs to PRF2 So, the output of PRF2 changes for each frame sent.
- MIC is computed as a function of the data in the frame and also some fields in the MAC header such as the source and destination addresses. It also uses as input a key derived from the PTK which was computed during the four-way handshake.

CCMP(CBC MAC Protocol):

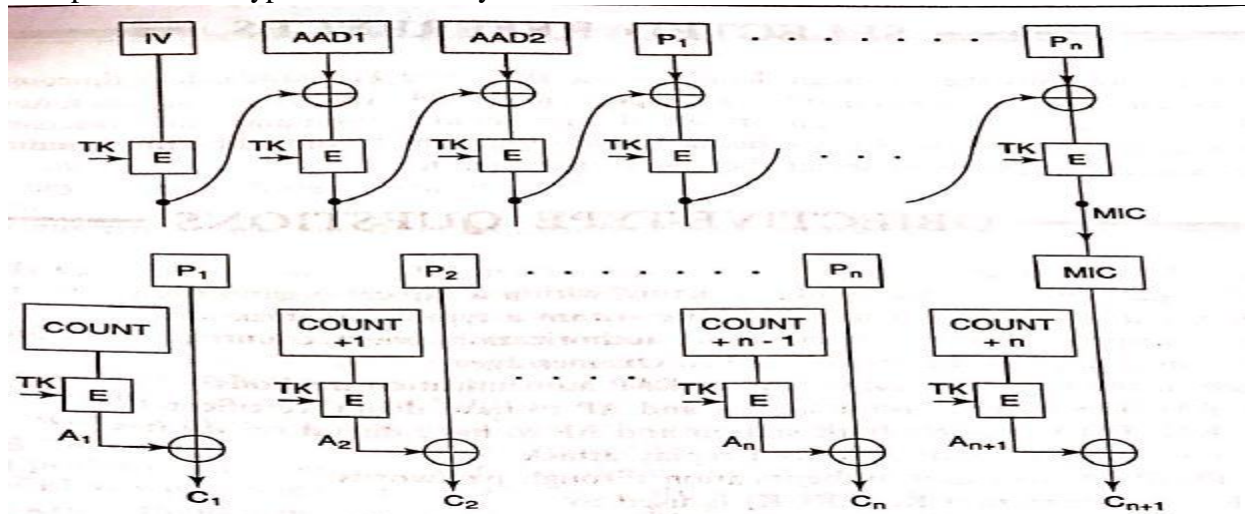
- The implementation of 802.11i that uses AES is referred to as WPA2. Its technical name is counter mode with CBC MAC protocol(CCMP).

MIC Computation:

- In CCMP terminology, this count is referred to as a packet number (PN).
- The count is maintained at both sender and receiver ends.
- The PN is also included in a special CCMP header field in a CCMP frame.
- The PN is incremented by the sender after each frame is sent.
- Upon receipt of a fresh frame in that session, the receiver compares the value of PN in the

CCM header versus the value stored by it.

- If the value is less than the stored value, the frame is likely to be a replayed frame and is hence discarded. The first task in preparing a frame for transmission is to compute a MIC.
 - The MIC is computed using AES in Cipher Block Chaining (CBC) mode with block size The key for performing encryption in each stage of Fig below is TK(temporal key).
 - The IV for the MIC computation is a "nonce," which includes the 48-bit PN.
 - The second and third blocks used in the MIC computation are specific fields in the frame header such as the MAC addresses, sequence control, and frame type.
 - Next, the blocks in the frame data are sequentially processed resulting in an 8-byte MIC. The next step is encryption.
 - The frame data and the MIC are concatenated and then encrypted using AES in counter mode
 - Let n be the total number of blocks in the frame body + MIC.
 - The procedure for encrypting the i -th block is:
 - Compute $A_i = ETK(PN + i*j)$. Here, PN is the packet number and j is a constant known to both sender and receiver.
 - Compute i -th block of ciphertext = $A_i \text{ (xor)} P_i$.
 - Here, P_i is the i -th block of plaintext.
- The frame now includes two new fields — the CCMP header and the MIC.
- Upon receipt of the frame, the receiver reverses the operations performed by the sender.
 - It performs decryption followed by MIC verification.



3. Explain the different types of Firewalls.

Firewall Types: Firewalls can be classified into the categories

1. Packet Filters
2. Stateful Inspection
3. Application Level Firewalls

1. Packet Filters

- This involves checking for matches in the IP, TCP, or UDP headers.
- For example, it may be necessary to check whether a packet carries a certain specific source or destination IP address or port number.
- It is **often performed by the border router or access router** that connects the organization's network to the Internet.

➤ In effect, the border router becomes the first line of defence against malicious incoming packets.

Consider an external mail server (IP address = ABC) that wishes to deliver mail to an Organization. For this purpose, it should first establish a TCP connection with the organization's mail server, MS.

➤ Consider the arrival of a packet with the following attributes:

➤ Source IP address = ABC

➤ Destination IP address = MS

➤ TCP destination port = 25 (SMTP port)

➤ ACK flag set

➤ Such a packet would be part of a normal flow provided a connection between ABC to MS has been established. But suppose such a connection has not yet been established. Should the packet still be allowed in? The simple packet filter will allow the packet to enter even if no prior connection between ABC and MS was established.

It should be noted that such packets are often used to perform port scans.

➤ A simple packet filter merely inspects the headers of an incoming packet in isolation. It does not view a packet as part of a connection or flow. Hence, it will not be able to filter out such packets arriving from ABC.

Stateful Inspection

➤ A firewall uses packet TCP flags and sequence/acknowledgement numbers to determine whether it is part of an existing, authorized flow.

➤ If it is participating in the establishment of an authorized connection or if it is already part of an existing connection, the packet is permitted, otherwise it is dropped.

In the above example of the packet from ABC, the stateful packet inspection firewall will realize that it has not encountered the first two packets in the three-way handshake and will hence drop this packet.

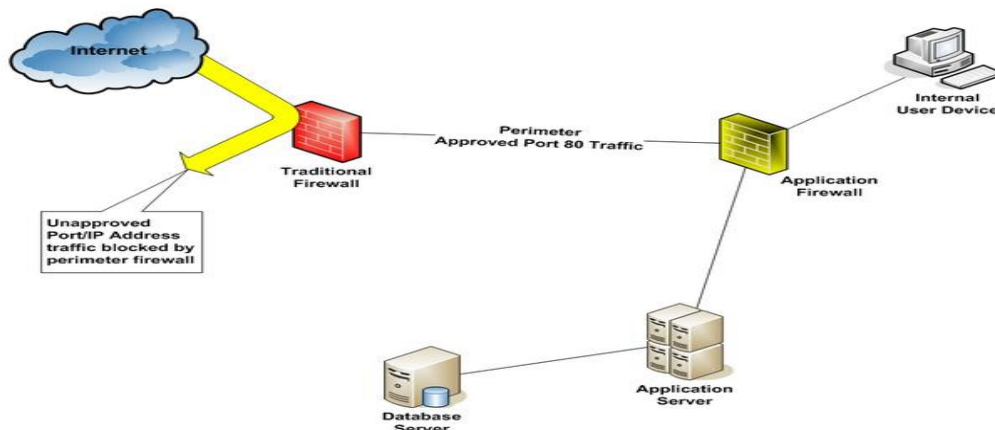
Application Level Firewalls

➤ A packet-filtering firewall, even with the added functionality of stateful packet inspection, is still severely limited.

➤ What is needed is a firewall that can examine the application payload and scans packets for worms, viruses, spam mail, and inappropriate content. Such a device is called a deep inspection firewall.

➤ A special kind of application-level firewall is built using proxy agents. Such a "proxy firewall"

acts as an intermediary between the client and server. The client establishes a TCP connection to the proxy and the proxy establishes another TCP connection with the server



To a client, the proxy appears as the server and to the server, the proxy appears as the client. Since there is no direct connection between the client and the server, worms and other malware will not be able to pass between the two, assuming that the proxy can detect and filter out the malware. Hence, the presence of the proxy enhances security.

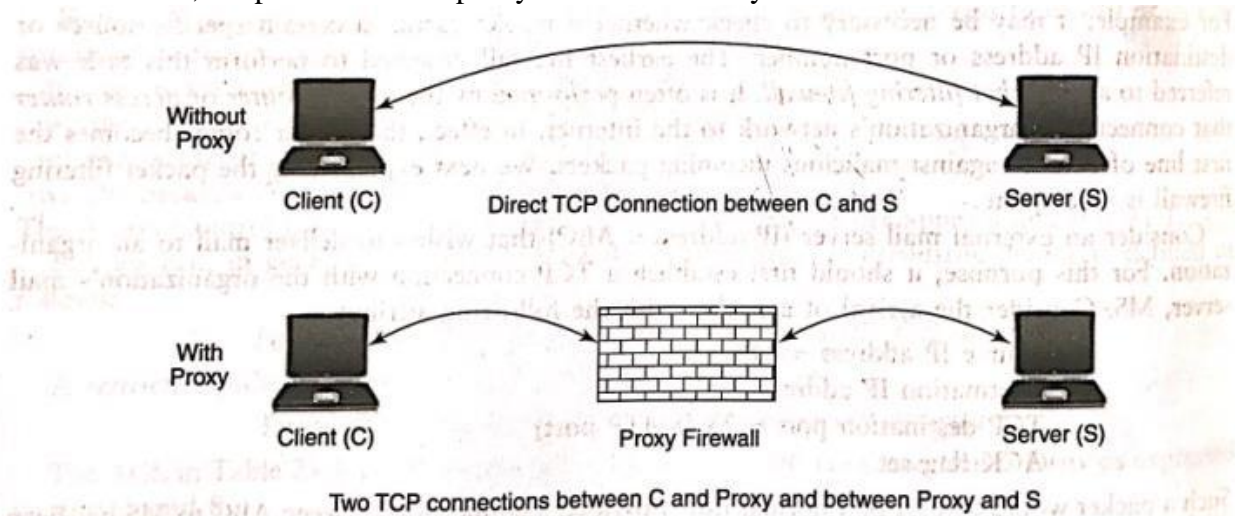


Figure 21.1 Proxy firewall

There are proxy agents for many application layer protocols including HTTP, SMTP, and FTP.

- In addition to filtering based on application layer data, proxies can perform client authentication and logging.
- An HTTP proxy can also cache web pages.
- Caching has a major impact on performance.
- If the webpage is cached in a web proxy server located in the client's organization, the response time could be greatly reduced compared to that where the page has to be fetched from the external web server.
- Also, caching reduces the demand on external communication bandwidth while easing the load on the web server.
- Firewalls are a necessary element in the security architecture of an organization that permit access to/from the external world.

4. Explain types of IDS with their tasks.

TYPES OF INTRUSION DETECTION SYSTEMS:

1) Anomaly versus signature based IDS

2) Host based versus network based IDS

Anomaly versus signature based IDS:

Anomaly based intrusion detection involves making a determination whether the behaviour of the system is a statistically significant departure from normal.

- The IDS will have to learn, over time, what constitutes normal activity, usage, and behaviour.
-
- The six conditions in Table below, are the examples of what an anomaly based IDS would monitor.
- Consider monitoring the number of TCP SYN packets (with the SYN flag set) and FIN Packets (with the FIN flag set) in each successive 10-second interval.
- A disproportionate number of SYN packets vis-a-vis FIN packets indicate several half-open TCP connections and possibly the onset of a SYN flooding attack.

Signature based IDS works by identifying specific Patterns of events or behaviour that indicate or accompany an attack.

- Each such pattern is called a signature.
- A signature-based IDS maintains a database of known signatures.
- It attempts to obtain a match between the currently observed behaviour of the system and an entry in this database.
- A real world signature-based IDS will have thousands of attack signatures against which to compare.
- An example of an attack signature is a specific bit sequence in a worm payload.
- In a signature-based IDS it is the presence of a specific signature that raises an alert.
- On the other hand, it is possible that a spread of the worm has caused much network traffic congestion and greatly increased CPU utilization on infected machines.

Host-based versus Network-based IDS:

Network-based IDS captures information about packets flowing through the network is referred to as network-based IDS.

- For reasons of performance, it is common to have stand-alone appliances that perform network-based intrusion detection. These typically run only the IDS and are hence not vulnerable to various worm and virus attacks.
- They may be deployed at multiple points in a large organization.

Host-based IDS is typically implemented in software and resides on top of the host's operating system.

- Its main job is to monitor the internal behaviour of the host such as the sequence of system calls made, the files accessed, etc.
- For this purpose, it makes use of system logs, application logs, and operating system audit trails to identify events related to an intrusion.
- **Operating system logs, for example, keep track of when users log in, the number of unsuccessful login attempts, the commands executed, network connections made, etc.**
- Application logs keep track of which files have been opened or which registry keys have been accessed during the run of an application.
- File system integrity checkers, for example, compute a cryptographic hash on the contents of each file. They detect file changes by comparing the computed hash of a file to its stored hash.

5. Worm Propagation models:

The Simple Epidemic Model:

The Simple Epidemic Model used to study the spread of infectious diseases among humans is an appropriate starting point.

The model assumes that there are only two types of entities in the population. Either an individual is susceptible or he is infected.

An infected individual can infect a susceptible person. Once infected, a person remains infected and does not recover.

Let N be the size of the total population.

Let N be the size of the total population. Let $I(t)$ be the number of infected individuals at time t . The number of susceptibles at time t is then $N - I(t)$. β is the initial infection rate, i.e., each infected person attempts to pass on the infection to β susceptibles in 1 time unit. The following differential equation captures the number of infected persons at time t .


$$dI = \beta I(t) \left(1 - \frac{I(t)}{N}\right) dt \equiv \text{rate of infection} \times \begin{matrix} \text{(susceptible} \\ \text{people)} \end{matrix} \quad (19.1)$$

or

$$\beta dt = \left(\frac{dI(t)}{I(t) \left(1 - \frac{I(t)}{N}\right)} \right) \quad (19.2)$$

In an infinite population, each infected person infects βdt susceptibles in time interval dt . However, in a finite population of size N , the probability that the target of an infective is already infected is $\frac{I(t)}{N}$. Such targets do not add to the population of newly infected. The factor $\left(1 - \frac{I(t)}{N}\right)$ in the above equations ensures that only previously uninfected entities are added to the count of the freshly infected in time interval dt .

Integrating both sides of Eq. (19.2) yields


$$I(t) = \frac{I_0 N}{I_0 + (N - I_0)e^{-\beta t}} \quad (19.3)$$

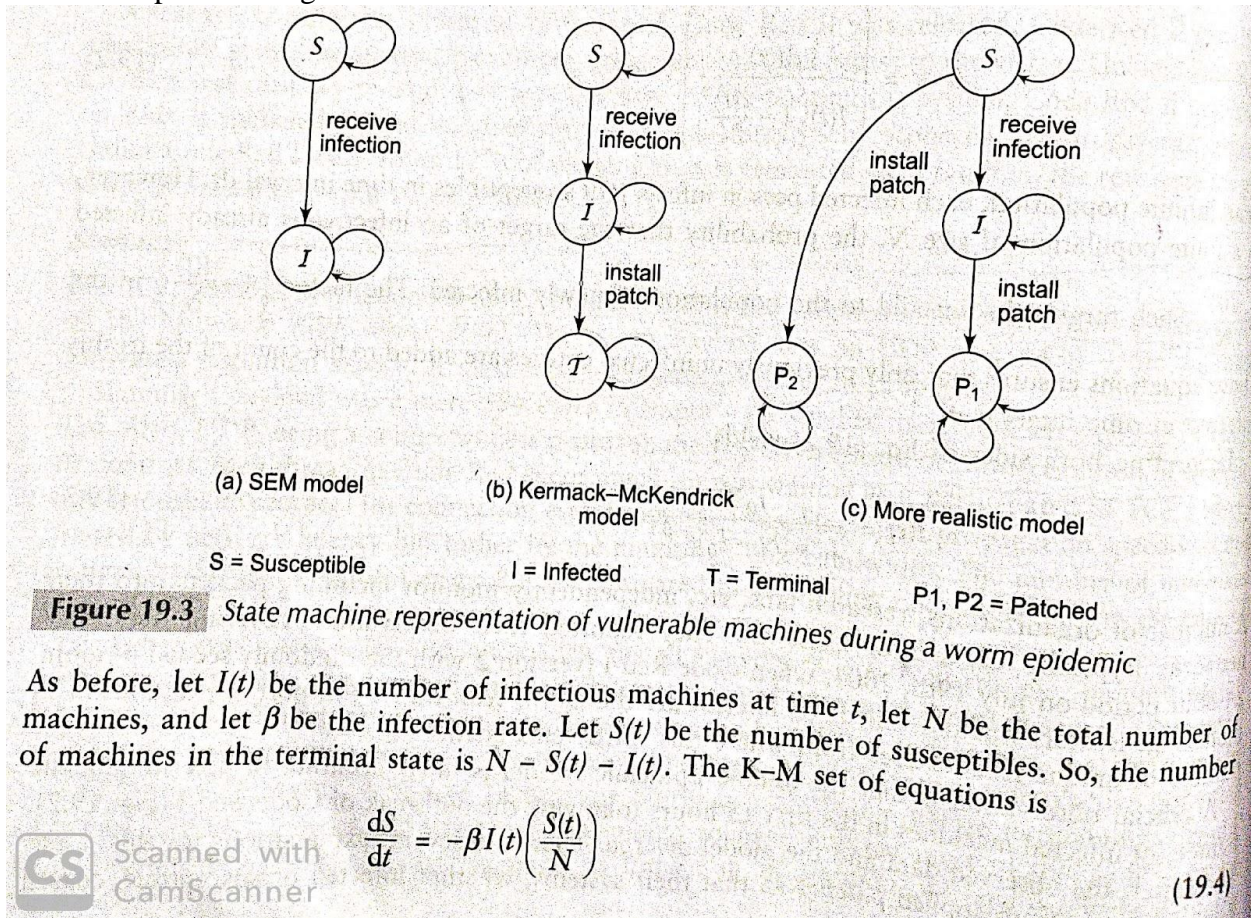
The simple epidemic model was effective and found to be accurate in determining the the infected devices in its first 15 hours of infection. There after the observed data and the model started diverging, while applied for Code Red worm detection.

Kermack McKendrick Model:

- The Kermack-McKendrick (K-M) model more accurately models the spread of human infectious disease by considering three categories of people:
 - those who are susceptible (state S)
 - those who are infectious (state I) and
 - those who are neither, i.e. individuals who are cured or those who have found to be

resist to the disease (terminal T).

- Initially, all individuals in the population are susceptible.
- It is possible to go from state S to I but not vice versa .



- The equation 19.4 describes the rate at which the susceptibles change into infectious. Where as next equation captures the machines in the terminal state would increase.
- The nodes in the Terminal state are neither susceptible nor infectious.
- Kermack-McKendrick model has better explained the spread of Code Red then the Simple Epidemic Model.

6. Define the following terms under the Information Technology Act, 2000

- i) Certifying authority ii). Cyber Appellate Tribunal
 - iii). Digital Signature iv). Secure System v). Controller

iii. Digital Signature:

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was

- unique to the subscriber affixing it;
- capable of identifying such a subscriber;
- created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such a digital signature shall be deemed to be a secure digital signature [Section 15].

ii). Cyber Appellate Tribunal

Cyber Appellate Tribunal

A person shall not qualify for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he

1. is, or has been, or is qualified to be, a Judge of a High Court; or
2. is or has been a member of the Indian Legal Service and is holding, or has held, a post in Grade I of that Service for at least three years [Section 50].

27.11.4 Term of Office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters the office, or until he attains the age of 65 years, whichever is earlier [Section 51].

v. Controller

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act, and may also, by the same or subsequent notification, appoint such a number of Deputy Controllers and Assistant Controllers as it deems fit.
2. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
3. The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
4. The qualifications, experience, and terms and conditions of service of Controller, Deputy Controllers, and Assistant Controllers shall be such as may be prescribed by the Central Government.
5. The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

i. Certifying Authorities

27.7.2 Recognition of Foreign Certifying Authorities

1. The Controller may, with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
2. Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
3. The Controller, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition [Section 19].

7. Explain various offences and punishments of cyber crime.

27.12.1 Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters, or intentionally or knowingly causes another to conceal, destroy or alter, any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with a fine which may extend up to ₹2 lakh, or with both.

Explanation: For the purposes of this section, 'computer source code' refers to the listing of programmes, computer commands, design and layout, and programme analysis of computer resource in any form [Section 65].

27.12.2 Hacking with Computer System

If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both [Section 66].

Note: In a related development, the Supreme Court on March 24, 2015 termed it unconstitutional struck down Section 66A of the IT Act which allowed arrests for posting offensive content on social media sites. The controversial provision made posting offensive material on social networking sites an offence punishable by up to three years in jail.

27.12.2 Punishment for Receiving Stolen Computer Resource or Communication Device

Whoever dishonestly received or retains any stolen computer resource of communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both [Section 66B].

27.12.3 Punishment for Identity Theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh [Section 66B].

27.12.4 Punishment for Cheating by Personation by Using Computer Resource

Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees [Section 66D].

27.12.5 Punishment for Violation of Privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both [Section 66E].

27.12.6 Punishment for Cyber Terrorism

1. Whoever,

(a) With intent to threaten the unity, integrity, security of sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(b) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals, or otherwise, commits the offence of cyber terrorism.