TERNA ENGINEERING COLLEGE, NERUL
Department of Computer Engineering

Cryptography and System Security (CSS)

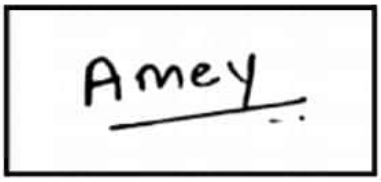
Assignment No 2

Sr. No.	Question	CO -mapped
Q. 1	DefineMD5, SHA1, MAC,HMAC,CMAC.	(CO-4)
Q. 2	Explain X.509, Needham Schroeder /Kerberos Authentication with example.	(CO-4)
Q. 3	Explain with ICMP flood, SYN flood, UDP flood, DDoS example.	(CO-5)
Q. 4	Explain the SSL, IPSEC, PGP, IDS, Honey pot.	(CO-5)
Q. 5	Explain in brief Software Vulnerabilities such as Buffer Overflow, Format String, cross-site scripting.	(CO-6)
Q. 6	Explain SQL injection, Logic bomb Rootkits algorithm with an example.	(CO-6)

CSS ASSIGNMENT - 2

AMEY THAKUR

COMPS TE B-50



AMEY TE B 50

Amey

PAGE NO.
DATE / /

Q1 Define

MD5

- The MD5 hashing algorithm is a one way cryptographic function that accepts a message of any length as input and returns as output a fixed length digest value to be used for authenticating the original message.

SHA 1

- SHA 1 or Secure Hash Algorithm 1 is a cryptographic hash function. which takes an input and produces a 160-bit (20 byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency.

MAC

- A Message Authentication Code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.

HMAC

- Hash Based Message Authentication Code (HMAC) is a Message Authentication Code that uses a Bryptographic key in conjunction with a hash function.

AMEY TE B 50 Amey

PAGE No. 14
DATE / /

CMAC

- In cryptography, CMAC (Cipher-Based Message Authentication Code) is a block cipher-based message authentication code algorithm. It may be used to provide assurance of the authenticity and hence the integrity of binary data.

AMEY TE B 50 Amey

Q2 Explain X.509, Needham Schroeder / Kerberos Authentication with example.

Ans:

X.509

- An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.
- An X.509 certificate contains information about the identity to which a certificate is issued and the identity that issued it. Standard information in an X.509 certificate includes:

Version

- Which X.509 version applies to the certificate (which indicates what data the certificate must include)

Serial Number

- The identity creating the certificate must assign it a serial number that distinguishes it from other certificate.

Algorithm Information

- The algorithm used by the issuer to sign the certificate.

Issuer Distinguished Name

- The name of the entity issuing the certificate (A certificate authority)

AMEY TE B 50

Amey

PAGE NO. 1.1
DATE / /

Validity Period of the certificate
- start / end date and time

Subject distinguished name
- The name of the identity the certificate is issued to.

Subject Public Key Information
- The public key associated with the identity.

Extentions (Optional)

- Many of the certificates that people refer to as Secure Sockets Layer (SSL) certificates are in fact X.509 certificates.

Needham Schroeder / Kerberos Authentication
- Kerberos infrastructure relies on Needham Schroeder Protocol.
- Needham schroeder protocol refers to a communication protocol used to secure an insecure network. The protocol got its name from the creators Roger Needham and Michael Schroeder.
- There are two types of Needham - Schroeder protocol.
  1. Needham - Schroeder protocol with symmetric key
  2. Needham - Schroeder protocol with Asymmetric key

AMEY TE B 50 Amey

PAGE No.
DATE / /

- Now lets understand Needham - Schroeder protocol with symmetric key encryption because its the one used in Kerberos infrastructure.

- Needham - Schroeder protocol allows to prove the identity of the end users communicating, and also prevents a middle man from evesdropping

- We will be using some terms

Nonce :

- Nonce is a randomly generated string which is only valid for some period of time. This is used in encryption protocol to prevent replay attack
- For example, if somebody captures a packet during the communication between me and a shopping website, he can resend the packet without decrypting it, and the server can accept the packet and do operations on it. To prevent this, nonce (the random value generated) is added to the data, so as the server can check if that nonce is valid or expired.

- Lets understand this protocol by taking an example communication between two machines called Machine A and Machine B.

- The main thing in this protocol is that there is a trusted middle man or call him an arbitrator. This trusted middle man is a server. If an X machine wants to communicate with Y machine. Then X has to contact the middle man server saying am interested in communicating with Y.

AMEY TE B 50 Amey

Lets see how it works.

A = Machine A

B = Machine B

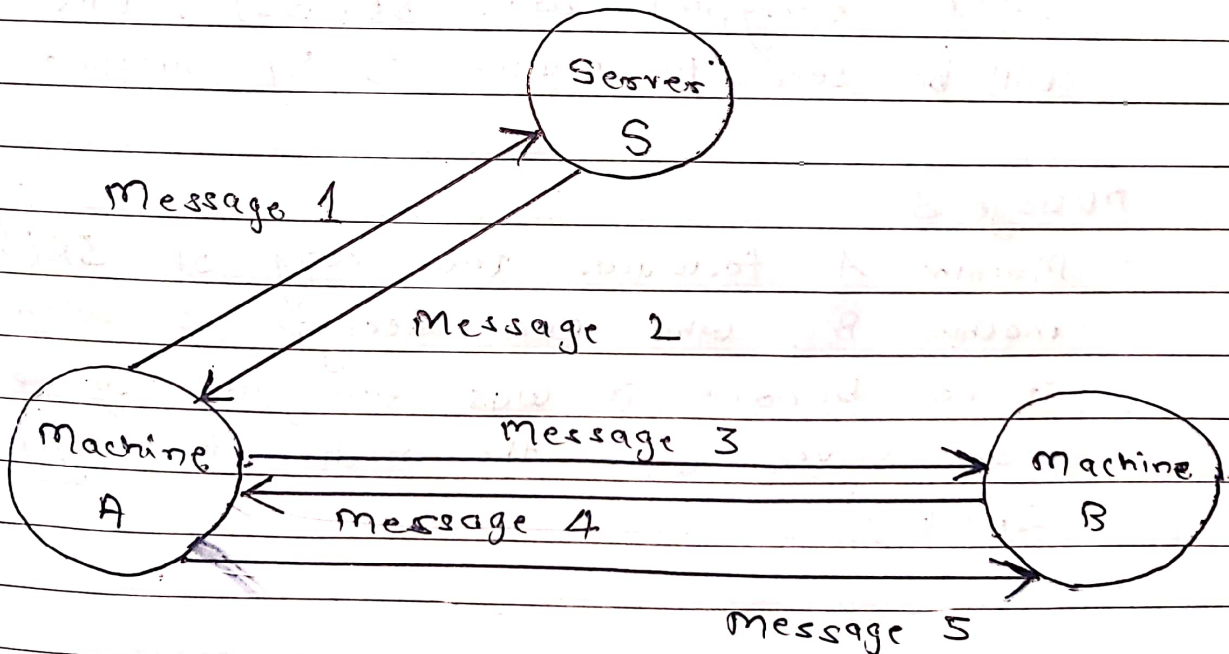
SK (AS) = This is the symmetric key known to machine A and middle man Server named S.

SK (BS) = This is the symmetric key known to machine B and middle man Server named S.

NON (A) = Nonce generated by Machine A.

NON (B) = Nonce generated by Machine B.

SK (S) = This is the symmetric key / session key generated by the server for both machine A and machine B.



AMEY TE B 50 Amey PAGE No. DATE / /

- Lets understand all the messages mentioned above.

- Initially before going ahead with the explanation, make it clear that the symmetric keys of both machine A, machine B are already shared with the middle man server. Also any other machine in the network also shares its respective symmetric keys with the middle man server.

Message 1:

- Machine 1 sends a message to Server S saying that I want to communicate with machine B.

- A → S (This message contains A and B and NON(A))

Message 2:

- Server S sends message 2 back to machine A containing SK(S), and also one more copy of SK(S) encrypted with SK(BS). this copy will be send to machine B by machine A.

Message 3:

- Machine A forwards the copy of SK(S) to machine B, who can decrypt it with the key it has because it was encrypted by the middle man server with the machine B's symmetric key SK(BS).

AMEY TE B 50 Amey

Message 4:

- Machine B sends back machine A a nonce value encrypted by SK(S) to confirm that he has the symmetric key or session key provided by the middle man server.

Message 5:

- Machine A performs a simple operation on the nonce provided by the Machine B and resends that back to machine B just to verify machine A has the key.

- There are still some vulnerabilities in this protocol for replay attacks which is fixed by the timestamp implementation in this, when used by Kerberos.

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.3 Explain

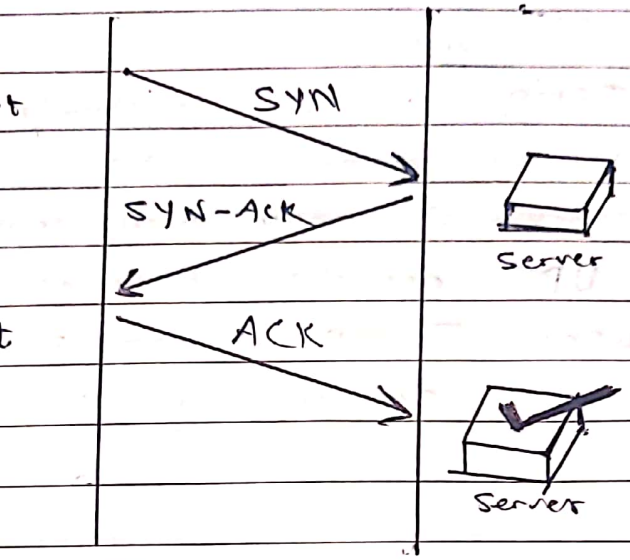
ICMP Flood

- Ping flood, also known as ICMP flood, is a common Denial of Service (DOS) attack in which an attacker takes down a victim's computer by overpowering it with ICMP echo requests, also known as pings.
- The attack involves flooding the victim's network with request packets, knowing that the network will react with an equal number of reply packets.
- Additional methods for bringing down a target with ICMP requests include the use of convention tools or code, such as hping and scapy.
- This strains both the incoming and outgoing channels of the network, consuming considerable bandwidth and resulting in a denial of service.

SYN Flood

- It is a TCP SYN flooding attack, a denial of service attack. In TCP, handshaking of network connection is done between sender and receiver through synchronous (SYN) and acknowledgement (ACK) message.
- An attacker initiates a TCP connection with server with a SYN message. The server in reply sends an acknowledgement message (SYN - ACK) message.
- The client (attacker) does not respond back with acknowledgement which causes server to wait.
- Due to which it is unable to connect with other client. This fills up the buffer space for SYN message preventing other for communicate.

AMEY TE B 50 Amey



3 Way Handshake

① Clients sends Synchronize (SYN) packet to server.
② Servers sends SYN-ACK to client
③ Client responds back with ACK packet.

UDP Flood

- A UDP Flood Attack is a Denial-of-Service (DOS) attack using the User Datagram Protocol, a connectionless computer networking protocol.
- Using UDP for denial of service attacks is not as easy as with the Transmission Control Protocol (TCP).
- However, a UDP flood attack can be initiated by sending a huge number of UDP packets to random ports on a remote host.
- As a result, the distant host will:

① Verify for the application listening at that port.
② See that no application is listening at that port.
③ Reply with an ICMP Destination Unreachable Packet.

AMEY TE B 50 Amey

PAGE No.
DATE / /

- Thus, for a large number of UDP packets, the ill-treated system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients.
- The attacker(s) may also spoof the IP address of the UDP packets, ensuring that the unnecessary ICMP return packets do not reach them, and anonymizing their network location(s)

DDoS

- A Distributed Denial of Service (DDoS) attack is an attack in which multiple compromised computer system attack a target, such as a server, website or other network resource and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

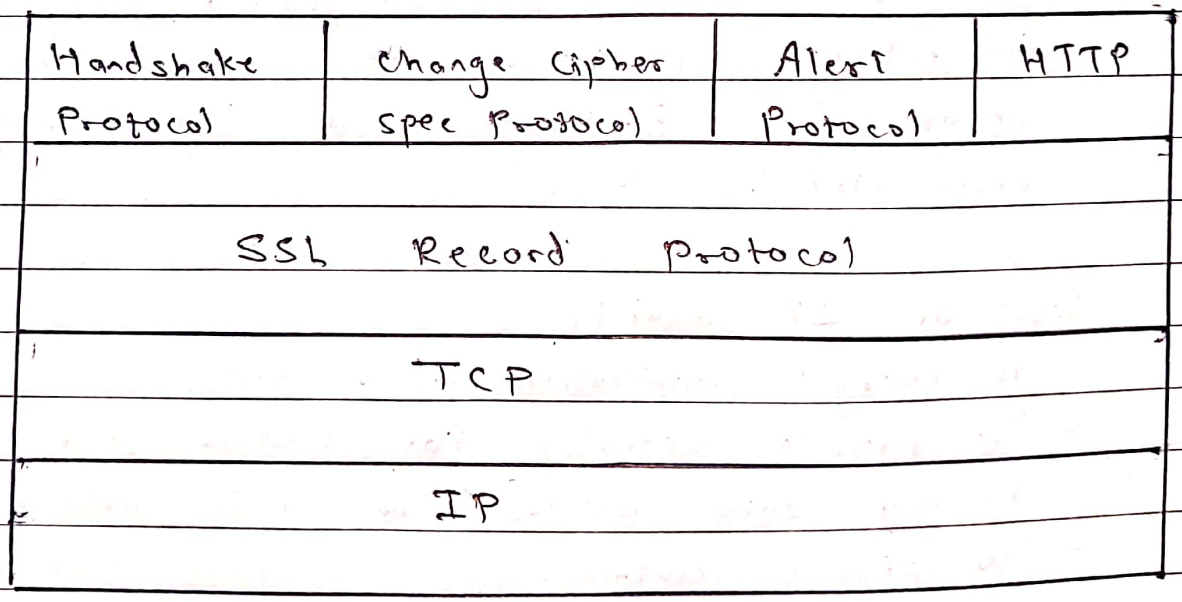
- Distributed denial of service, it is where an attacker uses your own computer to attack on another computer.
- It takes advantage of loopholes and security vulnerability to take control on for computer to send vulnerability spam or send huge data to other computers.
- The systems which are used for attacking victim computer are called as zombie systems.
- Tools to launch DDoS attack are Trinoo, Shaft, etc.

AMEY TE B 50 Amey

Q4. Explain

SSL

- Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.
- Secure Socket Layer Protocols
  1. SSL record protocol
  2. Handshake protocol
  3. Change - cipher spec protocol
  4. Alert protocol
- SSL protocol stack



- SSL Record provide two services to SSL connection
  1. Confidentiality
  2. Message Integrity

AMEY TE B -50 Amey

PAGE No.
DATE / /

Features of SSL

- Advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end to end secure service.
- This is a two layered protocol.

IPSec

- The IP Security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provides data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key Exchange and Key Management are defined in it.

Uses of IP Security

- To encrypt application layer data
- To provide security for routers sending sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPSec tunneling in which all data is being sent between the two endpoints is encrypted as with a Virtual Private Network (VPN) connection.

AMEY TE B 50 Amey

Components of IPsec

① Encapsulating Security Payload (ESP)
② Authentication Header (AH)
③ Internet Key Exchange (IKE)

PGP

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e. ① Privacy
  ② Integrity
  ③ Authentication
  ④ Non-Repudiation in the sending of email
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication and non-repudiation.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key and two private public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm and Email compatibility using the radix 64 encoding scheme.

AMEY TE B 50 Amey -

PAGE No.
DATE / /

IDS

- Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates output from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms
- Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.
- Intrusion Prevention Systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notification

AMEY TE B 50 Amey

Classification of Intrusion Detection System

1. Network Intrusion Detection system (NIDS)
2. Host Intrusion Detection System (HIDS)
3. Protocol-based Intrusion Detection System (PIDS)
4. Application Protocol-based Intrusion Detection System (APIDS)
5. Hybrid Intrusion Detection System.

Detection methods of IDS

1. Signature based method
2. Anomaly based method

Honeypot

- Honeypot is network attached system used as a trap for cyber attackers to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.
- Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attack used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.
- The cost of honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organizations resources still preventing attacks at the backend and access to any production system.

AMEY TE B 50 Amey

PAGE No.
DATE / /

- A honeynet is a combination of two or more honeypots on a network.

Types of honeypot
1. Research honeypots
2. Production honeypots

Advantages of Honeypots
- Acts as a rich source of information and helps collect real time data
- Identifies malicious activity even if encryption is used
- Wastes hackers time and resources.
- Improves Security.

Disadvantages of honeypots
- Being distinguishable from production systems, it can be easily identified by experienced attacker.
- Having a narrow field of view, it can only identify direct attacks
- A honeypot once attacked can be used to attack other systems.
- Fingerprinting (An attacker can identify the true identity of a honeypot.

AMEY TE B 50 Amey

Q5. Explain in brief Software vulnerabilities such as Buffer Overflow, Format String, Cross-site scripting.

Ans:

① Buffer Overflow

- It is probably the best known form of software security vulnerability.
- Most software developers know what a buffer overflow vulnerability is, but buffer overflow attacks against both legacy and newly developed applications are still quite common.
- In a classic buffer overflow exploit, the attacker sends data to a program, which it stores in an undersized stack buffer.
- The result is that information on the call stack is overwritten, including the function's return pointer.
- The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.

② Format Strings

- Format Strings are used in many programming languages to insert values into a text string.
- In some cases, this mechanism can be abused to perform buffer overflow attacks, extract information or execute arbitrary code.
- Format strings are used in many programming languages to insert values into a text string.

AMEY TE B 50 Amey

- To prevent these vulnerabilities, always specify a format string as part of program, not as an input.

③ Cross-site Scripting (XSS)

- It is a client side code injection attack.
- The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.
- The actual attack occurs when the victim visits the web page or web application that executes the malicious code.
- The web page or web application becomes a vehicle to deliver the malicious script to the user's browser.
- Vulnerable vehicles that are commonly used for Cross-site scripting attacks are forums, message boards and web pages that allow comments.
- There are two stages to a typical XSS attack.

① To run malicious javascript code in a victim's browser, an attacker must first find a way to inject malicious code (Payload) into a web page that the victim visits.

② After that, the victim must visit the web page with the malicious code. If the attack is directed at particular victims, the attacker can use social engineering and/or phishing to send a malicious URL to the victim.

AMEY TE B 50 Amey PAGE NO. DATE / /

Q.6 Explain SQL Injection, Logic bomb, Rootkits algorithm with an example

Ans:

SQL Injection

- It is a source code injection technique in which malicious SQL statements are inserted into entry field of database to dump data base content.
- Attacker targets the database organization where confidential data is stored.
- Its main focus is to get information from the database server stored in database table by sending malicious query since database can be accessible by query
- When legitimate user enters an additional database via web form, the attacker sends its own command through same web form field. The attackers before proceeding always checks whether organization's database has any loop is it vulnerable or not.

Logic Bomb

- A logic bomb, sometimes referred to as slag code, is a string of malicious code used to cause harm to a network when the programmed conditions are met.
- The term comes from the idea that a logic bomb "explodes" when it is triggered by specific event.
- Events could include a certain date or time, a particular record being deleted from a system or the launching of an infected software applicatio

AMEY TE B 50 Amey

PAGE No.
DATE / /

- The level of destruction caused by a logic bomb can vary greatly and the set of conditions able to set one off is unlimited.
- Common malicious actions that logic bombs are able to commit include data corruption, file deletion or hard drive clearing.
- Unlike other forms of malware that break into a secure system, logic bomb attacks tend to be cyber sabotage from a person within an organization who has access to sensitive data.
- One way that employees might exact revenge on a company if they believe they might be fired is to create a logic bomb that they diffuse each day, and that they alone are the only ones capable of putting off.
- That way, once they are no longer with the organization, the attack can begin, either instantly or after a predetermined time period.

AMEY TE B 50 Amey

PAGE No.
DATE / /

Rootkit

- A rootkit is a program, more often, a collection of software tools that gives a threat actor remote access to and control over a computer or other system.
- While there have been legitimate uses for this type of software such as to provide remote end user support, most rootkits open a backdoor on victim systems to introduce malicious software such as viruses, ransomware, Keylogger programs or other types of malware or to use the system for further network security attacks. Rootkits often attempt to prevent detection of malicious software by endpoint antivirus software.
- Rootkits can be installed in a number of ways, including phishing attacks or social engineering tactics to trick users into giving the rootkit permission to be installed on the victim system, often giving remote cybercriminals administrator access to the system.
- Once installed, a rootkit gives the remote actor access to and control over almost every aspect of the operating system. (OS).
- Older antivirus programs often struggled to detect rootkits, but most antimalware programs today have the ability to scan for and remove rootkits hiding within a system