COMPUTER ENGINEERING DEPARTMENT

SUBJECT: CRYPTOGRAPHY & SYSTEM SECURITY

COURSE: T.E. **YEAR: 2020-2021** **SEMESTER: VI**
DEPT: COMPUTER ENGINEERING
SUBJECT CODE: CSC604 **EXAMINATION DATE: 09/06/2021**

==========

CRYPTOGRAPHY & SYSTEM SECURITY
ANSWER SHEET

NAME : AMEY MAHENDRA THAKUR

SEAT NO. : 61021145

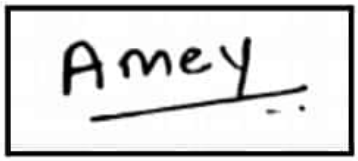
EXAM : SEMESTER VI

SUBJECT : CRYPTOGRAPHY & SYSTEM SECURITY

DATE : 09-06-2021

DAY : WEDNESDAY

STUDENT SIGNATURE:



Q 3

A]

Digital Signature

- Digital Signatures are essential in today's modern world to verify the sender of a document's and his identity.
- A digital signature is represented in a computer as a string of binary digits and computer is using a set of rules and regulations (algorithm) to identify the person signing the document as well as the originality of the data can be verified.
- A digital signature is defined the signature generated electronically from the digital computer to ensure the identity of the sender and contents of the message cannot be modified during transmission process.
- Digital signature techniques achieve the authenticity, integrity and non-repudation of the data over Internet.
- Concept of digital signature is that a sender of a message uses a signing key (Private key) to sign the message and send the message and its digital signature to a receiver over an insecure communication channel.

The receiver uses a verification key (Public key) of the sender only to verify the origin of the message and make sure that it has not been tampered with while in transit.

09-06-2021

STUDENT SIGNATURE: Amey

Signature generation.

Electronic File → Hash Value + Signature's Private key (Encrypt hash using private key) → Digitally signed File

Signature Generation.

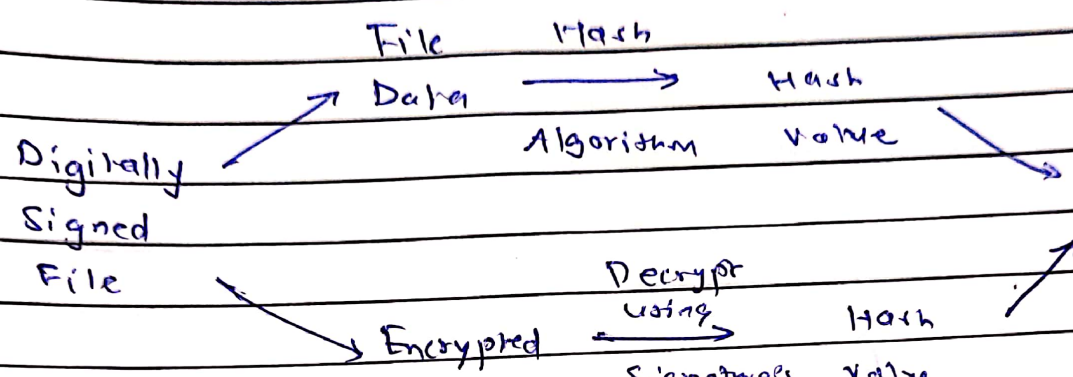
To generate a message signature, the sender follows:

1. Let 'h' be the hashing function & 'm' the message.
2. Generate a random number k, such that $0 < k < q$.
3. Compute $r = (g^k \bmod p) \bmod q$.
4. In the unlikely case that if $r = 0$, start again with different random k.
5. Calculate $s = k^{-1} (H(m) + xr) \bmod q$.
6. In the likely case, if $s = 0$, start again with a different random k.
7. Package the digital signature as $\{r, s\}$.

09-06-2021

STUDENT SIGNATURE: Amey

Signature Verification



Signature Verification.

To verify a message signature, the receiver follows:

1. Let 'h' be the hashing function and 'm' the message.
2. Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
3. Calculate $w = s^{-1} \bmod q$.
4. Compute $u_1 = h(m) * w \bmod q$.
5. Compute $u_2 = r * w \bmod q$.
6. Compute $v = ((g^{u_1}) * (y^{u_2})) \bmod p) \bmod q$.
7. If $v == r$, the digital signature is valid.

STUDENT SIGNATURE: Amey

09-06-2021

Q 3

R]

IDS

- Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alert when such activities are 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 user 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 networks look like as compared to malicious activity.
- Intrusion Prevention Systems also monitors network packets inbound the system to check the malicious activities involved in it and at once send the warning notification.

Classification of Intrusion Detection Systems

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

Detection methods of IDS are:

1. Signature - based method
2. Anomaly - based method.

Ways to classify IDS (Any two)

1. Network Intrusion Detection System (NIDS)

- Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. Thus IDS is placed along a network segment or boundary and monitors all traffic on that segment.

Advantages of NIDS

1. A well placed network-based IDS can monitor a large network.
2. NIDS just listen to a network; it does not interfere in a network.
3. NIDS can be made very secure against attack and made invisible to many attackers.

09-06-2021

STUDENT SIGNATURE: Amey

(2) Host Intrusion Detection System (HIDS)

- A HIDS and software applications (agents) is installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms.
- A Host Intrusion Detection System (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network.
- Host based IDS systems are used to monitor any intrusion attempt on critical server.
- Drawbacks of Host based IDS systems are:

(1) Difficult to analyze the intrusion attempts on multiple computers.

(2) Host-based detection systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations.

(3) HIDS can be disabled by attackers after the system is compromised.

09-06-2021

STUDENT SIGNATURE: Amey

NIDS	HIDS
① Well for sensing attacks from outside.	① Well for sensing attacks from inside.
② Examines packet headers and entire packet.	② Does not understand packet header.
③ Host independent	③ Host dependent.
④ Bandwidth needed	④ Bandwidth free
⑤ Slow down the network that have IDS client installed.	⑤ Slow down the host that have IDS clients installed.
⑥ Senses network attacks as payload is analyzed.	⑥ Senses local attacks before they hit the network.
⑦ Not reasonable for encoded and switches	⑦ Well suited for scrambled and switches organized.
⑧ High false positive rate	⑧ Low false positive rate.

STUDENT SIGNATURE: Amey

09-06-2021

Two ways to detect Intrusion Detection System

Signature-based IDS	Anomaly-based IDS
① Easier to implement	① More complicated.
② Cheaper - DIY	② Mostly commercial solutions.
③ Use patterns of well-known attacks	③ Use statistical measures, heuristics and system features.
④ Cannot detect previously unknown attacks	④ Can detect previously unknown attacks
⑤ The efficiency depends on new-ness of the signature file, its size.	⑤ Efficiency depends on how the IDS evolve itself as the time progresses.
⑥ The number of inaccurate results are very few or none.	⑥ Often generates false alarms (high false positive rate).

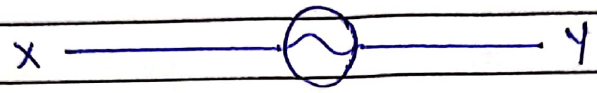
09-06-2021 STUDENT SIGNATURE: Amey

Q3

C]

Man in the middle attack (MIMA/MITM)

- Attacker relays and sometimes alters the communication between two parties without knowing to communicating parties.



Attacker

- It is explained as follows:

(1) X sends a message to Y, which is intercepted by Attacker.:
X " I want to deposit money in your account. Please send account number."

(2) Attacker relays this message to Y; Y cannot tell it is not really from X.

(3) Y receives a message from X and responds it with account number.
Y " My account number is 012345."

(4) Attacker again intercepts a message from Y replaces Y's account number with his own account number and relays this to X, claiming that it is Y's message.

- Attacker " My account number is 067891".:

(1) X receives message from Y and gets the account number of Y. Thus X believes that it is Y's account number and deposits money in that account.

(2) X and Y both think that it is a secure communication.

09-06-2021

STUDENT SIGNATURE: Amey

Flooding Attack

- Flooding attacks have been a standard part of an attacker's toolbox for denying service.
- The basic concept of flooding attack is

(1) either send a massive amount of traffic at a particular server or service with the aim of exhausting all the resources trying to respond to bogus traffic so that it cannot process legitimate requests for service

(2) Or send a massive amount of traffic onto a specific network segment with the goal of creating so much network congestion that legitimate traffic cannot reach the target server or service.

This type of attack isn't specific to UC as the traffic sent onto the network could really be any type.

Examples of flooding attacks are.

(1) ICMP Flood
(2) SYN Flood
(3) UDP Flood

09-06-2021

STUDENT SIGNATURE: Amey

① ICMP Flood

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 request includes the use of convention tools or code, such as bringing hping and scapy.
- This strains both the incoming and outgoing channels of the network, consuming considerable bandwidth and resulting in a Denial of Service

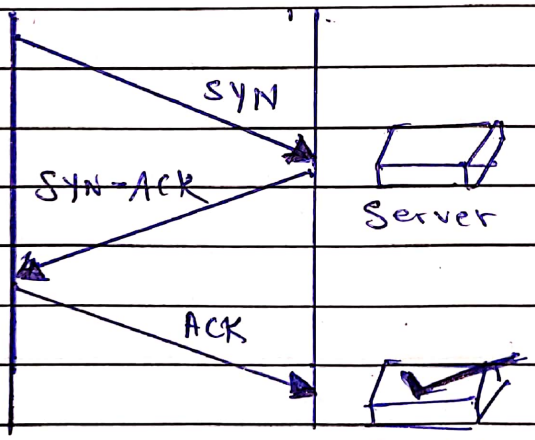
09-06-2021

STUDENT SIGNATURE: Amey

(2) SYN Flood

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



3 way Handshake

3 way Handshake

(1) Client sends synchronized (SYN) packets to server.

(2) Server sends SYN-ACK to client

(3) Client responds back with ACK packet.

09-06-2021 STUDENT SIGNATURE: Amey

③ UDP Flood

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 attack 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.
- 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).

STUDENT SIGNATURE: Amey

09-06-2021