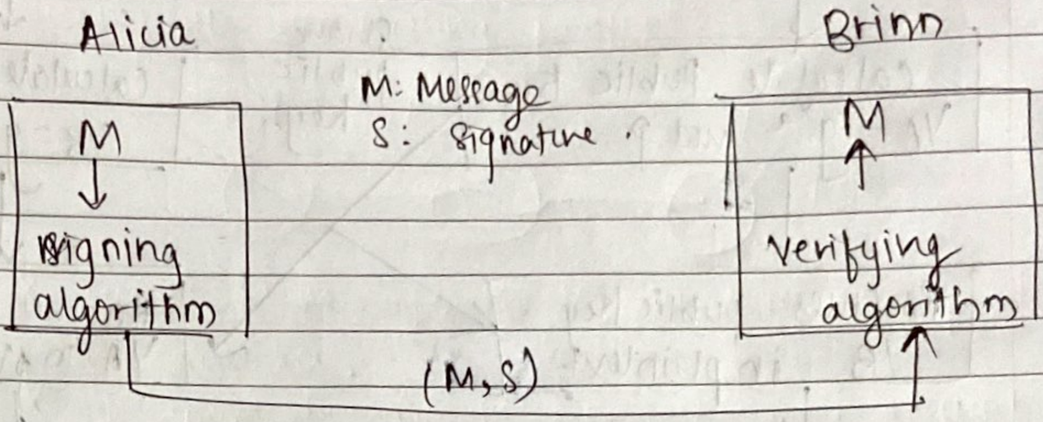
G2020 Repacca CSS
SEM: 06

7/12

Q3]

A]

~~Intrusion Detection systems~~.
Digital signature process /algorithm.



① The sender uses a signing algorithm to sign the message, when we sign the document digitally, we send the signature as a seperate document in all.

② The message and signature are sent to the receiver. The recipient receives them and it needs to apply a verification technique to the combination of the message and the signature to verify the authenticity

③ If the result is true, the message is accepted otherwise it is rejected

④ The signer uses her private key applied to a signing algorithm to sign the document.

⑤ The verifier uses the public key of the signer, applied to the verifying algorithm to

G2020
SEM: 06

Rebecca CSS

8 /12

Q3]

A]

verify the document.

⑥ when a document is signed, anyone receiving the signed document can verify it because everyone has access to sender's public key.

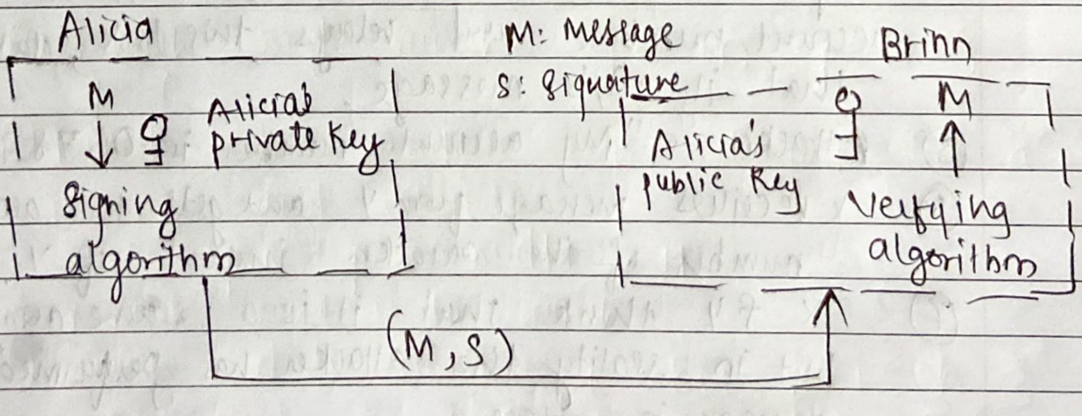
⑦ Sender must not use her public key to sign the document, because then anyone could forge her signature.

⑧ A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key

⑨ A crypto system uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

⑩ There is a one to one relationship between the signature and a message

⑪ Copy of the signed document cannot be distinctinted unless there is a factor of time on the document



G2020 Rebecca DWM
SEM:06

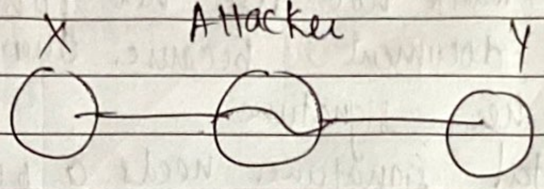
BARFI Page No.
Date

9 / 12

Q3]

C)

Man in the middle attack (MITM / MIMA).
Attacker relays and sometimes alters the communication between two parties without knowing to communicating parties.



① X sends a message to Y, which is accepted by the attacker.
X" I want to deposit money in your account. Send your account number".

② Attacker relays this message to Y; Y cannot tell ~~if X~~ it is not from X.

③ Y receives a message from X and responds it with account number
Y" My account no is 012345"

④ Attacker gain 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.

⑤ Attacker: "My account number is 06789"

⑥ X receives message from Y and gets the account number of the acctacker instead of Y.

⑦ X & Y think that it is a secure communication but in reality the attacker has performed the damage is done.

62020
SEM: 06
Rebecca

CSS

10/12

Q3]

c]

Flooding :

① Once the DDOS network has been setup and the infrastructure for communication between the agents and the handlers is establised, all that an attacker needs to do is issue commands to the agents and start sending packets to the victim host.

② Flood attack occur when the system receives too much traffic for the server to buffer and causing them to ~~flow down~~ slow down and eventually stop

③ Popular flood attacks include ICMP flood, SYN flood, UDP flood.

④ ICMP flood

- Internet control Message protocol is mainly used to determine whether or not data is reaching its intended destination
- commonly, ICMP is used in routers
- Ping flood also known as ICMP flood is when the attacker take down a victim's computer by overwhelming it with ICMP echo requests also known as pings.
- The attackers send large number of echo requests and hence the victims machine starts responding to each ICMP packet by sending an ICMP echo reply packet.
- The victims machine takes twice bandwidth of the attacker once for receiving the packets and once for sending replies causing a delay

Rebecca

11/12

⑤ SYN Flood

- The attacker exploits part of the normal TCP three way handshake to consume resources on the targetted server and render is unresponsive
- First, the client sends a SYN packet to the server in order to initiate the connection
- The server then responds to the initial packet with a SYN/ACK packet in order to acknowledge
- Then client returns an ACK packet.
- In SYN Flood the attacker sends a high volume of SYN packets to the targetted server, often with spoofed IP addresses
- The server then responds to each one of the connection for a certain time and leaves an open port ready to receive the response
- While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new port connection for a certain length of time, one all the available ports have been utilized the server is unable to function normally

⑥ UDP Flood

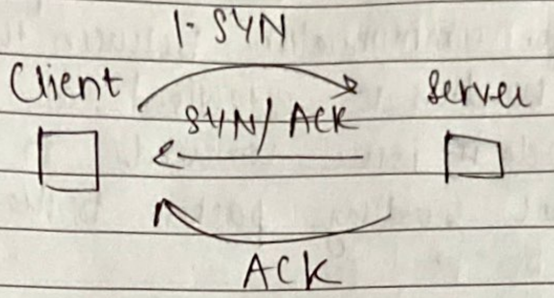
- A huge amount of UDP packets are sent to the victim host. Trinoo is a popular DDoS tool that uses UDP Floods as one of its attack payloads.

G2020
SEM:06 Rebecca [redacted] CSS

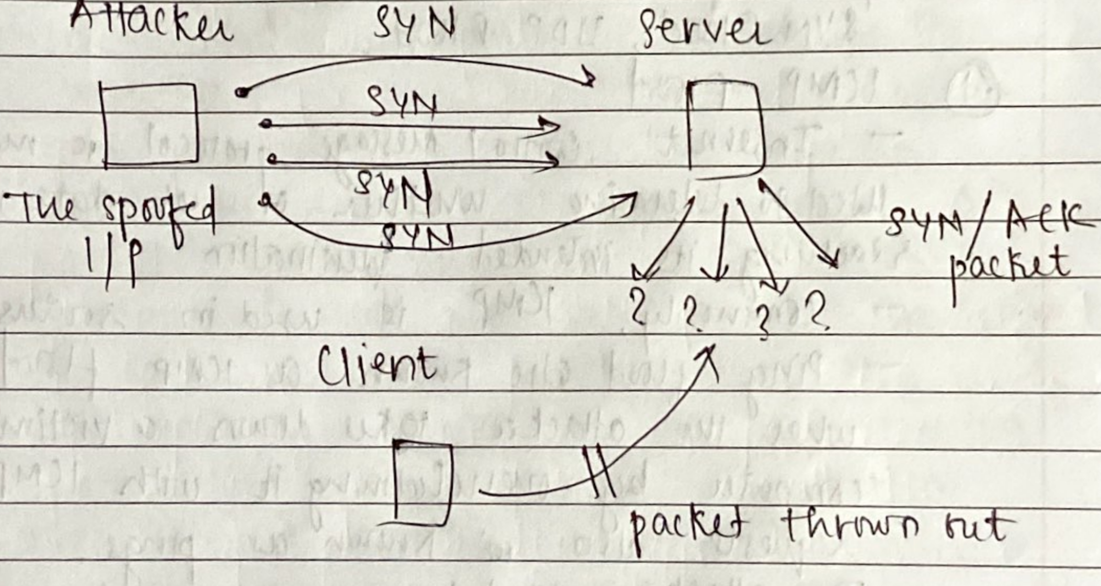
BARFI Page No.
Date

12/12

SYN Flood



SYN Flood Attack


Attacker
SYN
Server
SYN
SYN
SYN
The spoofed
I/P
SYN/ACK
packet
? ? ? ?
Client
packet thrown out