Chapter

4

SPOOFING

What is Spoofing (Pemalsuan)?

- **A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer indicating that the message is coming from a trusted host.**

  (www.webopedia.com)

- **To perform (eg : IP spoofing), a hacker must first use a variety of techniques to find (eg : IP address) of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.**

Types of Spoofing?

There are 3 types of spoofing :

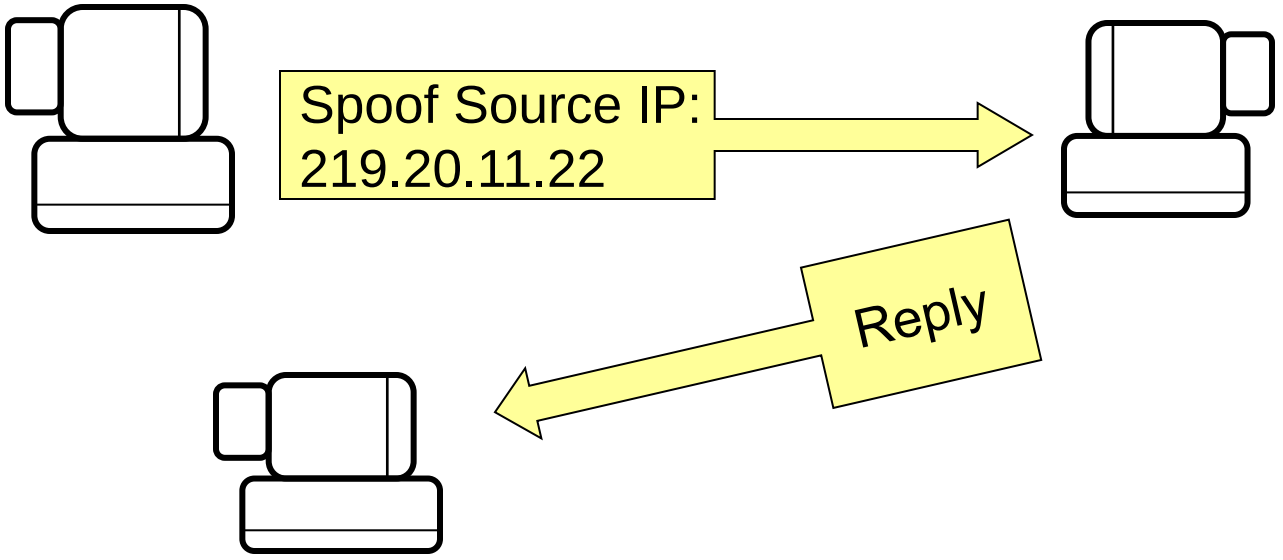
- 1) IP Spoofing
  - Attacker uses an IP address of another computer to acquire information or gain access.
- 2) Email Spoofing
  - Attacker uses the email address of another person
- 3) Web Spoofing
  - Attacker creates a convincing but false copy of the World Wide Web.

IP Spoofing

- IP spoofing is used to gain unauthorized access to a computer.
- The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system.
- Attackers must go through some complicated steps to accomplish the task. They must:
  - Acquire a target
  - Acquire an IP address of a trusted machine
  - Disable communication of the trusted machine (e.g. syn flooding)
  - Sample a communication between the target and trusted hosts
  - Guess the sequence numbers of the trusted machine
  - Modify the packet headers so that it appears that the packets are coming from the trusted host
  - Attempt connection to an address authenticated service or port.
  - If successful, the attacker will plant some kind of backdoor access

IP Spoofing

- When victim replies back to the address, it goes back to the spoofed address, not the attacker's address – Flying Blind.



IP Spoofing

- Flying blind or one-way attack – is an attack where the attacker can only send packets to a machine with a spoofed address, but cannot receive any packets back.

IP Spoofing

- In order to understand IP Spoofing, you must look at the 3-way handshaking used in connection establishment, by the particular case of sequence number
- guessing, one must look at the 3-way handshake used in the TCP open
- sequence [2].

IP Spoofing

3 Types of IP Spoofing:

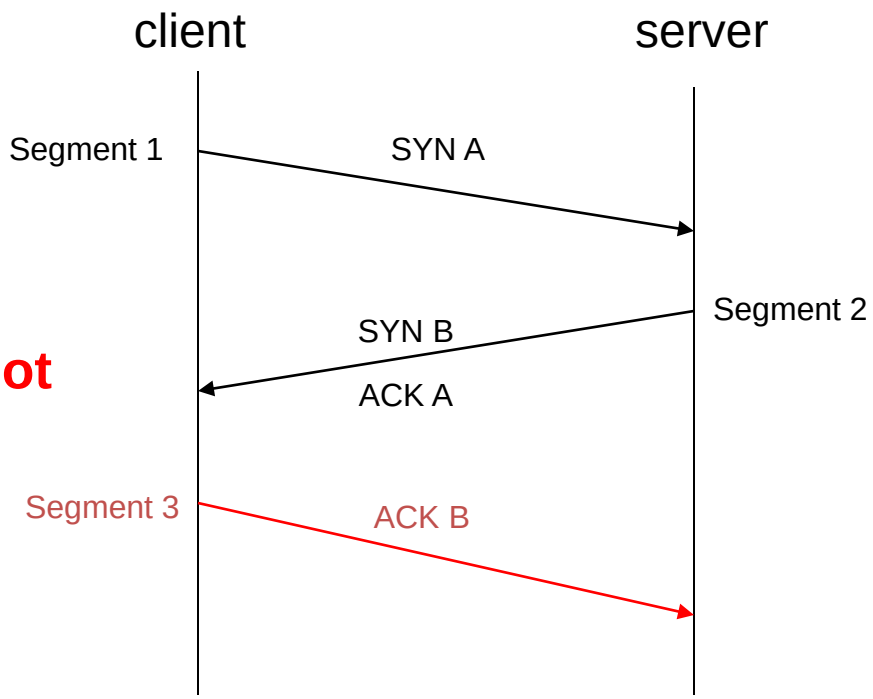
- Basic address change
- Use of source routing to intercept packet
- Exploitation of a trust relationship on a Unix machine.

IP Spoofing - Basic address change

- Attacker go into a network configuration and change the IP address.
- This is a low technique because all replies go back to the address he is spoofing, not to the attacker machine.
- So, a **three-way handshaking (for TCP) cannot be completed**, because the replies go back to a machine that knows nothing about the session.
- But, spoofing the address will makes it harder to trace back to the attacker.

IP Spoofing - Basic address change
3-way handshaking

- Half Open Connection



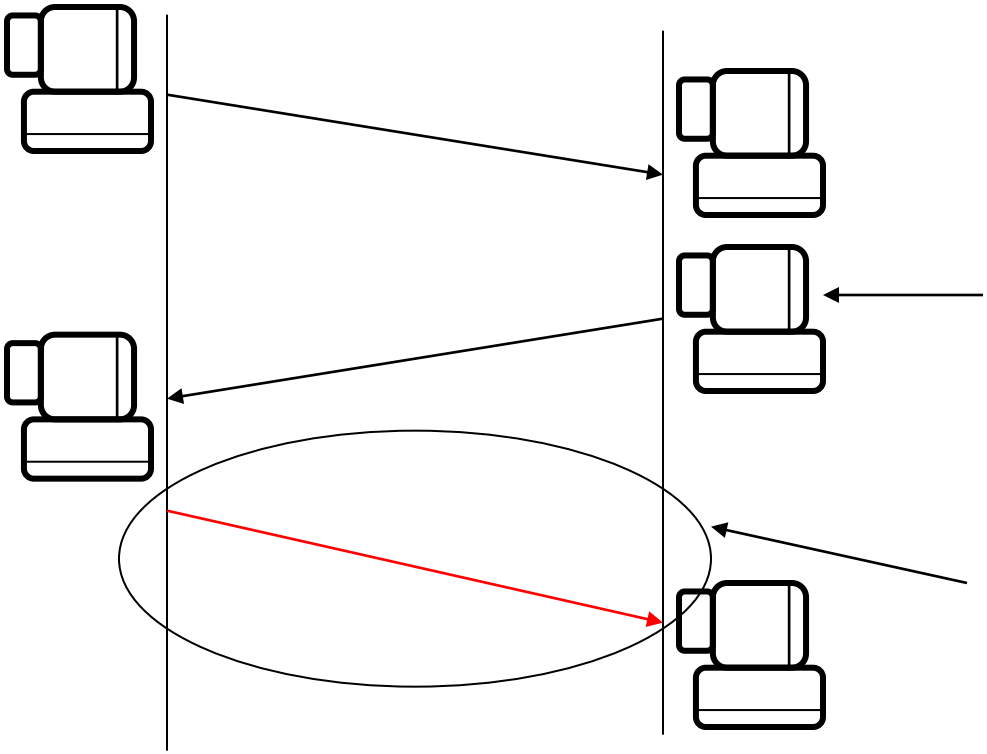
3-way handshaking not complete!

IP Spoofing - Basic address change

- For the UNIX machine, you can just type :

  “ifconfig <interface> x.x.x.x” to change the IP address.

IP Spoofing - Basic address change



IP Spoofing - Basic address change

- Protection :
  - 1) Limit who has access to configuration on a machine. So, you can stop employees from performing spoofing.
  - 2) Apply the basic filters / built-in spoofing filters at router. This filter do not allow any packets that are entering your network from the outside to have a source address from your internal network. So, you can protect your company from being the victim of spoofing.
    - **Ingress filtering** – is the type of filtering that drop the packet if the packet entering your network from the outside AND it is originates from inside your network – to avoid spoofing done to your network.
    - **Egress filtering** - is the type of filtering that drop the packet if the packet leaving your network from the inside AND the source address is not an address from your local network – to avoid spoofing done from your network.

IP Spoofing – Source routing

- Problems with normal spoofing : the traffic goes back to the spoofed address, and attacker never see it.
- How if attacker want to see both sides ?
  - By make sure that a packet takes a set path through the Internet, and it goes through the attacker's machine : Source Routing.

IP Spoofing – Source routing

- Normally IP routing is dynamic - where each router making decision about which path to take, to send packet.
- But, with source routing, sender can specify the route.
- Source routing – is built into the TCP/IP protocol suite. It lets you to specify the path a packet will take through the Internet.

  2 types of source routing :
- 1) Loose source routing (LSR) – Sender specifies a list of IP addresses that the packet must traverse, but the packet can also go through any other addresses that it needs to. U do not care about the exact path the packet takes through the network, as long as it goes through these addresses.
- 2) Strict source routing (SSR) – Sender specifies the exact path that the packet must follow. If the exact path cannot be taken, the packet is dropped, and an ICMP msg is returned to the sender. U care about the exact path the packet must take, and if it cannot take this path for any reason, the packet is not sent.

IP Spoofing – Source routing

- So, only **loose source routing** is suitable to be used.
- Note : If the sender specifies source routing to get to the destination, the destination machine will automatically uses the same source routing to get back to the sender, which is an attacker!

IP Spoofing – Source routing

- Example : Traceroute output of ordinary traceroute to www.newriders.com:
- Type : *Traceroute www.newriders.com*

Output :

Tracing route to scone.donet.com [205.133.113.87] over a maximum of 30 hops ;

1	5ms	4ms	2ms	10.4.0.1
2	5ms	5ms	7ms	208.246.68.97
3	7ms	7ms	7ms	208.246.68.130
4	9ms	11ms	7ms	Loopback0.GW2.DCA1.ALTER.NET [137.39.2.154]
5	7ms	7ms	15ms	105.ATM2-0.XR1.DCA1.ALTER.NET [146.188.161.34]
6	79ms	14ms	14ms	195.ATM9-0-0.GW1.PIt1.ALTER.net [146.188.162.73]
7	67ms	270ms	234ms	oarnet-gw.customer.ALTER.NET [157.130.39.10]
8	45ms	54ms	45ms	dlp1-atm2-0.dayton.oar.net [199.18.202.101]
9	47ms	50ms	46ms	donet2-atm3-0s1.dayton.oar.net [199.18.109.226]
10	49ms	50ms	50ms	scone.donet.com [205.133.113.87]

Trace complete.

IP Spoofing – Source routing

- Example : Traceroute output using loose source routing with an IP address 205.171.24.5 to www.newriders.com:
- Type : *Traceroute –g www.newriders.com 205.171.24.5*

Output :

Tracing route to scone.donet.com [205.133.113.87] over a maximum of 30 hops ;

1	**2ms**	**4ms**	**3ms**	**10.4.0.1**
2	**7ms**	**7ms**	**9ms**	**208.246.68.97**
3	**11ms**	**10ms**	**11ms**	**208.246.68.130**
4	**27ms**	**145ms**	**64ms**	**Loopback0.GW2.DCA1.ALTER.NET [137.39.2.154]**
5	**728ms**	**21ms**	**25ms**	**105.ATM2-0.XR1.DCA1.ALTER.NET [146.188.161.34]**
6	**74ms**	**106ms**	**82ms**	**295.ATM7-0-XR1.DCA8.ALTER.NET [146.188.163.14]**
7	**33ms**	**54ms**	**43ms**	**189.ATM7-0.BR1.DCA8.ALTER.NET [146.188.162.209]**
8	**136ms**	**60ms**	**150ms**	**wdc-brdr-03.inet.qwest.net [205.171.4.69]**
9	**768ms**	**14ms**	**32ms**	**wdc-core-03.inet.qwest.net [205.171.24.69]**
10	**69ms**	**126ms**	**81ms**	**wdc-core-02.inet.qwest.net [205.171.24.5]**
11	**101ms**	**47ms**	**110ms**	**wdc-core-01.inet.qwest.net [205.171.24.1]**

:

IP Spoofing – Source routing

- At step 8, the packet took different path.
- The packet went through the IP address that specified earlier.
- So, loose source routing can be use for spoofing.
- An attacker sends a packet to the destination with a **spoofed address** but specifies **loose source routing** and puts his IP address in the list. Then, when receiver responds, the packet goes back to the spoofed IP address, but after it goes through the attacker's machine.
- So, with source routing, attacker is not 'flying blind' because he can see both sides of the conversation.

IP Spoofing – Source routing

- Protection :
  - 1) Disable source routing at your routers. If your router blocks all traffic that has source routing specified, an attacker cannot launch this type of attack.

IP Spoofing – Trust relationships

- Mainly in UNIX, machines can set up trust relationships to make it easier to move from machine to machine.
- If a user authenticated by one server and that server has a trust relationship with other servers, the user can move freely between the servers w/o re-authenticating (does not have to re-type password).
- So, what attacker can do : Attacker knows that server A trusts anyone coming from machine Y (IP address = 10.10.10.5). He then spoofs his address to 10.10.10.5, and he is allowed access without a password, because he is trusted.

IP Spoofing – Trust relationships

- Protection :
- 1) Do not use trust relationships
- 2) Limit who has a trust relationship
- 3) Do not allow trust relationships to be used via the Internet

Email Spoofing

Is done for 3 main purposes :

- 1) Attacker wants to hide their identity
  - He does not want the receiver know the email came from him
- 2) Attacker wants to impersonate someone or get someone else in trouble, he can spoof that person's email.
  - Whoever receives the email will think it came from the person the attacker is impersonating, and will blame that person.
- 3) Attacker used email spoofing as a form of social engineering
  - He spoofs his email address so that you think his request (eg: confidential files) come from your boss.

Email Spoofing

3 basic ways / types to perform email spoofing :

- 1) Similar email address
- 2) Modify mail client
- 3) Telnet to port 25

Email Spoofing

1) Similar email address
   - Attacker register an email address that look similar to someone's name (eg: your boss). He then request confidential information from victim.
   - When victim reply the email with information as requested, the attacker will get the information he wants.

Email Spoofing

Protection :

- Educate the user that email is not a secure communication.
- Implemented policies : that any work-related activities have to use work email, rather than external email.
- Use a public key encryption : sender attached a digital signature, which is signed with his private key, and you can encrypt with his public key – so you can assume the message came from him.

Email Spoofing

2) Modifying a mail client

- When email sent from user, there is no authentication or validation of “is the sender is the true sender?”
- So, if attacker use email client (eg : Eudora, Out), he can go at the ‘From line’ and type in any address he wants to appear in the ‘From line’, but the reply goes back to the real address not to the person spoofing.

Email Spoofing

Protection :

- Create and enforce an email policy, where termination of employee is the solution.
- Make sure logging features is performed on all systems, especially mail server to find out who is using email spoofing.

Email Spoofing

3) Telnet to port 25

- More complicated technique is to telnet to port 25 on a mail server.
- Protocol used on port 25 = Simple Mail Transfer Protocol (SMTP)
- SMTP is used by email server to send email across the Internet.
- How attacker send email ?
  - Attacker compose a message
  - Attacker send to his mail server
  - His mail server (A) contacts receiver's mail server (B) (port 25)
  - A transfers the message to B.
  - Receiver's mail server (B) forwards the message to the receiver.

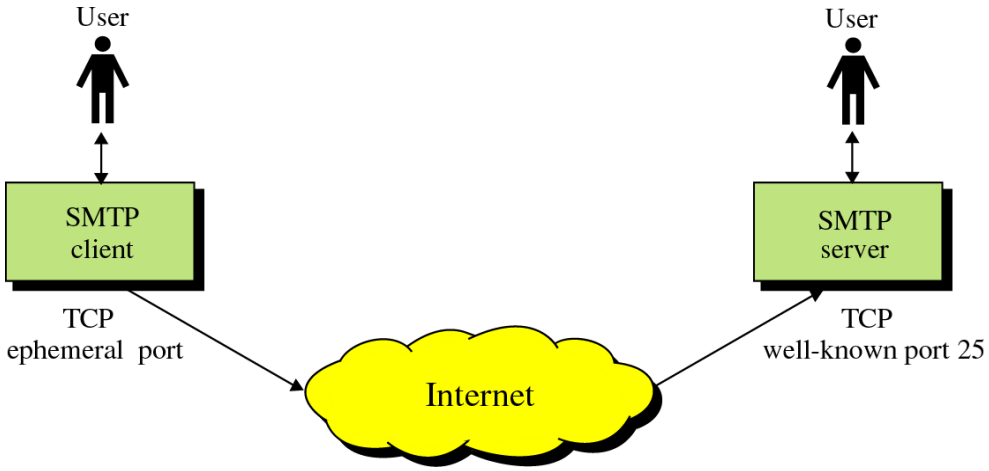
Email Spoofing

SMTP Concept

SMTP – the TCP/IP protocol that supports email on the Internet.

Email exchange needs SMTP client and SMTP server to communicate.

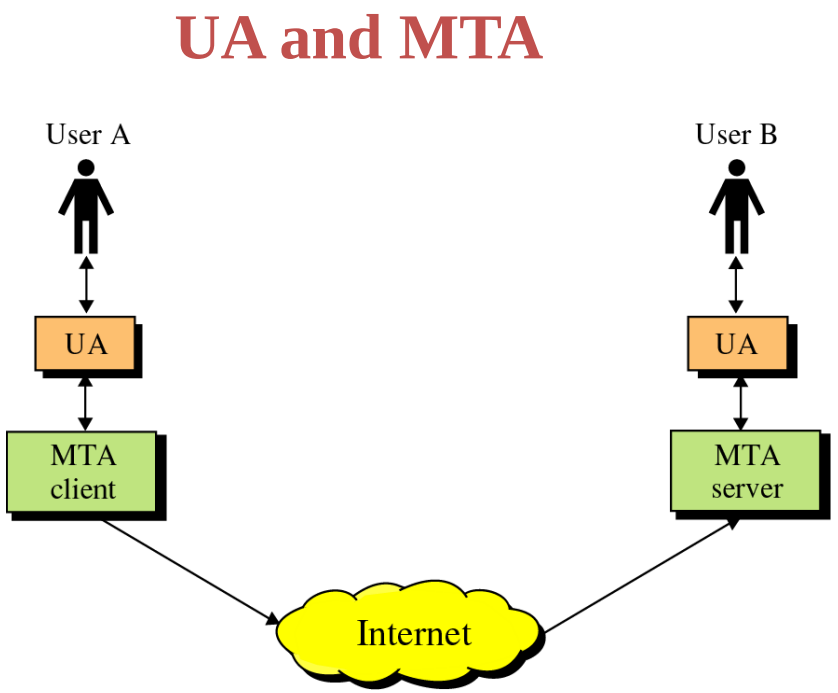
SMTP server uses the well-known port = 25.



Email Spoofing

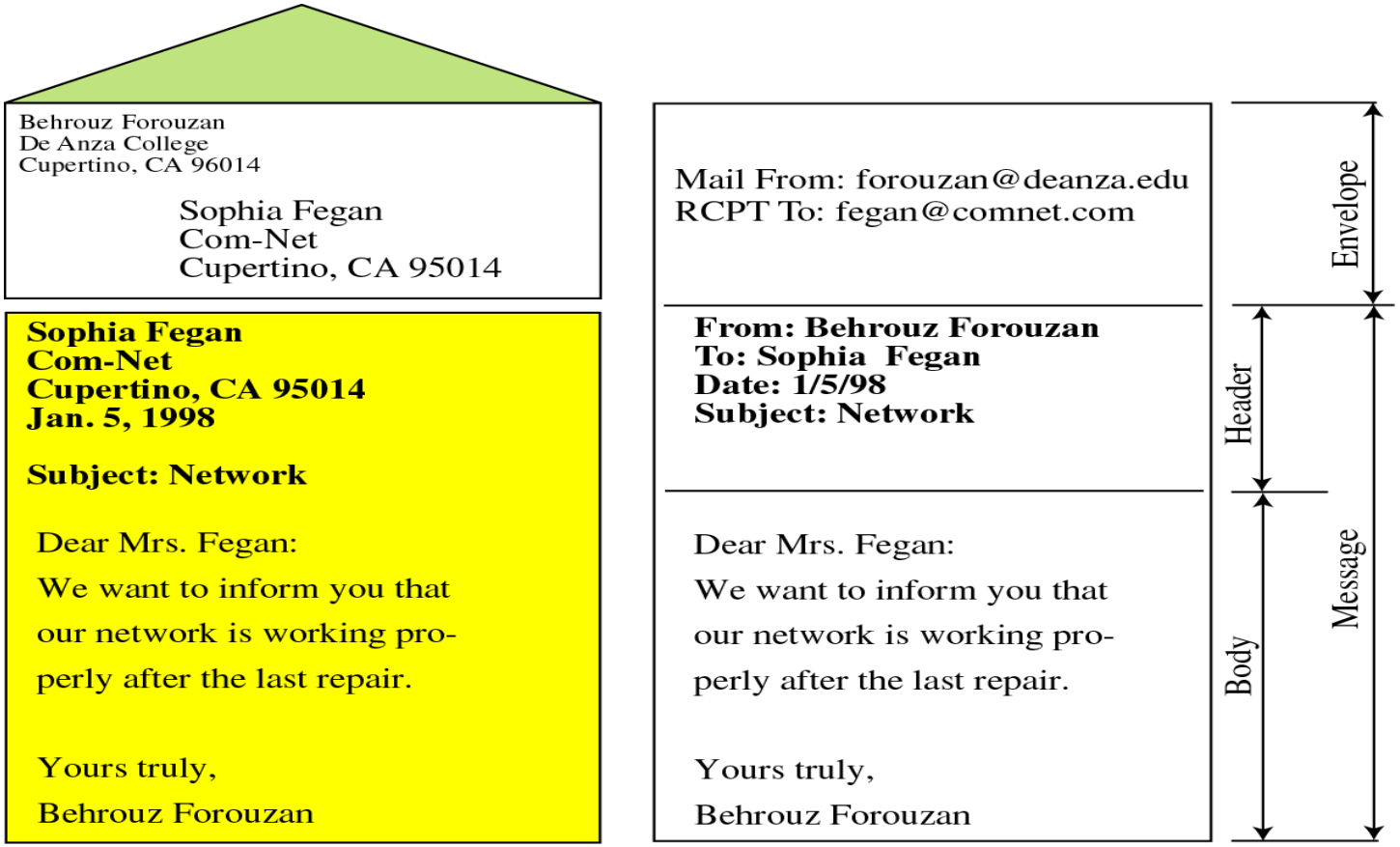
Both SMTP client and SMTP server has 2 components :

- 1) User agent (UA) – prepares the message, creates the envelope, and put the message in the envelope.
- 2) Mail transfer agent (MTA) – transfers the mail across the Internet.



Email Spoofing

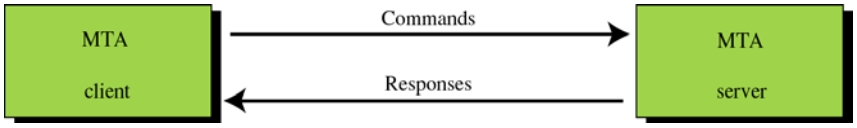
Format of an email



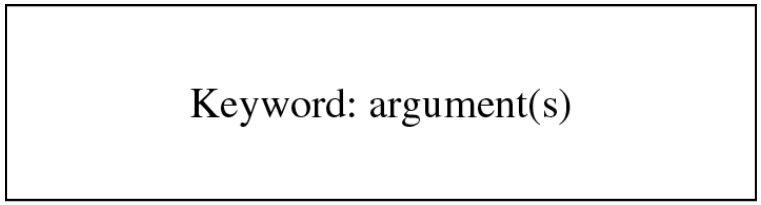
Email Spoofing

Commands and responses

SMTP uses **commands** and **responses** to transfer messages between an MTA client and MTA server.



Command format

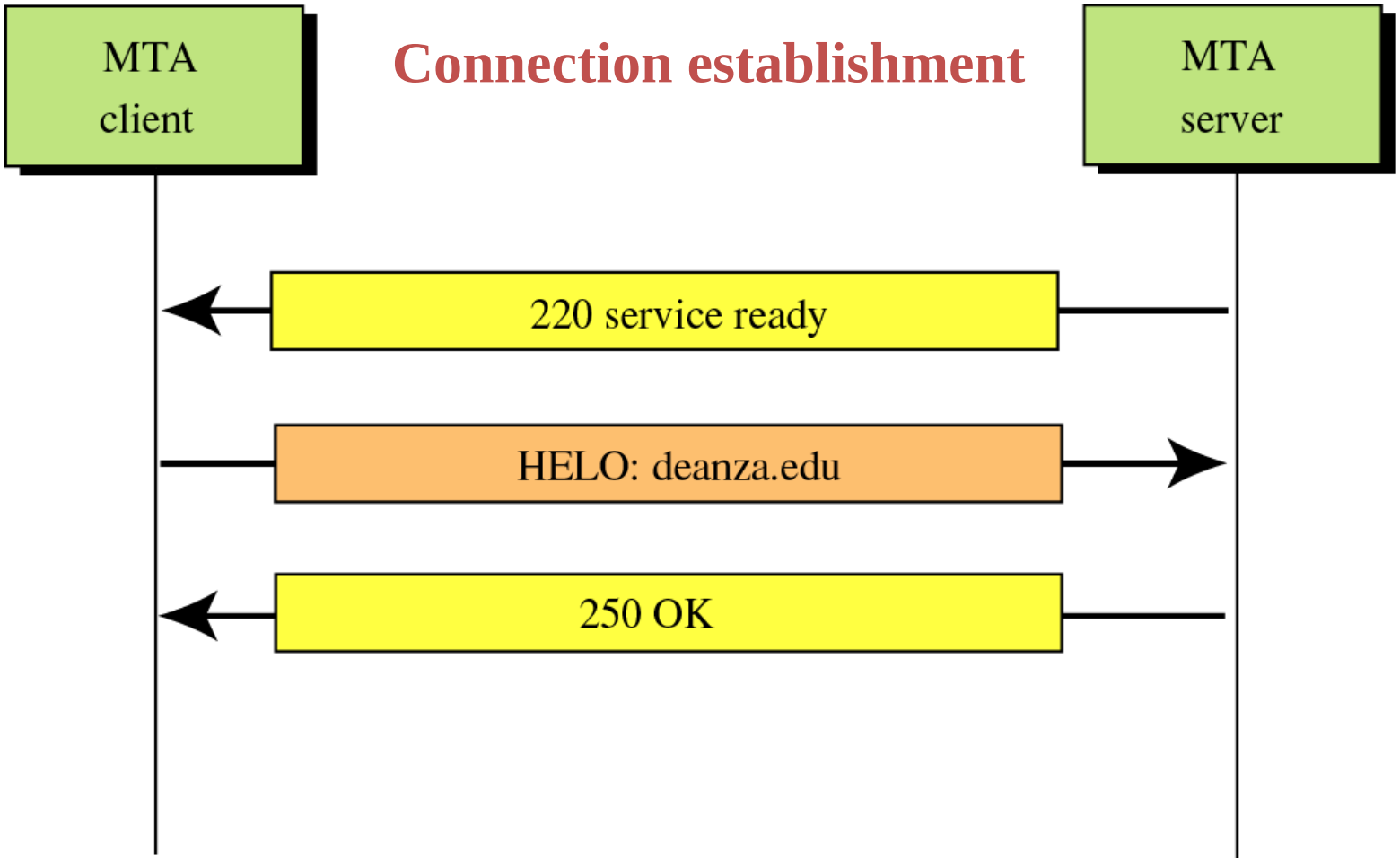


Email Spoofing

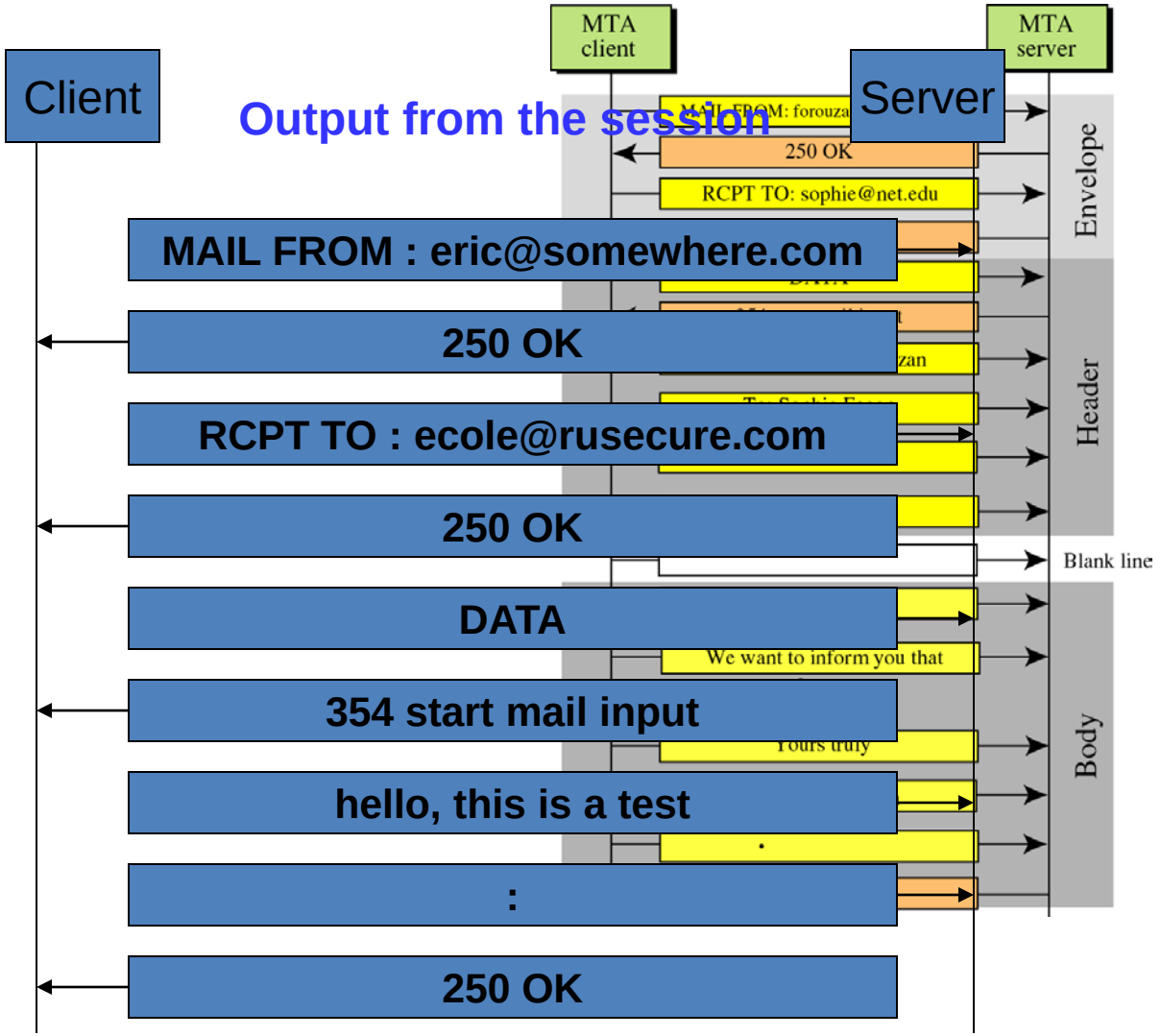
Example of Commands

Keywords	Arguments
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Receiver of the message
DATA	Body of the mail
QUIT	.

Email Spoofing



Email Spoofing



Email Spoofing

- So, the message was sent to the receiver with the spoofed “From address”.
- System administrator then realize that attackers are using their systems for spoofing, so new email servers do not allow relaying.
- A mail server should only being sending or receiving mail for a specific domain name or company.
- **Mail relaying** = a technique where attacker tries to use a mail server to send mail to someone else on a different domain or relay his mail off of another mail server.

Email Spoofing

Other methods to attack?

- Attacker can runs his own mail server. But, it can be trace back! Because attacker IP address is in the mail header.
- Attacker can uses a program to overwrite the IP address with garbage data, so that the IP address of the spoofed mail server could not be viewed. But, it can only be done if the user do not apply a patches to the mail server.
- Setup a virtually mail server on any OS. Program called 'Phasma' (http://www.8th-wonder.net) for windows is used to perform mail spoofing. Just keyed-in the mail server, To, From, Subject, data and send.

Email Spoofing

Protections :

- Always validate that receiver's domain is the same domain as the mail server, if it is not, message is dropped.
- Also validate that the sender's domain is valid.
- Use new SMTP serves that capable to validate for any remote connection on the mail server that the 'To' and 'From' addresses are from the same domain as the mail server. If not, the message is dropped.
- This is to avoid attacker from connect remotely and send a message to someone within the company from a spoofed address.

Email Spoofing

Protections :

- Have all the latest patches installed on your mail server
- Attackers cannot spoof your email from the outside. So, make sure your spoofing and relay filters are properly configured. Because the filters check each mail message and make sure that the ‘To’ and ‘From’ addresses are the **same domain** as the one that email servers resides on.
- **But attacker can still spoofing an internal user A, and sending it to an internal user B.**

Web Spoofing

1) Basic web spoofing

- **Registered and owned a domain name is a first come and first served concept. It is a trend to give your domain name, the same as your company's name.**
- **People don't like / don't bother to look at the URL while browsing Internet.**

Example :

- **Mr Eric Cole is a businessman. He wants to develop his own online website to sell his products. He would like to choose the url as : www.eric.com.**
- **But, the url had been used by someone else (Mr Eric Hote).**
- **So, what can be done by Mr Eric Cole?**

Web Spoofing

- What can be done ?
- 1)Request Mr Eric Hote to sell the url www.eric.com to him OR
- 2) Request Mr Eric Hote to include a link on his website that says : *If you looking for Eric Cole's Company, click here*, and it takes the user to the Eric Cole's website : www.ericcompany.com
- Does Eric Hote can be trusted?

Web Spoofing

Phishing

- The act of sending email to a user falsely claiming to be an established legitimate enterprise in an attempt to get the user into giving private information that will be used for identity theft.

Web Spoofing

Protection for web spoofing :

- 1) Sites must use a server-side certificates because it is harder to spoof. The purpose of the certificate : to ensure that the site you are connecting to is really belong to the company you are expecting.
- A server-side certificate is a certificate that the server presents to a client to prove they are who they say they are. Like a driving licensed.
- 2) Educate users to always look at the url to help them realize where they are browsing.

Web Spoofing

- 2) Man-in-the-middle attacks
- Can be used for all different types of exploits.
- MITM – attacker has to position himself so that all traffic coming and going to the victim goes through him.

Scenario 1 :

  - Attacker intercept and modify the traffic
  - User connect to an e-commerce site, and order 1 book. Attacker intercept the traffic and modify the amount to 100 books.

Web Spoofing

Scenario 2 :

- You send an email to your client to tell him that you would like to meet the client at 2 PM on Wednesday. Attacker then intercept and modify the traffic between you and your client, and change the date and time to Tuesday on 4 PM, and send it to your client.
- So, you think the meeting is on Wednesday at 2 PM and your client think the meeting should be held on Tuesday at 4 PM.

Web Spoofing

Scenario 3 : Act as a proxy

- A proxy – is a system that sits between 2 computers that are communicating and, opens a separate connection between each systems.
- So, attacker passing all information between the victim and the receiver of the communication.
- Example : Computer A and B were communicating through a proxy. So, Computer A would open a connection to the proxy, and the proxy would open a second connection to Computer B.
- So, if you encrypt the traffic, the attacker can still read it because the traffic is being encrypted between the victim and the attacker, and the attacker and the receiver. So, there are actually has 2 encrypted traffic instead of one.

Web Spoofing

Scenario 4 : replay attack

- Attacker records all the traffic between a user and a server, including authentication information, and requests for data.
- So, next time, the attacker sends the same traffic or replays it back to the server to impersonate that user and gain access.

Web Spoofing

Protection :

- If the attacker just reading your traffic, it is ok to use an encryption.
- But, for the attacker that acts like a proxy, encryption does not help because you have 1 connection to the attacker, and the attacker has a separate connection to the receiver. So, the attacker can : un-encrypt the traffic, read, modify, and re-encrypt it, for the receiver.
- Both sites (sender and receiver need a strong security perimeter)