

# Introduction to Network Security

## Chapter 9

### Email

# Email Topics

- SMTP
- POP & IMAP
  - Protocol
  - Vulnerabilities and countermeasures
- MIME
  - Vulnerabilities and countermeasures
- General Email Countermeasures

# Email

Simple Mail Transfer Protocol:

First we will look at Electronic Mail systems in general and then we will look at SMTP. A basic electronic mail system performs four functions:

Creation: A user creates and edits a message, generally using a rudimentary editing capability. Most systems also allow the user to create a message using the system editor or a word processor, and then incorporate the resulting file as the body of the message.

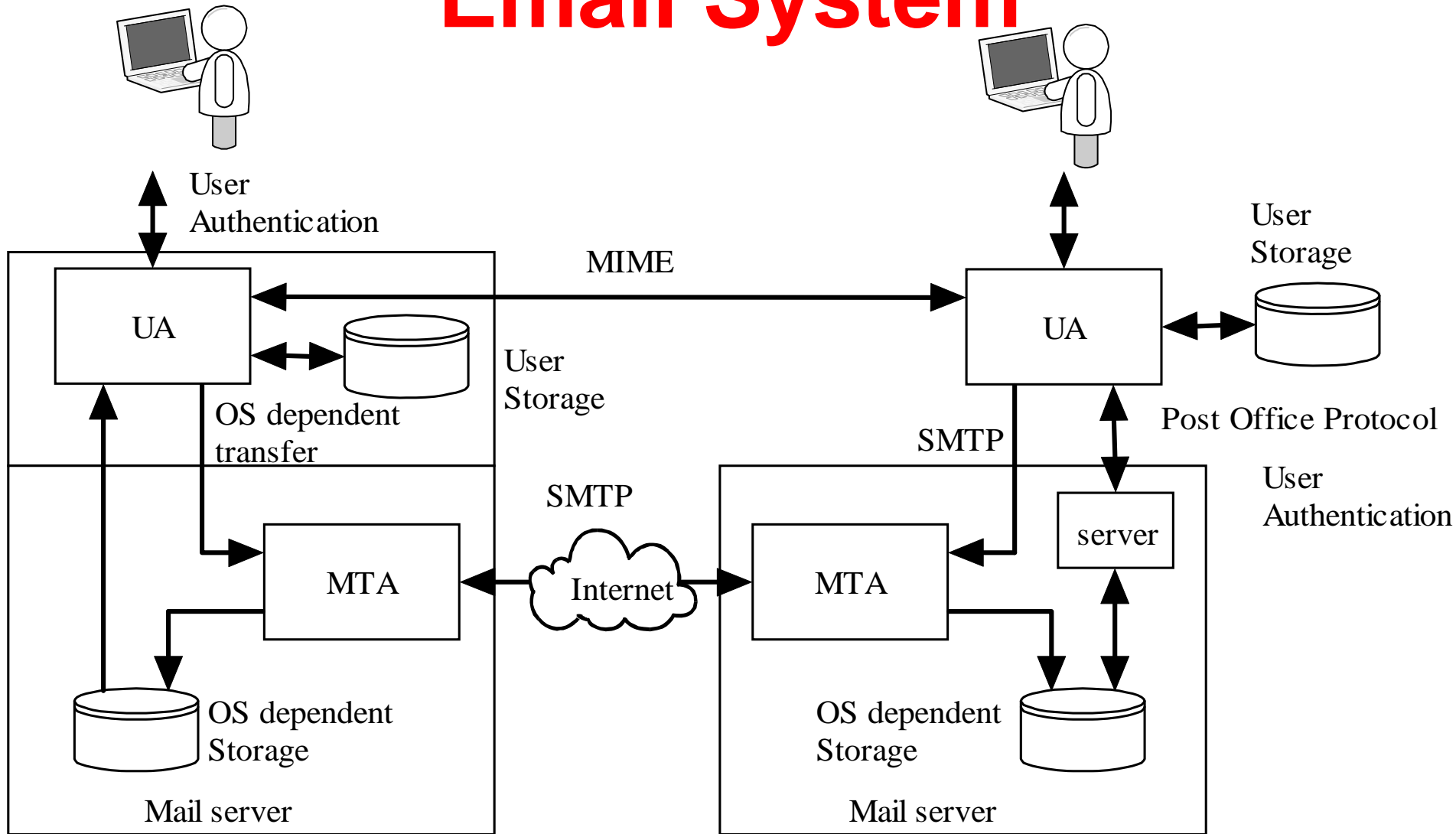
# Email

**Sending:** The user designates the recipient (or recipients) of the message, and the facility stores the message in the appropriate mailbox(es)

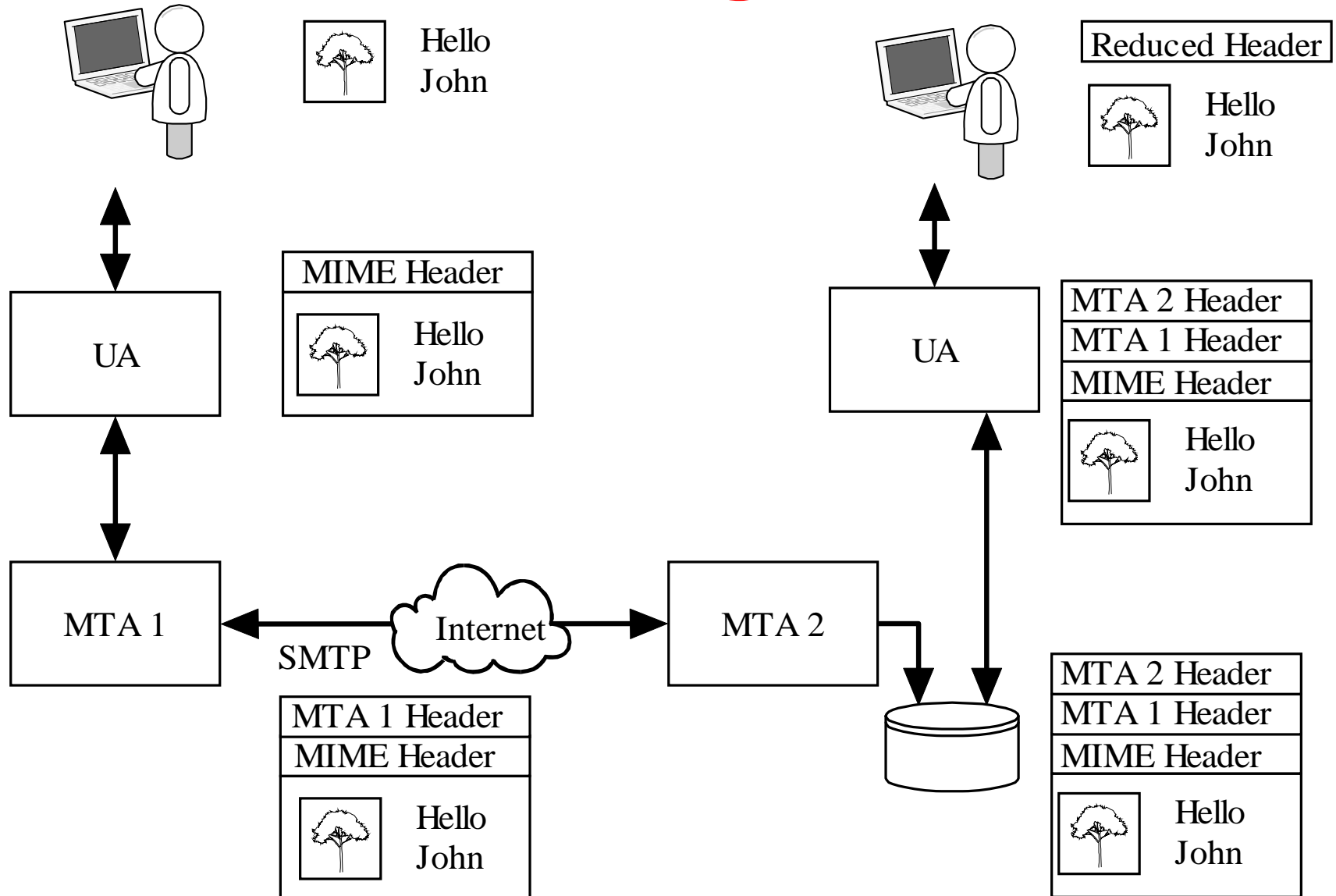
**Reception:** The intended recipient may invoke the electronic mail facility to access and read the delivered mail

**Storage:** Both sender and recipient may chose to save the message in a file for permanent storage

# Email System



# Email Message Format



# Email

The SMTP protocol is the standard protocol for transferring mail between hosts. The protocol was defined in RFC 821 and later formalized as MIL-STD-1781.

SMTP is not concerned with the format or content of the messages themselves, with two minor exceptions.

SMTP requires a 7 bit ASCII character set.

SMTP adds logging information to message that indicates the path the message took.

# Email

The SMTP protocol attempts to provide reliable operation, but does not guarantee to recover from hosts that lose files. No end-to-end acknowledgment is returned to a message's originator when a message is successfully delivered, and errors are not guaranteed to be returned either. However, the mail system is sufficiently reliable that this is not an issue.

In most cases mail goes directly from the mail originator's machine to the destination machine. However, mail will occasionally go through intermediate systems.

The SMTP protocol is made up of a set of simple commands.



# Email

SMTP has 14 commands.

Command syntax is a set of 4 letter commands with parameters  
Not all commands need to be implemented

The commands are:

CMD Syntax	Action
------------	--------

HELO <domain>	Used by the sending system to identify itself (HELO eeclass.ee.iastate.edu)
---------------	--

# Email

CMD Syntax      Action

**MAIL FROM: <path>**      Identifies who the message is from.  
(MAIL FROM doug@iastate.edu)  
error messages have a NULL from field  
to prevent answers.

**RCPT TO: <forward path>**      Identifies who the message  
should be mailed to. There is  
separate RCPT for each  
recipient.

# Email

CMD Syntax	Action
<b>DATA</b>	Indicates that the next transmission contains the message text. Terminated with a line containing <CR LF>.<CR LF>
<b>RSET</b>	Terminate current transaction
<b>SEND FROM: &lt;path&gt;</b>	Used instead of MAIL if message should be displayed on user's terminal.

# Email

CMD Syntax	Action
<b>SOML FROM: &lt;path&gt;</b>	(Send or Mail) Used instead of MAIL if message should be mailed or displayed on user's terminal.
<b>SAML FROM: &lt;path&gt;</b>	(Send And Mail) Used instead of MAIL if message should be mailed and displayed on user's terminal.
<b>VERFY &lt;string&gt;</b>	Returns to the sender the full name of the user specified in the parameter
<b>EXPN &lt;string&gt;</b>	Returns to the sender a list of mailboxes corresponding to the alias provided

# Email

CMD	Syntax	Action
<b>NOOP</b>		Performs no actions: returns a "250 OK" for debugging
<b>QUIT</b>		Sent after completion of transfer, prior to closing TCP connection.
<b>TURN</b>		Reverses the role of SMTP sender and receiver.

A reply code is returned for each command sent. The next slide shows the reply code format.

# Email

The reply codes are designed to make implementation of SMTP easier.  
Each digit of the three digit code has a unique purpose.

First digit specifies whether the response was good, bad, or or incomplete.

The second digit specifies what type of error occurred.

The third digit details specific failures.

The values for the codes are given on the next slide.

# Email

- 1XX Positive Preliminary Reply - The command has been accepted, but the receiver requires more information. (not used by SMTP, used by other protocols)
  
- 2XX Positive Completion Reply - The requested action has been successfully completed. A new request may be initiated.
  
- 3XX Positive Intermediate Reply - The command has been accepted, but action is being held, pending receipt of further information. The SMTP sender should send another command specifying this information.

# Email

4XX Transient Negative Completion Reply - The command was not accepted, however, the error condition is temporary

5XX Permanent Negative Completion Reply - The command was not accepted.



# Email

- X0X Syntax Error or unimplemented commands
- X1X Information: reply to requests for information
- X2X Connections - reply to the request for connection
- X3X Unspecified
- X4X Unspecified
- X5X Mail System - indicates the status of the receiver during, for example, a transfer.

The next slide has come common reply codes.

# Email

- 211 System status or system help reply
- 214 help message
- 220 service ready
- 221 Service closing transmission channel
- 250 Requested mail action okay, completed
- 251 User not local; will forward to <forward path>
- 354 Start mail input
- 421 Service not available; closing channel
- 450 Mail box busy
- 451 requested action terminated; local error in processing
- 452 Requested action not taken; insufficient system storage

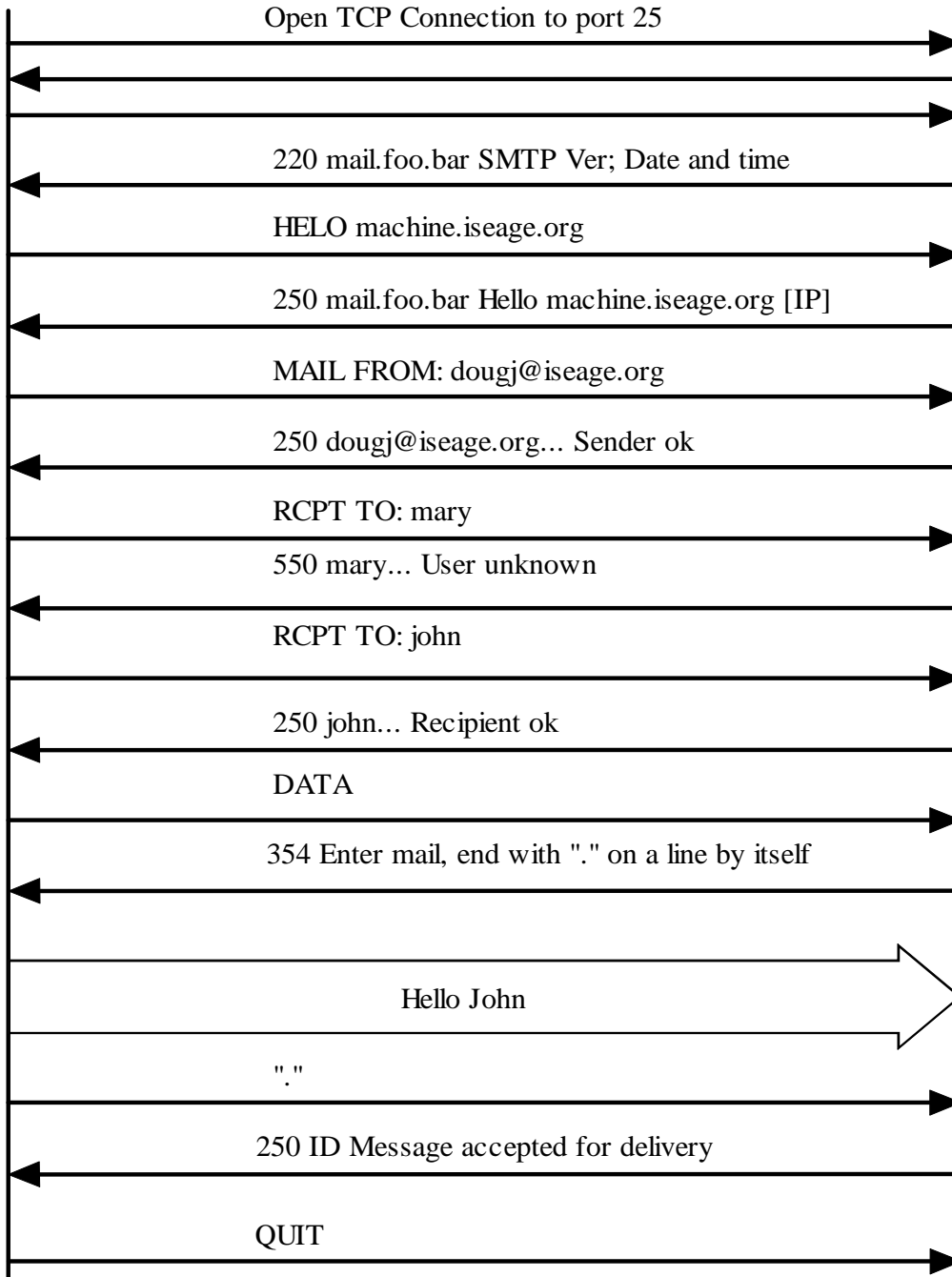
# Email

- 500 Syntax Error, command unrecognized
- 501 Syntax Error in parameters or arguments
- 502 Command not implemented
- 550 mailbox not found
- 551 user not local; please try <forward path>
- 554 transaction failed

SMTP  
Client

SMTP  
Server

# SMTP



# Header based

- Not common
- Some buffer overflow issues in old implementations

# Protocol Based

- Not common in command/response protocols
- Out of order commands are reported back as errors
- Multiple open connections could limit access to the email server.

# Authentication Based

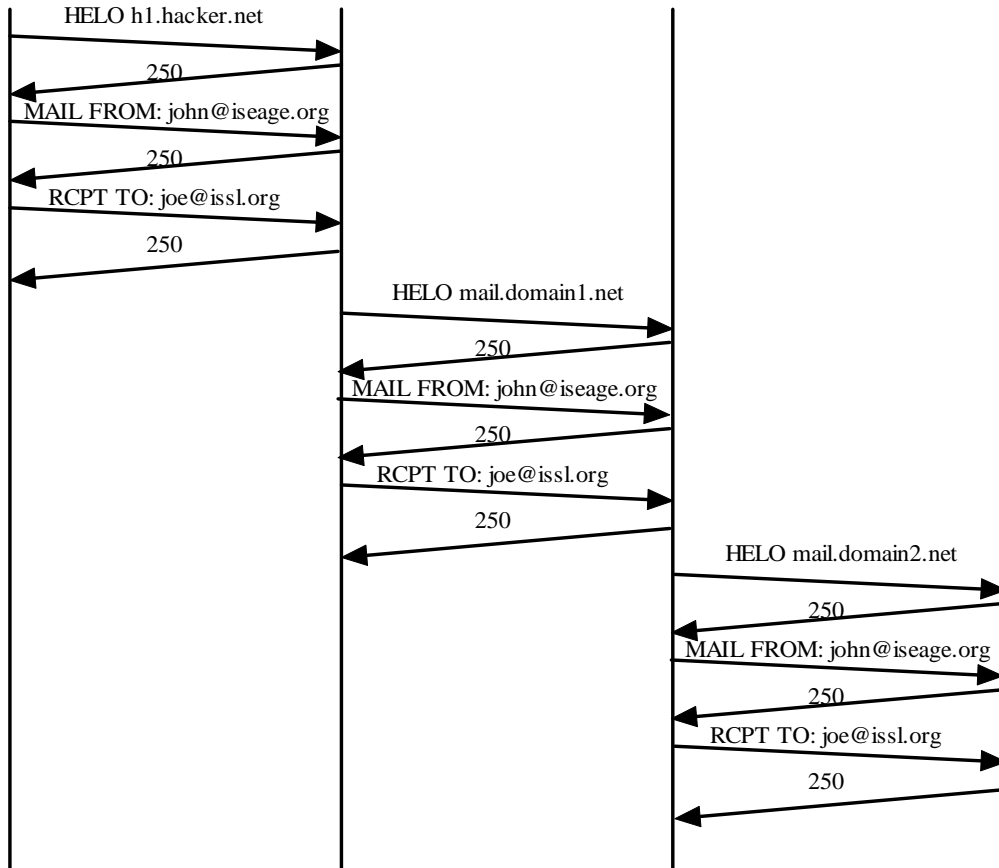
- Most common attack
- No authentication in SMTP
- Sender tells MTA the name of the sender
- Spam and phishing attacks
- Sometimes we want to spoof the senders address (email relay)

Client - UA  
h1.hacker.net

MTA 1  
mail.domain1.net

MTA 2  
mail.domain2.net

MTA 3  
mail.domain3.net



# Email Address Propagation

UA Header
Mail Message

MTA1 Header
UA Header
Mail Message

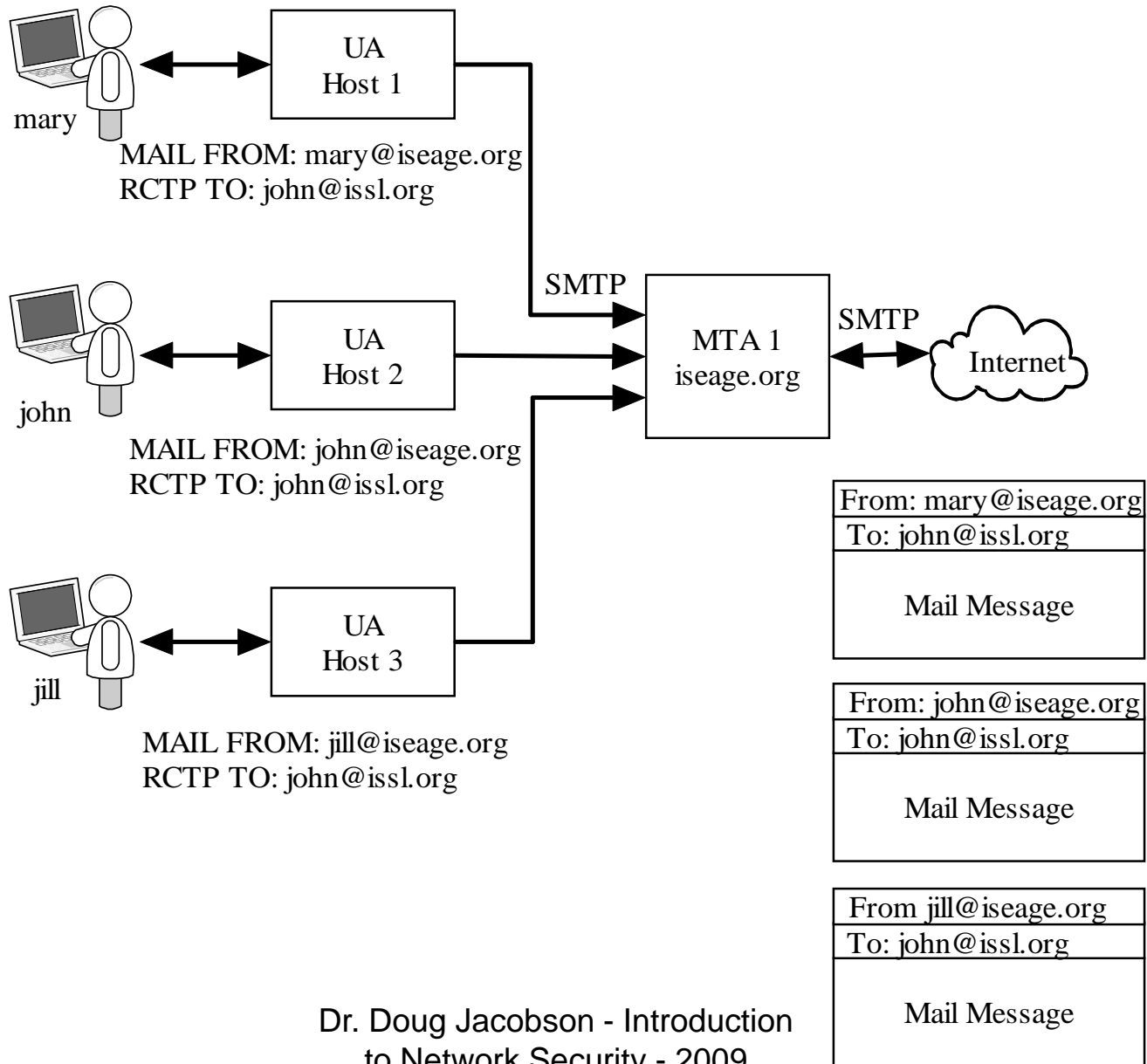
MTA 2 Header
MTA 1 Header
UA Header
Mail Message

MTA 3 Header
MTA 2 Header
MTA 1 Header
UA Header
Mail Message

Dr. Doug Jacobson - Introduction to Network Security - 2009



# Email Relay

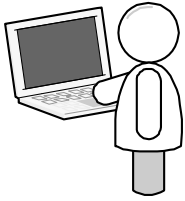


# Traffic Based

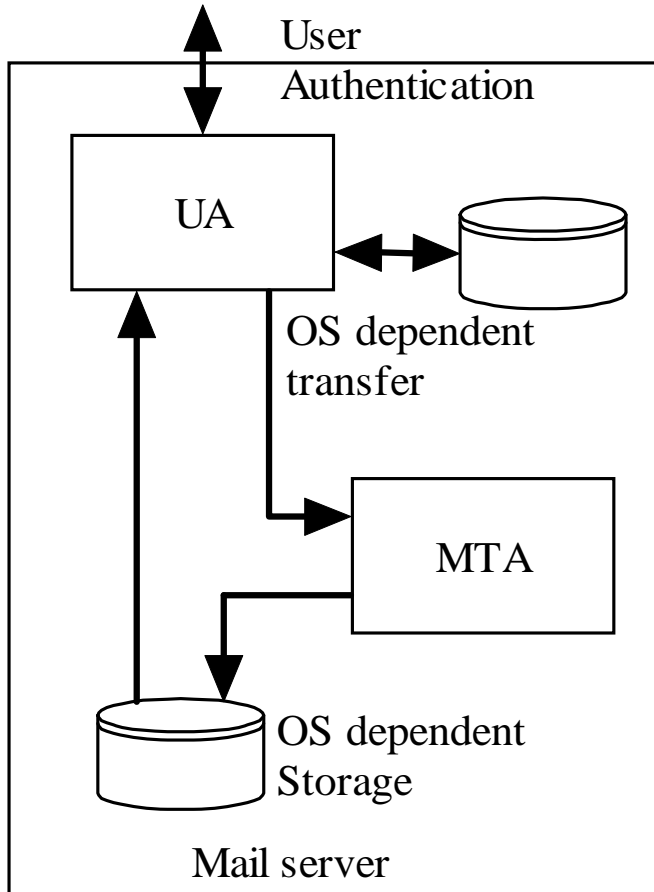
- Flooding of the email server
  - Too many messages
  - Messages are too large
  - Sending email to B from A with C as the return address could cause an attack on C
- Sniffing

# General Countermeasures

- STARTTLS cause SMTP to use transport layer security (encrypted traffic)
- AUTH provides a method for users to authenticate with the MTA.
- Typically used for remote access to MTA for relaying
- Being discussed as a method to reduce spam

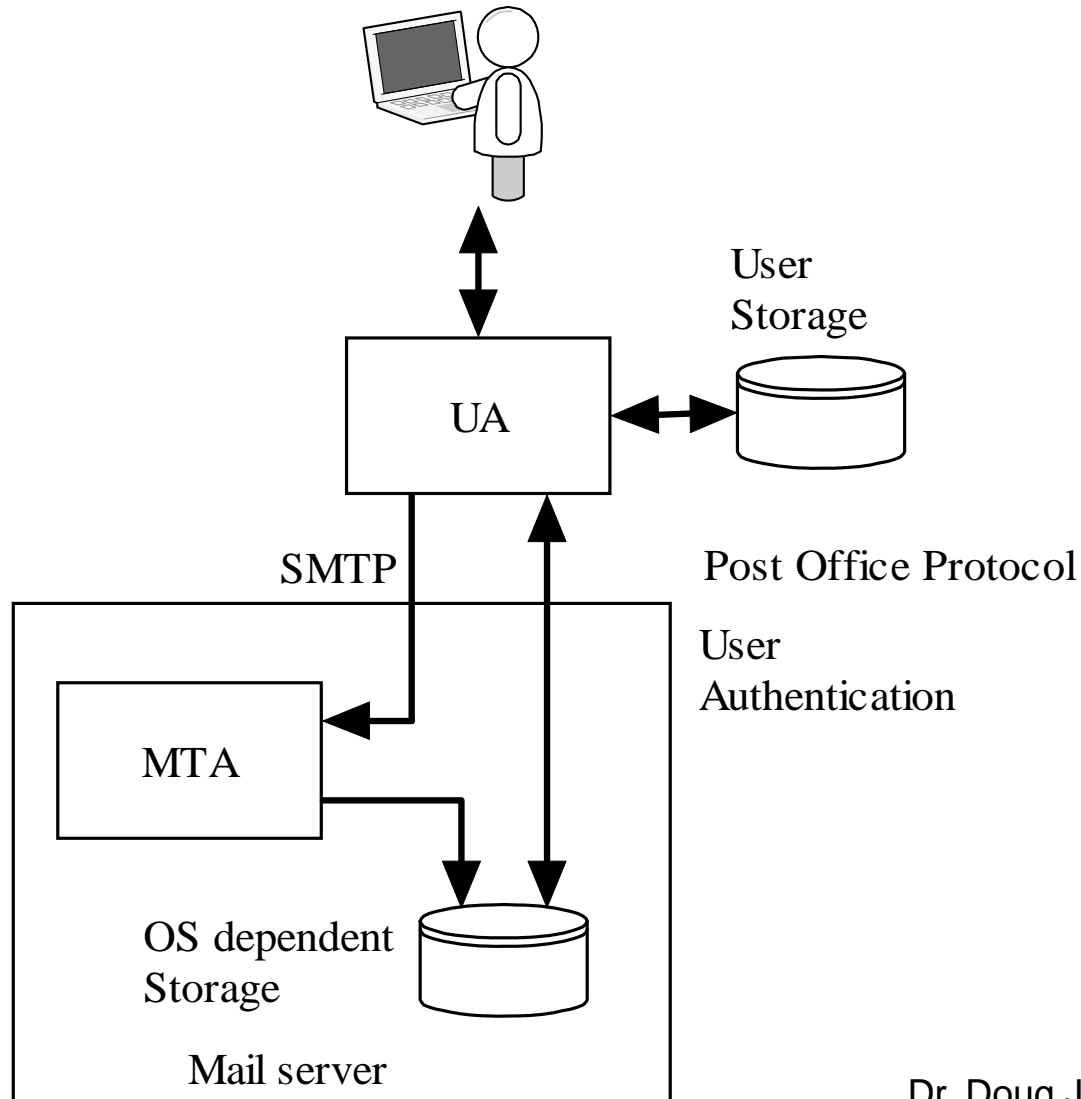


# Local User Agent



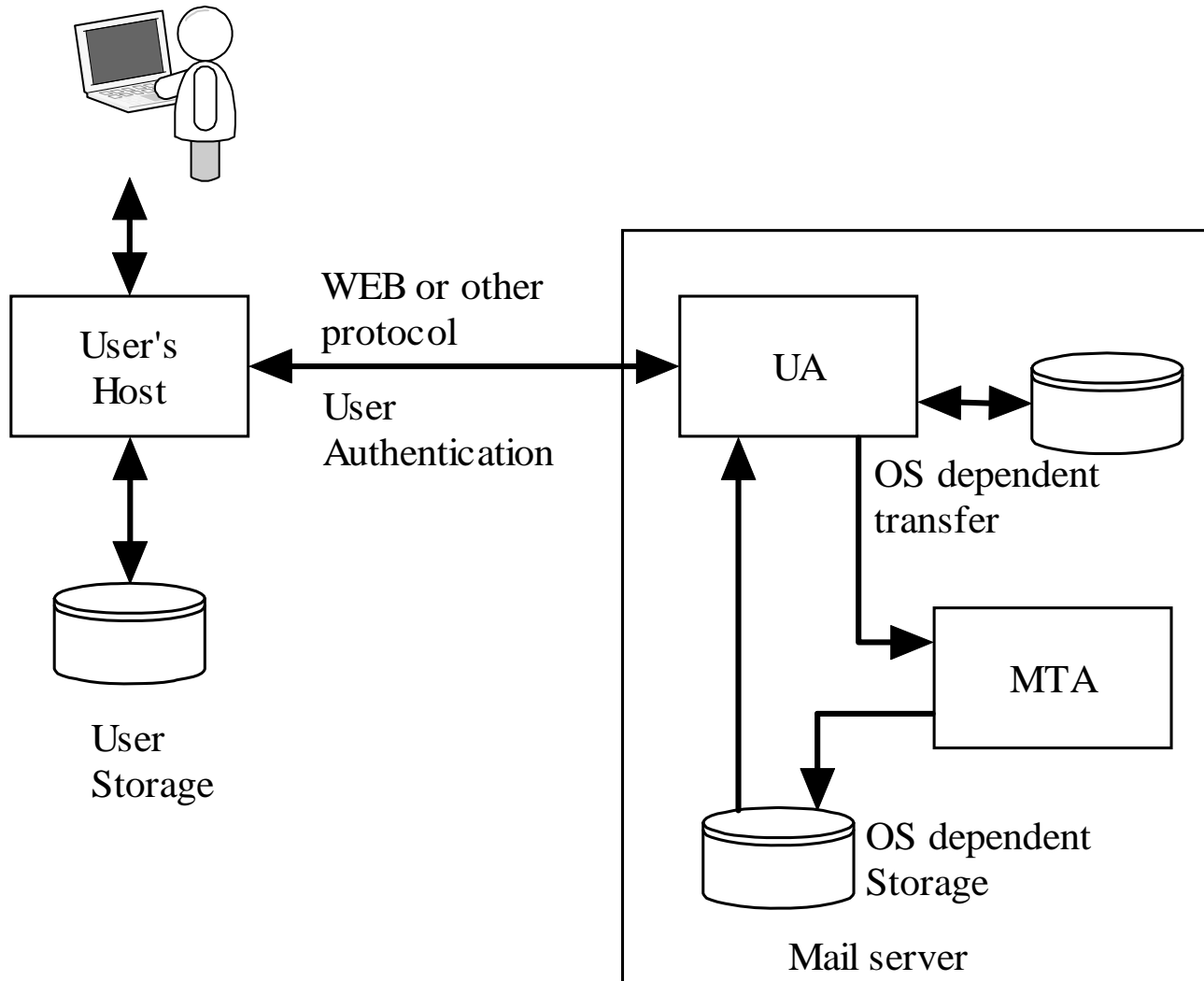
Local User agent

# Remote User Agent



Remote User Agent

# Remote access to local UA



# POP

Post Office Protocol

Used to transfer mail between the mail server and a PC

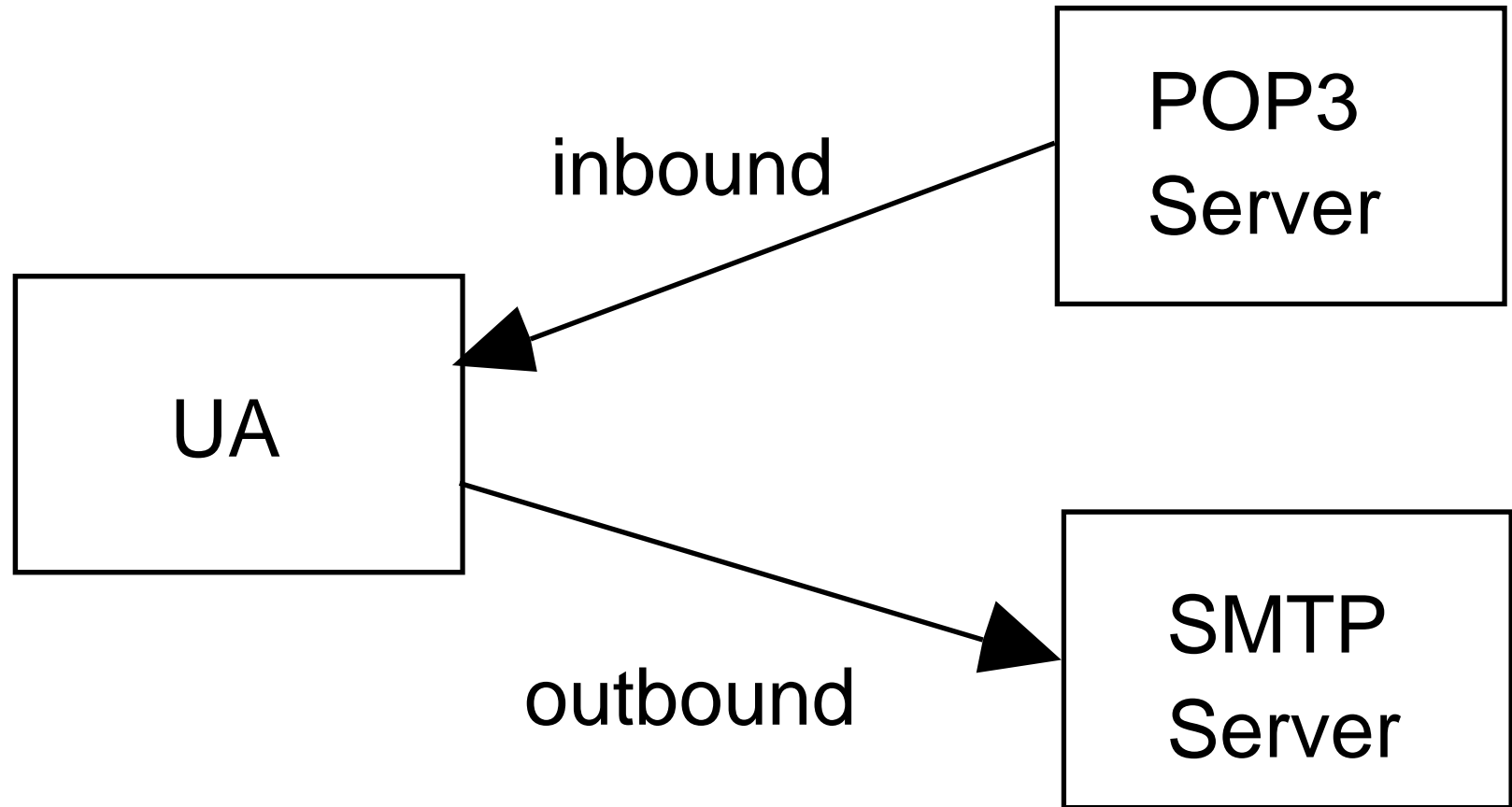
Provides user Authentication

# POP3 protocol

- POP3 client “logs in” to a POP3 server (TCP port 110)
- Login name and password in clear text
- User can configure how often mail is checked
  - this means the login and password can be sent many times a day
  - easy to capture since when there is no mail there are only a few packets exchanged.



# POP3 block diagram



# POP3 Commands

- USER name      Login name
- PASS string      User password
- STAT              returns number of messages
- LIST [msg]        returns the size of msg or all messages if  
   [msg] is not supplied
- RETR msg          send client the full message [msg]
- DELE msg          Delete message from server
- NOOP              No operation
- RSET              Reset deletion indicators

# POP3 Commands

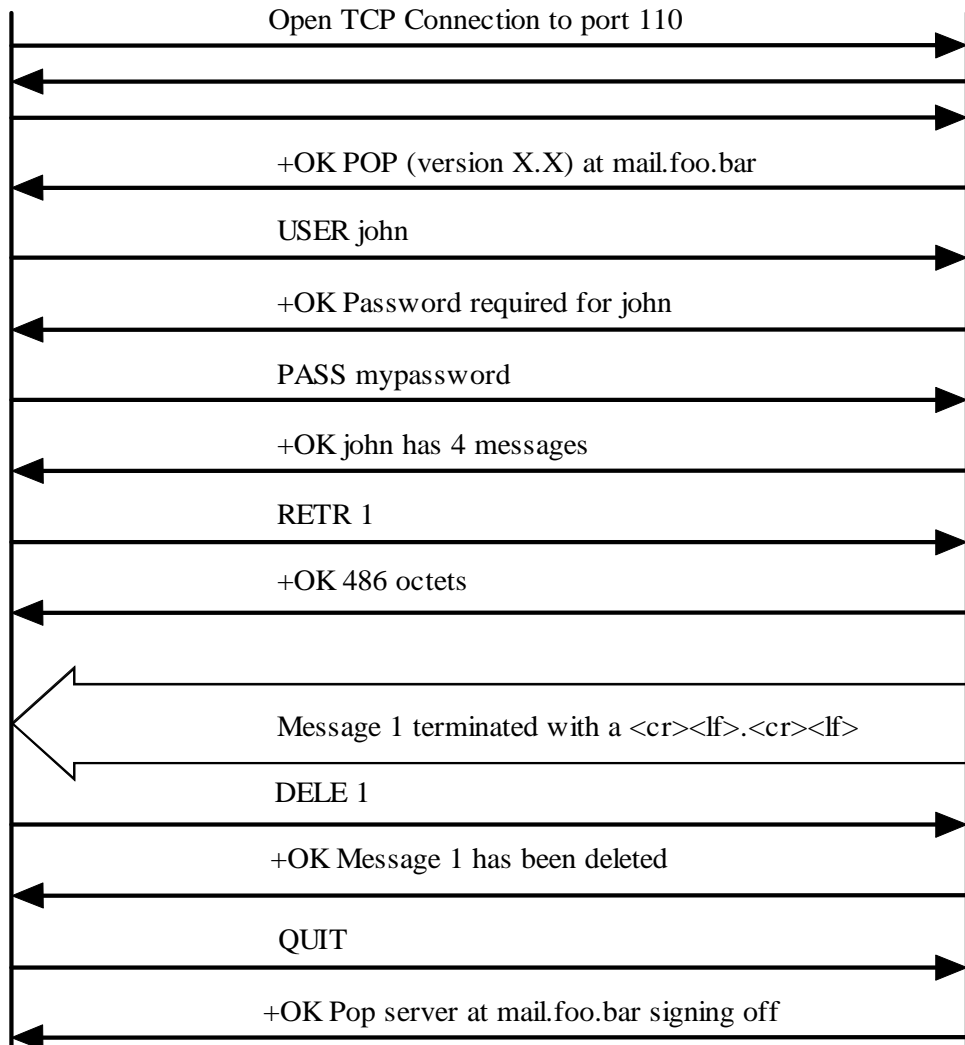
- Quit                                      Quit the session
- APOP name digest                      Optional authentication
- TOP msg n                                return first n lines of message
- UIDL                                      returns a unique ID string for the requested message, does not change during session. Message ID can used to request message.

# POP3 Responses

- Two response codes
  - -ERR message
  - +OK message

POP3  
Client

POP3  
Server

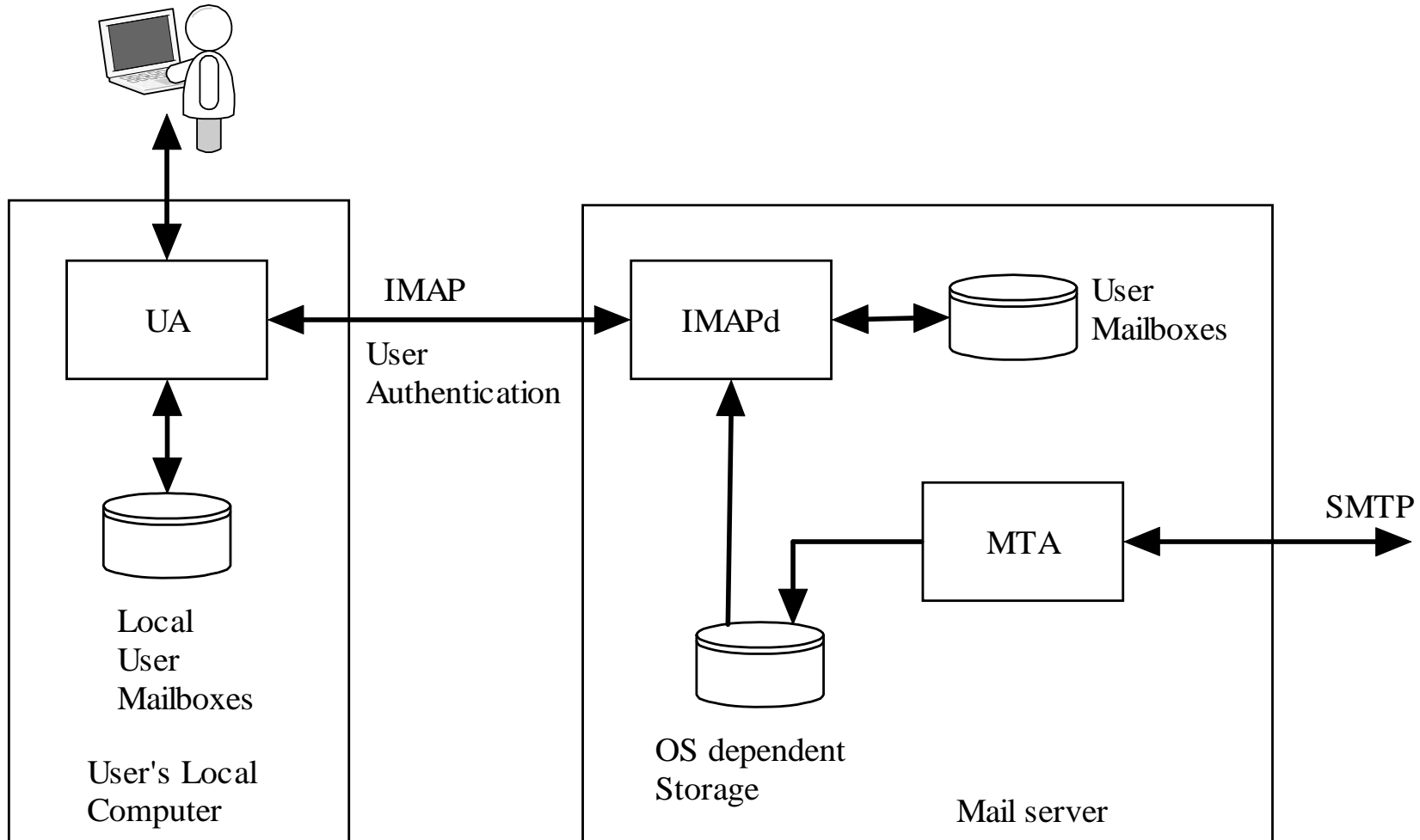


# POP3 Protocol

# IMAP

- Supports message retrieval
- Support message filing
- POP, does not work well in a multiple client configuration since mail is deleted after it is read.
- IMAP can keep messages on the server and can be used by multiple clients.

# IMAP Mail Boxes



# IMAP Commands

- CAPABILITY List server capabilities
- NOOP No operation
- LOGOUT
- AUTHENTICATE type
- LOGIN name passwd
- SELECT mailbox
- EXAMINE mailbox read only version of select
- CREATE mailbox
- DETELE mailbox



# IMAP COMMANDS

- **RENAME** current-name new-name      rename mailbox
- **SUBSCRIBE** mailbox      add mailbox to servers list of active mailboxes
- **UNSUBSCRIBE** mailbox
- **LIST** ref mailbox      provide a list of mailboxes
- **LSUB**      provide a list based on subscribe
- **APPEND** mailbox mess      Append the message to the mailbox
- **CHECK**      Flush mailboxes to disk
- **CLOSE**      Close mailbox, all messages marked as deleted are removed

# IMAP Commands

- EXPUNGE Remove messages marked as deleted
- SEARCH criteria Search the mailbox for messages that match
- FETCH message-set get message
- PARTIAL message len get partial message
- STORE
- COPY message-set Mailbox copy a message to another mailbox
- UID gets unique ID for messages

# Header & Protocol based

- Very few header or protocol based attacks

# Authentication Based

- User authentication over the network
- Password guessing using POP or IMAP
- Every attempt can be logged
- Restrict POP and IMAP authentication to know IP addresses
- Use web client for remote access

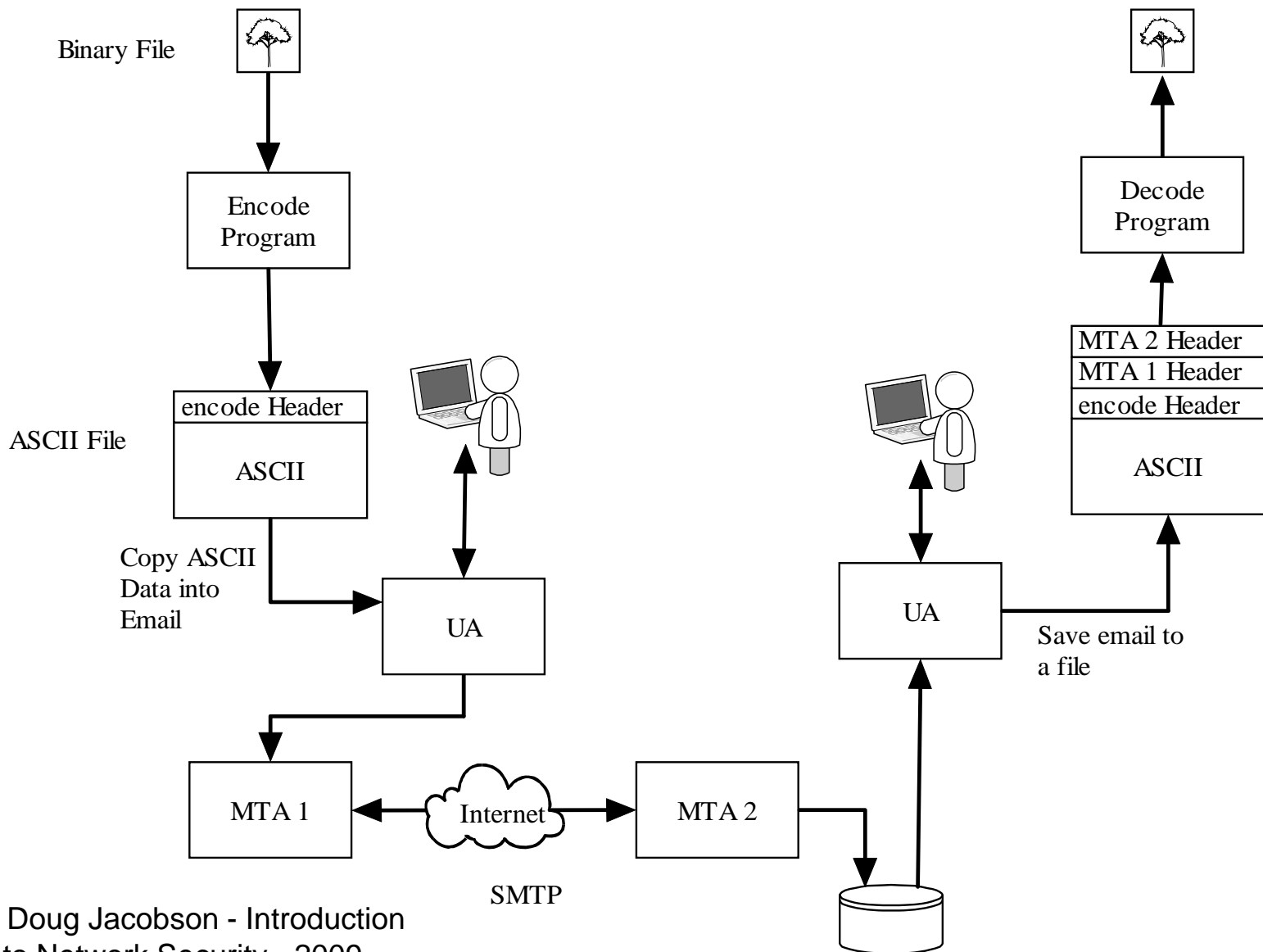
# Traffic Based

- Flooding is not much of an issue
- Sniffing is an issue
  - There are encrypted versions of both IMAP and POP, but they are not widely used.

# MIME

- Multipurpose Internet Mail Extensions
- Email message format
  - Embedded pictures
  - Embedded code
  - Attachments

# Encode and Decode



# MIME Structure

SMTP Headers
MIME Version
MIME Headers
Email Object
MIME Headers
Email Object
MIME Headers
Email Object
MIME Headers
Email Object



# MIME Headers

<b>MIME Header</b>	<b>Function</b>
MIME-Version:	Indicates a MIME message. The current version is 1.1
Content-Type:	Indicates the type of content contained in the message
Content-Transfer-Encoding:	Indicates how the content is encoded
Content-Id:	Optional Identifier used for multiple messages
Content-Description:	Optional description of the object that can be displayed by the user agent
Content-Disposition:	Optional description of the method to use to display the object in receiving the user agent

# Content-Type

Type	Subtype	Description
	Plain	Unformatted text
Text	Html	Text in HTML format
Multipart	Mixed	Multiple ordered objects
	Parallel	Multiple object, not ordered
	Digest	Multiple ordered RFC822 objects
	Alternative	Alternate methods of representing the same object
Message	RFC822	Encapsulated message
	Partial	Part of a larger message
	External-Body	Object is a reference to an external message
Image	JPEG	JPEG Image
	GIF	GIF Image
Video	MPEG	MPEG movie
Audio	Basic	Audio object
Application	Postscript	Adobe Postscript object
	Octet-stream	8 bit binary object

# Multipart MIME

- Next three slides show a multipart MIME message

Email Header

MIME-Version: 1.0

UA Header

Content-Type: multipart/mixed;

boundary="-----090603080000040609050705"

This is a multi-part message in MIME format.

```
-----090603080000040609050705
Content-Type: multipart/alternative;
boundary="-----000407030803000901080005"
```

```
-----000407030803000901080005
Content-Type: text/plain; charset=ISO-8859-1;
format=flowed
Content-Transfer-Encoding: 7bit
```

ASCII text message

```
-----000407030803000901080005
```

```
Content-Type: multipart/related;
boundary="-----080803090003030603090002"
```

```
-----080803090003030603090002
Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
```

```
HTML Text
<br>
HTML Text
```

```
-----080803090003030603090002
Content-Type: image/gif;
name="logo.gif"
Content-Transfer-Encoding: base64
Content-ID: <part1.09040604.05020804@iastate.edu>
Content-Disposition: inline;
filename="logo.gif"
```

GIF File in base64

```
-----080803090003030603090002 --
```

```
-----000407030803000901080005 --
```

OR

```
-----090603080000040609050705
Content-Type: image/gif;
  name="logo.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
  filename="logo.gif"

GIF File in base64

-----090603080000040609050705 --
```

# Content-Description

# Content-Disposition

- Content-Description: <description>
  - Lets user “tell” the User Agent what type of file is attached
  - Allows malicious code to look like something else
- Content-Disposition: (Inline, Attachments)
  - Allows inline documents which will be displayed by the user agent
  - Allows malicious code be open automatically

# Header based

- Headers can be used to hide actual content type
- HTML documents with hyperlinks where the text is different than the link
- Countermeasures:
  - User education



# Protocol Based

- Different than normal protocols (no message exchange)
- Attachments can be malicious (viruses, worms, Trojan horses).
- Some can be auto opened (inline)
- Countermeasures:
  - Disable UA functions
  - Scanners, filters
  - Education

# Authentication Based

- MIME does not support authentication
- Can support email monitoring
  - “Web Bugs”
    - 1x1 pixel picture stored on a web site
    - When email is read the file is downloaded
    - Web server will log access to the file and information about the machine that accessed it.
- Countermeasures:
  - Disable User Agent function to auto display pictures

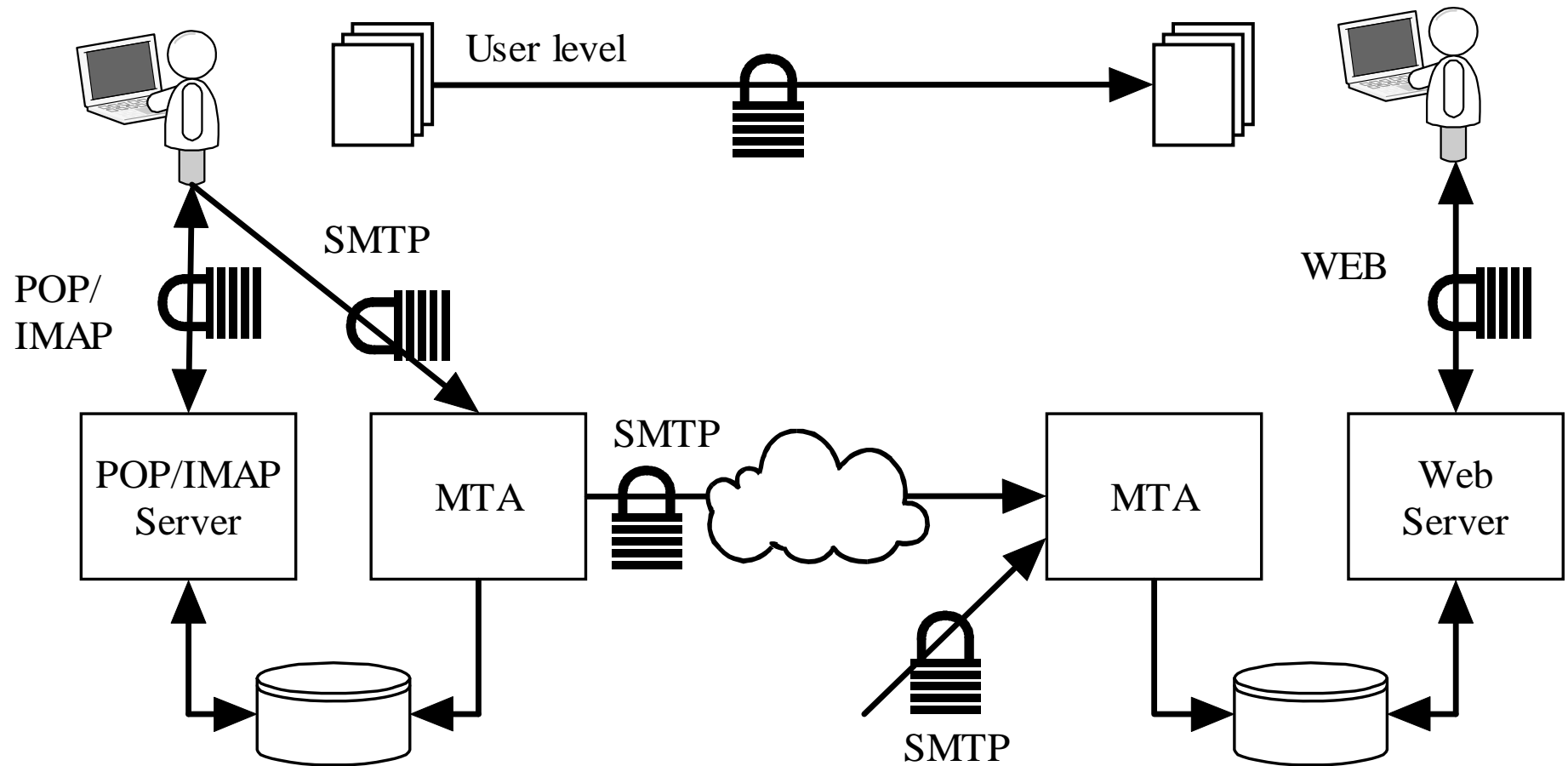
# Traffic Based

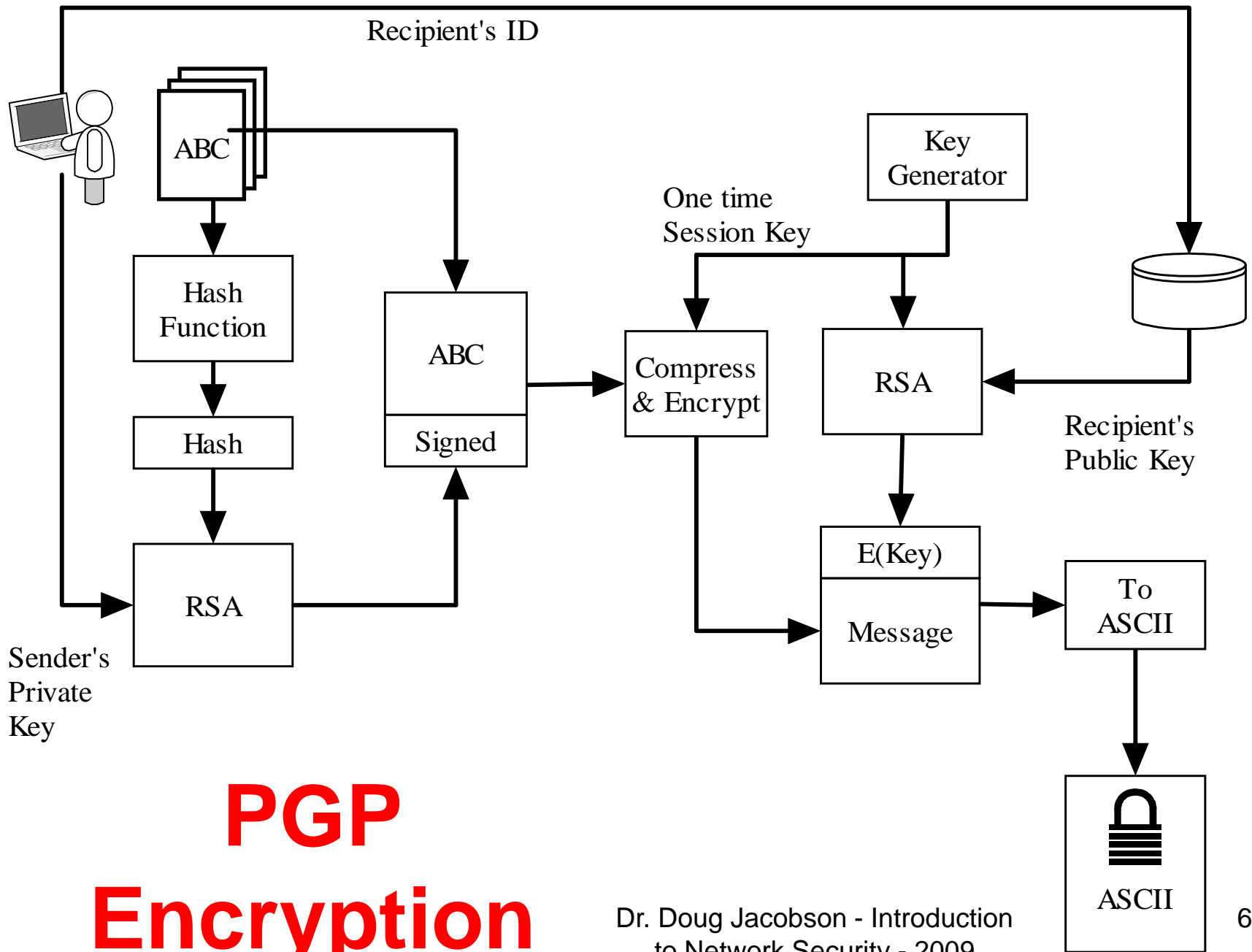
- Enables flooding of the email server
  - Large messages
- Sniffing

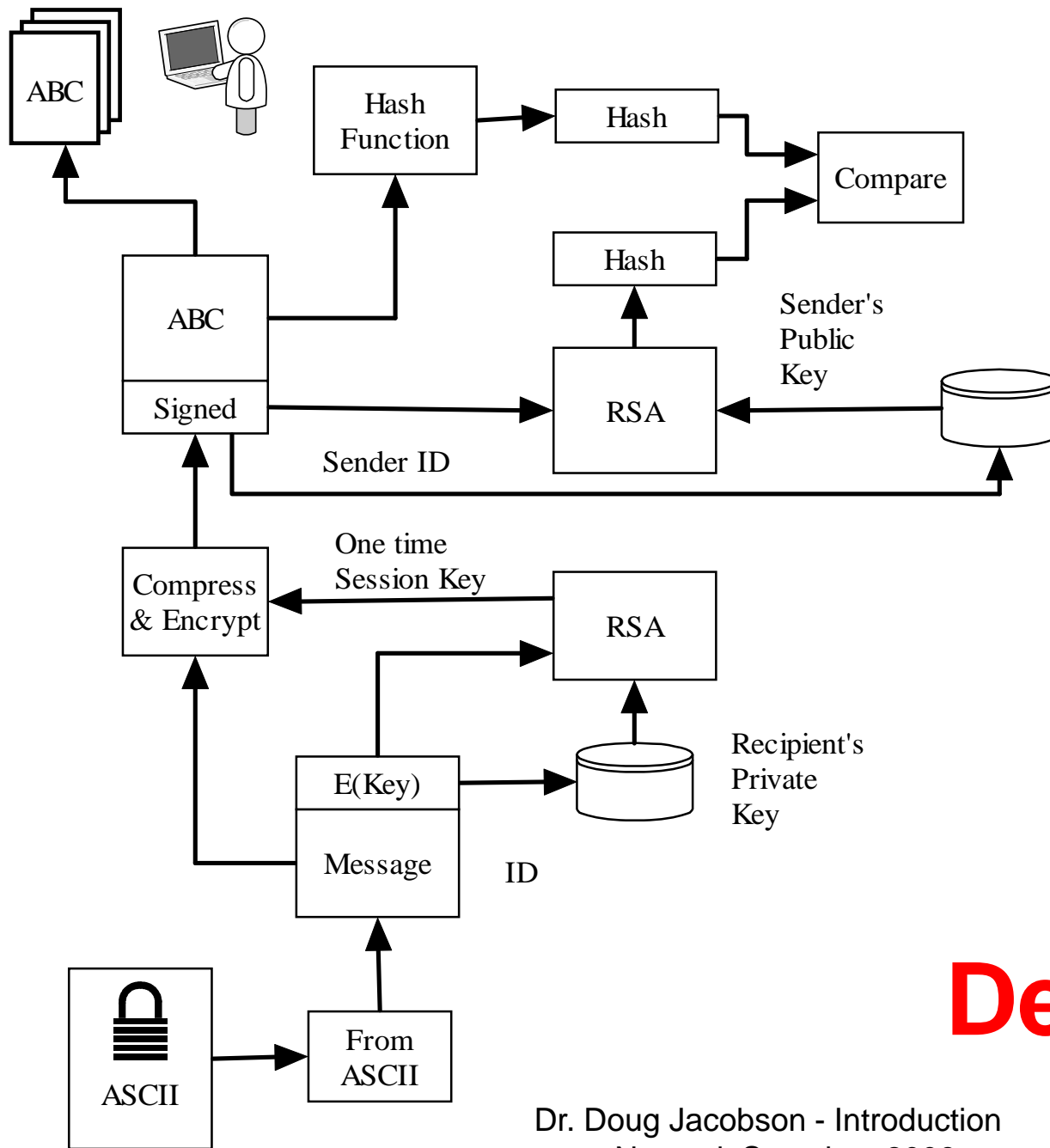
# General Email Countermeasures

- Encryption & authentication
- Email filtering
- Content Filtering
- Email Forensics

# Encryption & Authentication







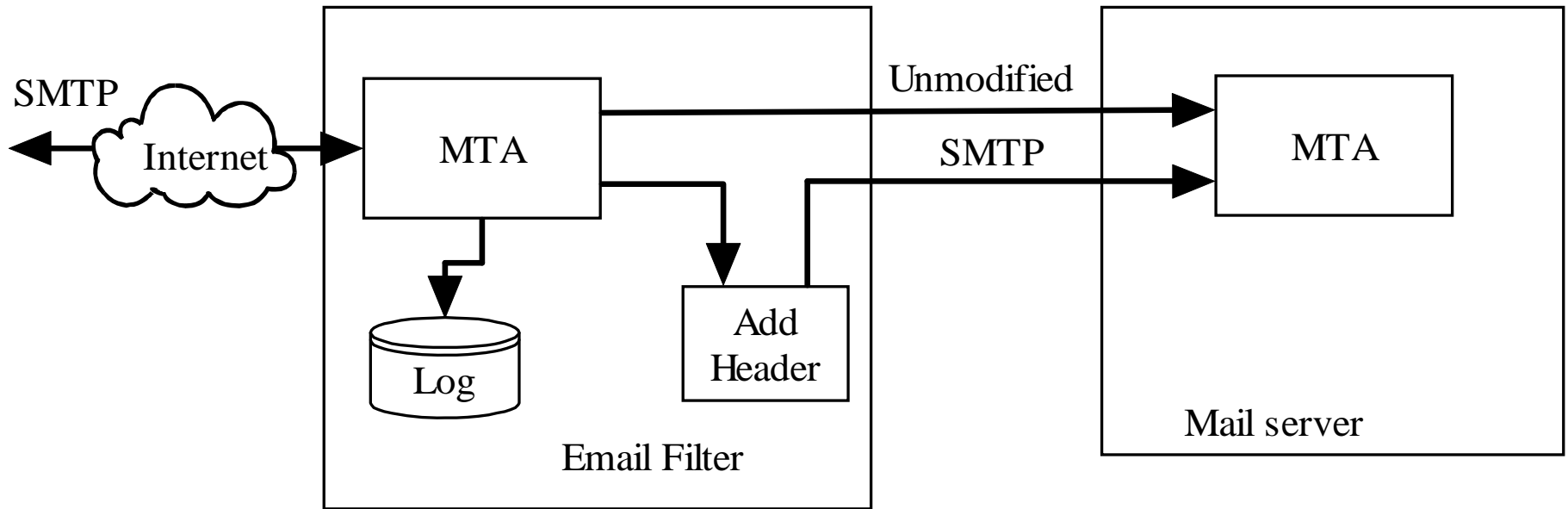
# PGP Decryption

# Email Filtering

- Check email
  - Based on email addresses
  - Based on domain address
  - Based on malicious payload
- Either Block, pass, or modify the email



# Email Filtering



# Spam Filter

- Uses learning to decide what content is spam.
- System is “trained” to know is spam
- Spam filter will mark the message as spam.
- Some User agents support spam detection and will move spam email into a spam folder

# Bypassing a Spam Filter

- Keyword loading
- Misspelled keywords
- Picture only
- Picture with background words

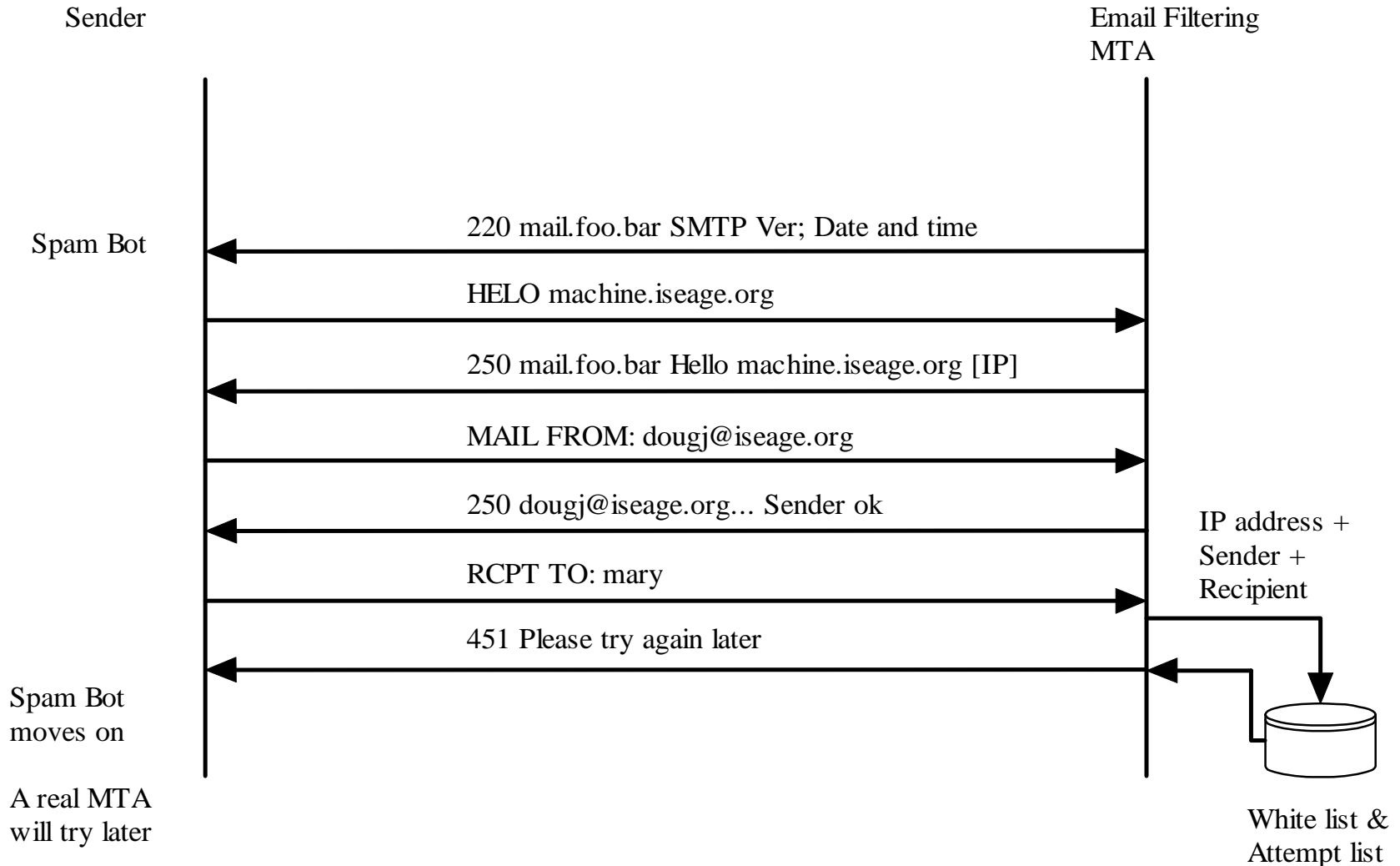
# Filtering list

- **Blacklist**
  - A list of bad users & domains
  - Spammers just change domains
- **Whitelist**
  - A list of good users and domains
  - Very restrictive

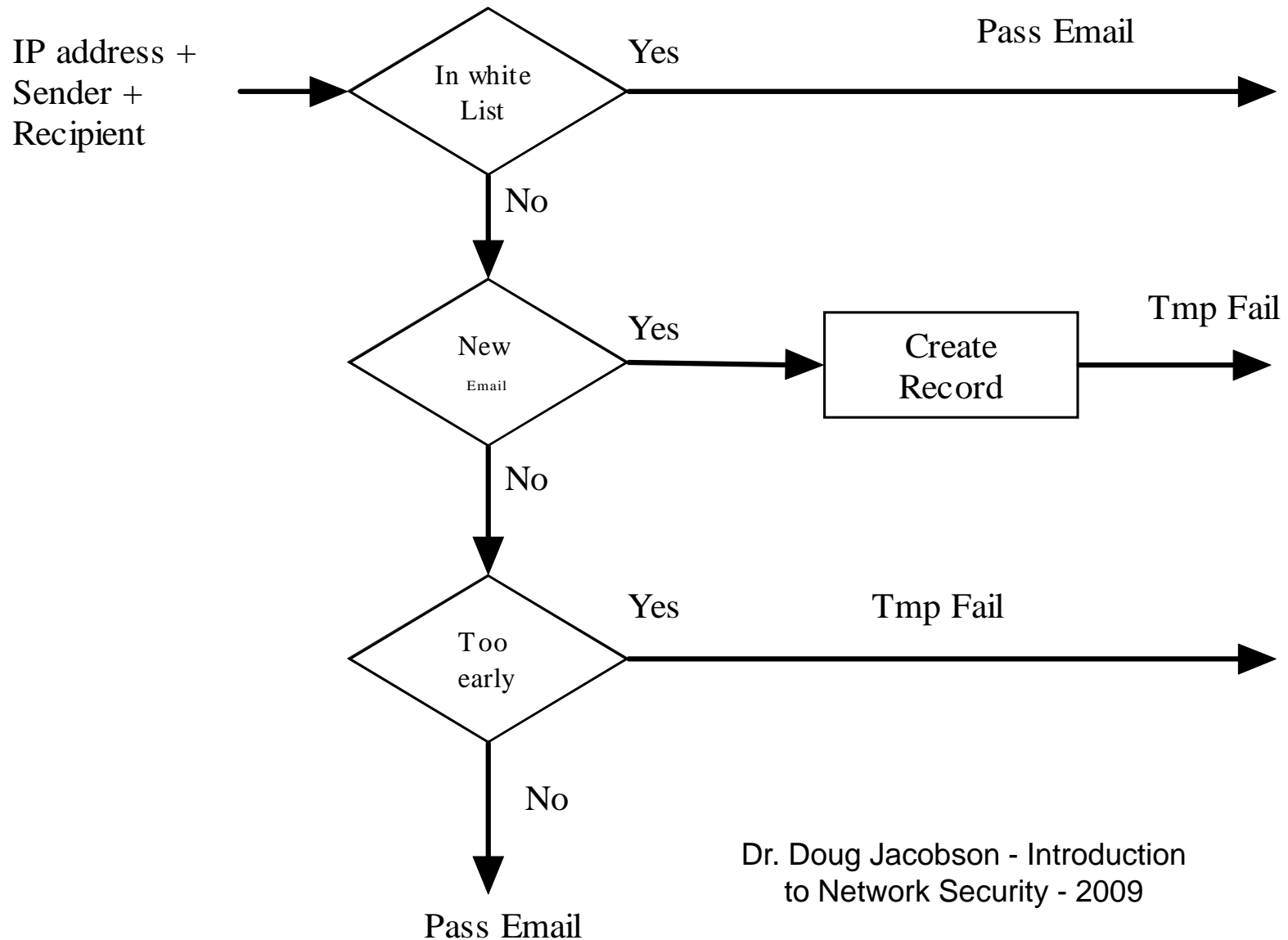
# Greylist

- Reject all email with a temp reject
- Maintain a whitelist that is not subject to filtering
- Add machines to the grey list when they resend the email

# Greylist



# Greylist



# Bypassing a grey list

- Use real MTA to send email



# Content filter

- Examine the payload for:
  - Viruses
  - Worms
  - Trojan horses
- Often based on a signature
- Requires constant update of signatures

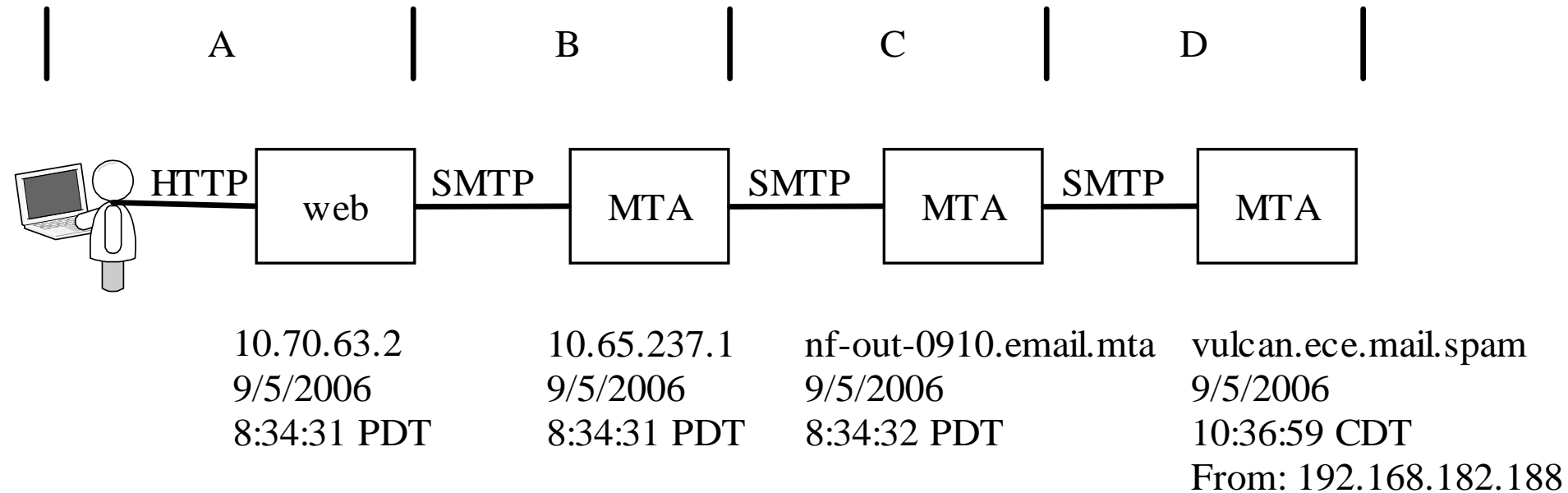
# Outbound content filtering

- Used to keep private information from leaving
  - SS Numbers
  - Account Numbers
  - Medical records
- Will either log, stop, or encrypt violating emails

# Bypassing a content filter

- Encryption
  - There are encrypted viruses
- Compression

# Email Forensics



# Email Forensics

Received: from nf-out-0910.email.mta (nf-out-0910.email.mta [192.168.182.188])

by vulcan.ece.mail.spam (8.12.8/8.9.3) with ESMTTP id k85FaxBT1486661

for <john@ee.mail.spam>; Tue, 5 Sep 2006 10:36:59 -0500 (CDT)

Received: by nf-out-0910.email.mta with SMTP id p77sol1381355nfc

for <john@ee.mail.spam>; Tue, 05 Sep 2006 08:34:32 -0700 (PDT)

DomainKey-Signature: a=rsa-sha1; q=dns; c=noaws;

s=beta; d=spammer.fake;

h=received:message-id:date:from:to:subject:mime-

version:content-type;

b=BD9tHbNaozYZj9gNQqXmkrnHNA3N8+3W4NAPcFJkKsKyX8DdOTS7Dp1VNunGx66SLcU5rYiDxCnY6SuVCKtWq73DDH7MYEfWgaOtYdl/hILBIRVnCbLxGtyCoIT7I8use4F4RgCzZWc3Oc6fjqNzgGLE5s3RFQ9eVPhS+HxW+DA=

Received: by 10.65.237.1 with SMTP id o1mr4809264qbr;

Tue, 05 Sep 2006 08:34:31 -0700 (PDT)

Received: by 10.70.63.2 with HTTP; Tue, 5 Sep 2006 08:34:31 -0700 (PDT)

Message-ID:

<ab156e9f0609050834v528b5b2eld9204458fe6409a1@mail.spammer.fake>

Date: Tue, 5 Sep 2006 10:34:31 -0500

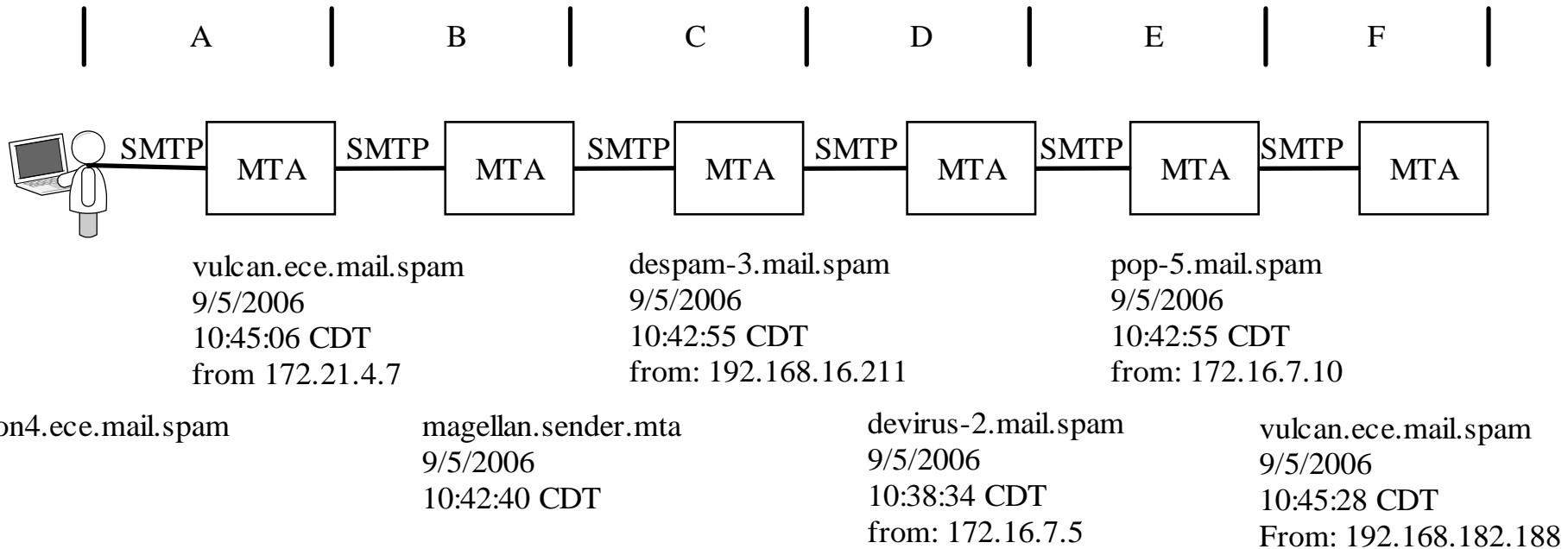
From: "Harry Mudd" <Harry6502@spammer.fake>

To: john@ee.mail.spam

Subject: mail trace 2

MIME-Version: 1.0

# Email Forensics



# Email Forensics

F Received: from pop-5.mail.spam (pop-5.mail.spam [172.16.7.12])  
by vulcan.ece.mail.spam (8.12.8/8.9.3) with ESMTTP id  
k85FjSBT1508024  
for <john@EE.MAIL.SPAM>; Tue, 5 Sep 2006 10:45:28 -0500 (CDT)

E Received: from devirus-2.mail.spam (devirus-2.mail.spam [172.16.7.10])  
by pop-5.mail.spam (8.12.11.20060614/8.12.11) with SMTP id  
k85Fgt28016542  
for <john@mail.spam>; Tue, 5 Sep 2006 10:42:55 -0500

D Received: from (despam-3.mail.spam [172.16.7.5]) by devirus-2.mail.spam  
with smtp  
id 0df9\_ae8af2c2\_3cca\_1ldb\_969a\_001372537fef;  
Tue, 05 Sep 2006 10:38:34 +0000

C Received: from magellan.sender.mta (magellan.sender.mta  
[192.168.16.211])  
by despam-3.mail.spam (8.12.11.20060614/8.12.4) with ESMTTP id  
k85FggtT020053  
for <john@mail.spam>; Tue, 5 Sep 2006 10:42:55 -0500

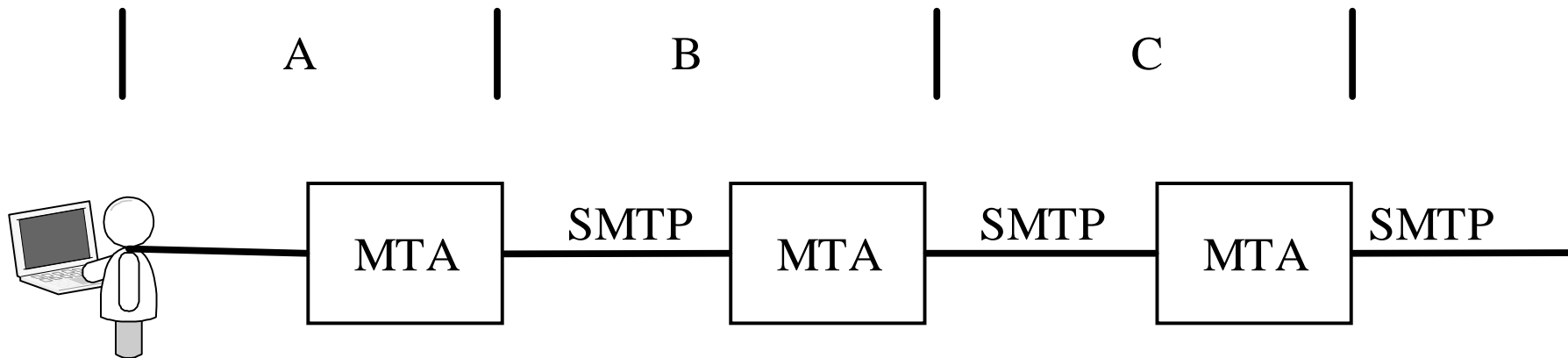
B Received: from vulcan.ece.mail.spam (vulcan.ece.mail.spam [172.20.5.6])  
by magellan.sender.mta (8.13.6/8.13.6) with ESMTTP id  
k85Fgemo030599  
for <dwj@sender.mta>; Tue, 5 Sep 2006 10:42:40 -0500 (CDT)  
(envelope-from john@mail.spam)

A Received: from [172.21.4.7] (babylon4.ece.mail.spam [172.21.4.7])  
by vulcan.ece.mail.spam (8.12.8/8.9.3) with ESMTTP id  
k85Fj6BT1501144  
for <dwj@sender.mta>; Tue, 5 Sep 2006 10:45:06 -0500 (CDT)  
Message-ID: <44FD9AEC.4040103@mail.spam>  
Date: Tue, 05 Sep 2006 10:42:36 -0500  
From: Harry Mudd <Harry@mail.spam>  
Organization: ISU Information Assurance Center  
User-Agent: Mozilla Thunderbird 1.0.7 (Windows/20050923)  
X-Accept-Language: en-us, en  
MIME-Version: 1.0  
To: Dave Johnson <dwj@sender.mta>  
Subject: test 4  
Content-Type: text/plain; charset=ISO-8859-1; format=flowed  
Content-Transfer-Encoding: 7bit  
X-Filter-MailScanner-Information: Please contact the ISP for more  
information  
X-Filter-MailScanner: Found to be clean  
X-Filter-MailScanner-SpamCheck: not spam, SpamAssassin (score=-2.6,  
required 6, autolearn=not spam, BAYES\_00 -2.60, SPF\_PASS -0.00)  
X-Filter-MailScanner-From: john@mail.spam  
X-PMX-Version: 5.2.0.264296, Antispam-Engine: 2.4.0.264935, Antispam-  
Data: 2006.9.5.82442  
X-Perlmx-Spam: Gauge=IIIIIIII, Probability=7%, Report='\_\_C230066\_ P5 0,  
\_\_CP\_URI\_IN\_BODY 0, \_\_CT 0, \_\_CTE 0, \_\_CT\_TEXT\_PLAIN 0, \_\_HAS\_MSGID 0,  
\_\_MIME\_TEXT\_ONLY 0, \_\_MIME\_VERSION 0, \_\_SANE\_MSGID 0, \_\_USER\_AGENT 0'

Spam  
Filters

Dr. Doug Jacobson - Introduction  
to Network Security - 2009

# Email Forensics



Logged into MTA	ns09.egujarat.net 9/9/2006 22:29:41	ns09.egujarat.net 9/9/2006 22:29:41 from 127.0.0.1	despam-2.mail.spam 9/9/2006 15:18:28 CDT from: 202.149.46.162
-----------------	---	---	--



# Email Forensics

(Removed local headers)  
Received: from ns09.egujarat.net (202 -149-46-162.static.exatt.net [202.149.46.162] (may be forged))  
by despam-2.iastate.edu (8.12.11.20060614/8.12.4) with ESMTTP id k89KIRCr017274  
for <dougj@iastate.edu>; Sat, 9 Sep 2006 15:18:28 -0500

D

Received: from ns09.egujarat.net (localhost.localdomain [127.0.0.1])  
by ns09.egujarat.net (8.13.5/8.13.5) with ESMTTP id k89H5sYI007263  
for <dougj@iastate.edu>; Sat, 9 Sep 2006 22:37:19 +0530

C

Received: (from administrator@localhost)  
by ns09.egujarat.net (8.13.5/8.13.5/Submit) id k89Gxf4q006335;  
Sat, 9 Sep 2006 22:29:41 +0530

B

Date: Sat, 9 Sep 2006 22:29:41 +0530  
Message-Id: <200609091659.k89Gxf4q006335@ns09.egujarat.net>  
To: dougj@iastate.edu  
Subject: Password change required!  
From: "eBay Inc." <admin@eBay.com>  
Content-Type: text/html

A

X-egujarat-MailScanner-Information: Please contact the ISP for more information  
X-egujarat-MailScanner: Found to be clean  
X-MailScanner-From: administrator@ns09.egujarat.net

Spam Filter 2

X-PMX-Version: 5.2.0.264296, Antispam-Engine: 2.4.0.264935, Antispam-Data: 2006.9.9.124943  
X-Perlmx-Spam: Gauge=XXXXXXXXXXXXXXXXXXXX, Probability=99%,

Spam Filter 1

<p></p>  
<BR>

Logo

Dear sir, <BR>  
<BR>  
We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD. <BR>  
<BR>

If this is not completed by <STRONG>September 15, 2006</STRONG>, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation. <BR>  
<BR>

Dr. Doug Jacobson - Introduction to Network Security - 2009

Phishing Site

<A href="http://linux.net zero.idv.tw/~ming/.change/index.php?MfcISAPICommand=ChangeFPP" target=\_blank>Click here to Change Your Password</A></TD>