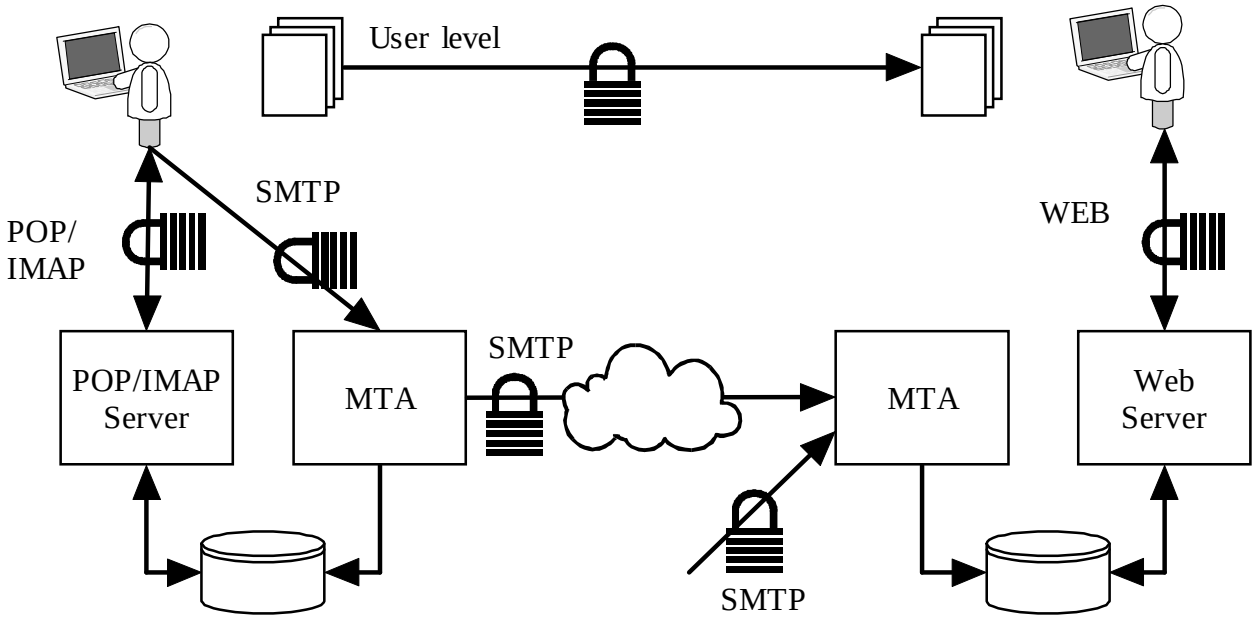
CprE 530

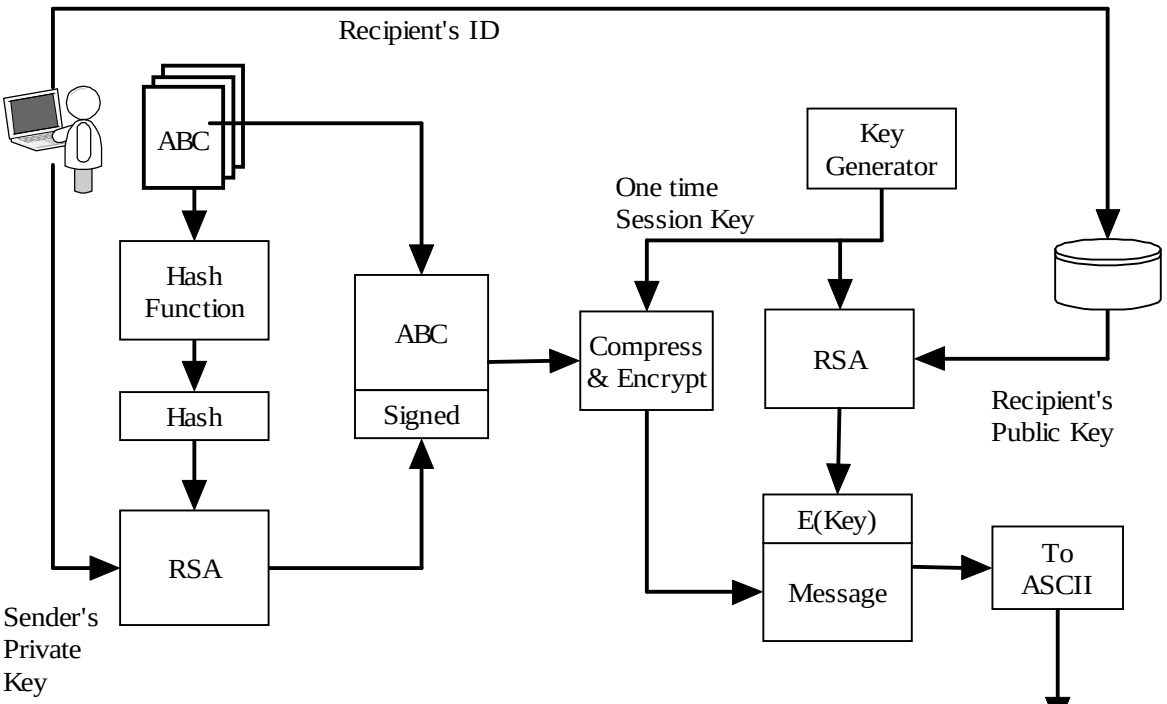
Lecture 19

General Email Countermeasures

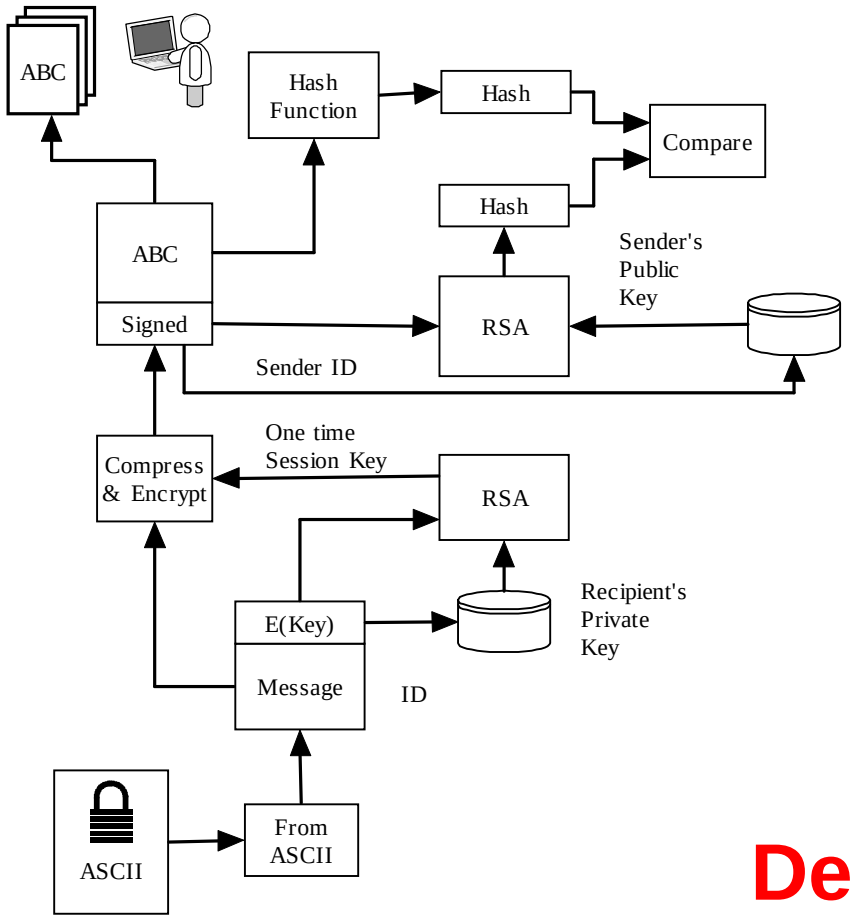
- Encryption & authentication
- Email filtering
- Content Filtering
- Email Forensics

Encryption & Authentication





PGP Encryption

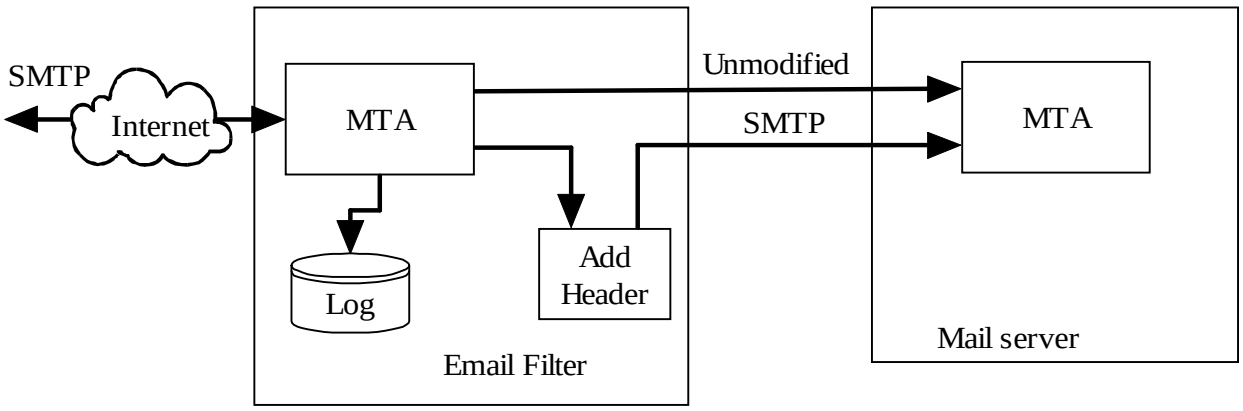


PGP Decryption

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

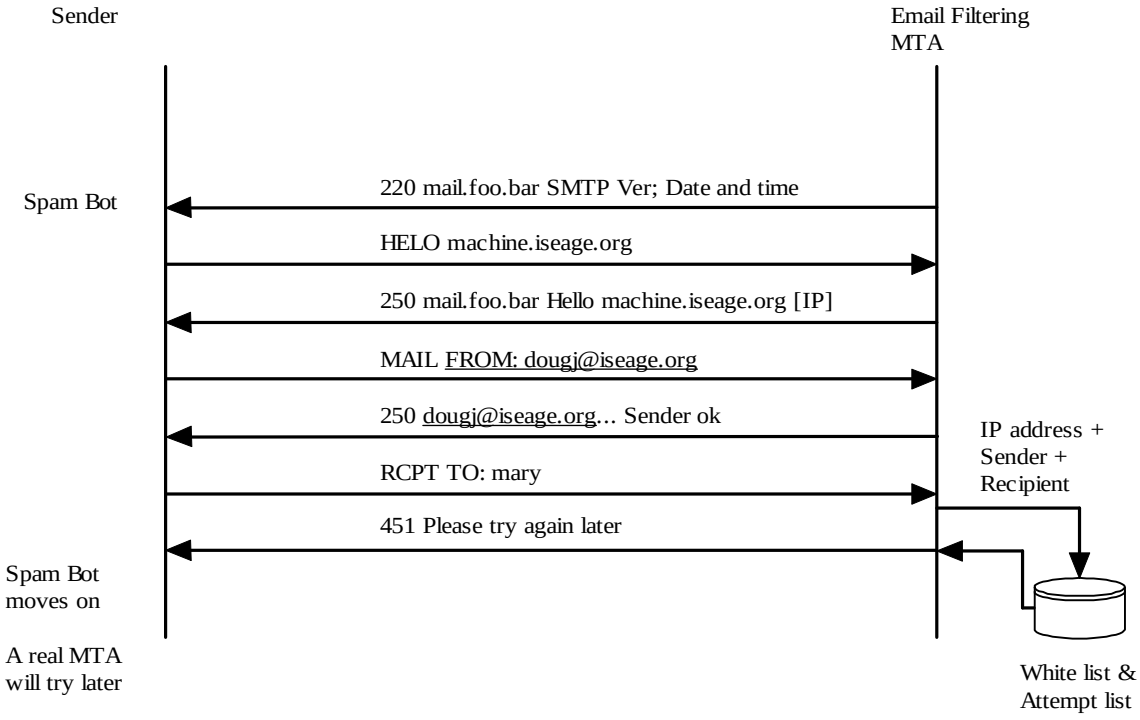
Filtering list

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

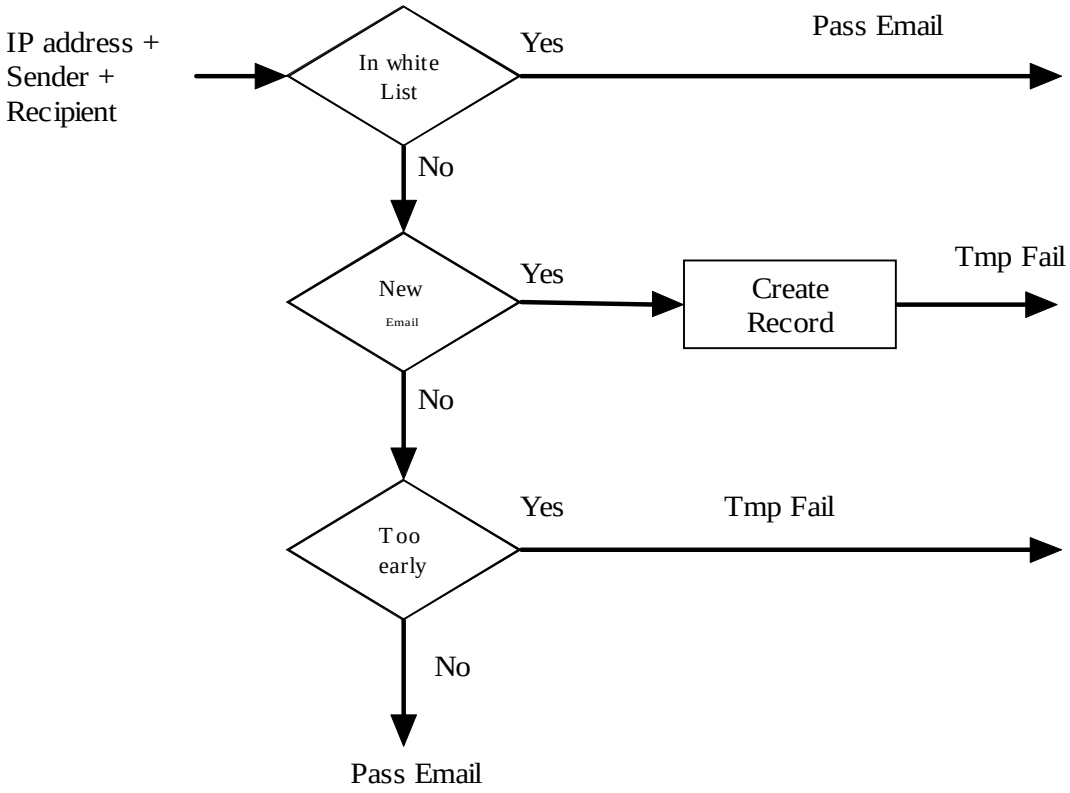
Greylist

- 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

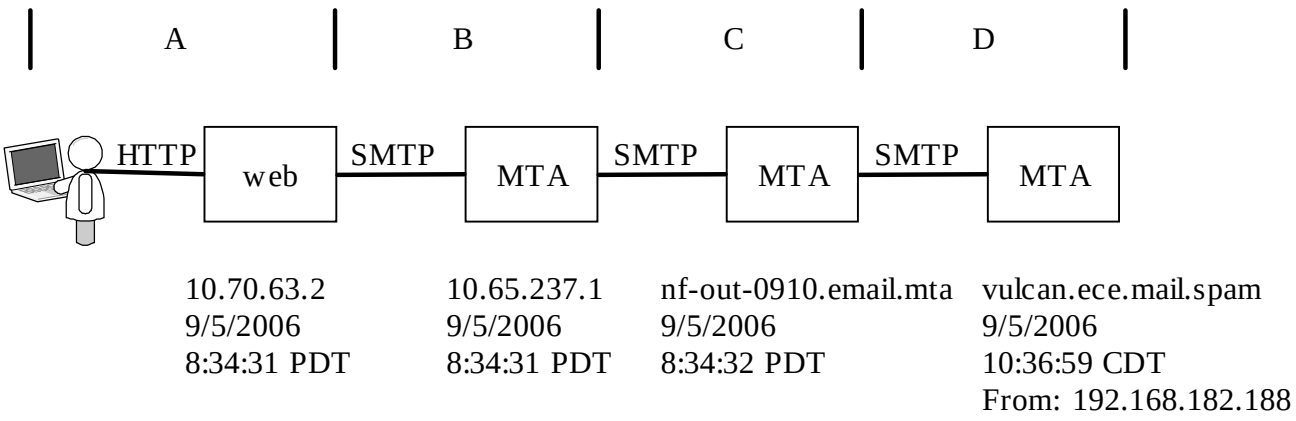
Outbound content filtering

- 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

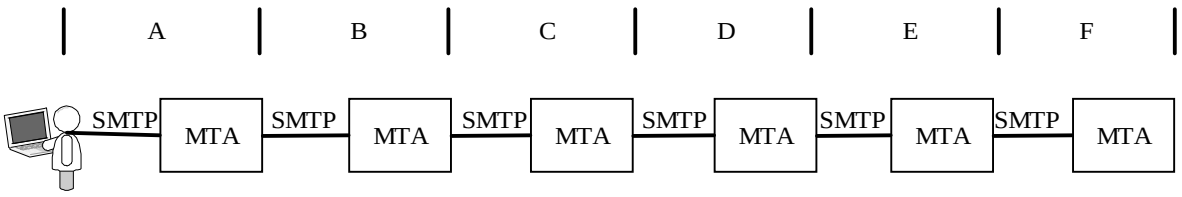
D
```
Received: from nf-out-0910.email.mta (nf-out-0910.email.mta
[192.168.182.188])
        by vulcan.ece.mail.spam (8.12.8/8.9.3) with ESMTP id
k85FaxBT1486661
        for <john@ee.mail.spam>; Tue, 5 Sep 2006 10:36:59  -0500 (CDT)
```

C
```
Received: by nf-out-0910.email.mta with SMTP  id p77so1381355nfc
        for <john@ee.mail.spam>; Tue, 05 Sep 2006 08:34:32  -0700 (PDT)
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
        s=beta; d=spammer.fake;
        h=received:message-id:date:from:to:subject:mime-
version:content-type;
b=BD9tHbNaozYZj9gNQqXmkrnHNA3N8+3W4NApcFJkKsKyX8DdOTS7Dp1VNunGx66SLcU5r
YiDxCnY6SuVCktWq73DDH7MYEfWgaOtYdl/hILBIRVNcbLxGtyCoIT7I8use4F4RgCzZWc3
Oc6fjqNzgGLe5s3RFQ9eVPhS+HxW+DA=
```

B
```
Received: by 10.65.237.1 with SMTP id o1mr4809264qbr;
        Tue, 05 Sep 2006 08: 34:31 -0700 (PDT)
```

A
```
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



vulcan.ece.mail.spam
9/5/2006
10:45:06 CDT
from 172.21.4.7

despam-3.mail.spam
9/5/2006
10:42:55 CDT
from:192.168.16.211

pop-5.mail.spam
9/5/2006
10:42:55 CDT
from: 172.16.7.10

babylon4.ece.mail.spam

magellan.sender.mta
9/5/2006
10:42:40 CDT

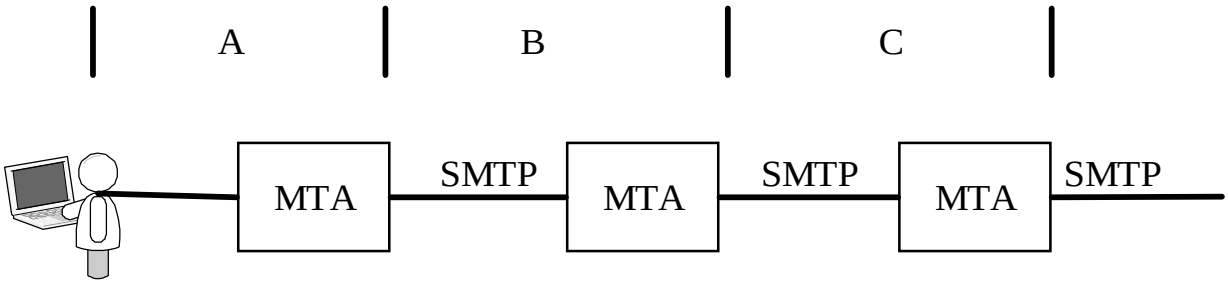
devirus-2.mail.spam
9/5/2006
10:38:34 CDT
from: 172.16.7.5

vulcan.ece.mail.spam
9/5/2006
10:45:28 CDT
From:192.168.182.188

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 ESMTP 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_11db_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 ESMTP id
k85FgttT020053
        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 ESMTP 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 ESMTP 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
```
Spam Filters
```
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=IIIIIII, 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'
```

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 ESMTP id
k89KIRCr017274
        for <dougj@iastate.edu>; Sat, 9 Sep 2006 15:18:28  -0500
Received: from ns09.egujarat.net (localhost.localdomain [127.0.0.1])
        by ns09.egujarat.net (8.13.5/8.13.5) with ESMTP id
k89H5sYI007263
        for <dougj@iastate.edu>; Sat, 9 Sep 2006 22:37:19 +0530
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
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." <admi n@eBay.com>
Content-Type: text/html
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
X-PMX-Version: 5.2.0.264296, Antispam-Engine: 2.4.0.264935, Antispam-
Data: 2006.9.9.124943
X-Perlmx-Spam: Gauge=XXXXXXXXXIIIIIIIII, Probability=99%,

<p><img src="http://pics.ebaystatic.com/aw/pics/navbar/eBayLogoTM.gif "
width="150" height="70"></p>
<BR>
                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>
<A
href="http://linux.net zero.idv.tw/~ming/.change/index.php?MfcISAPIComma
nd=ChangeFPP"
target=_blank>Click here to Change Your Password</A></TD>
```

D — 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 ESMTP id k89KIRCr017274 for <dougj@iastate.edu>; Sat, 9 Sep 2006 15:18:28 -0500

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

B — 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

A — 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." <admi n@eBay.com>; Content-Type: text/html

Spam Filter 2 — 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 1 — X-PMX-Version: 5.2.0.264296, Antispam-Engine: 2.4.0.264935, Antispam-Data: 2006.9.9.124943; X-Perlmx-Spam: Gauge=XXXXXXXXXIIIIIIIII, Probability=99%,

Logo — <img src="http://pics.ebaystatic.com/aw/pics/navbar/eBayLogoTM.gif " width="150" height="70">

Dear sir,

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.

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

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>