CAUCE

Coalition Against Unsolicited Commercial Email

Basic e-mail forensics

John R. Levine

&

Neil Schwartzman

Underground Economy#13
September 2013

Where is everything?

These Slides :

http://www.taugh.com/ue13/

Resources :

http://www.cauce.org/ue2013.html

Our goals for today

- Understand the parts of a mail message
  - Headers (delivery)
  - Body (payload)
- Tell truth from fiction
- Identify responsible parties (Follow the $)
- Look for patterns in spam campaigns

CAUCE

Coalition Against Unsolicited Commercial Email

Basic e-mail forensics
Part I : The Basics

Neil Schwartzman
Executive Director, CAUCE

What is an IP Address?

What is an IP Address?

- 213.248.117.66 www.interpol.int

What is an IP Address?

- 213.248.117.66 www.interpol.int
- 64.57.183.103 cauce.org

What is an IP Address?

- 213.248.117.66 www.interpol.int
- 64.57.183.103 cauce.org
- Hotmail.nl
  - 157.55.43.17
  - 157.55.43.18
  - 157.55.43.19
  - 157.55.43.16

What is an IP Address?

Private numbers:

- 192.168.xxx.yyy
- 10.1.xxx.yyy
- 172.16.xxx.yyy ➔ 172.31.xxx.yyy
- 127.zzz.xxx.yyy
- 169.254.xxx.yyy

What is an IP Address?

Oh No! They ran out of traditional IP version four (IPv4) addresses!

What is an IP Address?

IPv6

- New (since 2000)
- Many of the tools we are using today don't yet work with it
- It will run in parallel with V4 for a while
- Here's what an IPV6 Address looks like

What is an IPv6 Address?

Here's what an IPV6 Address looks like:

www.google.com

2a00:1450:4009:808::1011

What is a Domain?

Domains

- CNN.com
- hotmail.nl
- J.ANSIETA@interpol.int
- Neil@cauce.org
- John.levine@cauce.org

What is the Domain Name Service (DNS)?

Browser:

“CNN.com, please”

Browser

CNN, please

ISP DNS:

I know CNN.com!

It is at 157.166.249.11


Browser
CNN, please
ISP DNS:
I know CNN.com!
It is at
157.166.249.11
CNN

Browser

CNN, please

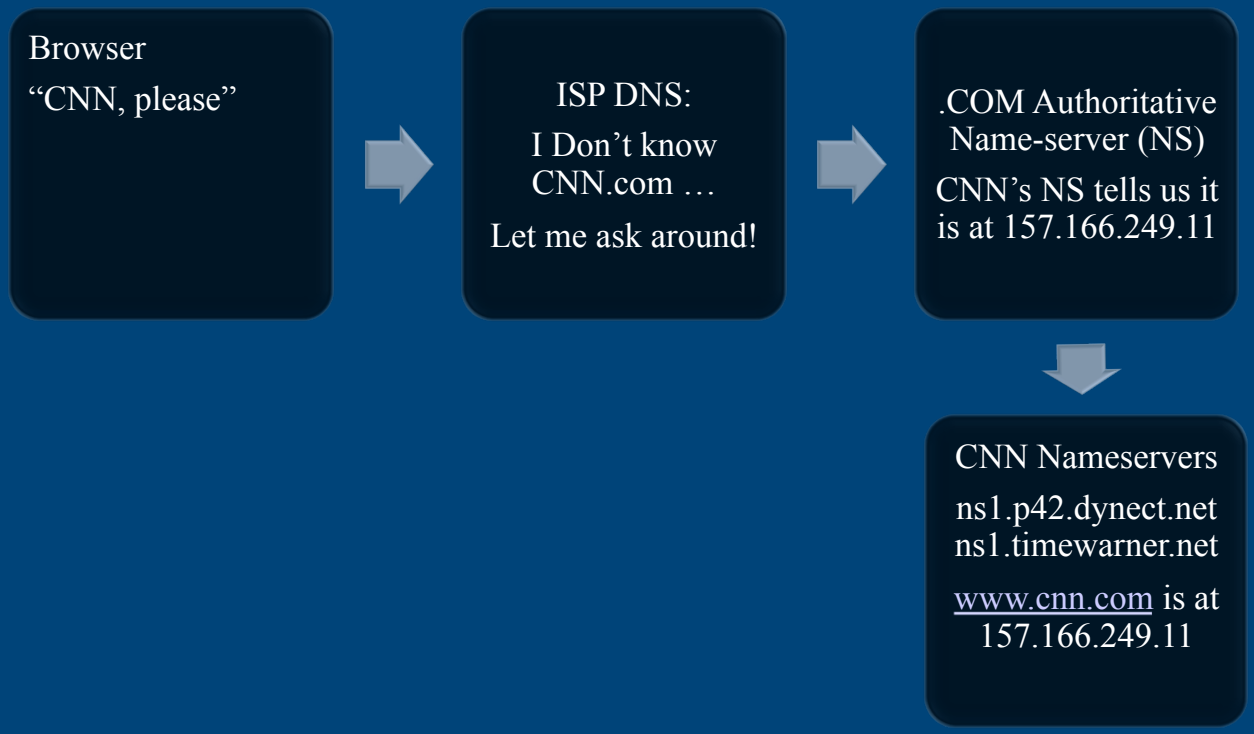
Browser

CNN, please

ISP DNS:

I Don’t know CNN.com …

Let me ask around!


Browser
"CNN, please"
ISP DNS:
I Don't know CNN.com …
Let me ask around!
.COM Authoritative Name-server (NS)
CNN's NS tells us it is at 157.166.249.11
CNN Nameservers
ns1.p42.dynect.net
ns1.timewarner.net
www.cnn.com is at 157.166.249.11

Browser :

"CNN, please"

ISP DNS:

I now know CNN.com

and I'll remember it for later

Lab Time!

- Dig
- WHOIS
- nslookup

CAUCE
Coalition Against Unsolicited Commercial Email

Lab #1

Dig 157.166.249.11

CAUCE

Coalition Against Unsolicited Commercial Email

Lab #1

WHOIS CNN.com
WHOIS CAUCE.ORG
WHOIS YourOrg.tld
WHOIS 64.57.183.103

CAUCE

Coalition Against Unsolicited Commercial Email

Lab #1

NSlookup CNN.com
NSlookup CAUCE.ORG
NSlookup YourOrg.tld

CAUCE

Coalition Against Unsolicited Commercial Email

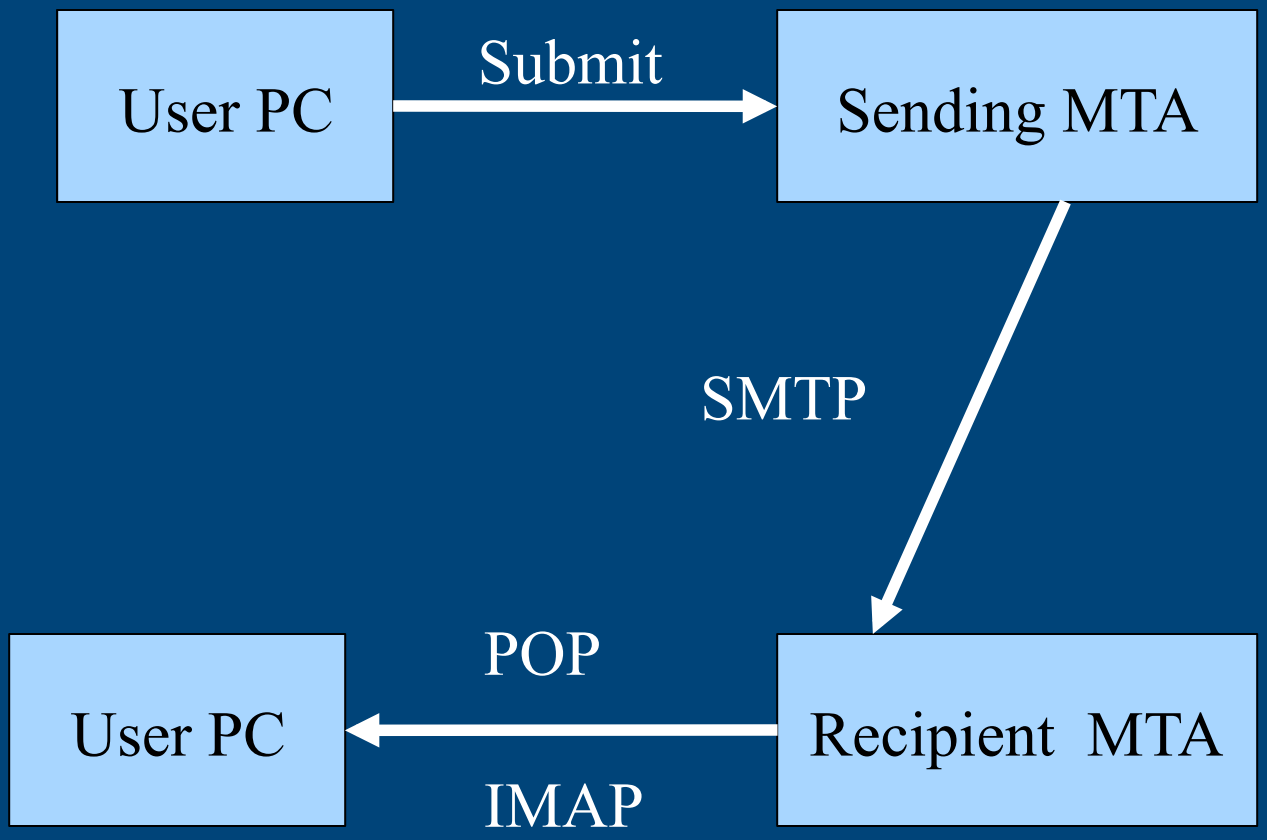
Basic e-mail forensics
Part II : Message Delivery

John R. Levine
President, CAUCE

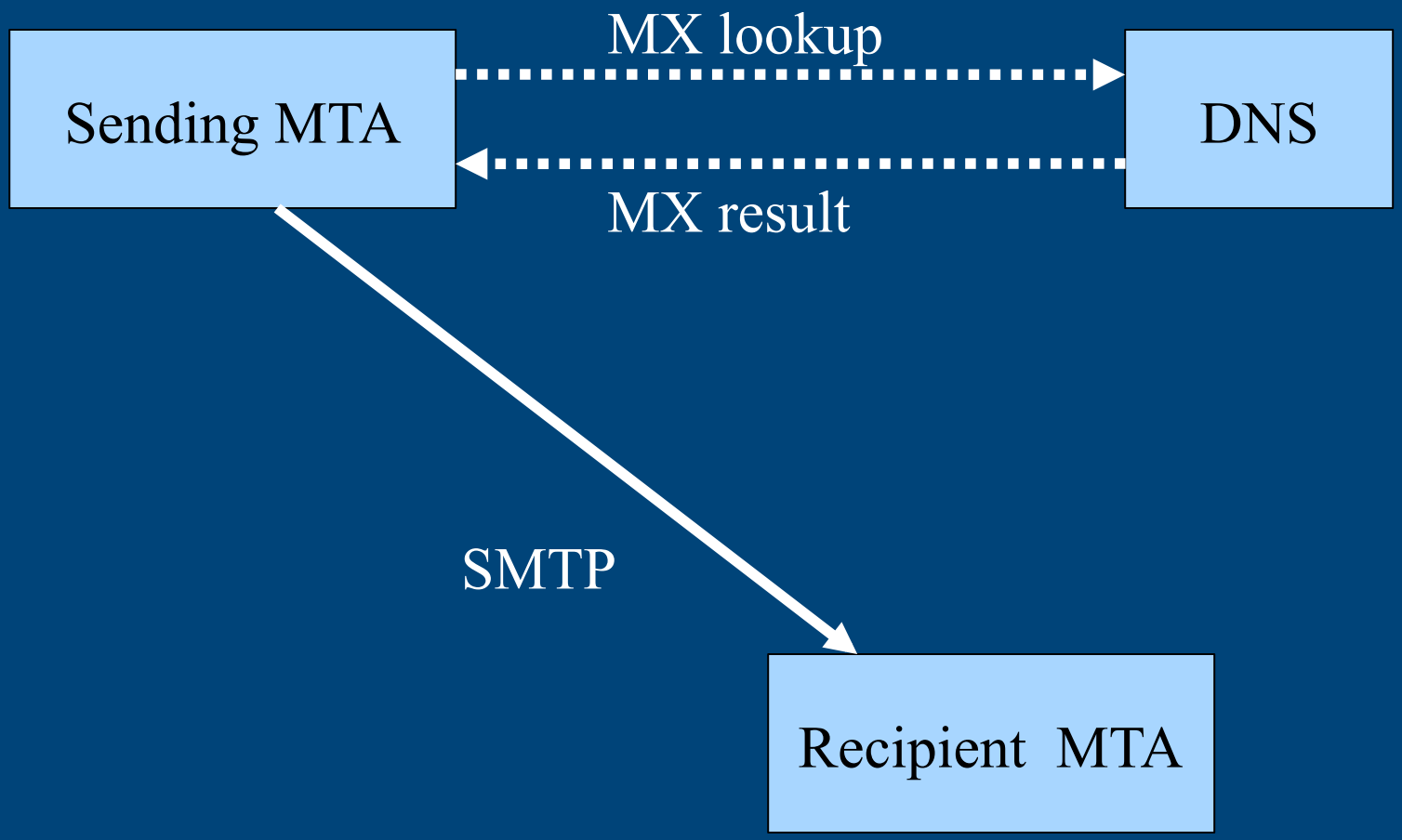
Part I Topics

- The route that mail takes
- Names and addresses
- Parts of a mail message
- Tracing a message's path
- Telling fact from fiction
- What's in a message: MIME and attachments

SMTP mail


User PC
Submit
Sending MTA
SMTP
User PC
POP
IMAP
Recipient MTA

SMTP mail



SMTP Session

Connect from 64.57.183.34

```
                                    220 mail1.iecc.com ESMTP
HELO leila.iecc.com
                                    250 mail1.iecc.com
MAIL FROM:<johnl@iecc.com>
                                    250 2.1.0 Sender ok.
RCPT TO:<comments@cauce.org>
                                    250 2.1.5 Recipient ok.
DATA
                                    354 Send your message.
Blah blah
.
                                    250 2.6.0 Accepted.
QUIT
                                    221 2.0.0 Good bye.
```

SMTP Session

Connect from **64.57.183.34**

```
HELO leila.iecc.com
                                    220 mail1.iecc.com ESMTP
MAIL FROM:<johnl@iecc.com>
                                    250 mail1.iecc.com
RCPT TO:<comments@cauce.org>
                                    250 2.1.0 Sender ok.
DATA
                                    250 2.1.5 Recipient ok.
                                    354 Send your message.
Blah blah
.
                                    250 2.6.0 Accepted.
QUIT
                                    221 2.0.0 Good bye.
```

Parts of a mail message

- Header
  - Manual parts
  - Automatic parts
- Body

```
Date: Mon, 4 Apr 2011 09:20:34 -0400
From: Andre.Leduc@ic.gc.ca
To: johnl@taugh.com
Subject: proposal for "Basics of E-Mail Fore

Hi John,

Our session starts at ...
```

Manual vs. Automatic Header

- Manual headers
  - Created by sender
  - To:, From:, Subject:, Date:, …
  - All easily faked

Automatic headers

Added by mail system

Real ones are reliable

Spammers add fake ones

Regular vs. Trace Headers

- Regular headers
  - Created when message is first sent
  - Or maybe when delivered

Trace headers

Added at the top when message passes through a mail system

Analogous to a postmark

All automatic

SMTP and Automatic Headers

- Headers created from SMTP session info
- Tells you how they got there
- Each hop adds headers at the top of the message
  - Creates a chain of custody
  - Well, if you're lucky

SMTP Session

Connect from 64.57.183.34

```
                                    220 mail1.iecc.com ESMTP
HELO leila.iecc.com
                                    250 mail1.iecc.com
MAIL FROM:<johnl@iecc.com>
                                    250 2.1.0 Sender ok.
RCPT TO:<comments@cauce.org>
                                    250 2.1.5 Recipient ok.
DATA
                                    354 Send your message.
Blah blah
.
                                    250 2.6.0 Accepted.
QUIT
                                    221 2.0.0 Good bye.
```

HELO and EHLO

- Sending host identifies itself
  - In theory, at least
  - Useful to check name if no rDNS

```
EHLO scmze001.ssan.egs-seg.gc.ca
HELO yahoo.com
HELO oemcomputer
```

Header types

- Familiar visible ones
  - **From: Sender:**
  - **To: Cc: Bcc: Reply-To:**
  - **Subject: Date:**
  - **Resent-From: Resent-To: ...**
- Less familiar:
  - **Message-ID: From_**
  - **Return-Path: Delivered-To:**
  - **Mime-Version: Content-Type: Content-Transfer-Encoding:**
  - **Received:**

Received headers

- Usually added each trip through a mail server
- Often records SMTP sessions
- Spammers often add fake ones

```
Received: from scmze001.ssan.egs-seg.gc.ca
 (scmze001.ssan.egs-seg.gc.ca [205.194.19.85])
  by mail1.iecc.com ([64.57.183.56]) with ESMTP via TCP
  id 169741201; 04 Apr 2011 13:21:23 -0000
```

Typical received headers

- From host / IP
- By host
- Id
- Date

- For user
- With
  - SMTP/ESMTP
  - Internal stuff

HELO

IP

```
Received: from mail06.o2online.de ([82.113.101.34])
    by mail.davjam.org with ESMTP id m9CEoHsu019439 for
    <blacklist-me@davjam.org>; Sun, 12 Oct 2010 15:50:25 +0100

Received: from User ([193.120.116.182]) by mail06.o2online.de
(8.12.11.20060308/8.12.11) with ESMTP id m9CElgXf009277;
       Sun, 12 Oct 2010 16:47:47 +0200
```

Following the header chain

- Look for matching hosts and IP addresses
  - But remember that bad guys can do that too

```
Received: from avas-mr01.fibertel.com.ar (avas-mr01.fibertel.com.ar
   [24.232.0.214]) by tarpit2.thrush.com (8.14.1/8.14.1) with ESMTP id
   l9448OYJ014492 for <spamvictim@target.site>;
   Thu, 4 Oct 2007 00:08:26 -0400 (EDT)

Received: from pc97.telecentro.com.ar ([200.115.245.97]:3577
   "EHLO andres" smtp-auth: "manuelcastillo@fibertel.com.ar"
   rhost-flags-OK-FAIL-OK-FAIL) by avas-mr01.fibertel.com.ar
   with ESMTPA id S866473AbXJDDPY convert rfc822-to-8bit;
   Thu, 4 Oct 2007 00:15:24 -0300
```

A more complex chain

```
Received: from QMTA10.emeryville.ca.mail.comcast.net
(qmta10.emeryville.ca.mail.comcast.net [76.96.30.17])
 by mail2.panix.com (Postfix) with ESMTP id 4824334814
 for <sethb@panix.com>; Sun, 12 Oct 2008 10:21:01 -0400 (EDT)
Received: from OMTA01.emeryville.ca.mail.comcast.net
([76.96.30.11])
       by QMTA10.emeryville.ca.mail.comcast.net with comcast
       id RqKP1a00E0EPchoAAqM0i7; Sun, 12 Oct 2008 14:21:00 +0000
Received: from smailcenter45.comcast.net ([204.127.205.145])
       by OMTA01.emeryville.ca.mail.comcast.net with comcast
       id RqLa1a00638kpyc8MqLaBp; Sun, 12 Oct 2008 14:21:00 +0000
X-Authority-Analysis: v=1.0 c=1 a=eb9NMfVVeg676gYa4jgA:9
 a=iUq6S4YwdhfTmiOFdj4A:7 a=Lu_SeRBmK5rpI5pj6iEf5i01hLwA:4
a=EfJqPEOeqlMA:10
 a=zxxVM3CWV3sA:10
Received: from [41.220.75.3] by smailcenter45.comcast.net;
       Sun, 12 Oct 2008 14:20:33 +0000
From: 2muchego@comcast.net (ROBERT INVESTMENT)
Subject: Risk Free Loan==Apply Now
```

But sometimes ...

```
Return-Path: <decal1calamitous@gmail.com>
Received: (qmail 13007 invoked from network); 15 Oct 2008 23:50:09 -0000
Received: from confoco.com (confoco.com [157.100.193.238])
  by mail1.iecc.com ([208.31.42.56])
  with ESMTP via TCP id 66347408; 15 Oct 2008 23:50:06 -0000
Received: from DM (unknown [125.116.102.46])
    by confoco.com (Postfix) with SMTP id 764B3DA14F9;
    Wed, 15 Oct 2008 18:43:29 -0500 (ECT)
Received: from prance-podge.gmail.com (HELO Delldim5150)
([157.100.193.238]) by colorimeter-noaa.gmail.com with ESMTP;
     Fri, 17 Oct 2008 06:44:02 +0300
Date: Fri, 17 Oct 2008 04:46:02 +0100
From: "Miranda T Pat" <decal1calamitous@gmail.com>
To: webmaster@about-the-web.com
Subject: D e ntists List for the United States
```

To and From addresses

- Visible headers are just comments
  - **`From: Sender: Reply-To:`**
  - **`To: Cc: Bcc:`**
- Less visible headers show SMTP addresses
  - **`From_`**
  - **`Return-Path: Delivered-To:`**

Spot the sender

```
From nobody@server4.mjbconsulting.com Wed Oct 15
   04:11:25 2008
Received: from server4.mjbconsulting.com
   (server4.mjbconsulting.com [64.38.12.82])
 by mail2.panix.com (Postfix) with ESMTP id
   8D3BA34821
 for <sethb@panix.com>; Wed, 15 Oct 2008 04:11:24
   -0400 (EDT)
Received: from nobody by server4.mjbconsulting.com
   with local (Exim 4.69) (envelope-from
   <nobody@server4.mjbconsulting.com>)
   id 1Kq1TL-0002r3-GY
 for sethb@panix.com; Wed, 15 Oct 2008 01:11:12
   -0700
To: sethb@panix.com
Subject: You are a winner !!!
From: NOKIA <info@nokia.com>
```

More on headers

- Can often use to guess where the mail came from
- Also to check on authentication
- But we'll return to that later

Lab time!

- Follow the header chain
- Where did these messages come from?

Lab time! Lab #2

- Take one of the five spamples and put the headers into the Google Header Analysis Tool
- Find the Sending IP – check the IP reputation at Sender Score and Sender Base
- Use the DCC Tool to check to see how many copies of this spam are known to have been sent

Message defects

- Spamware is written sloppily
- Match up the defects to match up the spammer

- Missing date or message ID
- Peculiar punctuation, spelling

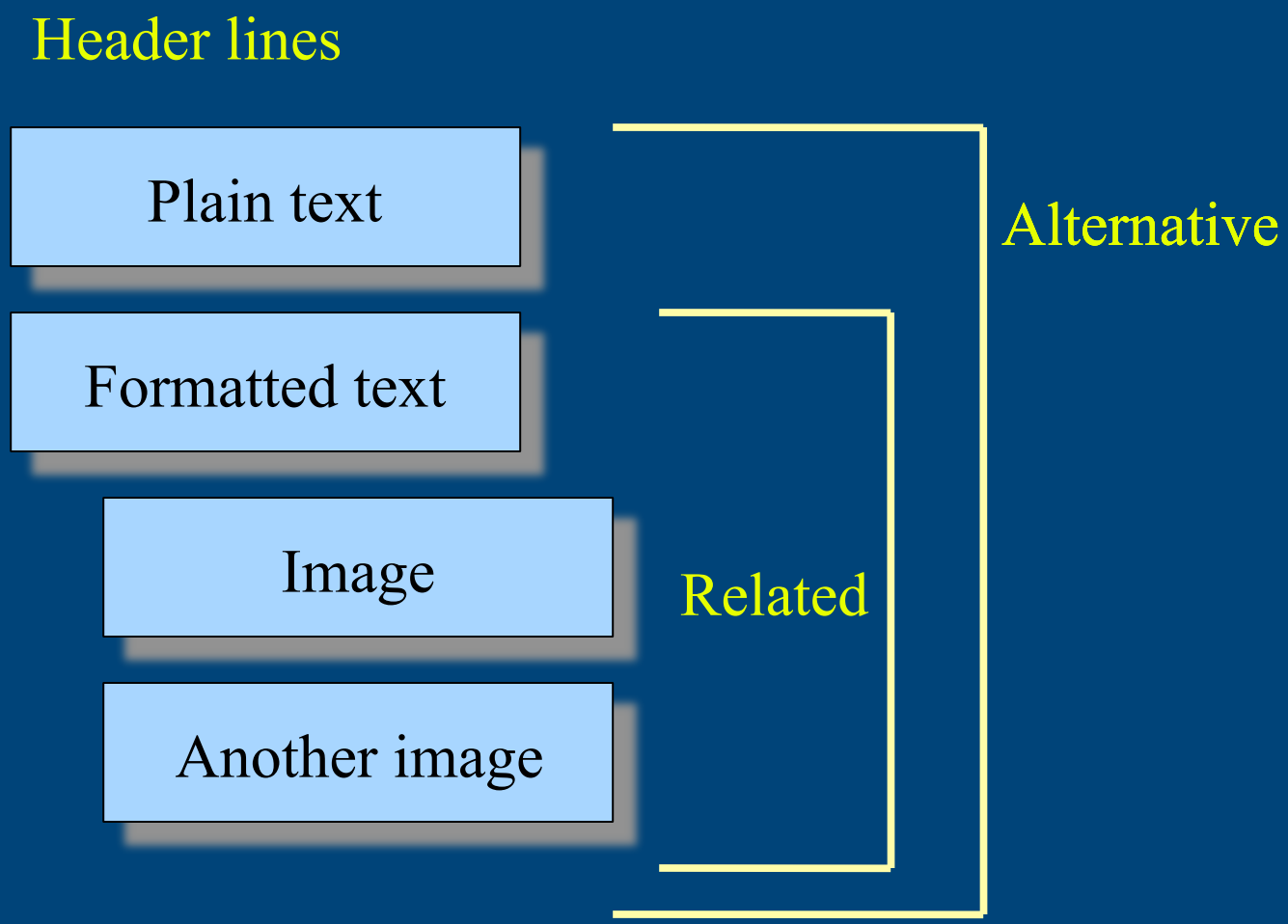
MIME (Multipart Internet Mail Extensions)

- Originally, mail was all text
- Now mail is still all text
- But we have ways to disguise other stuff as text

Taking apart MIME

- Anything beyond plain text is MIME
  - HTML mail
  - Multi-version mail
  - Attachments
  - Embedded pictures
- Your mail program is too helpful here
  - ~~Microsoft Outlook~~
- Look at the actual source, which is all text

MIME Structure



MIME Structure

- Content-Type: multipart/*something*
  - Multipart/alternative
  - Multipart/mixed
  - Multipart/related
- Often nested

```
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="part1_c3b.1c72d5d2.341c46b9_alt_boundary"

--part1_c3b.1c72d5d2.341c46b9_alt_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

All: I've attached the latest draft.
```

Formatted mail

- Pure HTML (Mostly in bulk mail)
  ```
  Content-Type: text/html; charset="US-ASCII"
  ```
- Alternative text/HTML (very common)
  ```
  Content-Type: multipart/alternative;
  boundary="part1_c3b.1c72d5d2.341c46b9_boundary"
  ```
- ```
  --part1_c3b.1c72d5d2.341c46b9_boundary
  Content-Type: text/plain; charset="US-ASCII"

  Hi there

  --part1_c3b.1c72d5d2.341c46b9_alt_boundary
  Content-Type: text/html; charset="US-ASCII"
  Content-Transfer-Encoding: quoted-printable

  Hi there
  ```
  ```

MIME encodings

- Quoted printable
  `this=20is=20some=20text=41`

- Base64
  - Decoders easily available
  - http://www.toastedspam.com/decode64
  - http://base64decode.org/

```
VGhlIGJveSBzdG9vZCBvbiB0aGUgYnVybmluZyBkZWNrLA0KSGlzIGZsZWVjZSB3YXMgd2hpdGUg
YXMgc25vdywNCkhlIHN0dWNrIGEgZmVhdGhlciBpbiBoaXMgaGF0LA0KSm9obiBBbmRlcnNvbiwg
bXkgSm8hDQo=
```

MIME attachments

- Multipart/mixed
  - Text (perhaps multipart/alternative)
  - Other type: image, PDF, executable virus, DOC, embedded message, …
- Multipart/related
  - HTML codes in text can refer to other parts to include images in messages
  - Can embed bad stuff, but that's not common

MIME character sets

- US-ASCII
  - Fine if you speak English
- ISO-8859-1
  - Mieux pour ceux qui parlent français, pas pour chinois
- UTF-8
  - Becoming de-facto standard
- Anything beyond ASCII requires encoding

SPF and DKIM

- SPF: *path authentication*
  - Did this message come from where it's supposed to come from
- DKIM: *message authentication*
  - Does this message have a valid cryptographic signature?

SPF

- Look up domain in SMTP **`mail from`** address
- See if the sending IP is listed
- If yes, it's probably real
- If not, maybe, maybe not
  - Highly reliable for “spam cannons”
  - Much less reliable for individual mail

DKIM

- Add a cryptographic signature to the message itself keyed to a domain
- Says it's the same message that it signed
- Only useful if you know the signer

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple; d=iecc.com;
    h=date:message-id:from:to:mime-version:subject:content-
type:vbr-info:user-agent; s=8452.4d970617.k1104;
i=tonia@submit.iecc.com; bh=FCqgWThO5VxRTq8pb4RTB9ekowZQOkOYKD
+x/R5Z/Jo=;
b=e4o0eXiWB8X75UZ5NDjtZrs9wMxJq1tew3esOG9F7AVWgsc26+9716fO8yywW
pxmB1/x2WLBEONkdKEaw+xjoz9Brx6AYdG77THhKn7+/
SseHMjyko0Ww5rRusLQRfDBANkkAA/
N2mQnfxyN5YMNy1FYqn9ko79bhyYTPlCBp/8=
```

Authentication Results

- Reports status of SPF, DKIM, etc.
- Credible when added by known system

Authentication-Results: iecc.com / 1; spf=pass
spf.mailfrom=rj29@gmail.com
spf.helo=mail-vc0-f174.google.com;
dkim=pass header.d=gmail.com

Recognizing mail sources

- User mail programs (Outlook, Thunderbird)
- Web mail (Hotmail, Yahoo, many others)
- Scripts on web sites
- Zombies

User mail programs

- Initial hop to mail server
- Usually identifies the program

```
Received: from flimsy.graphics.cornell.edu (graphics.cornell.edu
[128.84.247.51]) by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 172902421; 17 May 2011 16:52:52 -0000
Received: from [128.84.247.47] (sandman.graphics.cornell.edu
[128.84.247.47])  by flimsy.graphics.cornell.edu (Postfix) with ESMTP
    id BED5CA0246; Tue, 17 May 2011 12:52:45 -0400 (EDT)
Message-ID: <4DD2A7C9.509@graphics.cornell.edu>
Date: Tue, 17 May 2011 12:52:25 -0400
From: Hurf Sheldon <hurf@graphics.cornell.edu>
Organization: The Program of Computer Graphics
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.7)
Gecko/20100111 Thunderbird/3.0.1
MIME-Version: 1.0
```

Outlook messages (Exchange)

```
Received: from ht2-outbound.cloudmark.com (ht2-outbound.cloudmark.com
    [72.5.239.36]) by sbh17.songbird.com (8.13.8/8.13.8) with ESMTP id
oA9ILcBS006212 (version=TLSv1/SSLv3 cipher=RC4-MD5 bits=128 verify=FAIL)
    for <dkim-ops@mipassoc.org>; Tue, 9 Nov 2010 10:21:43 -0800
Received: from EXCH-C2.corp.cloudmark.com ([172.22.1.74]) by
    spite.corp.cloudmark.com ([172.22.10.72]) with mapi;
    Tue, 9 Nov 2010 09:51:04 -0800
From: "Murray S. Kucherawy" <msk@cloudmark.com>
To: "dkim-ops@mipassoc.org" <dkim-ops@mipassoc.org>
Date: Tue, 9 Nov 2010 09:51:03 -0800
Thread-Topic: [dkim-ops] Who uses DKIM these days?
Thread-Index: AcuAKGA1ILpY+aCYQfCA+QS5YqOBAAADWf4Q
Message-ID: <F5833273385BB34F99288B3648C4F06F1340E63E93@EXCH-
C2.corp.cloudmark.com>
References: <20101109061013.60424.qmail@joyce.lan>
    <4CD90BF7.3000304@sonnection.nl>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
acceptlanguage: en-US
```

Outlook messages (Simple)

```
Received: from smtp.clarityconnect.com (smtp.clarityconnect.com
[209.150.236.156]) by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 169749220; 04 Apr 2011 16:48:47 -0000
Received: from mail.clarityconnect.com (mail.clarityconnect.com
[209.150.236.153]) by smtp.clarityconnect.com with SMTP;
   Mon, 4 Apr 2011 12:47:36 -0400
Received: from OfficeDell (pool-96-238-143-158.syrcny.east.verizon.net
[96.238.143.158]) by mail.clarityconnect.com with SMTP;
   Mon, 4 Apr 2011 12:46:55 -0400
From: "Carol Palmer" <cohen-palmer@clarityconnect.com>
To: "'John R. Levine'" <johnl@iecc.com>
Subject: extension forms and estimated tax coupons
Date: Mon, 4 Apr 2011 12:46:54 -0400
Message-ID: <BA8B4B00A0504853B9B42627128BD191@OfficeDell>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_003A_01CBF2C6.635AC2D0"
X-Mailer: Microsoft Office Outlook 11
Thread-Index: Acvy5+dGuRaoAY9HQICqdL70Hts1BA==
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5994
```

Web mail

- Typically shows the IP of the web client
  - Gmail is the notable exception
- First hop header looks different

Hotmail

```
Received: from snt0-omc3-s36.snt0.hotmail.com (snt0-omc3-
s36.snt0.hotmail.com [65.55.90.175])
  by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 170002452; 09 Apr 2011 14:37:00 -0000
Received: from SNT112-W40 ([65.55.90.137]) by snt0-omc3-
s36.snt0.hotmail.com with Microsoft
    SMTPSVC(6.0.3790.4675);
     Sat, 9 Apr 2011 07:36:59 -0700
Message-ID: <SNT112-W40B4C387CA3869F02C018A83A60@phx.gbl>
Return-Path: mberman116@hotmail.com
Content-Type: multipart/alternative;
    boundary="_23000652-6dbe-49c3-89b6-fa7310324702_"
X-Originating-IP: [66.152.115.226]
From: Monty Berman <mberman116@hotmail.com>
To: johnl levine <johnl@unitarian.ithaca.ny.us>
Subject: FW: Summer services invitation to speak
Date: Sat, 9 Apr 2011 10:36:58 -0400
```

Yahoo

```
Received: from nm30-vm0.bullet.mail.bf1.yahoo.com (nm30-
vm0.bullet.mail.bf1.yahoo.com [98.139.213.126]) by mail1.iecc.com
([64.57.183.56]) with SMTP via TCP id 172928006; 18 May 2011 00:41:23
-0000
Received: from [98.139.212.152] by nm30.bullet.mail.bf1.yahoo.com with
NNFMP; 18 May 2011 00:41:22 -0000
Received: from [98.139.212.195] by tm9.bullet.mail.bf1.yahoo.com with
NNFMP; 18 May 2011 00:41:22 -0000
Received: from [127.0.0.1] by omp1004.mail.bf1.yahoo.com with NNFMP; 18
May 2011 00:41:22 -0000
Received: (qmail 23427 invoked by uid 60001); 18 May 2011 00:41:22 -0000
DKIM-Signature: v=1; a=rsa-sha256; ...
Message-ID: <440466.23384.qm@web161405.mail.bf1.yahoo.com>
X-YMail-OSG: M3kmum0VM1lJU0Y41MZBHy. ...
Received: from [66.152.118.17] by web161405.mail.bf1.yahoo.com via HTTP;
Tue, 17 May 2011 17:41:22 PDT
X-Mailer: YahooMailWebService/0.8.111.303096
```

Gmail

```
Received: from mail-iw0-f173.google.com (mail-iw0-f173.google.com
[209.85.214.173])   by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 172928197; 18 May 2011 00:45:23 -0000
Received: by iwl42 with SMTP id 42so1042148iwl.4
        for <abuse@no.sp.am>; Tue, 17 May 2011 17:45:22 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; ...
MIME-Version: 1.0
Received: by 10.42.67.80 with SMTP id s16mr969467ici.473.1305679521971;
Tue, 17 May 2011 17:45:21 -0700 (PDT)
Received: by 10.42.171.65 with HTTP; Tue, 17 May 2011 17:45:21 -0700
(PDT)
Date: Tue, 17 May 2011 20:45:21 -0400
Message-ID: <BANLkTik7iEzVn7GTTJXcNCXbOY_ykKUXGw@mail.gmail.com>
Subject: You can't find me
From: John Levine <john.levine@gmail.com>
To: abuse@no.sp.am
Content-Type: text/plain; charset=ISO-8859-1
```

Non-web Gmail

```
Received: from mail-qy0-f173.google.com (mail-qy0-f173.google.com
[209.85.216.173]) by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 172928682; 18 May 2011 00:56:15 -0000
Received: by qyk36 with SMTP id 36so2505183qyk.4
        for <abuse@no.sp.am>; Tue, 17 May 2011 17:56:14 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; ...
Return-Path: <john.levine@gmail.com>
Received: from joyce.lan (pedro.iecc.com [66.152.118.17])
  by mx.google.com with ESMTPS id k2sm649978qcu.31.2011.05.17.17.56.13
  (version=TLSv1/SSLv3 cipher=OTHER);
   Tue, 17 May 2011 17:56:14 -0700 (PDT)
Message-ID: <4DD3192D.3070507@gmail.com>
Date: Tue, 17 May 2011 20:56:13 -0400
From: John L <john.levine@gmail.com>
User-Agent: Mozilla/5.0 (X11; U; FreeBSD amd64; en-US; rv:1.9.2.17)
Gecko/20110511 Thunderbird/3.1.10
MIME-Version: 1.0
To: abuse@no.sp.am
Subject: you can't find me
```

Non-web Gmail

```
Received: from mail-iy0-f172.google.com (mail-iy0-f172.google.com
[209.85.210.172]) by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 172733672; 13 May 2011 22:03:01 -0000
Received: by iyn15 with SMTP id 15so3117224iyn.31
        for <johnl@iecc.com>; Fri, 13 May 2011 15:03:00 -0700 (PDT)
Received: by 10.231.74.84 with SMTP id t20mr1523056ibj.38.1305324180005;
        Fri, 13 May 2011 15:03:00 -0700 (PDT)
Return-Path: <lrf23@cornell.edu>
Received: from LauraPC (cpe-74-79-23-242.twcny.res.rr.com [74.79.23.242])
  by mx.google.com with ESMTPS id a8sm1104337ibg.31.2011.05.13.15.02.58
  (version=SSLv3 cipher=OTHER);  Fri, 13 May 2011 15:02:59 -0700 (PDT)
From: "Laura Ford" <lrf23@cornell.edu>
To: "'John R. Levine'" <johnl@iecc.com>
Subject: Project Homepage
Date: Fri, 13 May 2011 18:02:58 -0400
Message-ID: <001e01cc11b9$85c628c0$91527a40$@edu>
MIME-Version: 1.0
Content-Type: text/plain;
    charset="us-ascii"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Office Outlook 12.0
```

Generic web mail

```
Return-Path: <johnl@iecc.com>
X-Originating-IP: [64.57.183.34]
Received: from 127.0.0.1  (EHLO leila.iecc.com) (64.57.183.34)
  by mta1065.mail.mud.yahoo.com with SMTP; Fri, 09 Mar 2012 17:21:32
-0800
Received: (qmail 46627 invoked by uid 80); 10 Mar 2012 01:21:30 -0000
DKIM-Signature: v=1; a=rsa-sha256; c=simple; d=iecc.com;
    s=b622.4f5aac9a.k1203; ...
Received: from 66.152.118.17
        (SquirrelMail authenticated user johnl@iecc.com)
        by mail.iecc.com with HTTP;
        Fri, 9 Mar 2012 20:21:30 -0500
Message-ID: <f4a1e1098128b0d48ae9111edbf5cbd4.squirrel@mail.iecc.com>
Date: Fri, 9 Mar 2012 20:21:30 -0500
Subject: lunch would be nice
From: johnl@iecc.com
To: jrlevine2@yahoo.com
User-Agent: SquirrelMail/1.4.22
```

Script mail

- Web scripts send mail
  - Confirmations, notes to owners
- Many buggy scripts, often abused

Script / web

```
Received: from haygate.gojojar.com (b2.61.be.static.xlhost.com
[209.190.97.178]) by mail1.iecc.com ([64.57.183.56])
  with ESMTP via TCP id 172891348; 17 May 2011 10:55:29 -0000
Received: from [86.108.37.16] (helo=thebeejo.com)
    by haygate.gojojar.com with esmtpsa (SSLv3:AES256-SHA:256)
    (Exim 4.69) (envelope-from <mail26@thebeejo.com>) d 1QMHvy-0000Vf-CG
    for compilers@iecc.com; Tue, 17 May 2011 06:55:26 -0400
Date: Tue, 17 May 2011 12:32:28 +0300
From: "Transition Tech" <mail26@thebeejo.com>
To: "compilers" <compilers@iecc.com>
Subject: Business Analysis Training Program
X-mailer: Foxmail 6, 14, 103, 24 [cn]
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="=====Q2u_1U7RoJJIJM6dUUuMgSsHcD_jnZXslb_====="
Reply-To: training@transition-se.com
X-AntiAbuse: This header was added to track abuse, please include it with
any abuse report
X-AntiAbuse: Primary Hostname - haygate.gojojar.com
X-AntiAbuse: Original Domain - iecc.com
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - thebeejo.com
```

Zombieware

```
Return-Path: <rico.ops@terra.es>
Delivered-To: compilers-request@iecc.com
Received: (qmail 18351 invoked from network); 5 Oct 2007 19:16:12 -0000
Received: from outmailhost.terra.es (HELO csmtpout1.frontal.correo)
  (213.4.149.241) by mail.iecc.com with SMTP; 5 Oct 2007 19:16:11 -0000
Received: from hgcu.net (189.31.19.98) by csmtpout1.frontal.correo
       (7.3.105.2) (authenticated as rico.ops) id 470620D50001B7CF
       for compilers-request@iecc.com; Fri, 5 Oct 2007 21:17:20 +0200
Message-ID: <470620D50001B7CF@csmtpout1.frontal.correo>
       (added by postmaster@terra.es)
From: "rico.ops" <rico.ops@terra.es>
To: "compilers-request" <compilers-request@iecc.com>
Subject: traição
Date: Fri, 05 Oct 07 13:33:06 Hora oficial do Brasil
MIME-Version: 1.0
Content-Type: multipart/mixed;boundary= "----000_00BC_9D974EA3.6852A5A0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express
6.00.2462.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2462.0000
```

Looking for patterns

- Most spam is generated by scripts
- Occasional `%RECIPIENT%` bugs
- Patterns in layout, types of hashbusters

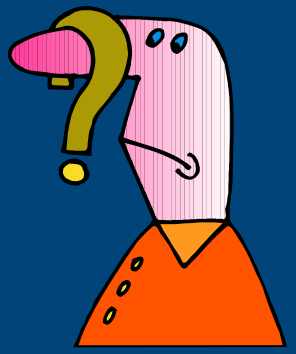
Bulk counting systems

- DCC
  - http://www.dcc-servers.net (official server)
  - Fully automated
  - Give it a message, it'll give you a count
  - http://Dcccheck.abuse.net (lookup server)

```
X-DCC-IECC-Metrics:
  gal.iecc.com 1107; bulk
  Body=127 Fuz1=1135
  Fuz2=many
```

Spam archives

- Usenet news.admin.net-abuse.sightings
  - Used to be several thousand a day, now just historical
  - Reasonably good quality
- Government archives
  - “Freezer” in Canada
  - “Fridge” at US FTC
  - Spammatters.com archive in Australia
  - Maybe Signal Spam in France
- Private collections
  - Many researchers and ISP keep them



Any questions?

CAUCE

Coalition Against Unsolicited Commercial Email

Basic e-mail forensics
Part III : Message Payloads

Neil Schwartzman
Executive Director, CAUCE

Part II Topics

- Sub-domains
- URIs
- WHOIS
- Nameservers
- Hosting IP Addresses
- Passive DNS

Sub-Domains

- BBC.co.uk
- My.Friend@ties.itu.int
- MyOther.Friend@oft.gsi.gov.uk
- http://news.bbc.co.uk

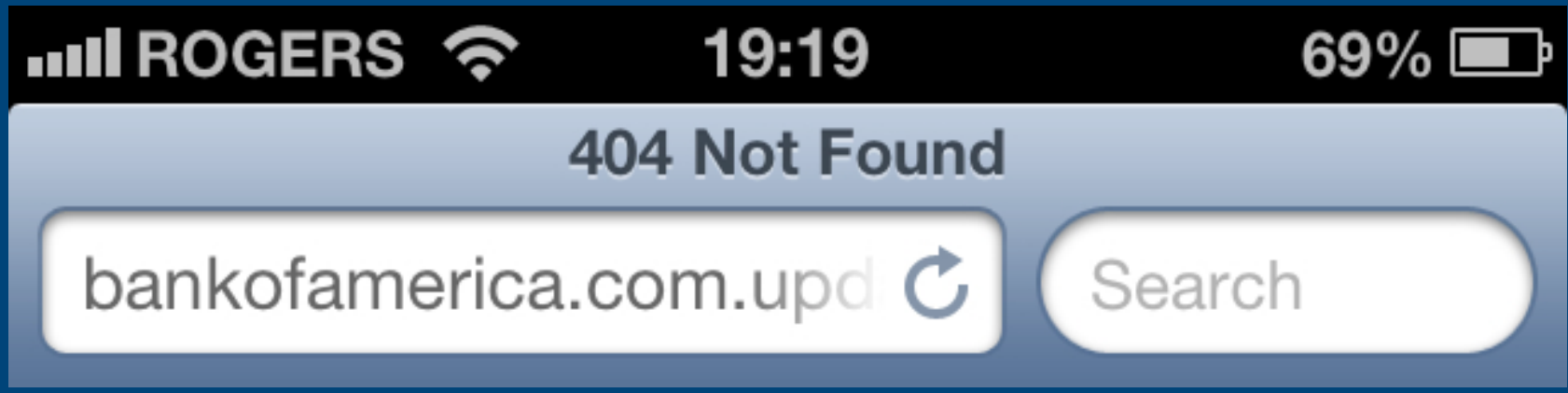
Fake Domains & Sub-domains

bbc-life.net
bbc-news.bbc-life.net
bbc-news.bbc-life.net
bbc-news.bbcchanel.com
bbc-news.bbcchanel.com
bbc-news.7daydietweightlossmealplan.com

Fake Sub-Domains

http://bankofamerica.com.update.sys.loginin.3220002322123 21.enessigorta.com/updat.sys.hey.bro.here/Sitkey.Signon.do/prospect.php

A long URL on iPhone …



URLs

http://News.bbc.co.uk
http://News.bbc.co.uk/index.html
ftp://bbc.co.uk
http://bbc-news.bbc-life.net

Compromised Host URLs

http://bbc.co.uk

http://bbc.co.uk/SyriaVote0829.php

http://bbc.co.uk/EvilMalwareHere.txt

http://bbc.co.uk/Flowers&Kittens.evl

Compromised Host URLs

http://www.japansec.com/bb.html
http://webhostingind.com/bb.html
http://muratlibelediyespor.org/bb.html
http://iklimsakarakoy.com/di.html

Be SAFE Sharing URLs: Break Then

http://www.japansec . com/bb.html

hxxp://webhostingind.com/bb.html

hxxp://muratlibelediyespor . org/bb.html

A host needs a home: Domain ➔ IP

http://bbc.co.uk - 212.58.253.67

http://news.bbc.co.uk - 212.58.246.129

http://MALWARE.bbc.co.uk - 67.215.65.132

http://bbc.co.uk/MALWARE.ppt - 212.58.253.67