%telnet summer2009.ukuug.org 25

220 summer2009.ukuug.org

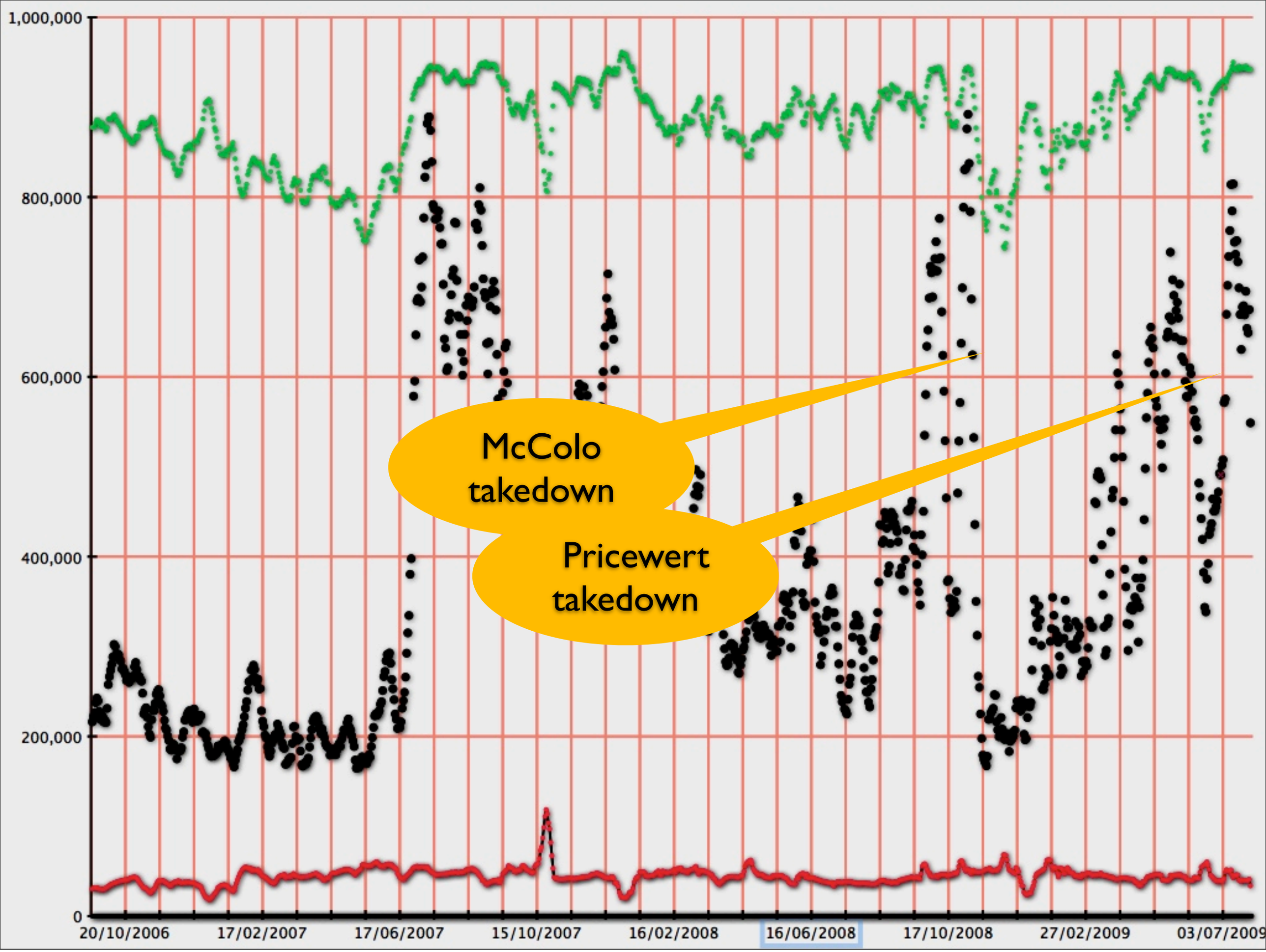
EHLO ian.eiloart

These are slides from my talk at ukuug summer 09 conference. They've been extensively modified to convey what I actually said, or wish I'd said!

Ian Eiloart, postmaster, University of Sussex, England.

- Fighting spam is about distinguishing between wanted and unwanted email. Currently, we're quite good a finding spam, but not so good at identifying wanted email. Whitelisting is haphazard, because we can't trust the envelope sender claim. We need to change that.

- In case you're in any doubt that spam is an ongoing problem, look at the following graph. It shows email deliveries (bottom line, red), email rejections (middle, black) and the % of mail rejected (top, green). Each datapoint is the daily number of emails averaged over the past seven days. For the green line, the scale should on the left should be read as zero to 100.


1,000,000
800,000
600,000
400,000
200,000
0
20/10/2006
17/02/2007
17/06/2007
15/10/2007
16/02/2008
16/06/2008
17/10/2008
27/02/2009
03/07/2009
McColo takedown
Pricewert takedown

Everyone's talking about it

CEAS.CC

- Furthermore, a lot of effort goes in to fighting spam that could otherwise be spent on making wanted mail more useful in various ways.
- At ukuug Summer 09, three of five email talks were about spam.
- At CEAS09, 33 of 34 papers were about spam! http://www.ceas.cc/2009

CEAS 09 programme

- Spam, Spam, Spam, Evaluating Online Text Classification Algorithms for Email Prediction, Spam, and Spam

War against spam

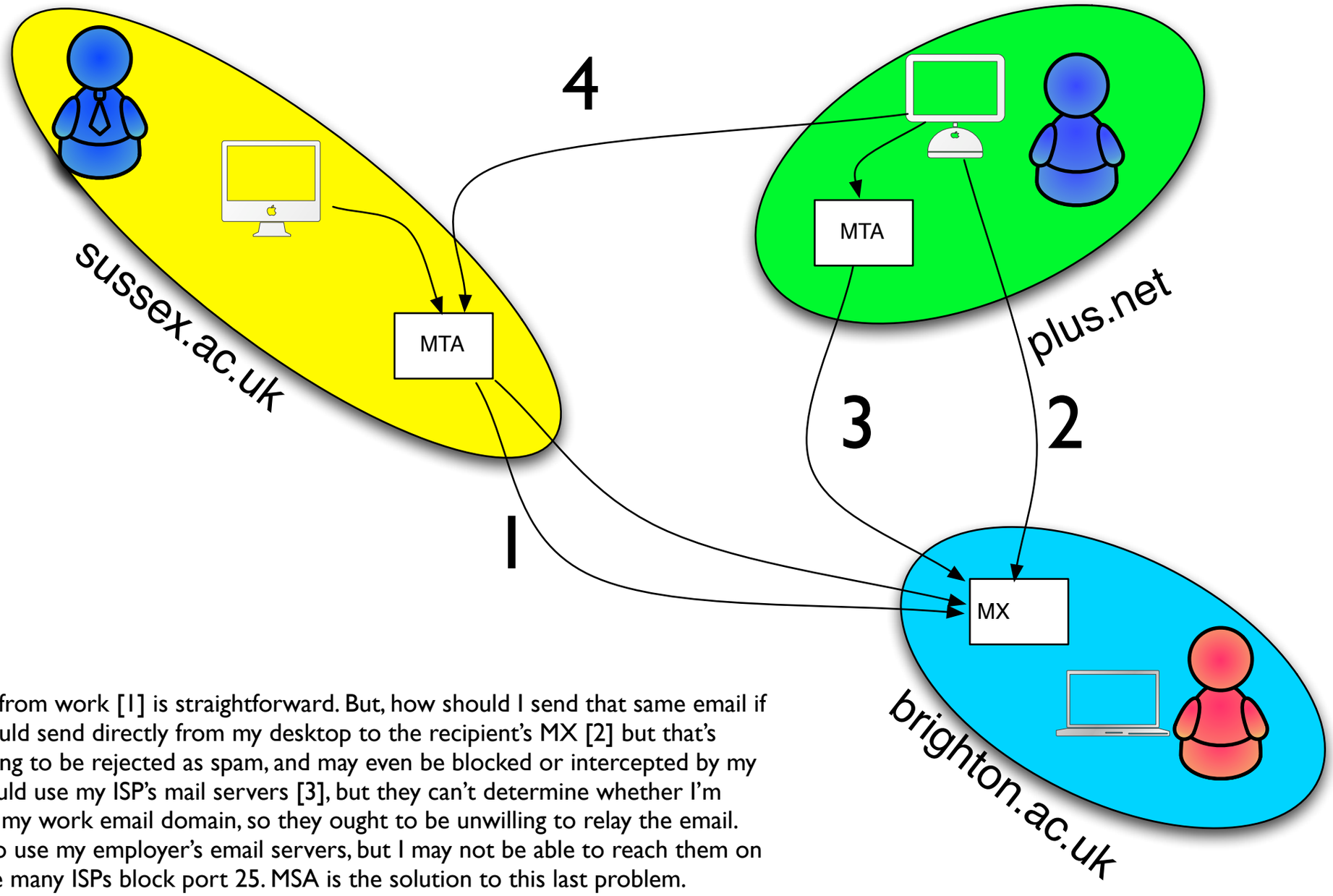
- my guess is that it'll take 5 to 10 years for sender reputation to become well established. Eventually, it'll be more important than IP address reputation.
- first, prevent sender address spoofing
- then, apply reputation services to the sender address
- reputation could be positive, negative or neutral for previously unseen addresses
- domain reputation might be applied to individual addresses, where either:
  - the domain reputation is sufficiently strong, or
  - the sender address reputation is neutral

Accountability

- It's easier to hold an email address owner to account, than an IP address owner for two reasons:
  - you have a address for the sender
  - the address is less likely to be shared by millions of people
- Assigning reputation to sender addresses gives better granularity
- But, requires confidence in sender address, so you have to be able to figure out which addresses aren't spoofed.
- Two technologies for recognising unspoofed addresses are catching on: SPF and DKIM. They can already give improved deliverability for senders, and spam rejection for receivers. Some day, you won't be able to deliver email at all without using one of these technologies, or some similar technology.
- Both require MSA

SMTP: RFC 5321

- The current standard for SMTP is rfc5321
- published Oct 08 Obsoletes 2821(April 98)
- Mentions 4409 (MSA) April 06 standard
- Mentions 4408 (SPF) April 06 experimental
- Mentions 4871 (DKIM) May 07 standard
- Some rival experimental protocols were also published in April 06, but haven't gained much traction.



Sending an email from work [1] is straightforward. But, how should I send that same email if I'm at home? I could send directly from my desktop to the recipient's MX [2] but that's almost always going to be rejected as spam, and may even be blocked or intercepted by my ISP's firewall. I could use my ISP's mail servers [3], but they can't determine whether I'm permitted to use my work email domain, so they ought to be unwilling to relay the email. Best practice is to use my employer's email servers, but I may not be able to reach them on port 25 - because many ISPs block port 25. MSA is the solution to this last problem.

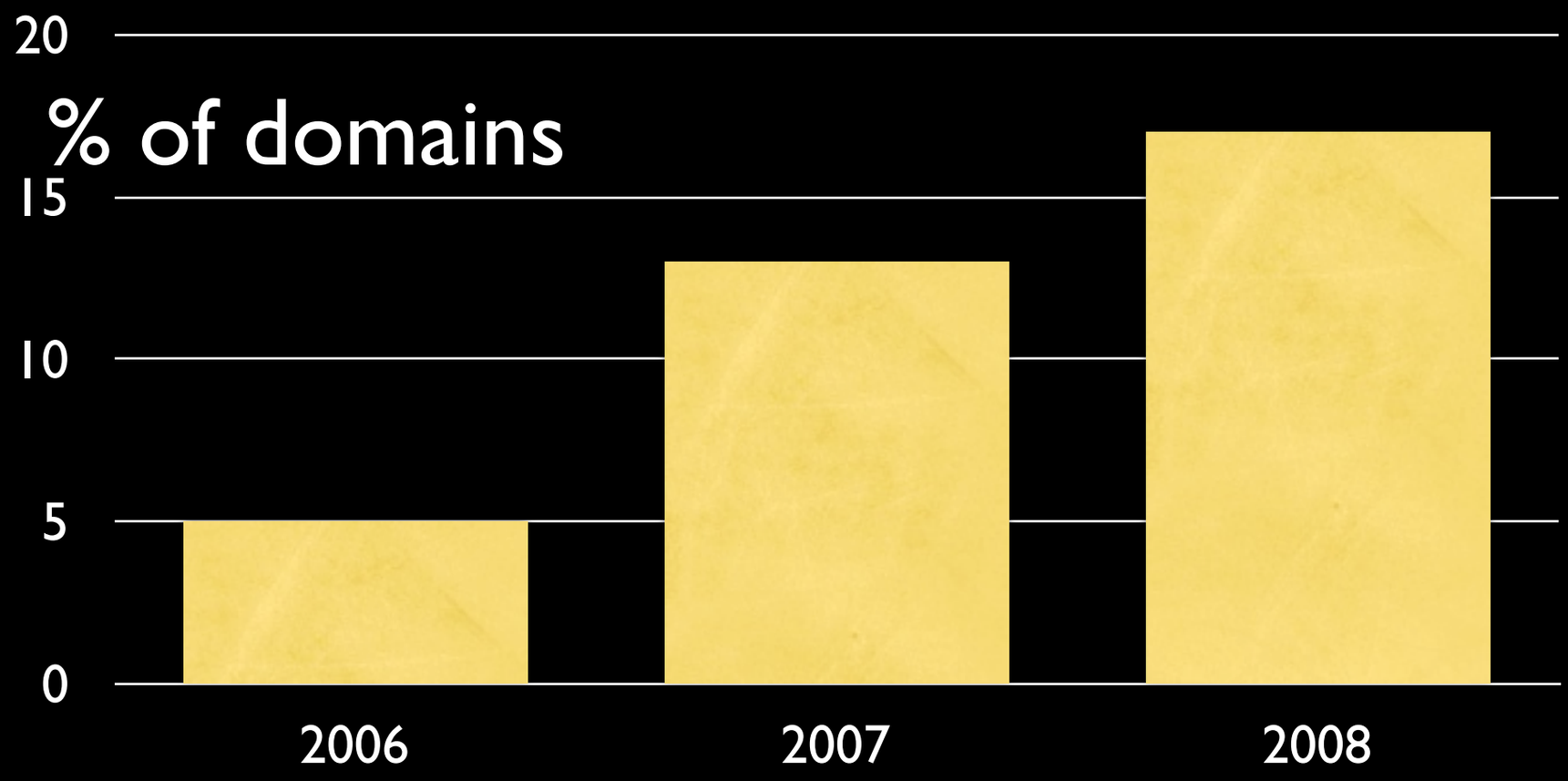
Message Submission Agent

- defined in rfc4409
- SMTP on Port 587
- for authenticated users only
- make them use it
  - require for ‘local’ email
  - make it the default port when you distribute email clients to your users
- Block outbound port 25
- Supported by most large email service providers like Gmail, Yahoo.
- Default for new Apple Mail, iPhone Mail accounts
- Preferred by Outlook 2007 Common Settings Discovery
- Thunderbird + Evolution need fixing.
- All mail clients should default to port 587

SPF Overview

- openspf.org/
- TXT or SPF record in DNS
- v=spf1 mx -all
- rewrite envelope sender address when forwarding
  - can use SRS (openspf.org/srs.html or some other scheme)
  - use proper mailing list software which rewrites sender domains
  - you must use a domain that you control

SPF takeup



http://dns.measurement-factory.com/surveys/

1 - 2 million domains were serveyed. In a separate Nov 2007 survey by spf-all.com 9.9% of 25 million domains were publishing SPF records. A sendmail.org survey of Fortune 500 companies and US banks found 90% published SPF records.

SPF users

gmail.com
hotmail.com
paypal.com
bl.uk
parliament.uk
live.com
ebay.com
facebook.com
blogger.com

friendster.com
skyrock.com
sina.com.cn
onet.pl
uol.com.br
craigslist.org
163.com
wp.pl
terra.com.br

xanga.com
badoo.com
maktoob.com
multiply.com
digg.com
about.com

All these domains publish spf records. You can check them at www.spf-all.com
Those in red, use "-all" records. So, if you think that SPF breaks forwarding, then your forwarding is already broken, and you probably need to fix it. On the other hand, you have a lot to gain by implementing SPF checks.

SPF deployment

- Implement MSA first, so you don't screw up your users.
- Work out where your mail servers are. That might be harder than you think. Check your firewall logs, and check your incoming mail logs. You still might miss outsourced services, though
- Publish SPF records in the DNS. It's advisable to start with ~all, not -all

why use SPF?

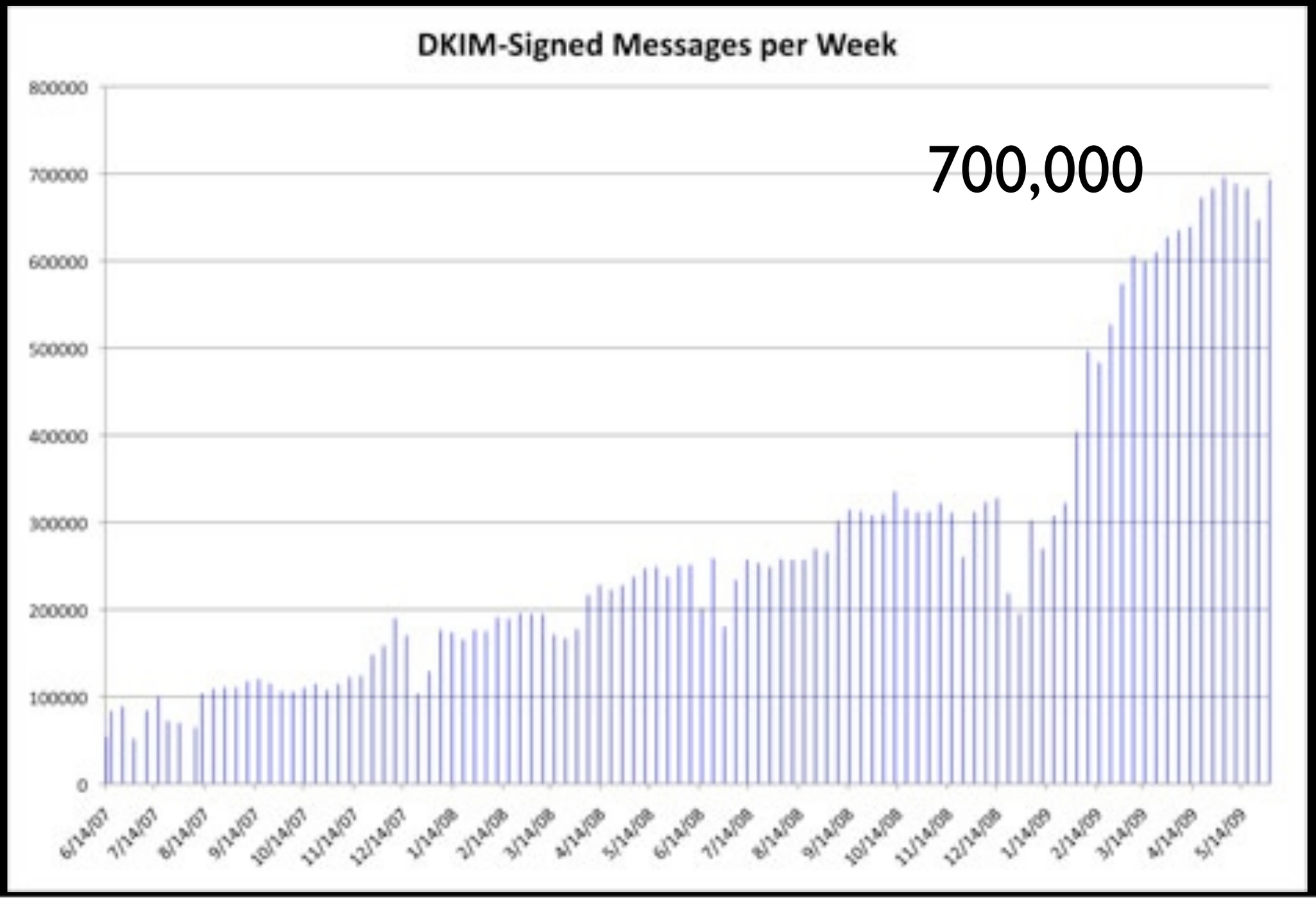
- `improves deliverability of your email.`
- **`-all`** for non-emitting domains helps others to spot when your domains have been spoofed.
- **`www.example.com spf v=1.0 -all`**
- people should be happier to whitelist your email addresses when they see a positive SPF pass, even with "**`~all`**"
- move to **`-all`** eventually

DKIM

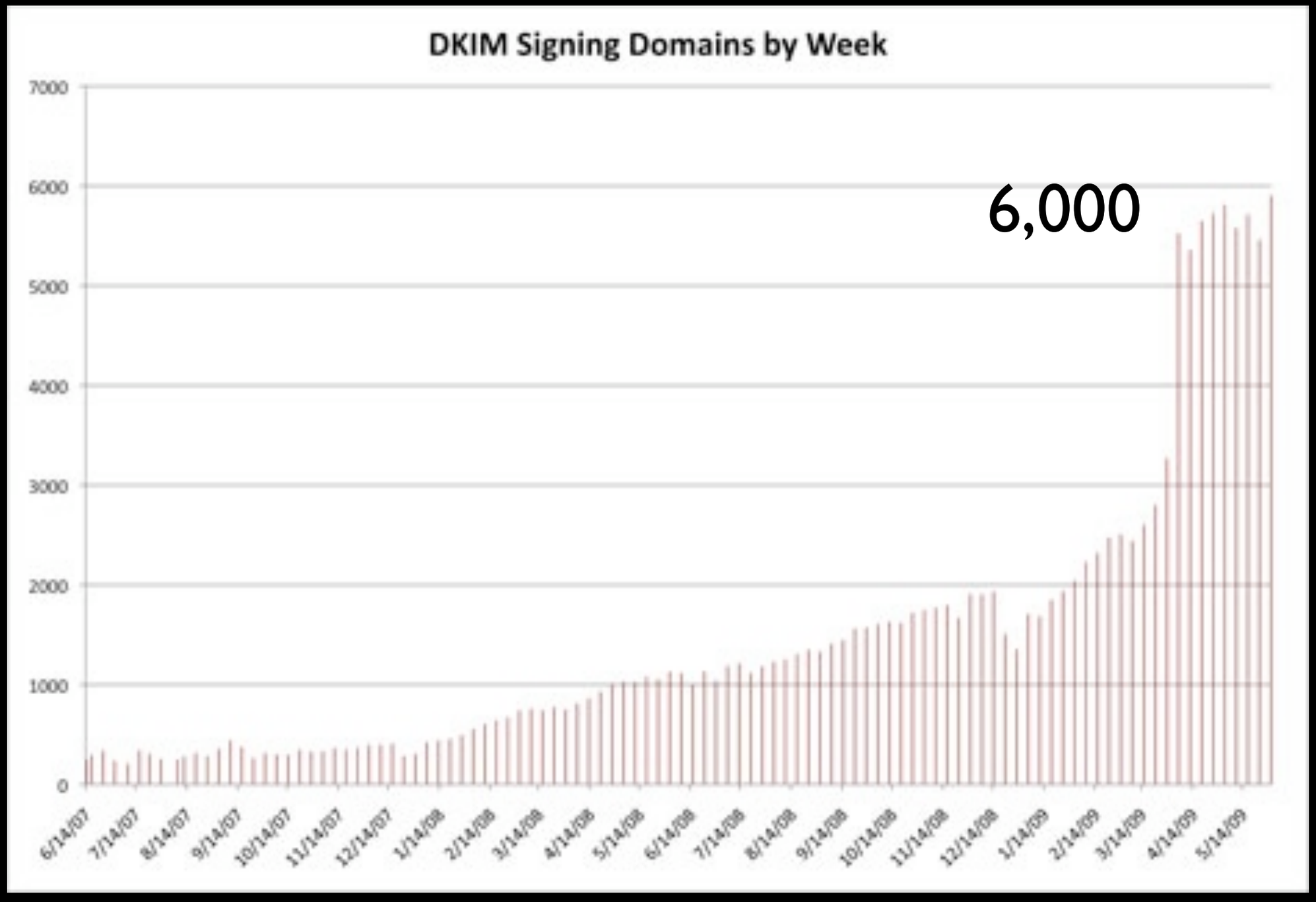
- dkim.org/
- rfc4871

- Can't trawl DNS for DKIM records- so hard to measure
- Traffic measurements up to 60% of Alexa 500 domains using DKIM.

blogs.cisco.com/



blogs.cisco.com/



DKIM header

```
Dkim-Signature: v=1; a=rsa-
sha256; c=relaxed/relaxed;
d=gmail.com; s=gamma;
h=domainkey-signature:mime-
version:received:date:message-
id:subject
:from:to:cc:content-type;
bh=JpNegSK3k3QWyYVKhyn8dgx8gvh
e3LbEuJiOnqX7JdY=;
b=oJ9f7kkYYWqQ2r6AGqBciopsgnDz
```

DNS record

- host -t txt gamma._domainkey.gmail.com
- k=rsa\; t=y\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4G NADCBiQKBgQDIhyR3oItOy22ZOaBrIVe 9m/iME3RqOJeasANSpg2YTHTYV +Xtp4xwf5gTjCmHQEMOs0qYu0FYiNQP QogJ2t0Mfx9zNu06rfRBDjiIU9tpx2T +NGIWZ8qhbiLo5By8apJavLyqTLavyPSrvsx

DKIM ADSP

Author Domain Signing Practices is a draft RFC. Look out for it's publication.

draft-ietf-dkim-ssp-10 (May 2009)

http://www.dkim.org/specs/draft-ietf-dkim-ssp-10.html

adsp._domainkey.aaa.example TXT "dkim=all" - we sign all email

"dkim=unknown" - we sign some, but probably not all email

"dkim=discardable" - feel free to discard any unsigned email purporting to be from our domain.

DKIM why?

- Yahoo feedback list
- Google list unsubscribe
- Prevents tampering

DKIM + SPF why?

- Complementary
- SPF allows per-rcpt whitelists
- DKIM gets you past forwarders
- bouncing becomes plausible

domain reputation → spoofed?

DKIM (sign, check, whitelist, reject)

SPF (publish, check, whitelist, score,blacklist, strengthen policy)

DKIM SSP (wait, publish, strengthen)

Lists re-sign

MSA (provide, promote, expect, require)

SRS (don't forward spam, deploy, use sacrificial IP address and domain)

DNSSEC

contact me:

Ian Eiloart,
Postmaster, University of Sussex
iane at sussex.ac.uk
ian at eiloart.com
@ianeiloart
@emailtech

QUIT

221 closing connection - thanks for coming

Connection closed by foreign host.