Email “Spam”

A Problem for the Diplomats

Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Presented at: B.C.S. Central London Branch, 18th Sept 2003

Summary

- What is “spam” now like ?
  - and how is it being sent
- Technical approaches
  - blacklisting
  - authentication
  - payment
  - filters
- Legislative approaches
  - UK, USA & worldwide

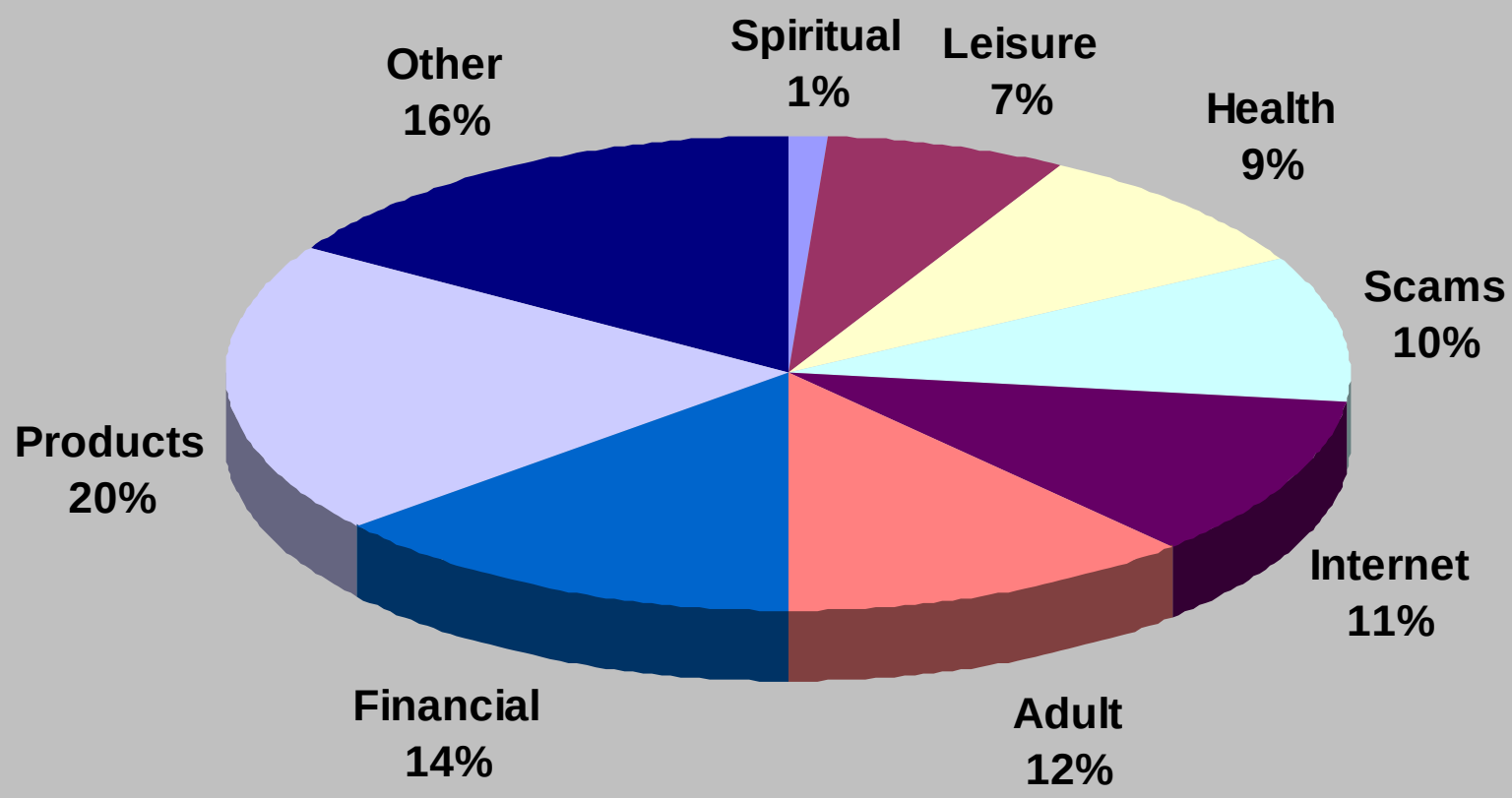
The ages of spam

- Clueless sales & marketing personnel
- Disposable dial-up accounts
- Open SMTP relay “rape”
- Broadband and open proxies
- Spam friendly trojans (sent via virus?)
- Brute Force password guessing

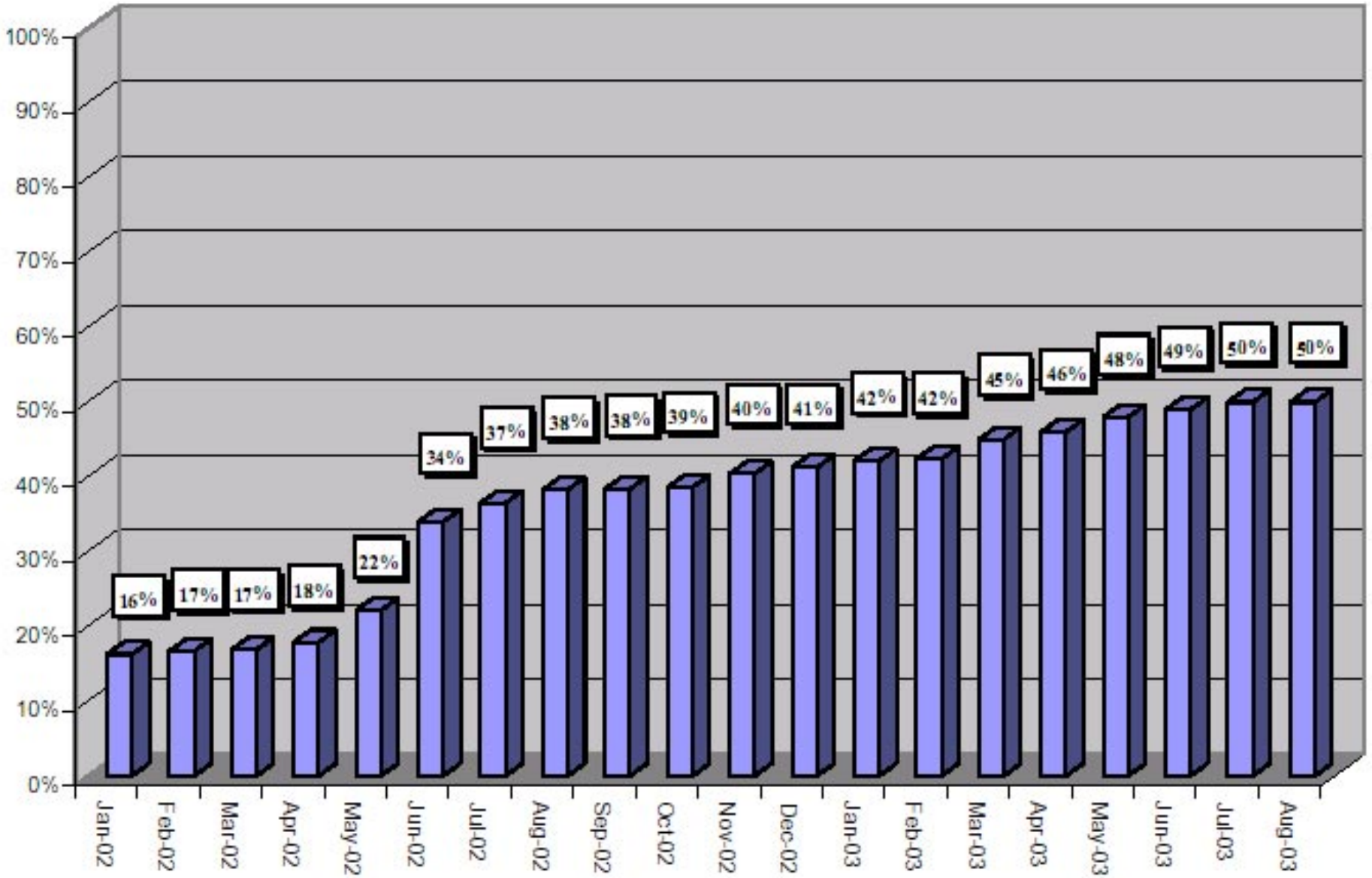
… and doubtless more tomorrow

August 2003: Spam Categories

(source: Brightmail probe network)



Percentages of Total Internet Email Identified as Spam
(as measured by Brightmail's Probe Network)



You think you get a lot of spam?

- junkname @ highwayman.com
  - April 2003: 2813 per day
  - May 2003: 5261 per day
  - June 2003: 6663 per day
  - July 2003: 7452 per day
  - August 2003: 8357 per day

PLUS

- richard @ various domains
  (demon, turnpike etc etc)
  - 200 per day
- richard @ locomotive.com
  (last used Summer 1994)
  - 110 per day

Why?

- More multiply addressed spam
  - seems to be a policy change by the senders
  - this affects my counts, but not overall traffic
- More senders
  - SpamHaus now lists 200+ major league spammers (often quoted as 140, because it was)
- My name will be on more lists
  - and lists come mainly from other lists

New spam variant: “phishing”

- Punter receives email from their bank indicating their details needs refreshing
- URL looks convincing

  http://www.mybank.com&account@107990442
- Website looks convincing
  - usually copied from the real thing !
- Currently sites are usually too greedy & punters smell a rat. This will change

Subject: Your Checking Account at Citibank.

citibank

Dear Citibank customer,

We are letting you know, that you, as a Citibank checking account holder, must become acquainted with our new Terms & Conditions and agree to it.

Please, carefully read all the parts of our new Terms & Conditions and post your consent.
Otherwise, we will have to suspend your Citibank checking account.

This measure is to prevent misunderstanding between us and our valued customers.

We are sorry for any inconvinience it may cause.

Click here to access our Terms & Conditions page and not allow your Citibank checking account suspension.

citi
Citi.com

A member of citigroup

Countermeasures: Blocklists

- Idea is to record where spam comes from and then refuse to accept any more email from that particular source
- Usual implementation is using DNS queries
- Has scaled pretty well from initial ideas of a few dozen rogue sites
  - SORBS 661541 open proxies
  - blackholes.easynet.nl 681696 open proxies

Problems with Blocklists

- Many lists: no standard rules or processes
- Operators are pretty much unaccountable
  - SPEWS only reachable via *nan-ae*
- Have been used for personal vendettas
- Listing mail relays can be disproportionate
- Common to list /24s, affecting server farms
- Legacy lists (& shut-downs) are a problem

Countermeasures: Authentication

- Idea is to only allow authenticated senders to send you email
- Popular idea with Verisign, Microsoft and others who might handle the certi£icate$
- Essentially a cryptographically supplied whitelist (with a third party attesting to stranger's probity)

Problems with Authentication

- Why should companies pay to send solicited email to their own customers?
- What happens when companies slip up?
  - how is the certificate be revoked?
- Spammers regularly compromise end-user systems – so will be authenticated anyway
- We've been authenticating IP addresses for years & it hasn't been a silver bullet

Countermeasures: Filtering

- Idea is to assess content of email and decide that it is spam and discard it
- Works well for viruses
- Modern systems should not (!) suffer from the Scunthorpe effect
- Systems like SpamAssassin use a great many rules
- Currently this is fairly effective

Problems with Filtering

- False positives can cost the recipient dearly
- Legitimate email often blocked
  - eg opt-in promotional material
  - eg newsletters
  - eg airline ticket confirmations
- Spammers can use the filters too and tune their material to get through it
- ie: spam is “evolving”

Darwin was Right!

Dear Friends, My name is Dave Rhodes. In September 1988 my car was reposessed and the bill collectors were hounding me like you wouldn’t believe. I was laid off and my unemployment checks had run out. The only escape I had from the pressure of failure was my computer and my modem. I longed to turn my advocation into my vocation. This January 1989 my family and I went on a ten day cruise to the tropics. I bought a Lincoln Town Car for CASH in Feburary 1989.

September 2003

```
<center><br><b><font face="Arial">DO NOT
DELETE THIS - <u>READ FIRST</u> - IT WILL
CHANGE YOUR LIFE!</font></b><p><font
face="Arial"><font size=+2>This <b>Really
Works</b>!</font></font><p><b><u><font
face="Arial"><font color="#FF0000"><font
size=+2>Give Your Future Five Minutes And
Read This Email</font></font></font></u>
</b><p><b><u><font face="Arial"><font
color="#FF0000"><font size=+2>It Will
Change Your Life!</font></font></font>
</u></b><p><b><i><font face="Arial">A One
Time Investment Of $25 Plus This Simple
```

More to come…

```
<font face=Verdana size=4><b>Onlin<!--
covetous -->e Ph<!-- articulate -->armacy
<br><font color=red>No Pr<!-- minimal -->
ior Prescr<!-- instigate -->iption Nee<!-
- reef -->ded!<br><font color=deeppink>No
Ph<!-- sunfish -->ysical Ex<!-- duffel --
>am Need<!-- revolution -->ed!</td></tr>
<tr><td width=100% bgcolor=blueviolet
colspan=3><p align=3Dcenter><font face=
Verdana color=white><big><big><b><marquee
border=1 scrollamount=5 scrolldelay=1>
Va<!-- plumbate -->lium ... Xa<!--
knudsen -->nax ... Vico<!-- confocal --
```

RTFM

Gain Up To 3+ Full Inches In §{Length|Size} Increase Your Penis Width (Girth) By 20% Stop Premature Ejaculation! Produce §{Stronger|Larger|Bigger}, Rock Hard Erections 100% Safe To Take, With §{No|no|Abosultely No} Side Effects Fast Priority Fed-Ex Shipping WorldWide §{Doctor Approved And Recommended|Doctor Recommended And Approved} §{No Pumps! No Surgery! No Exercises!|No Surgery! No Exercises! No Pumps!|No Exercises! No Pumps! No Surgery!} 100% Money Back Guarantee FREE Bottle Of VP-RX Worth Over

Bayes

- Idea is to take a probabilistic view as to whether email is or isn't spam for you
  - helps pfizer.com
- However does require training
- And assumes that spam remains the same & that your "good" email remains the same as well … so requires ongoing training!!

Countermeasures: Payment

- Idea is that if email wasn't free then sending spam would not be economic
  - seldom any analysis why of figure is "1 cent"
  - that's a third of a billion dollars! (per day)
- But of course no-one would charge for "good" email, by refusing to cash cheques
- At last - something to use those e-money designs for (especially the patented ones)

Problems with Payment

- But e-money doesn’t work (think bandwidth, think settlement costs, or just look around for a working example)
- Wicked “friends” might not remember to fail to charge the sender – so where’s the motivation to be an early adopter?
- And when your machine is hacked…. Will Microsoft settle your email tab?

Payment Mk II : Puzzles

- Idea is to pay in non-money money such as CPU time or human attention
- Hard to design puzzles that scale appropriately given the wide range of abilities available
- … and still doesn't tackle the "spammer takes over your machine" problem, they must steal your cycles!

Let’s build “Something Else”

- Why should email be push not pull ?
  - actually on POP3 it’s pull already
- Doesn’t really tackle the human attention issue (how do you decide what to pull?) Remember it’s not bandwidth cost that makes spam expensive!
- Main problem is that there’s very limited incentive to change to a new system

Legislation

- Need to know the jargon
  - “opt-in” means permission based
  - “opt-out” means refusing further permission
  - nothing to do with what the tick box is for!
- Opt-out often associated with “Universal Preference Services”
  - eg: TPS (phone), FPS (fax), MPS (mail)
  - no credible email system: since no-one will pay

E-Privacy Directive (July 2002)

- This is often called “soft opt-in”
  - ie: opt-in (permission based)
  - BUT also businesses can write to existing customers about “similar” goods and services provided that they offer an “opt-out” for that
- Must be seen as a realistic compromise
  - and ASA is finally showing some teeth relating to fake “opt-in” lists

UK Legislation

- DTI finally consulted on E-Privacy Directive in March 2003 (closed 19 June)
- Must be in place by the end of October
- Promised conclusions for August
- Latest promise is for mid-September…

- oops! (in fact it was announced the day I gave the talk)

USA: States

- 35 states now have local laws
  - generally entirely opt-out
  - labelling required by some (ADV: etc)
  - forgery of source is usually forbidden
- Generally ineffective
  - mainly used to hassle legitimate companies that make an error (because they can be found and they have some money!)

USA: Civil litigation

- AOL
  - long record of sueing those who forge them as a source or who “trespass” on their networks
- Yahoo/Microsoft/AOL
  - going after some of the major league spammers
- Amazon/Ebay etc
  - some “passing off” actions

USA: Federal

- Many proposals, a handful of which have cleared the Senate or Congress
- Most support for (because most lobbying for) proposals centred around “opt out”
  - which is bad news with 20million + businesses
- Anti-forgery is relatively uncontentious
- … and some inventive ideas
  - RICO, record-keeping requirements

What if “opt-out” passes?

- Effectively makes the major league spammers into legitimate businessmen
- Expect volumes to become impossible to handle without automated tools
- Cost of accepting email from strangers likely to become prohibitive

What of a ***very*** soft “opt-in”

- Europe’s rules require:
  - SAME COMPANY
    - so you cannot sell access to your user base
  - SIMILAR PRODUCT or SERVICE
    - so conglomerates don’t get any traction
    - usual example is Virgin Mobile/Virgin Trains
- Some ISPs and portals understand what there is to play for in this space!

Rest of the world

- Australia
  - looking at EU style approach
- Korea
  - have gone for labelling
- China
  - beginning to realise it affects their connectivity

The Foreign Office

- Isn’t this sort of threat to the national infrastructure exactly what the Foreign Office is meant to deal with ?
- But no obvious international bodies!
  - UN?
  - OECD?
  - World Trade Forum?

Summary

- ☹☹ you're going to get ***more*** spam ☹☹

  I'm not very special, just an early adopter
- Technical measures won't work forever
- Legislation needs to be got right
- It's basically OK in Europe, but the USA (and China) is still up for grabs. So why isn't this a major issue for Jack Straw?