Economical Impact of SPAM

Timo Ali-Vehmas
Timo.Ali-Vehmas@pp.inet.fi

1. Abstract

Unwanted Email is a phenomenon created by the fast growing Internet business bubble of late 1990's. It however did not disappear with the vaporising bubble but it stayed with us and has grown faster than any other service in Internet ever since. Unwanted email is now reaching mature state representing up to 50% of the overall email traffic. Unwanted email is a complex technical and primarily economical issue, which may, in worst case, lead to lower use of electronic services in general. Unwanted email, called also spam, has a possibility to become a Real Killer Application to the Internet, not in the Internet.

Economic impact of the spam is difficult to estimate quantitatively. Instead, a value system based analysis is carried out studying real and potential value generation in the networks of spammers and their partners. This is supplemented with selected pieces of quantitative information about volume of the business, merely as examples. There are several studies in the literature, how spam is impacting various value chains but there are very few references found for the spam value chain or system, itself.

Key words: unsolicited email, spam, ecosystem, value chain.

2. Introduction

Internet is today the most versatile communication network in the world. It serves it users well in large variety of applications, ranging from banking to gaming and from browsing to emailing. There were some 300 million users in the Internet in 2001 and the estimate for today is over 400 million ranging up to 125 million in the USA alone [1]. Internet penetration level is actually highest in Europe, Nordic counties and the Netherlands leading with about 60 % penetration but there is no direct correlation to penetration of spamming. Email has become one of the most important applications primarily because of its quite good interoperability and compatibility between different service platforms. Simple IETF specifications for email, such as Simple Message Transfer Protocol SMTP (IETF RFC 788), Post Office Protocol POP3 (IETF RFC 1081) and Internet Message Access Protocol IMAP4 (IETF RFC 2060) [2] and their extensions have been developed in idealistic research environment where malicious use of Internet has been almost a capital crime as a starting point. This approach has left email without proper protection against users who may have a different starting point and ethics than the research community. Another factor promoting wide use of Internet in good and in bad is the billing mechanisms, which do not separate uplink and downlink traffic and where all subscribers pay for both incoming and outgoing traffic. Further on with broadband access the tariffs are mostly flat or block rate based. This leaves the door open for anybody with very low entry fee to enjoy all the great benefits of the Internet, including email with no feedback measures whether the use is economically justified or not.

3. What is SPAM ?

Spam originally meant "Spiced Pork and Ham", a canned pork meat, which was not allowed to be marketed as real ham because of too low high value content, ie. ham. Internet community adopted the term from Monthy Python Flying Circus where spam was part of every meal of a restaurant, whether the customer wanted it or not. This is very good simplification also for much more serious business issue of today's Internet, the Unwanted Email.

Unwanted Email is not simply all emails that people receive unsolicited but it may be categorised better by dividing it up to three groups:

3.1. UCE and UE = UBE

Unsolicited Commercial Email (UCE) means emails, which have been sent to the receiver in order to advertise products or services. The actual sender of this email may or may not be the same body as the retailer of the advertised items. But not all the unsolicited commercial email is spam. It may well be that receiver has in some instance permitted his or her email to be addressed by commercial advertisements. According to current directives in EU 95/46/EU 97/7/EU and 97/66/EU such email advertisement is legal. Directive 2000/189/EU goes further defining for email and also for GSM Short Message Service that only Opt-in scheme may be used. Similar legislation is either available or being prepared in other major markets, Japan and the USA. Currently in the UK UCE is not

allowed to consumers but is still allowed to corporations. [26]

Unsolicited Email (UE) may be spam even if it not commercial. Also political and religious advertisement is regarded as spam. PEW Internet & American life project has been recently published a large survey about spam [3]. According to the survey, people are quite sensitive to spam today. As high fraction as 74 % (with error margin of 4%) of people consider even a personal or professional email from a person they do not know to be spam. Unsolicited Commercial or other Bulk email is also referred as UBE.

Clear difference is visible in this study to show that only 11 % of the interviewed people considered unsolicited commercial email as spam, if they only had given the permission for such transmission in advance.

There are hence two concepts of sending Unsolicited Bulk Email, which shall be recognised clearly separately.

- Opt-In. There is a permission given in advance by the receiver to the sender to send commercial or other emails, automatically. This should not be considered as spam

- Opt-Out. There is no permission given by the receiver but there is a reliable mechanism to the receiver to forbid such transmission for the future. This is not to be considered spam, necessarily.

Some member states in EU, including Finland have implemented Opt-In scheme in national legislation already several years ago. [4]

3.2. SPAM

But the problem really is when the Opt-out request is not used or not taken into account. This is the case when we really are talking about spam.

4. Market of SPAM

Different businesses utilise spam differently. Proportions of spam advertisement in different businesses and market give some indication about the losses because of spam. Total value of spam-based business is difficult to estimate.

There are very many different estimates of what is the content of spam but by with very large error margin they all agree. The top 3 categories are always a product business, financing and banking and the 3rd one, adult entertainment. Some estimates show the share of SCAM, ie. Nigerian chain letter -type swindle is also quite remarkable, which in other estimates may include in financial category.

Following estimate is provided by Brightmail, an anti-spam company, who is one of the most active participant in the global debate about spam and its consequences. The Anti-spam companies are discussed in detail in chapter 6.7. [5].

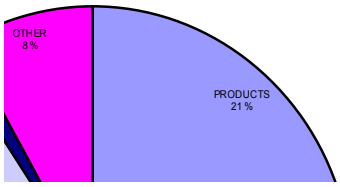

Figure 1. Content of spam, Source: Brightmail.

Another way to look at the market of spam is to study in what countries spam is most wide spread. Currently the USA is most vulnerable to spam by far. The USA represent probably one 3rd of the total internet users but for spam, its market share is almost two out of three. It would be a good study item to research what the factors in the USA making it so vulnerable to spam. [6].

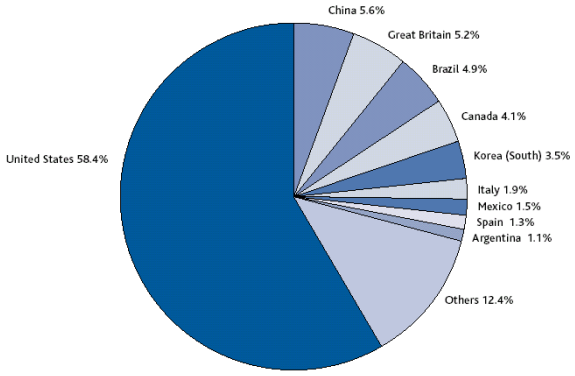

Figure 2. Markets of spam. Source: MessageLabs

5. Volume of SPAM

There is a lot of information available about the growth rate of spam in recent years and months. There are also

several estimations what this all means to the users and providers of Internet.

5.1 How we got here ?

Email as a broadly recognised phenomenon started early 1990's. By the middle of the decade it had been adopted by all major and also many smaller enterprises, universities - where it all began, and public authorities. General public was not yet exposed to email over internet until the great IT industry stock market bubble started to emerge. Still in 2001 spam was only 8% of the total email traffic according to one estimation by Brightmail, but already in 2002 it reached 30% of the total email traffic and for 2003 it is claimed that spam emails exceed the number of ordinary emails in the internet [5]. These figures must be dealt with some criticism. Most of the estimate, which were available for this this study, were provided by the firms developing tools and services to reduce spam, so called anti-spam companies. In some estimations [7] it can be interpreted that normal email has even go down because of the total absolute growth rate is lower than absolute growth rate of spam.

Separately an independent market research company, IDC estimates that in 2002 the proportion of spam is 18% of the total email traffic, which still is a considerable 5.6 Billion spam emails every day. Also IDC estimations on the growth rate of spam are more modest than in Brightmail's estimations, showing some 20% growth for spam and 15% for normal email. This would keep the spam figures for 2003 still below 20% of the total email traffic. [8]

A UK based anti-spam company, MessageLabs estimates are somewhere in between. These estimates show growth of email and growth of spam in very comprehensive way. [6]

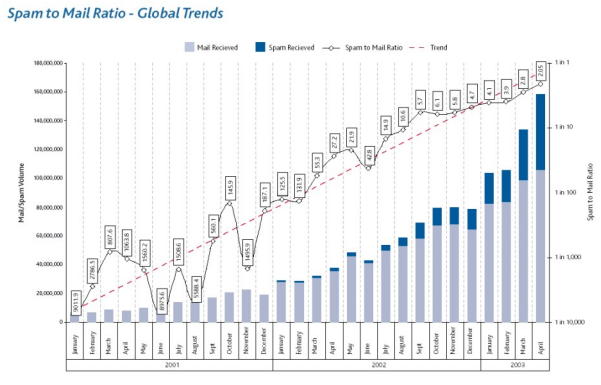

Figure 3. Growth of email and Spam. Source MessageLabs

There is also one additional element here, which may impact these estimations. For corporations and other larger communities, major part of the email is internal, within their own domain. This email is only occasionally, in case of a virus attack, polluted by spam. Therefore corporate email users typically see spam only as a percentage of incoming "external" emails, not as a percentage of all received emails. In some estimations this is clearly having major impact.

Hence, one difference in estimations clearly is whether the question is all email or email from Internet.

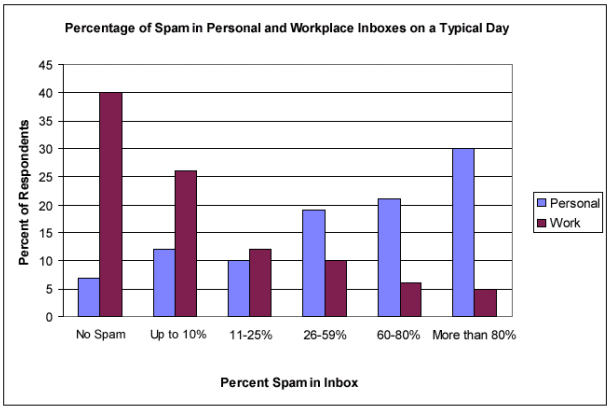

Figure 4. Consumers and Corporate user experience of spam. Source PEW Internet & American Life project.

As a conclusion of what kind of phenomenon unwanted email is today, it is easy to agree that first of all, it is a severe problem, its growth rate is now stabilising and it is becoming a mature business model.

We need to separate real spam from controlled unsolicited email. This is today in practise impossible task. Therefore this study tries to address both and to indicate also some common elements of these two.

6. Value system

Value chain normally means the overall flow of material or immaterial added value, where value flows downstream and money flows upstream. In many businesses the flow is far too simple model since there are many indirect links and sometimes money flows also downstream in the form of subsidies. Therefore also in this analysis a different term, value system is used, instead. Also Ecosystem is a term used for similar purpose.

The real issue however is that the overall value system related to spam is very fragmented, not too well understood and also partially underground. There are several commonalities with other clearly illegal

activities, such as money laundering. Therefore it is very difficult to get accurate quantitative figures which would be comparable and which would provide comprehensive base for analysis. Therefore this study is focusing on the value system itself. This approach may add more value than analysing some part of the value system in great details. It is important to understand the overall value system and the interrelations between the players, in order to even estimate the economic impact of spam. There are very few previous studies found, which cover the overall value system of spam [25].

One hopefully usable side effect may be to provide some means to fight the real spam, as a separate item from unsolicited emailing, which still in many cases is not spam.

Unwanted email value system includes some fundamental players.

- Spam hosting, which includes
  - Address generators
  - Content generators
  - Full service providers
- Spammers and their supporting
  - Spamming Software vendors
  - Hackers and hacked computers
- Legal UCE advertisers
- Various ISP on sender side
- Network operators
- ISPs supporting receivers
- Corporations
- Consumers
- Product and Service retailers who finance the UCE and also spam.

In the following chapters we discuss the role and motivation of each one of the players. We can show that most of the players are players against their own will. We may call them victims, but surely some of the players have very strong role in driving the use of email in advertisement, and unfortunately some of them do it ruthlessly, abusing the resources of others.

6.1 SPAM hosting

The Spam hosting community is very interesting part of the value system, which is at least partially underground, like roots of a tree. Spam hosting include large network of different kind of internet oriented small firms and individuals who earn their living by providing primarily content and address data bases for the actual advertisers, spammers or others.

6.1.1 Address database aggregators

Address database aggregation and reselling is a complex network of players, who create and develop the email address databases based on the various mechanisms.

Most visible mechanisms include:

- WEB portal clicking and related enquiry of email address and other contact information
- Search engines to look for Homepages and Newsgroups and email addresses on those
- Aggressive bulk email harvesting attacks (considering all random email addresses to be real, which do not pounce back.)
- Aggregation of the address databases created by mechanisms mentioned above and combining these with e.g. Opt-in data bases of their customers.
- Segmentation of the databases based on geographical, ethnic, habitual etc. basis
- Reselling the databases, providing subscriptions to continuous database service

Addresses are available at very low price, between $3 and $100 (or Euro…estimates are very rough) for one million email addresses [4]. Taking into account that there are only some 600 million email addresses, the total Internet email address database value would be between 1800 – 60000 USD. Without any added value, such as very good segmentation, business opportunity of bulk address processing is at the end of the day very small. It is likely that the content of these address databases is in most cases very poor, which actually do not generate spam from the receivers' perspective because the emails reach nobody. This type of spam flooding still loads the transport network and the receiving email servers badly. When taking into account that the number of major spammers is only a couple of hundreds by some estimates, the potential customer base for simple address aggregators is also quite limited.

6.1.2. Content creation

Content creation and aggregation for spamming is another partially underground activity. In legal unsolicited advertisement the content is directly generated together with the retailers. There is however some evidence that some retailers are using the spamming content creation and the spam hosting network as a decoy. The Spam hosting network or

firms generate faulty content, which is based on false claims and false information in general which is then put to several web portals as baits. When consumers respond to the bate, the network collect the email and other relevant information. But they never deliver anything, since there was probably nothing to deliver in the first place. But somehow, through several steps like in money laundering the address information finds its way to the legal retailer or service provider who can use this well qualified contact information for his similar business offering [9]. There is a report by the Federal Trade Commission of the USA which claims that 66 % of all spam has some false information in either sender address, subject field or in the text part. The value varies between 44 % contain false information in product oriented advertisement up to 96% false information in advertisements offering investments and business opportunities. [10].

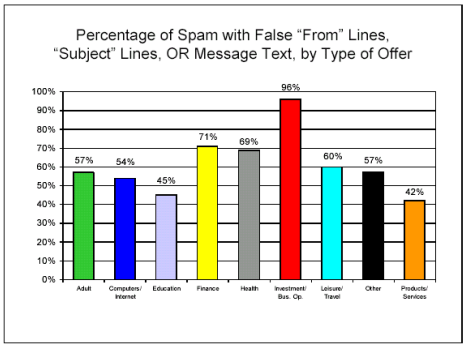

Figure 5. Portion of spam contain false information, Source Federal Trade Commission, the USA.

This indicates the strong invisible network in contact information harvesting but it is very difficult to estimate the total volume and financial importance of this partially underground business. It may well be that the address database market is only a tip of the iceberg where not so valuable email addresses are sold to email spammers at very low price but the really valuable contact information with additional contact and profile information on the owner of the email address is used for more sophisticated direct marketing, ranging from banking to time sharing free time and vacation offers.

6.2 SPAMmers

Spammers typically shall be discussed separately from spam hosting. Spammers are the actual organizations or individuals who push the button and make the spam email to flood to the network. There are several different type of spammers, some are simply some well known individuals who have several internet accounts and they use those accounts directly and openly to send the spam. They may be occasionally block listed in one IP address but they soon pop up from some other IP addresses. Detroit Free Press 12/2002 claimed that "spam king" Alan Ralsky operates 190 email servers to send his messages.

Some of the spammers may at least pretend to use Opt-out registers and some may even use them. There is one estimate claiming that majority of the openly but well organised and operated spamming may by driven no more than 200 different parties or persons. [9], [18]

As an example of another kind of spammer we could look at *"Ms. Betterly who quickly discovered that she could make a profit if she got as few as 100 responses for every 10 million messages sent for a client, and she figures her income will be $200,000 this year"*. Ms. Betterly was interviewed by Wall Street Journal in November 2002. [11]

The fatal type of spammer, which probably is the most difficult one to take under any control is the one who actually use viruses and other hacking methods to hijack unprotected computers. These people spread their spam email quite often without any commercial or other purpose. Their only aim may simply be to cause maximum harm to the selected receiver or receivers or to the overall Internet. Major part of the commercial oriented spamming takes place with this approach too. Some estimates are claiming up to 70% of all spamming to go via hijacked computers [9].

6.2.1. SPAM Software vendors

A dedicated group of software developers is giving a helping hand to the spamming community, many of which are just ordinary opportunistic people. These software developers have talents in email software but also in Internet technologies in larges scale. Some of the earlier hackers are using their experience in less risky way. There is no statistics available on these vendors.

6.3 Legal direct email advertisers

At this point we have to discuss also about another group of bulk email senders. In 2001 there were about 50 companies openly offering services for electrical direct marketing. These are sophisticated enterprises, which typically have full service approach with people and tools to serve their customers. But what is very important, these companies typically use in minimum reliable Opt-out approach to limit the really annoying amount of emails. Also the address databases are supposed to be of high quality. [4]

One company, 24/7REALMEDIA, advertises on their Web page: "Our products and services include our patented ad serving technology, **Open AdStream**®; web analytics via **Insight XE**™; full service search

engine marketing programs via **24/7 Search**; integrated online media packages as well as Web site representation via the **24/7 Web Alliance**; **online promotions**, **email marketing**, and direct to desktop solutions via the **24/7 Messenger**."

The 24/7REALMEDIA and its kinds have been recognised by now that successful business relation requires trust and trust can be built only with reasonable business ethics. Using Opt-out and/or Opt-in approaches the direct marketers achieve actually better sales than with massive wasteful spam campaigns. [12].

It is important not to mix these companies with spamming. As seen in chapter 2, very few email receivers, 11 % consider Opt-In email direct marketing as spam. There are eMarketing training and consulting firms available, too, which fortunately, at least in public messages, strongly encourage their clients to use Opt-In approach.

"Opt-in mail is more personal. You can personalize your message to each recipient. Third, opt-in means that the recipients have chosen to accept and read your messages. They're interested in the information you are offering."

What is even more important that most of the side effects to corporations, network operators and ISPs as we discuss in chapters 6.4 to 6.6 totally are avoided.

When estimating the impact of spam the direct email advertisers should not be included into the calculations.

6.4. Internet service providers

Internet service providers are the key group in spam value system in many ways. First of all there are ISPs such as TeliaSonera, who recently suffered concrete damage because of virus based spam attack. Direct costs involved were only about 3 M€ but it is very difficult to estimate all the bad will and publicity TeliaSonera received and what finally is the opportunity cost of lost old and new customers.

Economical impacts to IPSs include wasted memory and server capacity, wasted network capacity and nowadays more and more, capex and opex of a special servers to filter and mark the incoming emails for the protection of their network and customers. Major ISP's such as Time Warner (AOL) and MSN claim, that they filter and block 2.4 Billion emails per day, each. This may represent up to 80 % of all incoming traffic. [13]

It is obvious that free web email accounts really are the worst to receive spam because of no commitment is required by the mailbox owner to open such service. Naturally these mailboxes may also be used to false identity to subscribe some further questionable services. All of this behaviour is increasing the likelihood of receiving spam.

Total economical impact to IPS's is difficult to estimate but one claim by BellSouth is that there is some $3 - $5 cost penalty per each Internet subscriber. [14]. Assuming 400 million internet users [1], this would top up to $2 Billion. It may be more reasonable to scale this down to cover mainly USA and maybe the lower end estimation, too. Still the wasted effort is as high as $400 Million per month or abou $5 Billion per year.

There is the dark side of the coin too. It is quite likely that some ISPs are in deeper business relationship to spammers. There is some evidence that some spammers have paid quite high fees to their ISP's. These "pink contracts" are kept well confidential and therefore the actual amount of money is very hard to predict. But in most of the cases this can only be a fraction of the spammers' overall revenues and therefore so far it can be considered as just minor interesting detail. This however is one important element when analysing the overall value system. It is more and more obvious that this quite a small business, which spamming itself is after all, causes considerable harm to innocent Internet users and service providers. [9]

Naturally in case of legal direct email marketers it is obvious that there is a value and money transfer between them and their Internet services providers, but again, this is not part of economic impact of spam.

Unsolicited Email is a real problem in wireless industry only in Japan, where the leading wireless network and service provider, NTT DoCoMo have suffered from I-Mode spam for several years. There are some estimations, which propose that the damage to DoCoMo is of the order of $200 million. This is a significant amount of loss but is still relatively small when compared to the overall losses caused by spam for the wireline service and network operators. [26]

6.5 Network operators

Network operators are a group of players who simply pass the traffic through their backbone networks. Again very difficult to estimate the economical impact but taking into account the low real time requirements of email traffic and operators capability to differentiate real time traffic and best effort traffic at least in ATM backbone, we may assume that this kind of data transmission is still only a modest share of the total best effort traffic and is not able to severely threaten the backbone network operators. In many cases network operators get also positive revenue based on

the traffic the ISP and corporations generate and therefore we may assume that the economical impact may actually even balance out for network operators.

In some special situations, when there is a massive virus based, scheduled email attack, it may cause overloading also to backbone network and Internet root name servers. There are some cases, where the damages caused by one individual email worm may exceed 1 BUSD. This is quite significant amount of money but it is hard to include this to the overall calculations due to the attackers' quite different, almost terrorist behaviour. Also the purpose of these type of email attacks is more to simply case damage to the Internet itself rather than be a form of unsolicited email.

6.6 Corporations

It is estimated by independent market research firm, Radicati Group study, Anti Spam Market trends, 2003 –2007 that corporations worldwide have to spend up to $20,5 Billion in 2003 in servers and related operations in order to fight the incoming spam. It is unclear how much of the lost productivity is included. This may grow over $100 Billion by 2007. A separate study by Ferris Research proposes that lost productivity because of spam emails in USA in 2002 would be $8.9 Billion. [13]. It is questionable if these both figures should be counted at the same time, since if the tools the corporations are using are effective, then the lost productivity should be minimised. Some studies suggest that spam filters reduce the number of employees who suffer from spam from 19% to 5%. This would indicate that some portion of the wasted effort should be included, still.

Anyway this is clearly the highest figure of economical impacts listed in all material available for this study and hence it can be argued that the corporations are by far the biggest losers in the global flood of spam.

It is also important to note that anti-spam equipment and services may be quite costly. This leaves large number of small enterprises to really difficult situation. They must carefully decide what is the least costly approach to deal with spam, let it come through or acquire some anti-spam equipment or disconnect from Internet totally - or simply go out of business. For consumer it is possible to abandon an email address when it gets badly infected but for an enterprise email address is typically connected to brand value and to change the email address is not so simple thing to do.

6.7. Anti SPAM companies

Small portion of this great spending by the corporations and also ISPs goes to emerging hot business of anti-spam companies, who provide sophisticated tools and equipment to fight against spam.

This industry did not even exist 10 years ago but today their total revenue is estimated to be $650 Million [13]. Radicati Group has predicted that they have the potential to grow over $2 Billion by 2007 if the spamming is not limited or reduced by any other means. There are now some 20 to 30 companies providing services in this business domain. Brightmail, who claims to have 11% market share and also protecting some 300 million customers of ISPs is one of the most visible one. (Note: Does the claim above mean that there are close to 3 billion Internet email addresses or does it mean that the current 400 million internet users have about 7 email addresses, each, on average, probably not true?). This group of companies have their roots in the big Internet bubble also and they seem to carry on similar public messaging. It is hard to believe that all their claims are fully reliable. But again, it is more interesting to look at the behaviour of the companies and their role and connections in the value system of spam rather than to be precisely right with the figures of them and about them.

6.7.1 Technology Insight to anti-SPAMming

The Spamming is based on the very basic technologies of Internet as such. There is no novel technology needed for spamming. However the companies, fighting against spamming have developed several new approaches to this problem. It may be interesting to look at some of these even if it is not absolutely mandatory for economic oriented study like this.

There are several different technologies applied to build the servers, databases and management processes of the anti-spam companies [15]. The most simple methods use just black or block or white listings of the sites know to spread spam. This however is not very efficient and causes many problems because of false denial of service incidents. Also in the beginning simple finger prints or signatures were used as an evidence of spam which lead to many false alarms. Using some collaborative listings the fingerprints and various listings can be develop further. But all in all these technologies are used today only selectively as a second priority. [18]

Bayesian string filter

The novelty is in the way the spam mails are detected from the normal stream of emails. So called Bayesian

filter string classification is used today in most of the filters as core technology. The filter is adaptive to both spam and non spam emails and their characteristics. Filter is also customer specific. This is important because each victim of spam has different categorization what is spam and what is not. This is also where the biggest advantage is also over simple site black listing.

Best Bayesian string filters can converge quite well with only hundreds of emails. Training may be manual or training can be done in advance based on larger set of emails. The final novelty is that these filters will tune themselves to filter customer specific spam avoiding the problem of one filter does not fit all. Using Bayesian filters for spam protection were first introduced by Microsoft research and by Pantel and Lin in 1998 in AAAI-98 workshop [17].

With later enhancements it is possible to achieve six nines accuracy, typically with zero false positive detection, ie. one error per 1 million emails screened.

Squelch Spam email on protocol level

Instead of a simple black listing and blocking all the emails from a certain source address, it is also possible to delay the email protocol. This would cause a lot of reduced performance to the sender of spam [17]. This technology adds some costs per message also to the senders of spam while keeping the legitimate email untouched. All the emails, including those, detected as spam can be finally put through to push the false positive detections to zero.

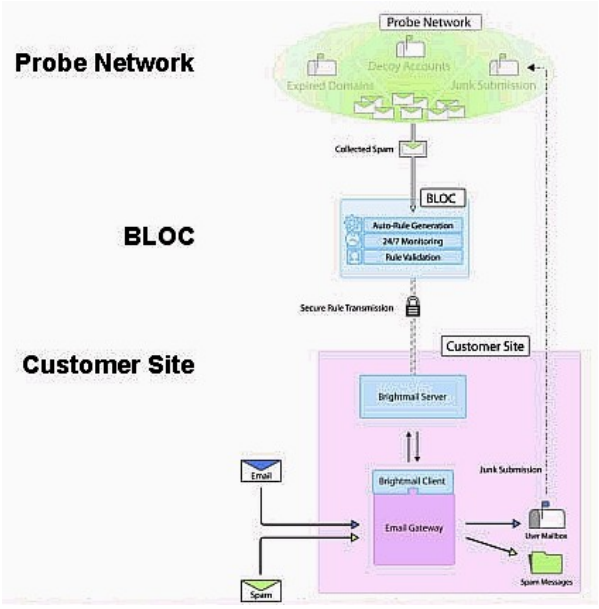

Figure 6. Brightmail patented spam filtering system. Source Brightmail [5]

Brightmail is using a special probing network, a fairly large set of email addresses opened up for this purpose only. They get large incoming flow of emails, which in this case all should be simply spam. In their back-office they calculate detection patterns based on the characteristics of emails. They know that all the information in typical spam message is unreliable as such, it will vary from sample to sample, even within one flooding, but they use this method to collect input training data for the actual spam filter servers connected to their customers' email servers.

There must be real time connection between the customer email server, Brightmail server and the Brightmail back-office because one spam flooding typically is lasting quite short time. The time from the first detection of a new spam mail and when first similar email arrives to their customer system is always very short and if the probe network is not competitive decoy, it may well be negative. In this business time really is money.

Brightmail is using traditional customer feedback as additional tool to pick up the spam mails that were not caught by the probe network. It is also obvious that there may be some "not-so-spam" emails, which each customer may want to include into the filter traning data.

Haiku

End users may also add some specific detection part to all their emails, which will cause strong positive non spam convergence in the spam detection filters, regardless if those are traditional or more sophisticated. Whether this is really providing a long term solution is maybe less important. But it will help cultural and ethic diversity to spread. Most of these specific pieces of text are poems or proverbs or similar.

6.8. Consumers

The Consumers are the big question mark in the value system. Several studies clearly state the consumers are very much against spamming as discussed in chapter 3.

Still the same studies show that up to 7 % of the interviewees have in fact ordered a product or service that was advertised in a spam email [3]. Further on, the same study proposes that in USA in 2003 some 44 % of all the email accounts are without any spam filter.

When adding some ignorant behaviour how to protect the personal email address in order not to get on the lists of spammers it is obvious that the market is easily

created. When only 0.001% positive feedback is enough to keep the flood of spam emails to pour in, the equation is ready: one hit per user per 7000 spams in the inbox, one could claim. The vast majority of the consumers are suffering because of the ignorant or reckless behaviour of others.

We should also remember that consumers' mailboxes look quite polluted because they most likely receive far less real email than the corporate users. Therefore the percentage of spam in consumers inboxes looks much more severe than it actually is as we discussed in chapter 5.

How much extra this will then cost to consumers? It definitely depends on the connection type the consumers have. In chapter 6.4 we estimated added costs to the ISPs, which naturally have to be paid by their customers, most of them being consumers. Additional cost may incur if the time based charging is used for the consumers access connections in case of PSTN, ISDN or wireless. This cost could in theory become quite significant but I assume the consumer to change his email account should it get too much loaded. Therefore I tent to believe that consumers' costs are of the order of the ISP's expenditure for anti-span servers and additional hardware and software in general.

If we compare the success rate required by the ordinary opt-out or No-opt spammers with their cheap address lists and the good screening level of the modern Bayesian filters, it gives some hope that these commercial spammers may not any more be able to reach their 10 per million success rate. This would impact to major part of the spamming value system but would still leave the door open for plain attackers whose only motivation may be to cause harm to Internet and its users.

6.9. Retailers using UCE

At the end of the value system are the great profit-mongers of spam, who use it for their marketing campaigns and for many other purposes.

It is also important at least to try to estimate the business volume based on spam emails. This is very difficult. There are however, some estimates available for business of adult content based on spam and also for SCAM, which are of the order of $2 and $3.2 Billion respectively. If these two represent some 15% of total spam each, one could estimate the overall value the consumers are spending should be of the order of $15 Billion. This estimation however is very unreliable. Especially banking and financing sector estimates would be have been quite interesting but this part of the value system is also most invisible. [13]

6.10 Value system of SPAM

Finally the overall picture of value system of spam can be shown. First of all it shall be noted that this graph includes both legal and less appropriate players of spam related value system. It is by far not clear, what are all the connections between all the players. This picture does not imply that all the players having some red colour would operate unethically, it rather implies that within these players there may be some who don't.

At the end of the day the picture can be interpreted also as a tree, with its roots underground, trunk transporting the value to the leaves and flowers and then finally the fruits are eaten by the harvester. More detailed analogy however is not applicable.

The role of anti-spam companies is anyway interesting because they may be able to fight the spam better that expected but at the same time they will spoil their future growth potential. Spamming in the future may more clearly be divided to pure Opt-in direct email marketing and then on the other hand to plain Internet terrorists who simply send garbage email in order to spread viruses and cause harm.

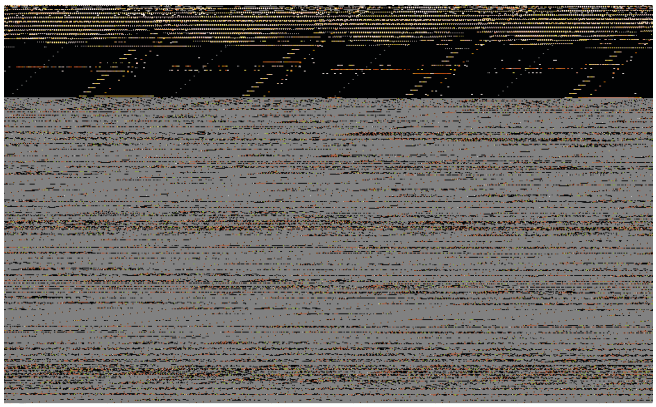

Figure 7. Value system of SPAM

Nowadays there are naturally many other actors in the spam related matters. These include legal people, lawyers and authorities, news agencies, market and other research organizations and so on. But the overall economical impact of spam is still considered moderate to these businesses. Therefore these aspects are not dealt in this study in more detail.

7. Economic Impact of SPAM

Based on the discussion above the overall money circulating in the value system can be as high as $40 billion, including the expenditure of corporations, business value of spam related sales or goods and

services and some additional costs for consumers, ISP's network operators and others.

In order to put this to some reference, at the same time the overall retail business in the USA is about $3000 billion. If the both figures are even roughly right, the economic impact of spam is significant.

It should be noted also that the losses for the corporations most likely exceed the value, which is generated by the parties utilising spam. It actually would be cheaper for corporations to buy all the adult content, respond to all Nigerian chain letters and get some "very advanced weight contol gadgets" for their employees. What a waste!

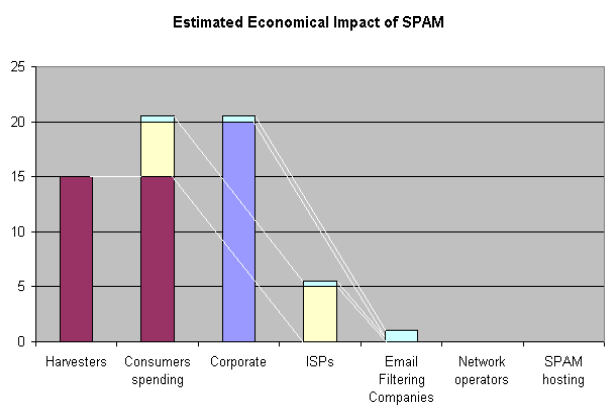

Figure 8. Estimated Economic Impact of spam

This unbalanced equation is there because sending spam is so low cost and most of the costs incur to the receiver. In order to be able to fight successfully against spam, this equation has to be changed.

Recently, November 22, 2003 similar results were published by Untad, [27] noting also the large variations of the estimations. It is important to take the absolute figures as rough estimates only, because of so much of the value creation and loss is not reported and takes place "under ground".

8. How to avoid SPAM in the future?

It is obvious that technology solutions alone will not be able to stop all the spam flooding to our mailboxes. Changing the equation discussed above will have major impact to the majority of the spam. Spam filters based on the black and white lists do not work but supported by novel test classification technologies such as Bayesian filters will improve the quality of filters to the level which make the low quality bulk spamming uneconomical. Also if we can misuse, even temporarily some email protocols to put some extra burden also to the senders of spam this will help turning the equations right.

In order to limit the spamming based on the hackers, one reasonable approach also is to make email virus scanning first recommended but later mandatory by the ISP's. All emails containing some virus or worm should be stopped already before it will reach its target computer. Consumers are not very well aware of all the risks in the Internet, they should be protected reasonably well by the service providers. Since consumers do not use spam filters nor virus protection, which obviously should be the tasks for service providers.

In long term it is also possible to develop better email protocols to include sender authentication for email, which would enable some sending charge to emails too. This would have a major impact as we have seen for instance in cellular business, where spam short messaging has not happened in large scale. The cost of SMS to the sender is a prohibiting factor. There are activities ongoing in this area both in Internet Community, where Anti Spam Research Group (ARSG), a daughter group of IETF has been established. [19]. Standardization is today in quite early phase and it may well be that we need to wait for the better email standards for quite some time. And even with Internet standards, it takes long time before the new standards are all also implemented and deployed.

Fourth element in this fight is the legislation in all countries, which should make all spamming illegal. Currently in some states in USA this is already the case but for instance in the UK Opt-out spamming is forbidden only for consumers. It has been shown that Opt-in is the only acceptable approach to differentiate legal electrical direct marketing from spamming. Dedicated interest groups are trying to drive the legislation in the USA in EU and elsewhere to tighten the laws against spam. In most of the cases this is very welcome approach as long as there is enough reasoning not call spam anything that moves in Internet. [20], [21], [22], [23].

Finally the education of the consumers is also important. They should be made much better aware of the risks of exposing their email address, responding to any internet surveys and enquiries, especially SCAM. Consumers should also require their service providers to protect them better as part of the service.

8.1 New risk areas for SPAM

Spam is now serious threat for use of Internet. Number of computers connected to Internet and email addresses of the consumers is today over 600 million.

Wireless devices have already some time ago reached the milestone of 1 billion devices and access numbers

in use. The calling party pay – concept has protected the wireless businesses in most countries but with the converged digital technologies mobile devices will include more and more features which may them fully internet compatible, including Multimedia Message Service (MMS) and regular email. Especially using email with wireless devices includes immediately the same risks as with ordinary email. Additionally, if email address is somehow bundled with telephone number, it may make it impossible for the end user to escape from polluted email address – he should change his telephone number at the same time. This is not acceptable approach. This risk has already materialised in Japan because the wireless messaging in Japan in based on email paradigm, not calling party pays concept such as SMS.

There are some markets where operators are using or considering use of called party pay – concept for MMS. They should be informed quite well about the risks involved. The MMS specification supports both concepts but only "send pays" is safe for spam. [24]

9. Conclusions

It is obvious that spam has very important role in Internet email, especially in the USA. Significant businesses are utilising spam in their direct marketing but serious business is moving gradually away from spam and they are strating to use acceptable electrical direct marketing methods, like Opt-in scheme, to select the receivers much more carefully. This is not only improving the feedback rate and success rate in making business but also reduces significantly the blind bulk email in the Internet.

The most severe harm spam is causing to corporations who have to fight spam in order to keep the business processes running and to keep the focus of the workforce in the business, not in the spam. The economical losses of the corporations may exceed the total market value created using spam as advertising media.

Novel schemes have been developed recently to fight against the spammers, which in longer run may make the business case for spamming negative. Additional legislation and regulation is needed fast to help the service providers and corporations to fight against spam and especially spam using viruses to hijack the consumer's computers and to limit the spamming now. Legislators have to balance between tight policies and adequate protection for the citizens and also protect the Internet, keep it clean and useful for so many good things, it can provide to us.

Educating the general public to avoid behaviour, which may facilitate spamming is important but as important it is to push the internet service provides and particularly wireless operators to think carefully the ways to keep the wireless part of Internet as clean as it has so far been.

Ultimate target can be no less that to clean the network all the way from all harmless emails, keeping in mind that email which may be unwanted to somebody may be appreciated by somebody else.

References

[1] Hobley Christopher, Just numbers, Number of Internet use, electronic commerce, IT and related figures for the European Community January 2001. http://europa.eu.int/ISPO/ecommerce/documents/Just_numbers.pdf

[2] Internet Engineering Task Force, List of Requests for Comments. http://www.ietf.org/rfc.html

[3] Fallows Deborah, Spam, How It is Hurting Email and Degrading Life on the Internet, October 22 2003. PEW Internet & Americal Life.

http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf

[4] Gauthronet Serge, Drouard Etienne; Ei-toivottu kaupallinen viestintä ja tietosuoja, Yhteenveto tutkimuksen (ETD/99/B5-3000/E/96 tuloksista, Euroopan Yhteisöjen Komissio. http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_fi.pdf

[5] Home page of Brightmail Incorporated. http://www.brightmail.com/spamstats.html

[6] Home page of MessageLabs Incorporated. http://www.messagelabs.com/viruseye/research/default.asp

[7] Liikanen Erkki, Press Conference, Spam: the Challenge. http://europa.eu.int/comm/commissioners/liikanen/media/slides/spam.pdf

[8] Mahowald Robert, Moser Karen, Holding back the Flood. An IDC White paper.

http://www.brightmail.com/pdfs/BMI_ROI_IDC.pdf

[9] Sullivan R., Brunker M. SPAM Wars. MSNBC news. August 2003 http://www.msnbc.com/news/SPAM_front.asp

[10] False Claims in Spam, A report by the FTC's Division of Marketing Practises, April 30 2003. Federal Trade Commission, the USA.

http://www.ftc.gov/reports/spam/030429spamreport.pdf

[11] Mangalindan Mylene, For Bulk E-Mailer, Pestering Millions Offers Path to Profit. Wall Street Journal Online, November 11 2002.

[12] 24/7REALMEDIA home page. http://www.247realmedia.com/index.html?navSource=TopNav

[13] Spam by Numbers, Eprivacy report, June 2003. http://www.eprivacygroup.com/pdfs/SpamByTheNumbers.pdf

[14] Malik Dale, Notes from "Economics of spam" Panel. FTC span forum April, May 2003-11-24 http://www.ftc.gov/bcp/workshops/spam/Presentations/malik.pdf

[15] Wood Paul, A Spammer in the works, White paper of MessageLabs http://security.iia.net.au/downloads/aspammerintheworks.pdf

[16] Cobb Stephen, The Economics of SPAM, Feb 2003 http://www.spamsquelcher.com/economics_of_spam.pdf

[17] Pantel Patrick, Lin Dekang, SpamCop, Spam Classification & Organization Program. http://www.isi.edu/~pantel/Download/Papers/aaai98.pdf

[18] Spamhouse Home page http://www.spamhaus.org/sbl/sbl-rationale.html

[19] Anti Spam Research Group (ASRG) Home page http://www.irtf.org/asrg/

[20] Coalition against Unsolicited Commercial Email (CAUCE) http://www.cauce.org/index.phtml

[21] Legislative proposals for a new Regulatory Framework for electronic communications

http://europa.eu.int/comm/information_society/policy/framework/index_en.htm

[22] S. 877 – CAN-SPAM Act of 2003, United States of America Senate. http://www.congress.gov/cgi-bin/bdquery/z?d108:s.00877:

[23] Legistaltive notice, Republican Policy Committee, US Senate http://rpc.senate.gov/_files/L43cm102203.pdf

[24] 3rd Generation Partnership Project, Specification for Mobile Multimedia Messaging service, TS 22.140 stage 1.

http://www.3gpp.org/ftp/Specs/html-info/22140.htm

[25] Tavilla Michael, DelBianco Steve, Let Email users take Spam off the menu http://www.itaa.org/isec/docs/NetChoiceSpamReport5-17.pdf

[26] Duke University, Duke Law and technology review. The future of wireless spam. http://www.law.duke.edu/journals/dltr/articles/2002dltr0021.html

[27] United Nations Conference on Trade and Development (Untad), E-Commerce and Development report 2003-11-26 http://www.unctad.org/Templates/webflyer.asp?docid=4228&intItemID=1528&lang=1